Design and Analysis of Access Control Protocols for Vehicular Ad-hoc Networks

Thesis submitted

by

Md. Ismail

Doctor of Philosophy (Engineering)

Department of Computer Science and Engineering
Faculty Council of Engineering and Technology
Jadavpur University
Kolkata, India

April 2024

Design and Analysis of Access Control Protocols for Vehicular Ad-hoc Networks

by

Md Ismail

Thesis submitted for the

Doctor of Philosophy (Engineering)

Degree of Jadavpur University, Kolkata, India

Supervisors:

Prof. Jamuna Kanta Sing
Department of
Computer Science and Engineering
Jadavpur University
Kolkata 700 032, India

Dr. Santanu Chatterjee
Research Centre Imarat
Defence Research and
Development Organization
Hyderabad 500 069, India

2024

Jadavpur University
Kolkata 700 032, India

INDEX NO.: 32/18/E

A. Title of the Thesis

Design and Analysis of Access Control Protocols for Vehicular Ad-hoc Networks

B. Name, Designation and Institution of the Supervisors:

1. Prof. Jamuna Kanta Sing
Professor
Department of Computer Science and Engineering
Jadavpur University
Kolkata 700 032, India

2. Dr. Santanu Chatterjee
Scientist
Research Centre Imarat
Defence Research and Development Organization
Hyderabad 500 069, India

C. List of Publications:

1. Journal papers

1. Md Ismail, Santanu Chatterjee, Jamuna Kanta Sing, *Senior Member, IEEE*, Saru Kumari, and Joel J. P. C. Rodrigues, *IEEE Fellow*, “Designing Anonymous Key Agreement Scheme for Secure Vehicular Ad-hoc Networks,” in ***IEEE Intelligent Transportation Systems (IEEE)***, Mar, 2024, DOI: 10.1109/TITS.2024.3373253. **(2022 SCI Impact Factor: 9.551)**

2. Md Ismail, Santanu Chatterjee, and Jamuna Kanta Sing, “An Efficient Rabin Cryptosystem-Based Authentication Mechanism for Vehicular Ad-hoc Networks,” in ***International Journal of System of Systems Engineering (Inderscience)***, pp. 190-211, 2024, DOI: 10.1504/IJSSE.2024.10055285. **(2022 SCI Impact Factor: 1.00)**

3. Md Ismail, Santanu Chatterjee, and Jamuna Kanta Sing, “A Secure Authentication Mechanism and Fine-grained Access Control for VANET Using Blockchain,” in ***International Journal of Ad Hoc and Ubiquitous Computing (Inderscience)***,**(2022 SCI Impact Factor: 0.70)** Communicated.

2. International conference papers

1. Md Ismail, Santanu Chatterjee, and Jamuna Kanta Sing, “Secure biometric-based authentication protocol for vehicular ad-hoc network,” in ***International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)***, pp. 229-234, IEEE, 2018, DOI: 10.1109/iSES.2018.00057.

2. Md Ismail, Santanu Chatterjee, and Jamuna Kanta Sing, “A Lightweight Blockchain Based Secure Authentication Scheme for Vehicular ad-hoc Network,” in ***International Conference on Deep Learning, IoT, Drone Technology, Smart Cities & Application (ICDIDSA 2023)***, AIP, 2023.

D. List of Presentations in National/International Conferences

1. Md Ismail, Santanu Chatterjee, and Jamuna Kanta Sing, "Secure biometric-based authentication protocol for vehicular ad-hoc network," in ***International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)***, Hyderabad, India, 2018.

2. Md Ismail, Santanu Chatterjee, and Jamuna Kanta Sing, "A Lightweight Blockchain Based Secure Authentication Scheme for Vehicular ad-hoc Network," in ***International Conference on Deep Learning, IoT, Drone Technology, Smart Cities & Application (ICDIDSA 2023)***, Nashik, India, 2023.

“Statement of Originality”

I **Md. Ismail, Registration No.: 1021804012** registered on **12^{th} June 2018** do hereby declare that this thesis entitled “**Design and Analysis of Access Control Protocols for Vehicular Ad-hoc Networks**” contains literature survey and original research work done by the undersigned candidate as part of Doctoral studies.

All information in this thesis have been obtained and presented in accordance with existing academic rules and ethical conduct. I declare that, as required by these rules and conduct, I have fully cited and referred all materials and results that are not original to this work.

I also declare that I have checked this thesis as per the “Policy on Anti Plagiarism, Jadavpur University, 2019” and the level of similarity as checked by iThenticate software is **6** %.

Md. Ismail

Signature of Candidate:

Date: 18-04-2024

Certified by Supervisors:

(Signature with date, seal)

1.

Jamuna Kanta Sing, Ph.D.
Professor
Dept. of Computer Science & Engineering
Jadavpur University, Kolkata-700032

2.

डॉ. शांतनु चटर्जी/Dr. SANTANU CHATTERJEE
वैज्ञानिक / Scientist
अनुसंधान केंद्र इमारत/Research Centre Imarat
डॉ. ए पी जे अब्दुल कलाम प्रक्षेपास्त्र काम्प्लेक्स / Dr. APJ Abdul Kalam Missile Complex
डी आर डी ओ, रक्षा मंत्रालय, भारत सरकार, हैदराबाद
DRDO, Ministry of Defence, Govt. of India, Hyd-69

Department of Computer Science and Engineering
Jadavpur University, Jadavpur, Kolkata
Kolkata 700 032, India

Certificate

This is to certify that the thesis entitled **"Design and Analysis of Access Control Protocols for Vehicular Ad-hoc Networks"**, submitted by **Md Ismail** (Index NO.: 32/18/E, Registration No.: 1021804012, dated 12/06/2018), registered in the *Department of Computer Science and Engineering, Jadavpur University, Kolkata, India*, for the award of the degree of **Doctor of Philosophy**, is a record of an original research work carried out by him under our supervision and guidance. The thesis fulfills all requirements as per the regulations of this Institute and in our opinion has reached the standard needed for submission. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Prof. Jamuna Kanta Sing
Department of
Computer Science and Engineering
Jadavpur University
Kolkata 700 032, India

Jamuna Kanta Sing, Ph.D.
Professor
Dept. of Computer Science & Engineering
Jadavpur University, Kolkata-700032

Dr. Santanu Chatterjee
Research Centre Imarat
Defence Research and
Development Organization
Hyderabad 500 069, India

डॉ. शांतनु चटर्जी/Dr. SANTANU CHATTERJEE
वैज्ञानिक / Scientist
अनुसंधान केंद्र इमारत/Research Centre Imarat
डॉ. ए पी जे अब्दुल कलाम प्रक्षेपास्त्र कांप्लेक्स / Dr. APJ Abdul Kalam Missile Complex
डी आर डी ओ, रक्षा मंत्रालय, भारत सरकार, हैदराबाद
DRDO, Ministry of Defence, Govt. of India, Hyd-69

Acknowledgments

First and foremost, I thank the Supreme Lord for his kindness for giving me opportunities and helped me to get Prof. Jamuna Kanta Sing and Dr. Santanu Chatterjee as my supervisors. I express my deepest sense of gratitute and thanks to Prof. Jamuna Kanta Sing and Dr. Santanu Chatterjee for their relentless support to guide and steer the course of research work journey.

I am extremely grateful to Prof. Jamuna Kanta Sing for his mentorship. His intellectual and moral support along with his kin interest has helped me profusely to shape and inculcate strong foundation for research and analysis. His immense knowledge and plentiful experiences helped me to bring out a tangible research out come and it has been encouraging me all the time of my academic research, professionalism and daily life. Really, I cherish his deep confidence in me as a research scholar.

I also extend my heart-felt gratitude and big thank to Dr. Santanu Chatterjee for his invaluable and immense support for all stages of Ph.D. programme. He is my driving force to carry research, analysis and simulation activities. It would be impossible and difficult long journey for me without his deep involvement and strong desire for companionship along the path of my research.

I also thank Prof. (Dr.) Nandini Mukhopadhyay, Head CSE, Jadavpur University for serving and steering as my Doctoral Scrutiny Committee.

I also would like to thank my Group Director Mr. Sanjay Kumar Sahani, Lab Director Mr. Katari Suchinder and all my colleagues for their direct or indirect continuous support during my entire period of research programme.

I also extend heart-felt gratefulness to my loving parents and family for continuous encouragement, moral supports and patience all through my studies.

I also thank specially Mr. Manas Kumar and all other friends for their whole hearted support for me during the course of my research work.

Finally, I would like to thank Jadavpur University and its all level of managements whose names are not mentioned here but have helped me lot for studentship and many other ways to realize the research programme.

Md. Ismail
18/04/2024

Md. Ismail

Abstract

A vehicular ad-hoc network (VANET) is a wireless network formed by bringing smart vehicles and road side fixed infrastructures for exchanging various information among multiple stake holders to improve traffic congestion, make responsible, reliable and comfortable safe road journey. Each moving vehicle can be characterized as a node in VANET allowing inter-vehicle distance approximately 100m to 300m. Implementing a sophisticated VANET can bring a countless benefits to its users. Ensuring security for highly scalable, dynamic fifth generation (5G), there are many challenges specifically to restrict unauthenticated users access and proper key agreement with fine-grained access control. Further, 6G cellular technology is going to support diverse connectivity requirements at microsecond speed with 1000 times faster latency compared to 5G and greater capacity via higher radio frequency. 6G networks includes most of the features of 5G viz. software defined networking (SDN), network slicing, multi-access edge computing (MEC) and network functions virtualization (NFV). Therefore, most of the security concerns and requirements still remain the most challenging in 6G. Avoiding free flow of information is also a crucial challenge keeping untouched the promising objectives of future generation technology. These 5G and 6G technologies aim to connect devices in milion/sqkm range with the improved performance, incredible transmission speed (terabit), and cost to serve vast transformative diverse automobile sector. VANET and intelligent transport system (ITS) together form a highly sophisticated dynamic complex system of systems (SOS) that provides data access infrastructure to mobility objects, basic stand-alone static elements to highly sophisticated dynamic elements to provide data access as per real-time need for modern traffic management and optimization. To ensure user's core security concern over crucial data in transit, it essentially demands a foolproof user authentication scheme for accessing desired services from VANET clouds. Critical life threatening occurrence of important and urgent high priority events have to traverse unprotected and insecure public/private networks. This openly shared information faces various serious security and privacy challenges. Recently various schemes have been designed to address numerous security concerns but very few schemes have concentrated to address all major attacks with efficiency and in compliance with functional and general security requirements of VANET. Fundamentally, VANET solves security challenges in centralized approach where

centrally trusted unit experiences single point failure issues and most of the traditional VANET approaches may not support high scalability in such dynamic hostile scenarios.

In this thesis, we focus to explore novel security in the area of design and analysis of access control schemes, scalable user authentication, lightweight blockchain-based authentication and suitable key agreement with fine-grained access control for VANET.

First, we propose a lightweight anonymous key agreement scheme (AKAS) with fine-grained authentication feature to address challenges related to restriction of unauthenticated users access and proper key agreement with fine-grained access control specifically for vehicle-to-vehicle (V2V) communication in VANET. In the proposed scheme, registered and authorized users can access services/information as per access privilege only. We have performed formal security analysis using real-or-random (ROR) model. Moreover, we have simulated our scheme using automated validation of internet security protocols (AVISPA) tools, simulation of urban mobility (SUMO), and objective modular network testbed in C++ (OMNET++). We have used the widely accepted AVISPA tool to study formal security verification for intrusion detection and attack mitigation accuracy. SUMO is a mobility simulator to simulate the dynamic behavior of VANET protocols. The ROR is used to proof formerly the security of cryptographic aspects of protocols. Whereas, a modular and component-based network simulation-bed can be developed by OMNET++ tool. Analysis and simulation results show that our scheme is secured against various well-known attacks. Further, we have compared the security and efficiency of our scheme with the existing schemes available in the literature and found that our proposed protocol is more secure, lighter, 5G, 6G friendly, scalable and even faster than the other related schemes.

Secondly, we propose a dynamic lightweight biometric-based authentication protocol for vehicle-to-vehicle (V2V) communication networks where user after successful registration can directly login from any local mobile terminal and access his /her services/information directly from the authentication servers. We have done the security analysis of our scheme and prove that our scheme provides location privacy, mutual authentication for averting spoofing attack, user anonymity and resistance against replay attack, modification and forgery attacks. We also compare the efficiency of our scheme with other related schemes and show that our authentication scheme is more secure and performs faster than other schemes available in the literature. In addition, our proposed scheme provides scalability as there is no limitations on number of user terminal but only the genuine user needs to be registered once for taking the services. No multiple registration or session based registrations are required.

In third study, we propose improved and enhanced Rabin cryptosystem based authentication mechanism to address all known major attacks with robustness keeping efficiency, scalability and dynamicism in picture. We have rigorously carried out security analysis by AVISVA and Proverif tools. The analysis has shown that our scheme guarantees positional privacy, user anonymity and mutual authentication to prevent spoofing attack, password guessing attack, insider privilege attack and temporal session attack. The comparison of protocol with available relevant schemes reveals that the proposed protocol is more efficient with efficacy. It supports light weight authentication process for legitimate users. This proposed scheme supports scalability as this does not depend on the volume of user access point and valid user requires to register only once for accessing the VANET services. Thus, session based and duplicate registration can be avoided by the proposed scheme.

At last, we propose lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users. We have defined a framework with edge computing and mobile edge computing to offload computation intensive tasks as well as optimization of data processing before sending it to blockchain based VANET network. We have done security analysis by Proverif tool and formally proved security strength using BAN logic. The security analysis shows that the proposed scheme resists various known security threats. Moreover, the performance analysis proves that our scheme faster and more efficient compared to other available relevant protocols. In addition, in the proposed scheme (LBAFA), we have incorporated blockchain technology to introduce decentralization and parallel computing over traditional centralized VANET. We have also used ECC to optimize the computation cost and CP-ABE to impose access control over the data in fine-grained manner based on user attributes.
The effectiveness of VANET heavily depends on smart traffic management, efficient user interaction and data transmission, collision detection and prevention, road safety, high scalability for large networks, avoiding the free flow of information, and addressing known security attacks with robustness. The critical performance

analysis, simulation results, formal security verification by simulation tools, and mathematical models including informal cryptographic analysis show that most of our proposed protocols are highly effective for VANET applications.
Keywords: Vehicular ad-hoc network (VANET); Intelligent transport system (ITS); Key agreement; User authentication, Biometrics; Blockchain; Fine-grained access control; Security.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A modern city needs to include vehicular ad-hoc networks (VANETs) and smart vehicles to be called a smart city. Manufacturers have incorporated various initiatives in the automobile sector by introducing smart vehicles with the support of the government [146]. The internet-of-things (IoT) devices have become more sophisticated and dominant than ever, and the application potential is growing rapidly [83]. As the widespread use of software systems increases and becomes an integral part of our daily lives, the complexity of these systems increases the risks of widespread security concern [131]. A VANET is a wireless network formed by bringing smart vehicles and roadside fixed infrastructure for exchanging various information among multiple vehicles to improve traffic congestion and make a responsible, reliable, and comfortable road journey. Each vehicle within 100 to 300m can get the benefits of VANET if users are equipped with a VANET-enabled system. In VANET, exposure of route profiles to unauthorized users and adversaries can cause traffic jams, robbery, kidnapping, and theft of personal information. The VANET intensively uses cellular network technology as an important component. With an exponential increase in demand from users, the future generation will now occupy the place of 5G. 5G plays an important role in fulfilling the various mobility requirements of VANET and intelligent transport systems (ITS). 5G enables VANET to connect devices in the milion/sqkm range with improved performance, incredible transmission speed (terabit), and reduced cost to serve a vast, transformative, and diverse automobile sector. The 5G-enabled VANET architecture is shown in Figure 1.1. 5G is a complete ad-hoc network that provides incredible speed in the range of terabit with no limitations to ITS. This 5G also provides virtual zero-distance connectivity among

VANET users with maximized data throughput and input-output operations per second (IPOS) [85] in the ITS scenario. This cellular network (5G) has successfully addressed the major challenges that are not efficiently resolved in 4G [69] but it is still experiencing various security challenges for user authentication and access control. Implementation of sophisticated VANET needs to address various aforesaid challenges. Moreover, the VANET has recently become an integral part of ITS, and the dissemination of important and urgent events is of the utmost priority in this dynamic scenario. However, critical life-threatening events have to traverse an unprotected and insecure public or private network. Therefore, the exponentially growing VANET has been going through various security concerns. Due to the high demand and popularity of VANET, it generates a huge volume of security-sensitive information. This openly shared information faces various serious security and privacy challenges.

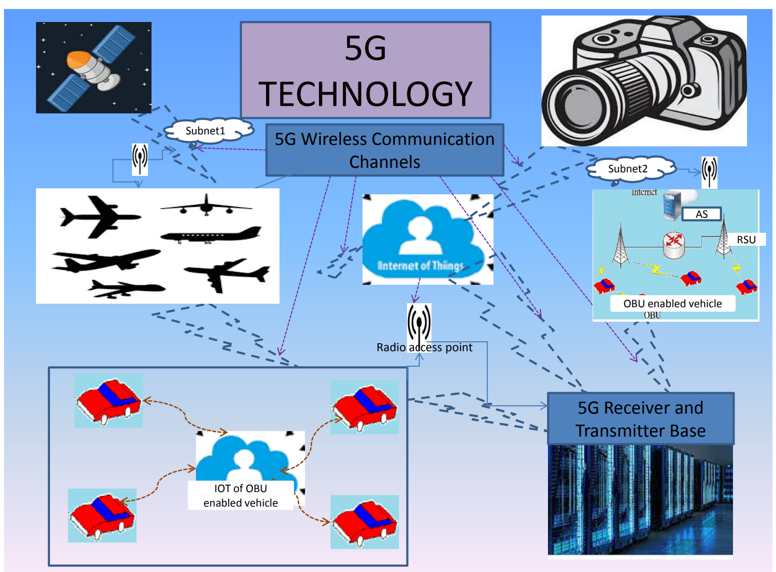

Figure 1.1: 5G-enabled VANET architecture.

1.1 Fundamentals and Major Setup of VANET

A VANET is a wireless network formed by bringing smart vehicles and roadside fixed infrastructure for exchanging various types of information among multiple stakeholders. VANET can be considered a variant of MANET. A VANET consists of mobile terminals (vehicles that dynamically change their locations), fixed roadside support units (RSUs for vehicles-to-vehicles communication), *AS* (authentication server) [84], and VANET-cloud as part of its core network architecture. The *AS* allows access to information objects from the VANET cloud to the genuine user only after a successful authentication process. The authentication server fetches the expected response, and then the response message gets encrypted by the valid authorizing key belonging to the query generator. The recipient user decrypts it if he or she has the authorization to access the information only. Figure 1.2 shows the major setup and various building blocks of the VANET.

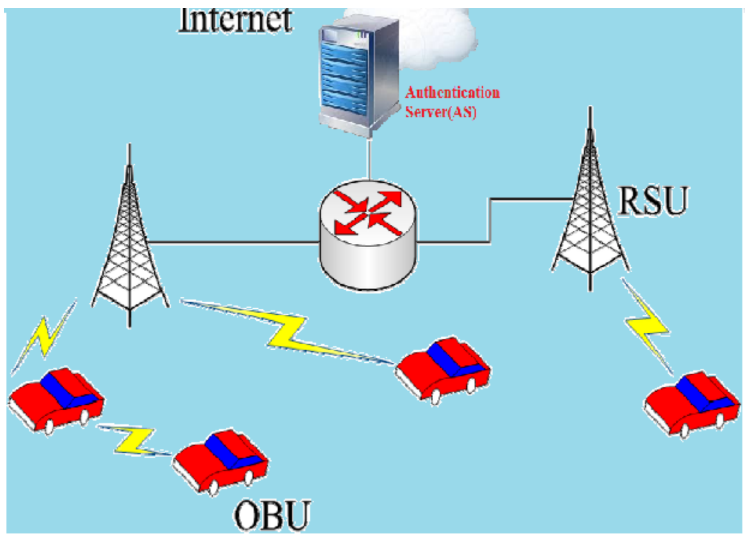

Figure 1.2: Major setup of VANET

1.2 Trust Model

Trust can be defined as a measure of belief on which the involved parties can rely or place confidence in someone or something to perform defined functionalities or roles. Trust is an important aspect of VANET to make it more useful and reachable to common societies. Chaung & Lee [110] and Saru Kumari et al. have proposed respectively trust-extended authentication mechanisms (TEAM) and enhanced TEAM. ETEAM is an extension of TEAM. TEAM is an authentication mechanism for vehicle-to-vehicle (v2v) communication in which three categories of vehicles, namely LE, TV, and MTV, are considered. Depending on the level of authentication, a normal vehicle can have two statuses of recognition, i.e., trustful and mistrustful state. Transitive trust transformation scenario is shown in Figure 1.4. A normal vehicle plays the role of a temporary law executor (LE) after a successful authentication procedure and maintains its trustful state until the validity of the session key expires. TEAM and ETEAM provide a special feature in VANET to update and increase the lifetime of the key using the trust model. An authentication scheme based on the transferable or shareable user's credential can indulge in thorough sharing of information or services, which may lead to an extremely complicated situation [93], [111]. Therefore, the trust model judiciously needs to be incorporated into VANET protocols. Mainly, the VANET trust estimation model has message-based and character or role-based features. A detailed taxonomy of trust models is shown in figure 1.3.

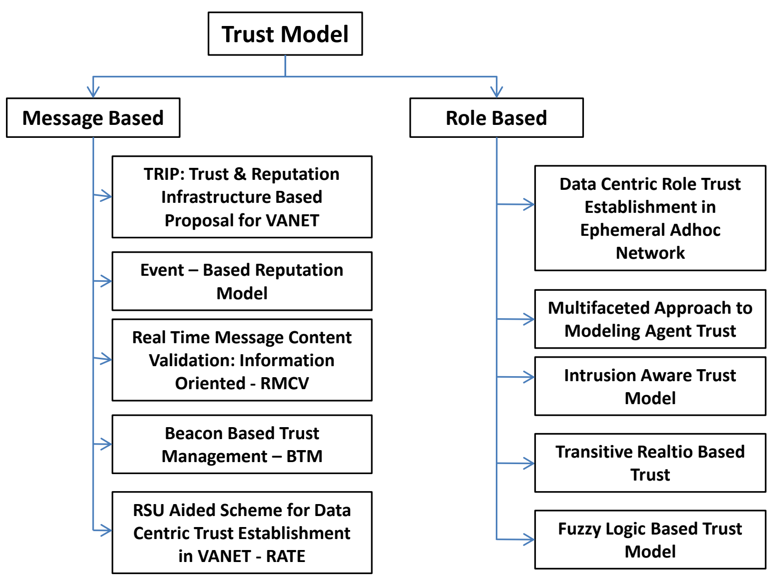

Figure 1.3: A taxonomy of trust models in VANET

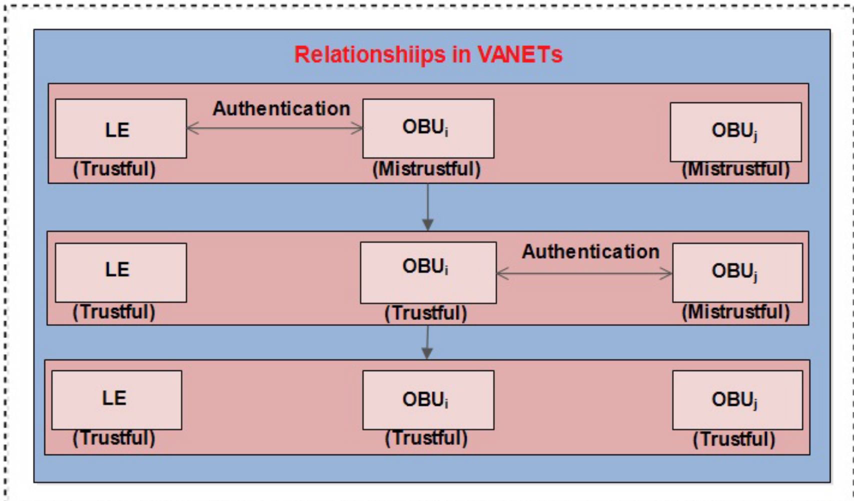

Figure 1.4: Transitive trust model of VANET

1.3 Hardware and Architecture of General VANET

To realize the VANET, a number of hardware and architectural elements are involved. Manufacturers have also started production of VANET friendly hardware and incorporated various smart features in the automobile sector by introducing smart vehicles with the initiatives of the government. A VANET is a wireless network formed by bringing smart vehicles and roadside fixed infrastructure for exchanging various types of information among multiple users. Each moving vehicle can be characterized as a node or terminal in VANET, allowing inter-vehicle distances of approximately 100m to 300m [163]. Implementation of VANET needs to interact with autonomous vehicles and VANET setups, which are heterogeneous in nature. The performance and utility of VANET can be appreciated better if the various interlinked sensors and hardwares perform optimally. So, interconnected sensor data should be tamper-proof and protected from adversaries. Figure 1.5 shows installed dependant sensor hardwares over an autonomous car. Autonomous or smart vehicles are connected to three main building blocks: the mobile terminal (vehicle), fixed roadside infrastructure (RSU), and authentication server (AS), and these are considered [84] as the core network architecture of VANET. The user mobile terminal is kept on every moving platform, which dynamically changes its position, and the RBU is a fixed stationary unit positioned at road sides. RSU helps to receive outside information and provides connections among vehicles as a legal gateway. Figure 1.2 depicts the architecture and various building blocks of a VANET environment.

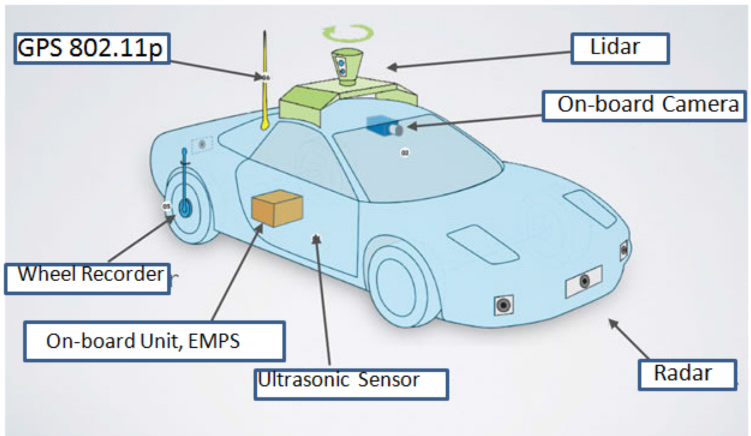

Figure 1.5: Interlinked sensor hardwares installed on an autonomous car

1.4 General Functional Requirements of VANET Protocols

The VANET protocols should satisfy the five basic requirements. These functional requirements are authentication, attack-resistant key establishment, strong non-repudiation, and identity privacy preservation with conditional traceability.

(i) Authentication: This requirement ensures that all the protocols should support mutual identification for the participating elements in VANET. The authentication has two types, namely message and entity authentication. The message authentication confirms that the received messages are issued by a valid entity and were not modified during transmission. Entity authentication performs mutual authentication, which confirms that the two entities are capable of identifying mutually.

(ii) Key establishment with attack resistance: Key establishment is an important process where the shared session key is made available among participating parties for future cryptographic use. This property ensures that the shared session key is perfect forward secrecy (PFS) proof and key-compromised impersonation (K-CI) attack-resistant.

(iii) Non-repudiation: This property enables a receiver that a third party cannot

deny its receiver the responsibility for generated messages. It stops adversaries from forging and generating messages in other roles.
(iv) Identity privacy preservation: This property allows vehicles to frequently broadcast messages about the state of their vehicles and their driving status. Identity privacy preservation ensures that nobody could access the session between the real identities of vehicles.
(v) Conditional traceability: This property allows trusted authorities (TA) to retrieve the details of vehicles in certain circumstances (e.g., traffic emergencies). Conditional traceability helps the TA to access the real information about vehicles from the database.

1.5 Overview of Blockchain Technology

Due to the rapid growth of VANET and its support for efficient traffic management, safe driving, and autonomous driving, a high volume of transactional data is produced. The blockchain technology has helped to replace third-party support for accessing data seamlessly and provide security & privacy for data. In this scenario, co-located vehicles and other IOT devices can carry out transactions through RSU. Generally, vehicles and IOT devices are facilitated by limited computation and storage facilities. Therefore, each RSU is considered a blockchain node. The RSUs act as a proxy for all individual devices in the blockchain-based of VANET. Blockchain inherently supports the distributed database paradigm for storing and retrieving data [65]. Security and privacy of VANET data are guaranteed by blockchain, and it also supports a high level of data sharing & transmission for VANET [99]. The main motivation of this study is to incorporate decentralization and parallel computation paradigms using blockchain-enabled VANET and fine-grained access control. This helps to achieve faster concurrency throughput for trustworthy events. The consensus mechanism of blockchain enabled VANET to achieve real parallelism and decentralized computation to enhance the utmost security and scalability. Therefore, the proof-of-work (POW) consensus mechanism is suitable for a public blockchain as this mechanism has provable security functionality inbuilt [142]. Figure 1.7 depicts the architecture and various building blocks of the proposed scheme.

1.6 Importance of Blockchain Concept in VANET

Autonomous smart vehicles have become an integral feature of modern cities. The vehicular ad-hoc network (VANET) is the main pillar of intelligent transport systems (ITS) for safe and comfortable journeys over the road. Government bodies and manufacturing sectors are playing vital roles in implementing ITS features [81]. A system of systems (SOS) of VANET and ITS has a collection of heterogeneously complex cyber and functionally independent systems interconnected over a vast geographical area [165]. Performance and functionalities are aggregated to achieve higher-level, unified goals. The main goal of VANET SOS is to ensure proper security and authentication in real-time for better utilization of various VANET SOS resources and to prevent unauthorized access by attackers. An SOS-based VANET and ITS system model for the proposed scheme is depicted in Figure 1.6.

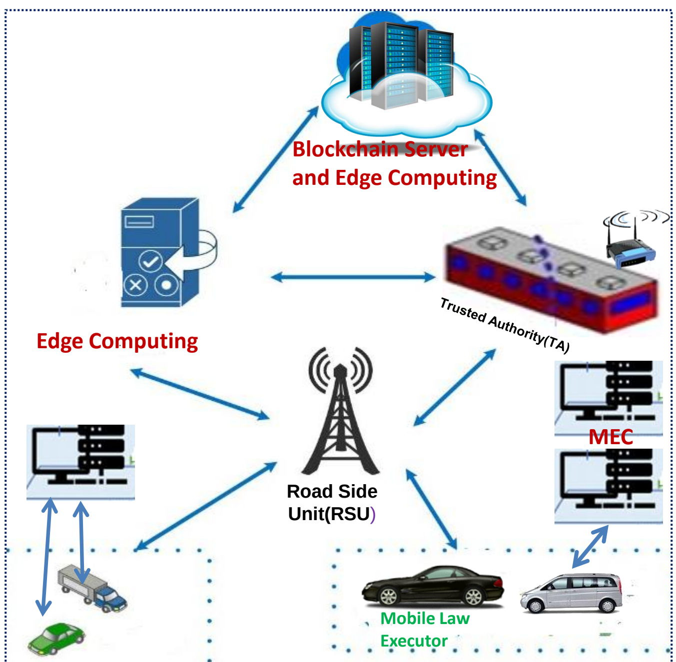

Figure 1.6: VANET and ITS system model.

With rapid technological growth, researchers have brought out numerous schemes and protocols for VANET to increase efficiency and effectiveness. However, most of the work was done for peer-to-peer delivery to prevent dynamic attacks in centralized form [114]. Recently, blockchain-based VANET has become an interesting field of research, and researchers have also found great potential to add more functional values to ITS and VANET [133]. Parallelism and decentralization are the main working principles for blockchain technology.

Most of the research work for blockchain-based VANET has been concentrated on blockchain design. Therefore, there is a need to exploit the possible extent to utilize the benefits of parallel computing and the authentication process in a blockchain-based VANET. Therefore, it is important to study lightweight blockchain-based secure authentication and fine-grained access control for VANET using the promising features of blockchain technology. VANET authentication and a proper algorithm are used to measure the trustworthiness of the message and node after successful authentication by the respective RSU. So, a suitable blockchain should be designed to realize the real decentralization of VANET.

It is also important to incorporate fine-grained access control for the VANET cloud server to enable access to data by a particular user only. Traditional access control schemes like the advanced encryption scheme (AES) and RSA cannot support fine-grained access control. Therefore, attribute-based encryption (ABE) came into play to support one-to-many encryption for data confidentiality and fine-grained access control over data. Based on the encryption and decryption policies, ABE can be divided into two types: key policy based ABE and the cipher policy based ABE [67], [20]. The KP-ABE has control over data based on access policy but without the knowledge of the receiver. However, the CP-ABE has control over data as well as control over the receiver. In a dynamic environment, the CP-ABE is more suitable for node participation in a blockchain-enabled VANET scenario. In this thesis, we explore lightweight, secure authentication mechanisms for blockchain-based VANET and fine-grained access control using blockchain technology and CP-ABE.

1.7 System Model and Components of Blockchain-Based Protocol

The main blockchain-enabled system model interacts with various heterogeneous components. The model and architecture mainly consist of seven elements: edge computing (EC), mobile edge computing (MEC), inter-planetary file system (IPFS), vehicle, mobile law executor (MLE), roadside unit (RSU), and trusted authority

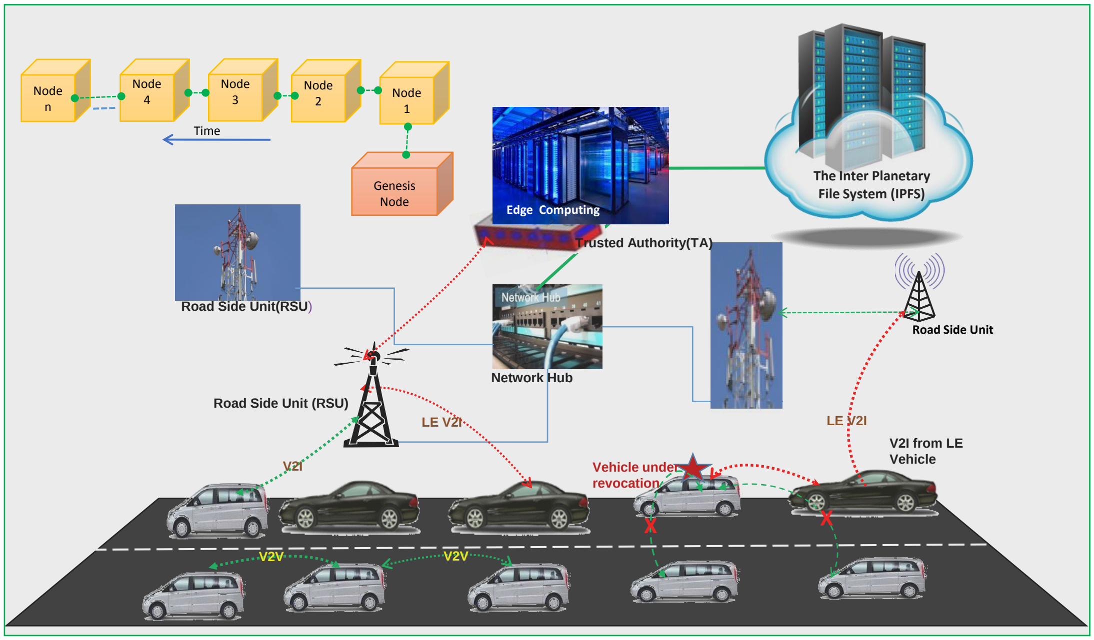

Figure 1.7: Proposed VANET architecture with blockchain.

(TA). These seven entities are interconnected, and the entities have various roles and functionalities. In Figure 1.6, different communication setups among network entities in the blockchain-enabled system model are depicted.

Edge computing

The edge computing component provides an important function to achieve parallelism in a decentralized way and offload complex work and computation. Because of limited resources, RSUs may experience network performance and computation delays if all transactions in the consensus work of the blockchain are executed by the RSUs. Therefore, this proposed scheme achieved parallel computation and fast processing by offloading the intensive, time-consuming computation work to edge computing.

Mobile edge computing

A high volume of transactional data is produced in the VANET environment. The network performance will be affected, and a high delay will also be added if all the blockchain consensus processing is executed by RSUs. Therefore, our scheme offers the functionality to offload intensive computational jobs to dynamic MEC, and the final result is shared with RSU. Thus, this also prevents the effects of RSU failure issues.

IPFS

IPFS is a distributed global data storage solution for large-scale persistent data storage. It is a peer-to-peer (p2p) decentralized file system to communicate the static and mobile edge computing features of a blockchain-based VANET system. This file system can combine block exchange incentives (BCE), distributed hash tables (DHT), and self-certified namespaces. It inherently can avoid single-point failure issues [158].

Vehicle

Vehicles are considered as data producers and consumers. Due to resource limitations, vehicles share transactional data with IPFS through RSU.

Mobile law executor

Mobile law executors are trustworthy vehicles (TV). The MLEs are generally considered to be trustworthy by default. MLE can be defined as authorized public transportation or police vehicles that are equipped with MEC and mobile TA-enabled features. The MLE helps the TA to authenticate vehicles other than LE that can participate in the blockchain network after successful authentication.

RSU

RSU is a roadside static unit deployed along the roadside, and it is equipped with a high-end processing system and networking setup. RSUs are considered nodes of the blockchain and are used as proxy nodes for vehicles to share data in IPFS. Most of the extensive high-computing processing is executed by edge computing and MEC for the respective RSU.

Law executor and trusted authority

The major responsibility of trusted authority (TA) cum LE is to perform registration of RSUs and vehicles within a defined area. It also carries out various computation-intensive data processing tasks with the help of edge computing. Whereas, the mobile law executor is responsible for authorizing vehicles and RSUs for a small area of coverage.

1.8 VANET Characteristics and Hardware Constraints

A VANET has fewer challenges to manage self-organization, low bandwidth, self-management, and no concept for centralized node features. However, a few characteristics, like frequent disrupted networks, highly dynamic traffic density, uncontrolled traffic flow, and inherently variable mobility patterns, are very challenging for VANET to handle. Some of the characteristics are briefly discussed below.

1.8.1 VANET Dynamic Network Topology

The dynamic topology of VANET is fundamentally a function of speed and available paths. Generally, a vehicle moves 27 m/s over the national highway. Standard VANET has a transmission range of 100m to 300m. Therefore, the communication link exists between two apart moving vehicles only for 2 to 4 seconds. VANET has to work over such a highly dynamic topology.

1.8.2 Frequent Disrupted Network

The highly dynamic topology characteristic means that there is always a chance of a disrupted link between two moving-away vehicles every 4 to 5 seconds. Therefore, this disrupted link issue needs to be addressed to support seamless communication. Generally, RSU provides seamless connectivity where link disruption is present due to the low density of vehicles.

1.8.3 Mobility Patterns

The disrupted network feature leads VANET to maintain nodes dynamic [59] positions and mobility states to estimate various probable movement patterns for every vehicle within the defined range. However, a proper estimation model should be part of the VANET design to predict mobility patterns and vehicle speed.

1.8.4 Communication Environment

The nature of mobility is highly variable, from normal road to highway scenarios. The design of the prediction model and its algorithm should cater to these variable communication environments. It is easier to develop a mobility model for non-populated areas than for highly densely populated areas due to the obstructing objects like buildings and other structures in populated areas.

1.8.5 Delay Constraints

Hard delay constraint is an important characteristic of VANET to improve traffic congestion and make a responsible, reliable, safe, and comfortable road journey. VANET and intelligent transport systems (ITS) together form a highly sophisticated, complex system of systems that provides data access infrastructure to mobility objects, from basic stand-alone static elements to highly sophisticated dynamic elements to provide data access as per the real-time need for modern traffic management and optimization.

1.8.6 Interaction with On-board Sensors

Implementation of VANET needs to interact with autonomous vehicles and VANET setups, which are heterogeneous in nature. The performance and utility of VANET can be appreciated better if the various interlinked sensors and hardware perform optimally. So, sensor data should be tamper-proof and protected from adversaries. Figure 1.5 presents various roles of sensor hardware over an autonomous car in the VANET scenario.

1.9 Applications

VANET is widely deployed for various applications ranging from complex military uses to civilian uses in modern smart cities. In many implementations, VANET has to work in a hostile and unfriendly environment to handle targeted tracking, battlefield surveillance, and intruder encounter detection. Further, VANET and intelligent transport systems (ITS) have been jointly playing a crucial role in modern traffic management, safe driving, and traffic optimization. VANET and ITS together form a highly sophisticated dynamic system that provides data access infrastructure to mobility objects. Due to the high demand and popularity of VANET, it generates a huge volume of security-sensitive information. This openly shared information faces various serious security and privacy challenges. Therefore, to ensure users' core security concerns over crucial data in transit, VANET essentially needs to extend its application to a foolproof user authentication scheme for accessing desired services from VANET clouds. Most of the time, VANET operates over wireless channels, where adversaries get opportunities to eavesdrop, interrupt, and intercept radio conversations. So, in such a hostile environment, normal protocols and algorithms may not achieve desirable outcomes without sufficient security measures and application provided by VANET.

Consider the situation of battle field surveillance where anti-terrorist-squadron (ATS) is involved in capturing a terrorist vehicle. A large number of connected sensors are equipped to get help from VANET, and they can easily track the desired vehicle. The application of VANET can be broadly categorized under broader head. Figure 1.8 shows the various applications of VANET in a precise manner.

1.10 General Security Properties of VANET

The VANET scheme should comply with a few basic properties. These properties are authentication, integrity, confidentiality, strong non-repudiation and identity privacy preservation, conditional traceability, authorization, and freshness [43].

- *Authentication:* The authentication has two types, namely message and entity authentication. The message authentication confirms that the received messages are issued by a valid entity and were not modified during transmission. Entity authentication performs mutual authentication, which confirms that

General Purpose	▪Ad-Hoc Enabled Car Communities ▪Ad-hoc Service Architecture ▪Distribution of Geographical Data
Driver Assistance	▪Traffic Notification System ▪Remote Vehicle Diagnostics ▪Road Topology Predictor ▪Environment Evaluator ▪Automatic Toll Collection ▪Parking Spot Locator
Safety	▪Emergency Response Community ▪Ad-Hoc Enabled ITS Car Navigation ▪Lane Change Assistance ▪ Safety Forward Collision Warning ▪Electronic Emergency Brake Light ▪Automatic Accident Notification ▪Tracking of Stolen Vehicles
Entertainment	▪Internet Connection ▪Access desired object from VANET cloud
Military	▪Tracking of Known Criminals ▪Handling Targeted Tracking ▪Battlefield Surveillances ▪Intruder Encounter and Detection

Figure 1.8: Applications of VANET [95].

the two entities are capable of identifying mutually.

- *Integrity:* This requirement ensures that the messages or entities exchanged must not be modified.
- *Confidentiality:* This property ensures the VANET communication channels are protected and prevented from false report injection.
- *Availability:* This ensures that the expected network services should be available even in the presence of various attacks, including denial-of-service attacks.
- *Strong non-repudiation:* This property enables a receiver that a third party cannot deny its receiver the responsibility for generated messages. It stops adversaries from forging and generating messages in other roles.
- *Identity privacy preserving:* This property is applied to prevent vehicles from frequently broadcasting messages about the state of their vehicles and their driving status. Identity privacy preservation ensures that nobody could access the session between the real identities of vehicles.

- *Conditional traceability:* This property allows trusted authorities (TA) to retrieve the details of vehicles in certain circumstances (e.g., traffic emergencies). Conditional traceability helps the TA to access the real information about vehicles from the database.

- *Authorization:* This ensures that the user is allowed to access desired information if and only if they have a unique privilege over the objects.

- *Freshness:* Ensures that the event or message is current and that no adversary should be able to replay old messages or events.

In addition to these general requirements, forward and backward secrecy should be incorporated as a new terminal may be installed in case the old terminal fails.

- *Forward secrecy:* This feature ensures that once one node disconnects from the network, it should not be allowed to access subsequent conversations once it commits final exit.

- *Backward secrecy:* This ensures that a newly joined node in the network must not have access of any previously communicated messages.

1.11 Key Agreement in VANET

To realize the security requirements discussed in Section 1.12.1, generally, predistribution of keys is adopted in most of the schemes. In this approach, a set of pre-loaded key generation elements is deployed before the actual participation of nodes or terminals in VANET. Once successful deployment is over, the participating terminal tries to discover neighboring terminals to establish the desired session among them using the preloaded shared keying information. The simple and deterministic solution to implement this approach is to use a single master key for the defined VANET for a single mission and session. Before an actual deployment, the entire terminals are provided with the same master mission key in case of predistribution of key scenarios. After successful key establishment phase, any defined neighboring nodes can exchange securely among themselves using that master key. However, this approach is easy to implement, but it has one major drawback in case a single terminal compromises a key in a network. This key compromise can reveal the master secret key, and thus it allows adversaries to get access to all conversations over the network. To solve this, a group key could be shared among them and erased the shared key. However, the main issue with such an erasing approach is that it cannot allow new nodes once the initial phase of deployment is completed.

The pre-distribution with random key can be considered another way to provide secure exchange of messages. First, Eschenauer and Gligor proposed the random key pre-distribution scheme [60] in 2002. It has the following three main phases:

- From randomly generated symmetric keys, the authentication server (AS) picks up a large key pool for the *key pre-distribution phase*. Each key is uniquely identified in the symmetric key pool. The AS then selects a random subset from the key ring. It has a smaller size than the pool, and the key ring is loaded into its memory before VANET deployment.

- In *direct key establishment phase*, each node determines all its neighboring nodes within its transmission range. Key ids from the key ring are exchanged to establish a secret key pair between two neighboring nodes. The common key id of the key ring is considered as the secret key for the particular nodes pair. Then, the established key is used for future secure message exchanges. A challenge-response method is used to verify the newly discovered nodes.

- The *path key establishment phase* can be taken as an optional phase. In the event that two neighbors fail to establish a key agreement phase, a secure path is available between them. This available, secure path can be used to communicate directly. However, this causes communication overhead over the VANET network. Therefore, a smaller key size is better for high network performance, and this scheme also provides high network connectivity with high probability. On the other hand, key compromised impersonation attack chances get increased. Some alternatives to path key establishment are available in the literature with better trade-offs between network connectivities, overheads, and resilience to prevent node capturing, [48], [155], [36], and [42].

After that, several studies to improve the basic random key distribution protocol are proposed, and some of them are [58], [102], [25], and [46]. A tangible volume of key pre-distribution [58] and authentication protocols are proposed to improve VANET networks [38], [39], [25].

1.12 User Authentication in VANET

After successful user authentication only, the VANET allows a legitimate user to query and receive real-time data from VANET when he or she requests it. To make VANET services accessible to a larger part of society, numerous researchers propose this authentication scheme [37], [40], [44]. This scheme helps genuine users for accessing information entitled for authorized users only. Once the validity of the user and owner of the objects get confirmed through the local terminal, an automatic general authentication process is initiated. After successful authentication, the AS processes the information object. Then AS retrieves the desired information and encrypts the information object with the authorization key of the user. The received information will be decrypted by the user if and only if he or she is an authorized person to access that information. Therefore, the user authentication issue becomes a very important scope of research in VANET security.

User authentication can offer to protect and prevent VANET information from being accessed by illegal users and adversaries (attackers)[45], [41]. In the following subsection, we enlist the security requirements and functionality requirements for VANET.

1.12.1 Security Requirements

As per general standards, user authentication in VANET must prevent the following attacks:

- **Replay and man-in-the-middle attacks:** A replay attack can be considered a threatening condition where an adversary tries to cheat other legitimate users in VANET using information captured through the wrong means. Therefore, an unauthorized third party records the exchanged conversation through this attack. In a man-in-the-middle attack situation, an adversary tries to intercept the exchanged messages and can operate to change, delete, or modify the message content delivered to the legitimate recipients. Thus, these types of attacks pose serious consequences, and a user authentication scheme should prevent them.

- **Multiple uses of login-id attack:** Multiple uses of the same login-id attack can be vulnerable when some systems use password/verifier table to process user login and authenticate the users. If the authenticating system allocates the same login ID and password to more than one legitimate user, then those users can involve or launch this attack.

- **Stolen-verifier attack:** This attack indicates that any user's login ID or password can be stolen from the verifier table. So, this attack can happen when the AS performs user verification using the stored verifier/password table. It is better if AS does not allow VANET administrators to maintain the verifier/password table locally to avoid such a type of attack. Therefore, the standard authentication scheme of VANET may not have the feature to store a verifier or password table to verify the user.

- **Password guessing attack:** Through this attack, an adversary can guess the password either online or offline [82] to misuse and retrieve the secret exchanged messages between legitimate users. By doing so, attackers can also gain access to the secret information. So, the design of the authentication scheme should address this attack and be robust.

- **Password change attack:** Here, an adversary can change the password illegally to attack a legitimate user. Say, this attack scenario can affect a smartcard-based user authentication protocol in case the smartcard of the legal user gets compromised. The adversary can breach and misuse the information stored in the smartcard to threaten the user [102].

- **Resilience against node capture attack:** The node capture attack can be dangerous [49] for an authentication scheme in VANET. This attack provides a quantified figure of impact on the implementation of a scheme if some terminals are captured by an attacker [46], [50]. In other words, this enables us to find out the effect of a terminal being compromised on the rest of the VANET network and terminals. In other words, this enables us to estimate the effect on a terminal if it is compromised on the VANET networks and terminals. That is if a non-compromised sensor node S_i needs to calculate the probability an adversary is able to decrypt the secured conversations between the terminals S_i and a user U_j once the c_i terminal is already compromised. If we assume this probability is denoted by $P_e(c_i)$. If $P_e(c_i) = 0$, then we call such a protocol is *perfectly secure* and *unconditionally secure against terminal/node capture* *attack*. A user authentication scheme needs to be highly resilient to prevent node capture attacks.

- **Smart card breach attack:** In a normal scenario, the smartcard is considered safe and impossible to crack, but still there is a possible risk of the smartcard being cracked. An adversary or intruder can get access to cryptographic information if a smartcard is attained and can crack it with the help of power analysis attacks [115]. So, an ideal user authentication protocol needs to design incorporating a factor so that from the compromised and cracked smartcard the adversary cannot gain the user's secret parameters.

- **Denial-of-service attack:** In a denial-of-service (DoS) attack, the adversary tries to diminish or eliminate VANET networking resources by flooding or injecting spurious data simulating its expected functions. DoS [154] can be caused intentionally by adversaries or malfunctioning hardware, a crunch of important resources, bugs in software, climatic conditions, or any combination of these factors. A robust user authentication protocol should protect VANET users from this attack.

- **Privileged-insider attack:** A privilege-insider attack can create a critical scenario if an insider to the AS like an administrator, has the special privilege to acquire the secret credentials of any legal user. At the time of designing user authentication, it needs to take care of such scenarios so that user credentials cannot be compromised based on their special roles [135], like system manager or administrator.

- **Masquerade attack:** In a masquerade attack [21], the adversary fabricates himself using a fake login attempt to convince AS to create a situation to force the server to believe that the login request is sourced from a genuine user. An ideal user authentication scheme needs to prevent such attacks.

1.12.2 Functionality Requirements

The following basic functionality requirements should be considered by the user authentication scheme:

- A genuine user should have provision to change his or her password easily and locally without any intervention of the *AS* at his or her will for security reasons.

- New terminals or nodes should dynamically be able to participate in the existing VANET terminals or nodes at any time during their operation.

- An ideal user authentication scheme should be designed to support minimum exchanges of messages or packets to complete the login and authentication of genuine users to work with the constraints of resources. In addition, it should support higher computational efficiency with a minimum storage requirement for each VANET node.

- A user authentication protocol should be scalable and lightweight, and the increase in the number of nodes should not impact the usability of VANET.

1.13 Access Control in VANET

VANET access control has to mainly perform *key establishment* and *node authentication*. In the *node authentication* step, participating terminals have to prove their genuine identity and also show that they have proper access to an object in VANET. However, in *key establishment*, the secret-shared has to be established between *AS* and user to protect secure message exchange. There are few essential requirements to be supported by any ideal access control scheme. These are discussed in [87], [168], [78] to evaluate an access control protocol. The access control feature can prevent unauthorized users from accessing data, and it also ensures data confidentiality. So, access control is necessary to provide protection the security and privacy of users data in VANET. In addition, it helps to meet the fine-grained access control feature for VANET data on authentication server as well as VANET cloud. There is also need to incorporate the access control mechanism to place data access control to ensure that particular data can only be accessed and decrypted by specific legitimate users [99]. These requirements are listed below.

1.13.1 Security Requirements

The following attacks should be addressed properly by the security requirement of access control in VANET:

- **Withstand with eavesdropping or injecting data:** An adversary generally tries to eavesdrop or inject fabricated information into the VANET networks. An ideal access control scheme has to prevent external parties from eavesdropping or injecting false parameters into the existing VANET network communications.

- **Resilience against node capture attack:** The node capture attack can be dangerous for an access control scheme in VANET. This attack provides a quantified figure of impact on the implementation of a scheme if some terminals are captured by an attacker. In other words, this enables us to find out the effect of a terminal being compromised on the rest of the VANET network and terminals. For example, for a non-compromised node S_i, it needs to calculate the probability that the adversary is able to decrypt the secure conversation between the terminals S_i and a user U_j once the c_i terminal is already compromised. If we assume this probability is denoted by $P_e(c_i)$. If $P_e(c_i) = 0$, then we call such a protocol is *perfectly secure* and *unconditionally secure against terminal/node capture attack*. A user access control scheme needs to be highly resilient to prevent node capture attacks.

- **Resilience against new terminal installation attacks:** An ideally designed access control protocol should prevent malicious terminal or node deployment attacks, wormhole attacks, Sybil attacks, and node cloning attacks. In the case of the Sybil attack [57], [116], a malicious terminal or node illegally operates on multiple identities. So, the impersonated identities can be from existing terminals or non-existing terminals. These malicious terminals can be installed directly by an attacker, or they may belong to compromised terminals in the VANET network. This type of attack poses a very serious challenge to distributed network storage, the routing process, the aggregation of data, voting, the fair allocation of resources, the detection of misbehavior, etc. In a wormhole attack [77], an adversary can build a tunnel to receive messages over one channel of the network, and in parallel, the adversary can replay responses over a different channel of the network. This attack can disturb the network topology dynamically by creating false scenarios to make two distant terminals believe they are their neighbors. So, it can be a very serious concern for routing protocols. In a node cloning attack [123], an attacker can create many replicas using compromised nodes at various places to spread inconsistency in the network. This attack is equally threatening as a Sybil attack, and the adversary can subvert the aggression of data, voting protocols, and detection of misbehavior by pumping fabricated data or diminishing legitimate data. Therefore, access control schemes need to be resilient against new terminal installation attacks.

1.13.2 Functionality Requirements of Access Control in VANET

The following few basic functionality requirements should be fulfilled by an access control scheme:

- An ideal access control protocol needs to support dynamic terminal addition to the existing VANET network at any time after the initial installation of terminals or nodes. This requirement may come when a new participating user shows a willingness to join VANET to utilize its services. Further, some terminals or nodes could be compromised by an adversary or exited for a maintenance job. Thus, new node participation is required to allow new elements to join or repaired elements to rejoin the VANET network.

- The mutual authentication between any two communicating terminals needs to be supported by the access control scheme for pairwise key agreement.

- An ideal access control protocol has to provide very secure connectivity so that the participating nodes can establish a secret pairwise key among them.

- An ideal user access control scheme should be designed to support minimum exchanges of messages or packets to complete login and access control for genuine users to work with the constrained nature of resources. In addition, it should support higher computational efficiency with a minimum storage requirement for each VANET node.

- An access control scheme needs to operate without AS to complete authentication and key establishment steps. Further, the dynamic node addition phase may not be allowed to avoid extra computation and communication overheads. In addition to that, this allows any two neighboring vehicles to establish and authenticate secret V2V communication locally without any involvement of the AS. So, access control should support the scalability to handle a large-scale VANET network.

1.14 User Access Control in VANET

In fine-grained user access control, the user is allowed to access desired information with a unique privilege only. This technique uses KP-ABE and the bilinear pairing cryptographic method using elliptic curve groups. Access rights for users can be provided by an efficient "fine-grained access control" for the utilization of various services. By doing so, users can be imposed with a set of access privileges. A set of attributes of the user forms the access policy, and the access policy is imposed by the policy enforcer. The following security and functionality requirements should be ensured for a user access control scheme.

1.14.1 Security Requirements

A user access control scheme should prevent spoofing attacks and resistance against privileged insider attacks, forgery, replay attacks, modification, stolen-verifier attacks, multiple login-id attacks and replay attacks, smartcard breach attacks, and DOS attacks. Further, this should be resilient against terminal capture attacks.

1.14.2 Functionality Requirements

The following basic functionality requirements should be supported by the user access control phase:

- It should provide a high level of scalability when a large network of terminals participates in VANET.

- This should support the dynamic password phase, allowing the user to change his or her password dynamically at their wish without any involvement of the

AS.

- User access control should be designed to support minimum exchanges of messages or packets to complete login and access control of genuine users to work with the constrained nature of resources. In addition, it should support higher computational efficiency with a minimum storage requirement for each VANET node.

1.15 Motivation of the Work

Limited resources, unmanned operations, and radio communication mediums have made the VANET network unrealizable to implement the security protocols designed for traditional uses. VANET and intelligent transport systems (ITS) together form a highly sophisticated, complex system of systems (SOS) that provides data access infrastructure to mobility objects, from basic stand-alone static elements to highly sophisticated dynamic elements to provide data access as per the real-time need for modern traffic management and optimization. To ensure users' core security concerns over crucial data in transit, it essentially demands a foolproof user authentication scheme for accessing desired services from VANET clouds. Critical life-threatening occurrences of important and urgent high-priority events have to traverse unprotected, insecure public and private networks. This openly shared information faces various serious security and privacy challenges listed in Section 1.12.1. Recently, various schemes have been designed to address numerous security concerns, but very few schemes have concentrated on addressing all major attacks with efficiency and in compliance with the functional and general security requirements of VANET. Fundamentally, VANET solves security challenges in a centralized approach where a centrally trusted unit experiences single-point failure issues, and most of the traditional VANET approaches may not support high scalability in such dynamic, hostile scenarios. To prevent those listed attacks, proper security protocols with user authentication, key distribution, user access control, and access control are extremely necessitated in VANET.

To provide the security requirements in VANET, researchers have come out with a lightweight and conditional privacy-preserving authenticated key agreement scheme for fog-based VANETs with symmetric cryptography methods for designing the main steps. This design can greatly reduce the computational and communication overhead of the authenticated key agreement process. However, this protocol concentrates only on authentication without fine-grained access control feature. Some lightweight, efficient, and concise secure authentication protocols are proposed to ensure the privacy and security of IIoT end devices with proper PFS features. However, this lightweight key agreement protocol does not support fine-grained access control functionality. Most of the authentication mechanisms are rigid because the VANET services are available to a particular circle, mainly to the vehicle owner, and the free flow of information among authorized users happens in an unrestricted way. With rapid technological growth, researchers have brought out numerous schemes and protocols for VANET to increase efficiency and effectiveness. However, most of the work was done for peer-to-peer delivery to prevent dynamic attacks in centralized form. Recently, blockchain-based VANET approach has become an interesting field of research, and researchers have also found great potential to add more functional values to ITS and VANET. Decentralization can minimize points of weakness in large VANET systems where there may be too much dependency on specific actors. This weakness can cause systemic failures, including the inability to provide expected services due to the possible exhaustion of resources. Decentralization can optimize the distribution of resources to provide improved performance and consistency, including a reduced likelihood of catastrophic failures. Parallelization incorporates a major step forward in blockchain technology for VANET systems, leveraging the power of multi-core processors. It also drastically reduces transactional complexity and increases the networks energy efficiency. This approach is a fundamental transformation of blockchain networks to make a large VANET more scalable and efficient by executing multiple transactions and processes simultaneously. This feature also improves scalability and enhances network performance. Therefore, parallelism and decentralization are the main working principles for blockchain technology. Most of the research work for blockchain-based VANET has been concentrated on blockchain design. Therefore, there is a need to exploit the possible extent to utilize the benefits of parallel computing and the authentication process of VANET. Further, most of the proposed protocols are either vulnerable to various known attacks or incur high computational and communicational overheads. Therefore, most of the related papers are not fulfilling all the features presented in Sections 1.4 and 1.10 functional requirements and security requirements in Section 1.12.1, so there is a need to further study VANET, which should fulfill all the requirements. Hence, we strongly feel that a large scope is still left for designing the ideal user authentication protocols and access control with proper user access control protocols that can meet all the security requirements, characteristic and realize all the functionality requirements mentioned in Sections 1.10, 1.12, and 1.14. These mentioned scopes for further improvement in VANET protocols motivate us to explore further in these dynamic research areas.

1.16 Objective of the Work

The VANET has become a very challenging and emerging field of research due to the larger scope still left for designing the ideal user authentication protocols and access control protocols with proper user access control features that can meet all the security requirements and realize all the functionality requirements. Various lightweight, efficient, and concise secure authentication protocols are proposed to ensure privacy and security. These schemes include single-pass key-based, dynamic password-based authentication, multi-factor authentication, and secure biometric-based authentication for user authentication in VANET networks. The ECC concept is used to optimize the computation cost, and CP-ABE is used to impose access control over the data in a fine-grained manner based on user attributes along with hash functions. KP-ABE cannot be a better choice for a VANET and IoT environment with many terminals because KP-ABE schemes try to empower the key generation authority, which decides the access authorizations at the time of creating decryption keys. Whereas, in CP-ABE, it gives more weight to the data generators as they decide the access authorizations at the time of encrypting data. Numerous schemes are explored in the user access control schemes, which make use of identity-based signatures, group IDs, and user access with fine-grained features. In this thesis, we focus on exploring novel security in the areas of design and analysis of access control schemes, scalable user authentication, lightweight blockchain-based authentication, and suitable key agreements with fine-grained access control for VANET.

1.17 Summary of Contributions

We have summarized the contributions of the thesis in the next few subsections.

1.17.1 Anonymous Key Agreement Scheme for Secure Vehicular Ad-hoc Networks

First, we propose a lightweight biometrics-based dynamic anonymous key agreement scheme (AKAS) with a fine-grained authentication feature specifically for vehicle-to-vehicle (V2V) communication in VANET, where we try to address both challenges. In the proposed scheme, registered and authorized users can access services or information as per access privilege only. We have performed formal security analysis using the ROR model. Moreover, we have simulated our scheme using AVISPA tools, SUMO, and OMNET++. Analysis and simulation results show that our scheme is secured against various well-known attacks. Further, we have compared the security and efficiency of our scheme with the existing schemes available in the literature and found that our proposed protocol is more secure, lighter, 5G-friendly, scalable, and even faster than the other related schemes.

1.17.2 Biometric-based Authentication Protocol for VANET

Secondly, we propose a dynamic, lightweight biometric-based authentication protocol for vehicle-to-vehicle (V2V) communication networks where the user, after successful registration, can directly login from any local mobile terminal and access his or her services or information directly from the authentication server. We have done the security analysis of our scheme and proved that it provides location privacy, mutual authentication for averting spoofing attack, user anonymity and resistance against replay attack, modification and forgery attacks. We also compare the efficiency of our scheme with other related schemes and show that our authentication scheme is more secure and performs faster than other schemes available in the literature. In addition, our proposed scheme provides scalability as there are no limitations on the number of user terminals; only the genuine user needs to be registered once to avail of the services. No multiple registrations or session-based registrations are required.

1.17.3 Rabin Cryptosystem-based Authentication Mechanism

In our third study, we propose an improved and enhanced Rabin cryptosystem-based authentication mechanism to address all known major attacks with robustness, efficiency, scalability, and dynamicism in mind. Moreover, the basic Rabin cryptosystem is a factoring-based efficient method, but its decryption process leads to failure as it generates 4 to 1 output. However, our proposed protocol is an enhanced method, and it may be noted that the enhanced method is unique and does not lead to failure. We have rigorously carried out security analysis by AVISVA and Proverif Tools. The analysis has shown that our scheme guarantees positional privacy, user anonymity, and mutual authentication to prevent spoofing attacks, password guessing attacks, insider privilege attacks, and temporal session attacks. The comparison of the protocol with the available relevant schemes reveals that the proposed protocol is more efficient in terms of efficacy. It supports a light-weight authentication process for legitimate users. This proposed scheme supports scalability as it does not depend on the volume of user access points, and valid users are required to register only once to access the VANET services. Thus, session-based and duplicate registration can be avoided by the proposed scheme.

1.17.4 Lightweight Blockchain-based Secure Authentication and Fine-grained Access Control in VANET

At last, we propose lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users. We have defined a framework with edge computing and mobile edge computing to offload computation-intensive tasks as well as optimize data processing before sending it to a blockchain-based VANET network. We have done security analysis using the Proverif tool and formally proved security strength using BAN logic. The security analysis shows that the proposed scheme resists various known security threats. Moreover, the performance analysis proves that our scheme is faster and more efficient compared to other relevant protocols available. In addition, in the proposed scheme (LBAFA), we have incorporated blockchain technology to introduce decentralization and parallel computing over the traditional centralized VANET. We have also used ECC to optimize the computation cost and CP-ABE to impose access control over the data in a fine-grained manner based on user attributes.

1.18 Organization of the Thesis

We have organized it as follows:

In **Chapter 1**, we give the fundamentals, architecture, and various aspects of VANET. We then present the motivations, and objectives of our research work on key agreement, user authentication, fine-grained access control, and user access control in vehicular ad-hoc networks. Further, we also discuss various functional and security requirements of VANET protocols. We also give a summary of the contributions of our research work.

In **Chapter 2**, we provide the mathematical preliminaries used to present our research works. We briefly discuss various properties of a one-way hash function. We also discuss the fundamentals and basics of the Rabin cryptosystem algorithm. We discuss the elliptic curve and its properties, the rules for point addition and scalar point multiplication over an elliptic curve, the elliptic curve digital signature algorithm, and the elliptic curve discrete logarithm problem. We also discuss various automated security verification tools used to validate our proposed protocols. We finally discuss various mathematical tools and models used to validate authentication protocols and their efficiency.

In **Chapter 3**, we discuss the research works already carried out by many researchers in the VANET security field. We then present an overview and comparative studies in the areas of design and analysis of access control schemes, scalable user authentication, lightweight blockchain-based authentication, and suitable key agreements with fine-grained access control for VANET.

Chapter 4 presents an anonymous key agreement scheme for secure vehicular ad-hoc networks. In this chapter, we show that our scheme is secured against various well-known attacks. Further, we have compared the security and efficiency of our scheme with the existing schemes available in the literature and found that our proposed protocol is more secure, lighter, 5G-friendly, scalable, and even faster than the other related schemes.

Chapter 5 presents a dynamic, lightweight biometric-based authentication protocol for VANET. We show the security analysis of our scheme and prove that it provides user anonymity, location privacy, mutual authentication to prevent spoofing attacks, and resistance against forgery, modification, and replay attacks. We also show that no multiple registrations or session-based registrations are required.

In **Chapter 6**, we propose an efficient Rabin cryptosystem-based authentication mechanism for VANET. We have proposed an enhancement over the basic Rabin that leads to failure as it generates 4 to 1 output. However, our enhanced method is unique and does not lead to failure. Our analysis shows that our scheme guarantees positional privacy, user anonymity, and mutual authentication to prevent spoofing attacks, password guessing attacks, insider privilege attacks, and temporal session attacks.

Chapter 7 presents a lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users. We incorporate blockchain technology to introduce decentralization and parallel computing over traditional centralized VANET. We also use ECC to optimize the computation cost and CP-ABE to impose access control over the data in a fine-grained manner based on user attributes.

Finally, in **Chapter 8**, we provide the summary of the work done, highlight the contributions, and suggest future directions for possible research work.

Chapter 2

Mathematical Background

We first discuss the basic properties of the one-way hash function and its useful properties. We then discuss the importance of elliptic curve cryptography (ECC) for various protocols in VANET. We also present important rules of ECC to define addition of two points, scalar point multiplication over an elliptic curve, and digital signature algorithm based on ECC. Then the discrete logarithm problem of the ECC is discussed. In the third section, we have discussed various automated security verification tools used to validate our proposed protocols. These tools are automated validation of internet security protocols (AVISPA) tools, objective modular network testbed in C++ (OMNET++), and simulation of urban mobility (SUMO). The major tools and mathematical models are explained briefly in the following subsections. Finally, we present the various data structures of blockchain and setups used to explain the blockchain-based scheme for VANET.

2.1 One-way Hash Function

A cryptographic hash function can be defined as an algorithm that takes a variable bit length as input data and generates a fixed-length string of bits called a cryptographic hash value as output. The hash function accepts a large set of data and generates apparently random output that is distributed evenly. The hash function inherently supports data integrity. A single-bit change in hash function input can change a significant number of bits in the generated hash function output. It is also computationally impracticable to find an input data object that outputs a pre-specified hash value. This is ensured by its one-way property. It is also mathematically infeasible to determine two input data objects that produce the same hash value, and this is called the collision-free property. This property of the hash function is often utilized to determine the data integrity.

Mathematically a one-way hash function can be defined as $h : \{0,1\}^* \rightarrow \{0,1\}^l$ receives an input x of variable length, where $x \in \{0,1\}^*$, and generates output $h(x) \in \{0,1\}^m$ as fixed-length string (say, m-bits), and this output is termed the hash value or the message digest. The hash function has the following features [144] that can produce a fingerprint of a message, a file, or any other data object.

- h may be applied to all sizes of data blocks.
- For a given input data x, the hash value $h(x)$ can be easily operated for implementation in software as well as hardwires.
- By definition, the produced output message digest $h(x)$ has a fixed, defined length.
- Its one-way property ensures that it is computationally very hard and infeasible to determine an input x even if $y = h(x)$ and the hash function $h(\cdot)$ are given.
- Another special property $h(\cdot)$ is called strong-collision-resistant. This ensures that determining a pair of inputs (x, y), such that $x \neq y$ and $h(x) = h(y)$ mathematically infeasible.
- However, its weak-collision-resistant property states that it is mathematically infeasible to find another value for a given input x, such that $y \neq x$ and $h(y) = h(x)$.

The hash function has numerous applications, and this can be applied practically to digital signatures, information security, cryptology, various forms of authentication, and message authentication codes (MACs). Therefore, this has become a fundamental building block for modern cryptographic protocols. In many applications, hash functions play a vital role in digital signatures, wide filed of cryptology, information security, message authentication codes (MACs) and other various forms of authentication. So, hash functions become the basis and strength of many cryptographic protocols. A single-bit change in hash function input can change significant number of bits in the generated hash function output. Therefore, small perturbations in its given input affect the output exaggeratedly, and this makes the hash function very special in cryptology. The SHA-1 is a one-way secure hash algorithm [7]. But Quark [17] defines a family of cryptographic hash functions designed for extremely resource-constrained scenarios, like for radio-frequency identification (RFID) tags. So, Quark can be used for a very lightweight system instead of SHA-1.

2.2 ECC Cryptosystem

Here, we briefly present the useful properties of an elliptic curve and an elliptic curve cryptography (ECC) cryptosystem as follows:

2.2.1 Fundamental of Elliptic Curve Over a Finite Field

Let us assume two constants a and $b \in Z_p$ and $p > 3$ is a prime, where $Z_p = \{0, 1, \ldots, p-1\}$, satisfying $4a^3 + 27b^2 \neq 0 \,(\mathrm{mod}\, p)$. Then $y^2 = x^3 + ax + b$ is a non-singular elliptic curve over a finite field $GF(p)$ with a set $E_p(a, b)$ of solutions $(x, y) \in Z_p \times Z_p$ to the congruence

$$y^2 = x^3 + ax + b \,(\mathrm{mod}\, p),$$

along with a special point $\mathcal{O}$ termed a zero point or a point at infinity.

It is noted that $4a^3 + 27b^2 \neq 0 \,(\mathrm{mod}\, p)$ may be considered a sufficient and necessary condition to confirm that the equation $x^3 + ax + b = 0$ results in non-singular solutions [117]. Otherwise, if $4a^3 + 27b^2 = 0 \,(\,\mathrm{mod}\ p)$, then that elliptic curve is considered as a singular elliptic curve. Let us assume $A = (x_A, y_A)$ and $B = (x_B, y_B)$ are two points in $E_p(a, b)$. Then $A + B = \mathcal{O}$ implies that $x_B = x_A$ and $y_B = -y_A$. We get $A + \mathcal{O} = \mathcal{O} + A = A$, for all $A \in E_p(a, b)$. In addition to that Hasse also asserts that $E_p(a, b)$, number of points represented by $\#E$, follows the given inequality [144]:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}.$$

So, we can say that an elliptic curve $E_p(a, b)$ over Z_p has approximately p points on it. Besides that, $E_p(a, b)$ forms a cyclic abelian or commutative group only under addition modulo p operations.

Point Addition on Elliptic Curve Over Finite Field

Let assume G be the base point on $E_p(a,b)$ of order n, that is, $nG = G + G + \ldots + G(n\,times) = \mathcal{O}$. If $A = (x_A, y_A)$ and $B = (x_B, y_B)$ are two points on elliptic curve $y^2 = x^3 + ax + b \pmod p$, $C = (x_C, y_C) = A + B$ is calculated as follows ([88], [144]):

$$x_C = (\lambda^2 - x_A - x_B)(\bmod p),$$
$$y_C = (\lambda(x_A - x_C) - y_A)(\bmod p),$$
$$\text{where } \lambda = \begin{cases} \frac{y_B - y_A}{x_B - x_A} (\bmod p), \text{if } A \neq B \\ \frac{3{x_A}^2 + a}{2y_A} (\bmod p), \text{if } A = B. \end{cases}$$

Scalar Multiplication on Elliptic Curve Over Finite Field

In elliptic curve cryptography, scalar multiplication can be defined as repeated additions. i.e., if $A \in E_p(a,b)$, then $5A$ is calculated as $5A = A + A + A + A + A \pmod p$.

Example 2.2: Let us consider two points $A = (11,3)$ and $B = (9,7)$ are in the elliptic curve $E_{23}(1,1)$ [30]. All the points of $E_{23}(1,1)$ are presented in Table 2.1 as well as in Figure 2.1.

Table 2.1: Points over the elliptic curve $E_{23}(1,1)$.

$(0,1)$	$(6,4)$	$(12,19)$	$(0,22)$	$(6,19)$	$(13,7)$	$(1,7)$	$(7,11)$	$(13,16)$
$(1,16)$	$(7,12)$	$(17,3)$	$(3,10)$	$(9,7)$	$(17,20)$	$(3,13)$	$(9,16)$	$(18,3)$
$(4,0)$	$(11,3)$	$(18,20)$	$(5,4)$	$(11,20)$	$(19,5)$	$(5,19)$	$(12,4)$	$(19,18)$

If we consider two points $A = (11,3)$ and $B = (9,7)$ in $E_{23}(1,1)$. For this case, $A \neq B$. In order to calculate $C = A + B = (x_C, y_C)$, we first calculate λ as

$$\lambda = \frac{7-3}{9-11} (\bmod 23) = 21.$$

So, x_C and y_C are calculated as

$$x_C = (21^2 - 11 - 9)(\bmod 23) = 7,$$
$$y_C = (21(11-7) - 3)(\bmod 23) = 12.$$

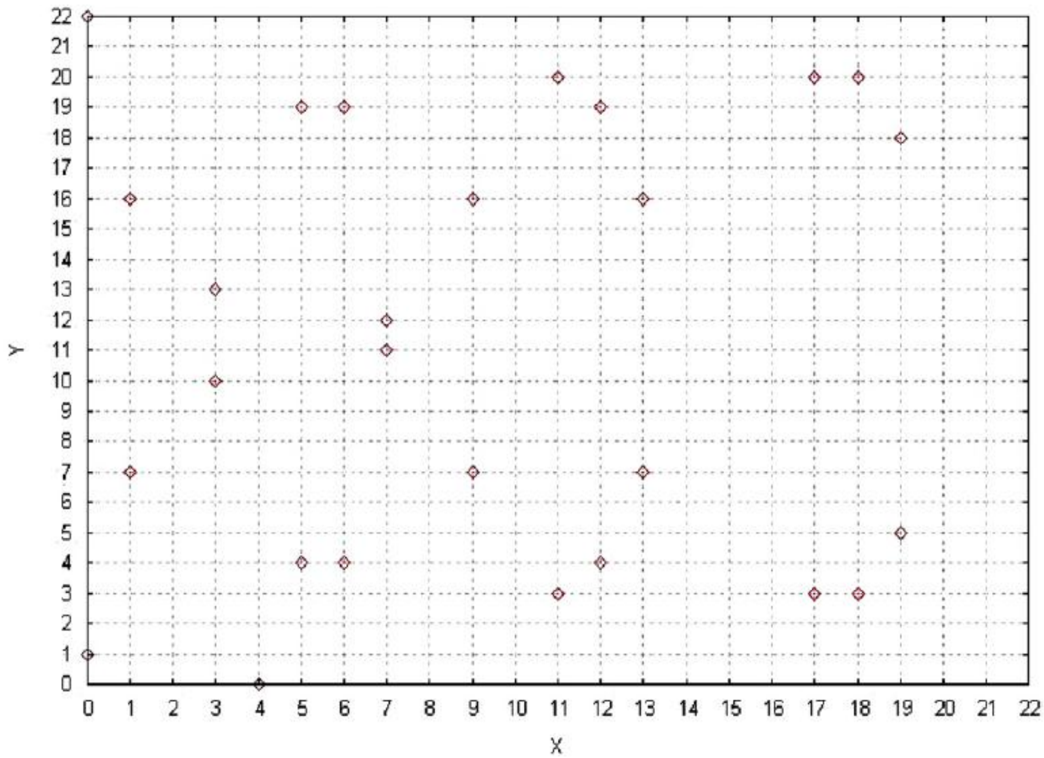

Figure 2.1: Example of elliptic curve in case of $y^2 = x^3 + x + 1 \pmod{23}$ [30].

Therefore, $A + B = (7, 12)$.
For calculating $2A$, first, we need to derive λ as follows:

$$\lambda = \frac{3(11^2) + 1}{2 \times 3} \pmod{23} = 7.$$

Hence, $C = A + A = (x_C, y_C)$ is calculated as

$$x_R = (7^2 - 11 - 11)(\mathrm{mod}\ 23) = 4,$$
$$y_R = (7(11 - 4) - 3)(\mathrm{mod}\ 23) = 0,$$

and thus, $2A = (4, 0)$.

2.2.2 ECC Encryption/Decryption

Before initiating the encryption and decryption processes, the plaintext message m is encoded as an elliptic curve (EC) point $P_m \in E_p(a, b)$ in this cryptosystem. This point P_m is then encrypted to produce a ciphertext and subsequently decrypted.

Key Generation

In this phase, every user B generates a key with the available information, like a base point $G \in E_p(a, b)$ of order n, such that $nG = \mathcal{O}$ and the EC $E_p(a, b)$ over the finite field $GF(p)$. User B picks up a private key n_B arbitrarily in the given interval $[1, n-1]$ and calculates its public key $P_B = n_B G$.

Encryption

In this step, the plaintext message, say P_m is encrypted. The user A first selects a random integer k in the given interval $[1, n-1]$ and calculates the ciphertext C_m. This ciphertext consists of points C_1 and C_2, where $C_m = (C_1, C_2)$, with $C_1 = kG$, and $C_2 = P_m + kP_B$, where P_B is B's public key. Finally, A shares the encrypted message C_m with user B through a public channel.

Decryption

In this step, ciphertext message C_m is decrypted. The user B first calculates point $C_1 = kG$ with its private key n_B and obtains $n_B(kG) = kP_B$. B then retrieves the plaintext message P_m by calculating $C_2 - n_B C_1 = (P_m + kP_B) - n_B(kG) = P_m + kP_B - kP_B = P_m$. It may be noted that the plaintext message P_m is obtained by adding kP_B and this is done by the user A. The value of k is only known to A, therefore, even though P_B is a publicly available, but none including attackers can remove the mask kP_B without having the information of the user B's private key n_B.

Example 2.3: Let us assume two users A and B work with the elliptic curve cryptosystem. By definition, the elliptic curve cryptosystem is applied on the elliptic curve $y^2 = x^3 + ax + b \pmod p$ with the parameters $E_{11}(1, 1)$, where $p = 11$, $a = 1$ and $b = 6$. It may be noted that $4a^3 + 27b^2 \neq 0 \pmod{11}$ and so, this elliptic curve is non-singular. We assume the base point G be $G = (2, 7)$. We have B's secret key n_B is $n_B = 7$. Then, B's public key is calculated as $P_B = n_B G = 7.(2, 7) = (7, 2)$. Let the user A wants to share a plaintext message $P_m = (10, 9)$ secure way to the user B. To perform this purpose, let A selects a random value $k = 3$. A then calculates the ciphertext $C_m = (C_1, C_2)$ as

$$\begin{aligned} C_1 &= kG \\ &= 3.(2,7) \\ &= (8,3), \\ C_2 &= P_m + kP_B \\ &= (10,9) + 3.(7,2) \\ &= (10,9) + (3,5) \\ &= (10,2), \end{aligned}$$

and sends C_m to B through a public channel. After receiving C_m, user B decrypts it to retrieve the original plaintext message P_m as

$$\begin{aligned} P_m &= C_2 - n_B C_1 \\ &= (10,2) - 7.(8,3) \\ &= (10,2) - (3,5) \\ &= (10,2) + (3,-5) \pmod{11}, \text{ since if } P = (x_P, y_P), -P = (x_P, -y_P) \\ &= (10,2) + (3,6) \pmod{11} \\ &= (10,9). \end{aligned}$$

2.2.3 ECC Signature

The working principles of the elliptic curve digital signature algorithm (ECDSA) [85], [100] and the digital signature algorithm (DSA) [145] are quite similar. The ECDSA has the following phases: key generation, generation of signatures and verification of signatures. These phases are briefly presented below.

Key Generation

Key generation makes use of the available information like, a base point $G \in E_p(a,b)$ of order n, such that $nG = \mathcal{O}$ and the EC $E_p(a,b)$ over the finite field $GF(p)$. For ECDSA these domain parameters are suitably chosen. Each entity $\mathcal{A}$ should do the following:

Step 1. Pick up a random or pseudorandom integer k in the interval $[1, n-1]$.

Step 2. Calculate $Q = kG$.

Step 3. $\mathcal{A}$'s public key is Q; $\mathcal{A}$'s private key is k.

Signature Generation

To sign a message, let m, be an entity $\mathcal{A}$ with ECC domain parameters $D = (p, n, Q, G,\ E_p(a, b), h(\cdot))$, where $h(\cdot)$ is a secure hash function and respective key pair (k, Q) should do the following steps:

Step 1. Choose a random or pseudorandom integer l, with $1 \leq l \leq n - 1$.

Step 2. Calculate $lG = (x_1, y_1)$ and $r = x_1 \mod n$. If $r = 0$ then go to step 1.

Step 3. Calculate $e = h(m)$ and $s = l^{-1}(e + kr) \mod n$. Then go to step 1 if $s = 0$.

Step 4. The signature of $\mathcal{A}$ is calculated as (r, s) for the message m.

Signature Verification

To verify $\mathcal{A}$'s signature (r, s) on m, the verifier $\mathcal{B}$ gets an authentic copy of $\mathcal{A}$'s domain parameters D and respective public key Q. After that $\mathcal{B}$ needs to do the following steps:

Step 1. Verify that r and s are integers in the defined interval $[1, n - 1]$.

Step 2. Evaluate $e = h(m)$.

Step 3. Calculate $w = s^{-1} \bmod n$, $u_1 = ew \bmod n$, $u_2 = rw \bmod n$ and $X = u_1G + u_2Q$. If $X = \mathcal{O}$, then the signature is discarded. Otherwise, calculate $v = x_1 \mod n$, where $X = (x_1, y_1)$.

Step 4. The signature is then accepted if and only if $v = r$.

2.2.4 Security of ECC Cryptosystem

The security strength of ECC cryptosystem mainly depends on the hardness of solving the elliptic curve discrete logarithm problem (ECDLP). The discrete logarithm problem (DLP) is discussed before defining ECDLP for better understanding.

Discrete Logarithm Problem [35]

If an element g in a finite group S of order is n, i.e., $n = \#S_g$ (S_g is assumed as the subgroup of S generated by g) and another element y in S_g. The problem is to determine the smallest non-negative integer number x such that $g^x = y$. This mathematical problem is known as the discrete logarithm problem (DLP). It is comparatively easier to compute discrete exponentiation $g^x \pmod n$ given g, x and n, however, it is computationally very hard to determine x given y, g and n, when n is very large.

Elliptic Curve Discrete Logarithm Problem [35]

Let $E_p(a, b)$ is defined as an elliptic curve modulo a prime p. For two points $P \in E_p(a, b)$ and $Q = kP \in E_p(a, b)$ and some positive integer k, where $Q = kP$ denotes the point P on EC $E_p(a, b)$ is added to itself k times repeatedly. Then the elliptic curve discrete logarithm problem (ECDLP) has to compute k the given P and Q. It is computationally easier to calculate Q given k and P, however it is computationally very hard to find out k given Q and P, if the prime p is very large.

2.3 Security Verification Tools

In this section, we discuss various automated security verification tools used to validate our proposed protocols. We have simulated our scheme using automated validation of internet security protocols (AVISPA) tools, SUMO, and OMNET++ tools. The major tools and mathematical models are discussed briefly in the following subsections.

2.3.1 An Overview of AVISPA Tool

AVISPA tool is fundamentally a push-button tool, and it stands for the automated validation of internet security protocols and applications. It also provides a platform to represent and specify protocols, including their security properties, in a modular and expressive way using defined formal language. It can integrate different backends that implement advanced analysis automatically [61]. The overall skeleton of the AVISPA validation tool is shown in Figure 2.2 [3]. We have incorporated the widely used AVISPA tool to study formal security verification for intrusion detection and attack mitigation accuracy [26], [47]. AVISPA uses high-level protocol-specific language (HLPSL) [119] to implement abstraction-based procedures and four back-ends. The executability of the protocols is verified by static analysis, and intruder roles are compiled to generate an intermediate format (IF).

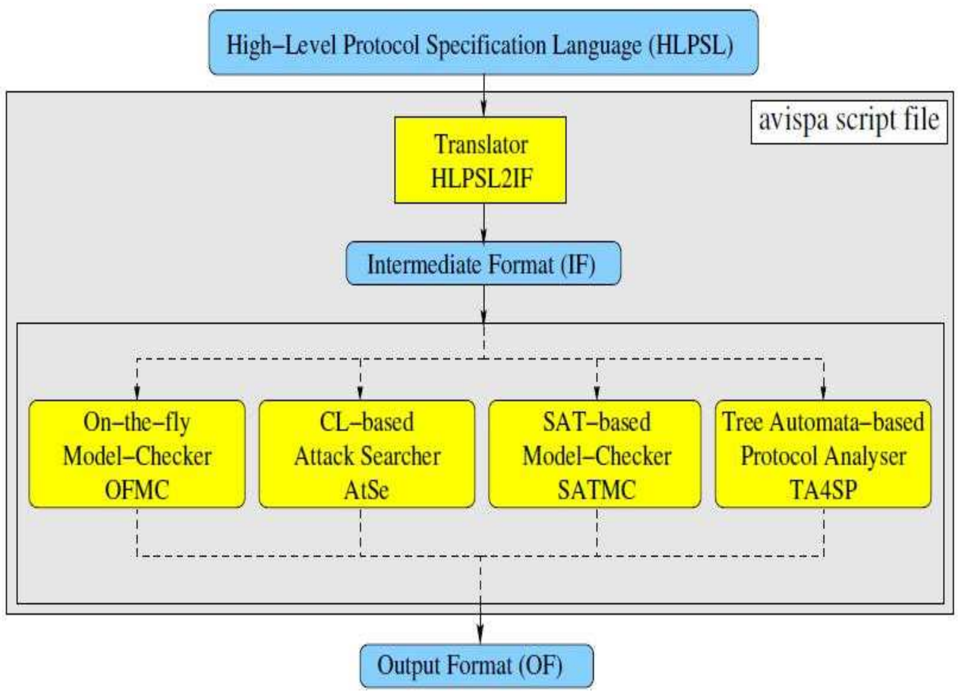

Figure 2.2: Architecture of the AVISPA tool [3]

The IF is the initial point to start the four automatic protocol analysis techniques. The IF is directly used by the AVISPA tool as it is a lower-level language than HLPSL.

The on-the-fly model-checker (OFMC) is the first back-end module with several symbolic techniques to study various state spaces on a demand basis [53]. The constraint-logic-based attack searcher (CL-AtSe) is the second back-end, and it translates security protocol specification as a transition relation from IF format into a set of constraints that can be effectively used to find if there are any attacks on protocols. The third back-end module is the SAT-based model-checker (SATMC), and it builds a propositional formula that can be provided to a SAT solver. Lastly, the fourth back-end module is TA4SP (tree automata based on automatic approximations for the analysis of security protocols), and it can approximate the intruder knowledge in the form of regular tree languages. The code should be written in HLPS language and this has different roles to be implemented [119]. These basic roles represent each participant to simulate the scenarios. Each role is independent and allocated with basic resources for communication channels, including some initial parameters. The intruder scenario is modeled using the Dolev-Yao model [120]. The role system also includes roles, the number of principals, and session numbers in its definition.

In AVISPA, the four back-end modules generate the output format (OF). After successful execution of the analysis, the output produces precise results under a specific stated condition.

- The first section presents the summary to indicate if the tested protocol is considered as safe, unsafe, or the analysis is inconclusive.
- The DETAILST is explained in the second section and it states the assumed conditions for which the tested protocol is projected as safe, or what conditions have been used to find attacks, or finally, why the analysis is an inconclusive.
- Other sections represent PROTOCOL, GOAL and BACKEND to print the name of the protocol, the defined goal of the analysis, and the back-end module used, respectively.
- Finally, the traces of attack (if any) are also printed in the standard Alice-Bob format.

The various keywords in HLPSL are briefly explained.

- *agent:* The value of type *agent* denotes principal names. The intruder is always considered to have the special identifier i.
- *public_key:* These values denote agents' public keys in a public-key cryptosystem. For example, a public (respectively private) key *pk* and its inverse private (respectively public) key are obtained by *inv_pk*.
- *symmetric_key:* This variable represents keys for a symmetric-key cryptosystem.

- *text:* In HLPSL, *text* is often used as nonces. These values can be used to form messages. If Na is of type *text (fresh)*, then Na' will be a fresh value that cannot be guessed by the intruder.

- *nat:* The *nat* type denotes the natural numbers in a non-message contexts.

- *const:* This type denotes constants.

- *hash_func:* This base type *hash_func* denotes the cryptographic hash functions. The base type function can also represent functions in the space of messages. It is also assumed that the intruders cannot invert hash functions (in essence, that they are one-way).

- *bool:* This type of variable is used to represent the Boolean values that are useful for modeling.

2.3.2 Overview of SUMO

The simulation of urban mobility (SUMO) is a mobility simulator to simulate the dynamic behavior of VANET protocols. In the traffic research field, there are four types of traffic flow, and these are modeled to distinguish as per the level of simulation details. These models are macroscopic models, microscopic models, mesoscopic model and sub-microscopic models. Different simulation granularities are shown in Figure 2.3. In macroscopic models, traffic flow is considered the basic entity. In microscopic models, the simulation is done for the mobility of all vehicles on the considered street. In this mode, the vehicle's physical abilities and the driver's controlling behavior are captured to study the traffic scenario [29]

The microscopic model SUMO was developed by Stefan et al. [89], [90] and this model is further extended by some advanced assumptions. Mesoscopic simulations are done between microscopic and macroscopic flow simulations. In this case, queue approaches are considered for vehicle movement. Whereas, in sub-microscopic models, further details about vehicles like engine RPM, speed, and drivers driving patterns are considered to study the mobility simulation. However, sub-microscopic models involve longer computation times compared to other models.

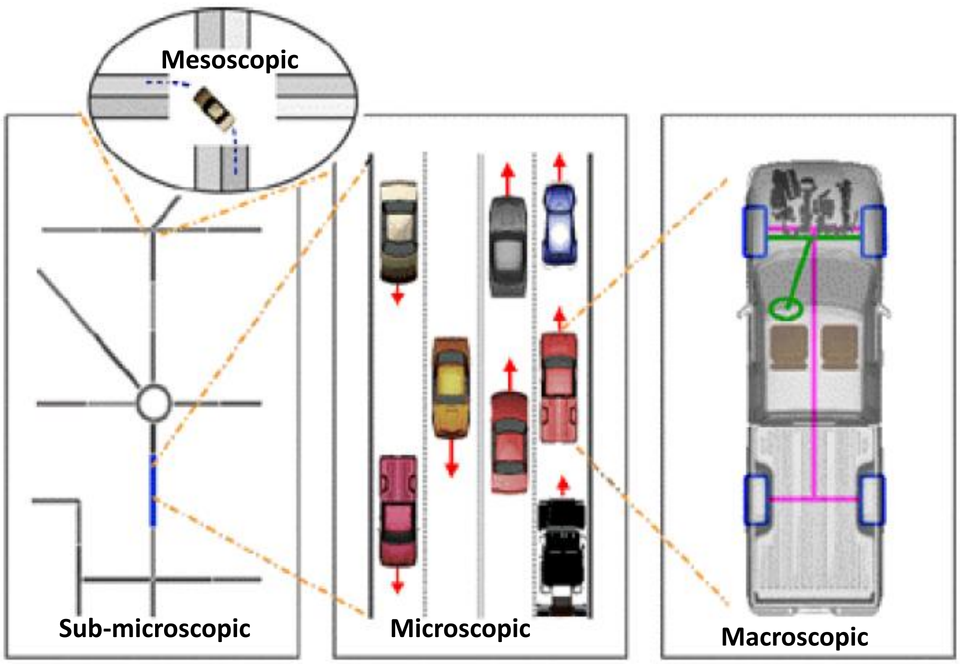

Figure 2.3: Simulation granularities in SUMO tool [8]

2.3.3 Features of SUMO

It can support import formats like OpenStreetMap, VISUM, VISSIM and NavTeq. The background for the development was to support the traffic research community with an open source, microscopic road traffic simulation tool so that various algorithms and protocols can be implemented and evaluated in a realistic traffic environment. SUMO is also widely used by the V2X community for realistic vehicle traces and for applications in an on-line loop with a network simulator. A graphical simulation environment of SUMO is shown in Figure 2.4. The SUMO has the following features [12]:

- Simulation with collision-free vehicle
- Various categories of vehicle types
- Multi-lane streets along with lane-changing facilities
- Junction-based traffic condition with right-of-way rules

Figure 2.4: A graphical simulation environment of SUMO [118]

- Hierarchal structure of junction types
- An openGL graphical user interface (GUI)
- Management of networks with several 10.000 edges (streets or roads)
- Faster execution speed (approximately 100000 vehicle updates/sec over a 1GHz machine)
- Run time interoperability with other applications using TraCI
- Missing values are estimated via heuristics.
- Dynamically performs user assignment

2.3.4 Network Simulator (OMNET++)

The OMNeT++ is an integrated development environment (IDE) based on the Eclipse platform. Network simulation environment by OMNeT++ is shown in Figure 2.5. It was developed by Andras and his teams since 2001 [151]. The major use of OMNeT++ are for simulation of computer networks and resource layout. It provides modular and component based architecture. OMNet++ can add functionalities for creating and configuring models using NED and INI files. It performs batch executions, and analyzes simulation results with the help of Eclipse IDE that provides C++ editing platform, SVN/GIT integration, and other advanced optional features like UML modeling and bugtracker integration through various open-source The OMNet++ is also compatible with traffic environ simulator SUMO.

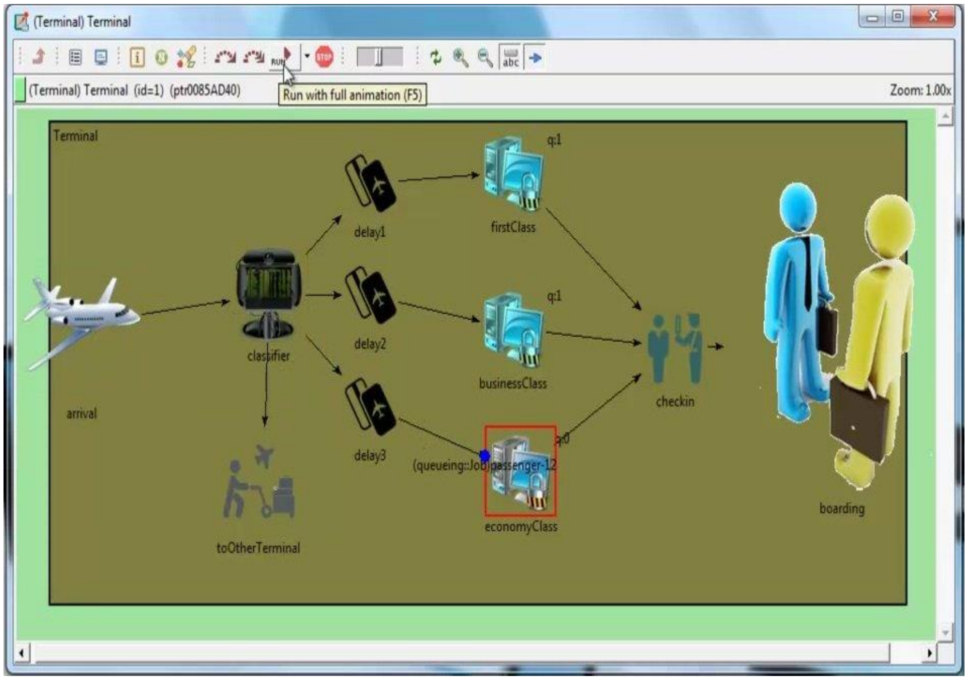

Figure 2.5: Network simulation environment by OMNeT++ [1]

2.4 Blockchin Data Structure

In this section, we explain the various data structures and setups used to present the scheme.

2.4.1 Mekle Tree (MT)

To find the availability of transactions in the blockchain, a merkle data structure is used. This data structure is represented by a merkle tree, and it maintains the hash value of transactions. The leaf nodes hold the hash value of the unit data, while the non-leaf node is used to store its left and right nodes' hash values. The merkle data structure can handle the deletion of transactions efficiently without affecting the security and integrity of the blocks [166]. An ideal binary merkle tree has three main properties: it has 2^n nodes, where n is the height of the merkle tree; each node can have 0 or 2 child nodes; and all leaf nodes maintain the same level [71]. A simple merkle tree is presented in Figure 2.6.

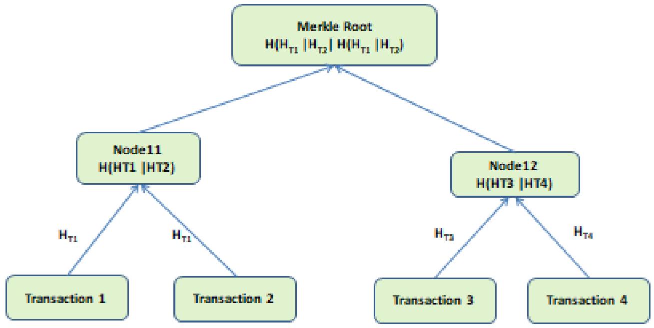

Figure 2.6: A simple merkle tree.

2.4.2 Access Structure and Access Tree

The access policy and attributes can be defined in the similar line of [68]. If we assume the universal attribute set of the system as $A = \{a_1, a_2, a_3, ..., a_{|A|}\}$. The user is assigned with a set attributes λ, where $\lambda \neq NULL$ and $\lambda \subset A$. Therefore, we can define access structure $\mathbb{A} \subseteq 2^{\{a_1, a_2, a_3, ..., a_{|A|}\}}$. $\mathbb{A}$ holds the monotone property [20], if $\forall B, C \in A \& B \subseteq$, so we have $C \in A$.

An access structure can be represented as access tree. In this chapter, we have represented access tree as τ for attribute set ω and access structure $\mathbb{A}$. We also define access tree τ which corresponds to access policy ψ. Let d_x denote the degree of the q_x and th_x threshold value nodes. So, we have $d_x = th_x - 1$. Each leaf node represents a unique attribute corresponding to its access policy, and non-leaf nodes represent OR or AND gate or $< t - out - of - n >$ threshold structures. If $\tau(\lambda) = 1$ i.e. if λ attribute set is accepted by the access tree, then the polynomial is computed recursively.

2.5 Summary

In this chapter, the basic principles of cryptography are reviewed and analyzed. Here, we have concentrated on those mathematical models and cryptographic techniques that are useful for designing VANET protocols. We also discuss the significance of one-way hash function and the importance of elliptic curve cryptography. In the third section, we have discussed various automated security verification tools and their working principles used to validate our proposed protocols. The major tools and mathematical models are explained briefly. Finally, we present the various data structures of blockchain and setups used to explain the blockchain-based scheme for VANET.

Chapter 3

Review of Related Works

In this chapter, we discuss the research work already carried out by many researchers in the VANET security field. We then present an overview and comparative studies in the areas of design and analysis of access control schemes, scalable user authentication, lightweight blockchain-based authentication, and suitable key agreements with fine-grained access control for the VANET.

3.1 Background of Security Protocols in VANETs

The major security concerns in the VANET lie in the proper design and analysis of access control schemes, scalability in user authentication, lightweight blockchain-based authentication, and suitable key agreements with fine-grained access control for the VANET.

3.1.1 Some well-studied authentication protocols in VANETs

A tangible volume of research has been carried out to address the multifold challenges of VANETs, and most of the work stressed upon the problem from privacy protection to general authentication mechanisms [128]. An anonymous certificate foundation is built by Raya and Haux [157] to conceal the original credentials of the users. In their scheme, a vehicle has to store a set of different public or private key pairs to mask traceability using unique key pairs. This scheme shows its difficulty for key distribution and key management in a large network. Lu et al. [137] present a short live anonymous certificate scheme to inhibit communication traceability, but this scheme suffers from performance issues with VANETs due to frequent interaction between RSU and vehicles.

The fixed-size anonymous certificate-based mechanism proposed by Zhang et al.[23] also fails to achieve its desired goals because of its total dependency on RSU, and failure of RSU leads to a complete breakdown of the mechanism. Studer et al. [9] based authentication mechanism has become ineffective as public keys are to be certified to verify the authenticity of the credentials of users.

To address a number of different kinds of aforesaid challenges posed by VANETs, a special effort was kept by Chaung & Lee [110] and Saru Kumari et al., respectively, in TEAM and enhanced TEAM. ETEAM is an extension of TEAM, where TEAM sends a user credential (user and PW) pair to the server (AS) as plain text, but ETEAM sends a user ID and hashed password concatenated with a random element. TEAM is an authentication mechanism for vehicle-to-vehicle (V2V) communication in which three categories of vehicles, namely LE, TV, and MTV, are considered. Depending on the level of authentication, a normal vehicle can have two statuses of recognition, i.e., trustful and mistrustful state. A normal vehicle is kept under the mistrustful category until it passes the laid-down authentication procedure. Once the vehicle has satisfied the authentication procedure in VANETs, it is elevated to the state of trustfulness. A special set of vehicles belonging to a certain defined organization is always considered as trustful and they play a role of LE and mobile AS.

A normal vehicle plays the role of a temporary LE [120] after a successful authentication procedure and maintains its trustful state till the validity of the session key expires. TEAM and ETEAM provide a special feature in VANET to update and increase the life of the key. TEAM and ETEAM both used for general authentication between vehicles and AS using the ID, password, and vehicle details of the user. User credentials have to be transferable or shareable among users when there may be a situation where users other than the real user have to use the VNAET services. An authentication scheme based on the transferable or shareable user's credential can indulge in thorough sharing of information or services, which may lead to an extremely complicated situation [93], [111]. For example, an adversary can trace or misuse a target vehicle, driver, or passenger to cause an undefined extent of loss if a transferable user's credential goes into the wrong hands. On the other hand, VANET services become very localized to specific users if a credential is imposed with features like a non-transferable or non-shareable user's credential. However, it is desirable that VNET services be extended to a variety of classes of users, depending on the users' needs and interests. To make VANET services reachable to all classes of users, a biometric smart card-based authentication mechanism can be a better idea.

3.1.2 Certificate-based Protocols in VANETs

Research communities have allocated a considerable amount of interest and activities to resolve the security concerns of vehicular ad-hoc networks. These research activities tried to solve everything from privacy shielding to general authentication aspects [128]. Munwar et al. [107] proposed a C2aaS protocol for cloud security where it processes data dynamically based on the security level of the data. The proposed model exhibits good security for confidential data and proficiently reduces cloud system overload. In the anonymous certificate approach, a dynamic platform needs to maintain several public-private key pairs to conceal the traceability that gets exposed by the use of a single key pair. However, this certification approach reveals inefficiency and difficulty in maintaining the provisioning of keys with the proper key distribution for a larger networking infrastructure. Anonymous certification idea with fixed size key technique developed by Zhang et al. [23] could not achieve its desired objectives as it totally depends on fixed roadside unit (RSU), and the inability of seamless performance of it causes direct collapse of the principle. The authentication approach by Studer et al. has shown its ineffectiveness because the credential of the user should be certified and verified for genuineness. Chaum et al. [31] have first introduced the concept of group signature-based authentication protocol. This scheme permits the delegation of signing to all its group members, and the signing candidate can be identified by the group in charge at the time of any dispute. However, the careful analysis shows that the ideal anonymity is compromised in the scheme because of a trade-off due to the close relationship between the length of the group and the level of anonymity. Jie et al. have presented 5G-enabled elliptic curve cryptosystem-based RSMA [169], and it supports batch authentication inherently. Although this supports high performance, it does not support fine-grained features.

3.1.3 Lightweight Authentication Protocols in VANETs

Qing et al. proposed a lightweight SAKE* [124] protocol to address various issues of IIoT and the critical security concern of authentication and key exchange (AKE). This is a very lightweight key agreement protocol with soundness, FPS, and other major functional security requirements. However, this protocol concentrates only on authentication without a fine-grained access control feature. Similarly, Yunru et al. proposed a lightweight, efficient, and concise SAPFS [161] protocol to ensure the privacy and security of IIoT end devices with proper PFS features. However, this lightweight key agreement protocol does not support fine-grained access control functionality. Most of the authentication mechanisms are rigid because the VANET services are available to a particular circle, mainly the vehicle owner, and the free flow of information among authorized users happens in an unrestricted way. Table 3.1 presents strengths and weaknesses with respect to the security features and requirements of various lightweight security protocols. This table indicates that recently lightweight available schemes are not able to resolve or address all the security and functional requirements. So, there is a need to design new protocols, which we have addressed during our research work.

Table 3.1: Availability of functionality features

Protocol	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8	ϕ_9	ϕ_{10}	ϕ_{11}	ϕ_{12}	ϕ_{13}	ϕ_{14}	ϕ_{15}	ϕ_{16}	ϕ_{17}
Chaung *et al.* [110]	✓	**X**	✓	✓	✓	✓	**X**	**X**	**X**	✓	**X**	**X**	✓	**X**	**X**	**X**	**X**
Zhang *et al.* [23]	✓	✓	✓	✓	**X**	✓	**X**	**X**	✓	✓	✓	**X**	✓	**X**	**X**	**X**	**X**
ETEAM *et al.* [130]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	**X**	**X**	**X**	**X**	**X**
Qing *et al.* [124]	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	**X**	**X**
Yunru *et al.* [161]	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	**X**	**X**
Li *et al.* [156]	✓	**X**	✓	✓	**X**	✓	**X**	**X**	**X**	✓	**X**	**X**	✓	**X**	**X**	**X**	**X**
Das *et al.* [129]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	**X**	**X**	**X**

ϕ_1 : provides mutual authentication; ϕ_2 : flawless password change phase; ϕ_3 : resists server spoofing attack; ϕ_4 : resists man-in-the-middle attack/replay attack; ϕ_5 : resists privileged-insider attack; ϕ_6 : resists lost smart card attack; ϕ_7 : strong user anonymity; ϕ_8 : resists session-specific temporary information attack; ϕ_9 : resists DoS attack; ϕ_{10} : perfect forward secrecy; ϕ_{11} : resists key-compromised impersonation (K-CI) attack; ϕ_{12} : circumventions dependence on open access control; ϕ_{13} : execute without identity-verification table; ϕ_{14} : low computation cost; ϕ_{15} : low communication cost; ϕ_{16} : resistance to unintended sharing attack; ϕ_{17} : prevents credential cloning attack.

3.2 Existing Access Control Schemes in VANETs

Some important existing related access control schemes are proposed in VANET and sensor networks. In this section, we briefly discuss these protocols.

Zhou et al. [11] presented an access control scheme. This is based on an elliptic curve cryptographic (ECC) algorithm for sensor and VANET networks. Their scheme performs with better efficiency than the RSA-based schemes. Their scheme has the following phases for deployment:

In the pre-deployment step, first the certificate authority (CA) decides a set of required parameters and node parameters to be preloaded into each node. In the deployment phase, all the nodes bootstrap and establish communication among them. Zhou et al.'s scheme can also support the addition of new nodes to the VANET network dynamically. This scheme can support peer-to-peer key establishment using preloaded certificates at the bootstrapping time. However, their proposed scheme faces drawbacks as it needs to exchange extra messages and incurs high communication costs for node authentication and key establishment.

Huang [111] presented an efficient access control protocol incorporating elliptic curve cryptography and hash chains. This scheme performs better for lightweight nodes with limited resources. This scheme is easily implementable in a dynamic access control environment because it requires updating old secrets and broadcasting information only once after a new node is added to the network. In this scheme, the initialization, key establishment, and authentication phases are directly carried out by the authentication server. Moreover, this scheme may not support scalability for a large-scale network.

Kim and Lee [54] found out that Huang's scheme [111] cannot withstand the replay attack and masquerading attack. Huang's scheme does not support hash chain renewability efficiently. In order to address the weaknesses in Huang's scheme, Kim and Lee [112] proposed an enhanced access control protocol for VANETs. Their scheme has the following four major phases:

The initialization phase, the key establishment step, the authentication step, and the new node addition phase. Their scheme was designed to support the hash renewability phase to address weaknesses in Huang's scheme and avoid exhaustion of the hash chain for new nodes. However, the renewability of the hash chain needs to communicate messages to the base station, and in turn, it adds high communicational overheads. Similar to Huang's scheme, Kim-Lee's scheme may not be scalable to support a large-scale VANET network. Further, Shen et al. [139] show that their scheme can be vulnerable to a fatal weakness against active attacks and man-in-the-middle attacks.

Huang [79] has come out with a simple dynamic access control protocol to prevent malicious nodes from joining VANET as well as sensor networks. This scheme [79] is based on the existing Schnorr signature [136] and is used during the authentication phase. This scheme also supports perfect forward secrecy by using the expiration time for each deployed node. Therefore, once the timer is expired, the active nodes can access any data from the network. However, this scheme cannot prevent an adversary from node-capturing attacks and the deployment of fake node attacks. Further, this proposed scheme needs high storage overheads and computational costs.

3.2.1 Existing User Access Control Protocols in VANETs

In this section, we present briefly the available related user access control schemes in VANET networks.

Watro et al. [152] designed the TinyPK scheme based on the RSA algorithm, and it is a useful lightweight terminal. Wong et al. [153] presented a dynamic and light-weight scheme using hash and xor operations, though it is claimed to be cost and security-effective. Yang et al. designed an improved dynamic password-based concept [148] to overcome the possible limitation of susceptibility to reply, forgery, and stolen-verifier attacks of the scheme [152] and [70]. Das et al. proposed smartcard-based authentication scheme [51] which is an improvement over [152] and [70]. However, Khan et al.[86] noted that the scheme [51] has left a room for insider-privileged attack, and he has improved over Das et al. scheme [51] by introducing pre-shared keys with encrypted passwords.

Shih et al. proposed a 2FAS scheme [27] based on hash features to fill the gap of [148] that is unable to support mutual authentication. Yeh et al. [162] have brought out an ECC-based authentication scheme to address the security concern of password phase in [27]. However, Han et al. [73] show that scheme [162] has difficulties for forward secrecy, key agreement, and user mutual authentication. Xue et al. proposed a smartcard-based authentication scheme to provide key agreement and mutual authentication. Li et al. [98] proposed mutual authentication based on temporal credential feature to address weaknesses of [98], [150] and [159]. Both the schemes [51] and [159] based on the same model [15] and proposed for hierarchal WSNs in real-time environments may not be suitable for VANETs. He et al. [75] proposed a scheme to eliminate the impersonation attack and modification attack of [159]. However, Choi et al. [28] explain that [75] could not address user impersonation attacks and tracing attacks as expected. Choi et al. analyzed that Shi et al. [140] ECC-based scheme is not suitable for unknown key-share attacks as well as smartcard stolen attacks and present the scheme based on biometric and fuzzy extraction features to solve the limitations of and is very useful for WSNs and VANET. To resolve all security concerns discussed above, Tai et al. proposed a scheme [149] claimed to be flawless. But we have found that most of the schemes are not suitable for mutual authentication and key establishment in the VANET environment due to their inherent security limitations.

3.2.2 Key Agreement Protocols in VANETs

Recently, many researchers proposed different protocols to address various challenges in VANET and solve the general authentication process in centralized form [128]. Roya et al. [127] proposed a PKI-based scheme for message integrity and authentication check, but this scheme faces cost overhead for managing certificates [76]. To resolve issues in the PKI-based scheme, Zhang et al. proposed a public encryption scheme with an ID feature, but this scheme could not prevent modification attacks [94]. Hao et al. [74] presented a CMAP scheme with distributed key management and short group signature features for VANET. The CMAP is able to verify the trustworthiness and validity of messages. However, it cannot prevent packet loss and security attacks. For increasing location-specific services, Lu et al. [104] presented a privacy-preserving scheme for highly dynamic networks. This scheme can prevent and detect multiple registration problems with backward secrecy functionality. However, this protocol is not able to manage its members efficiently. Feng et al. [65] proposed the BPAS protocol for allowing conditional tracking and revoking malicious users. However, this protocol cannot provide proper mutual authentication because of its centralized processing. Das et al. [52] proposed a key agreement and device access control protocol based on ECC for the IOT environment. This protocol efficiently establishes session keys and supports the secure exchanging of information. However, it suffers from certificate management overhead.

3.2.3 Blockchain-based protocols in VANET

Recently, several studies have been incorporated to address security and privacy issues in VANET. However, the majority of the work could not use the full potential of blockchain to the maximum extent possible. Lu et al. [105] proposed the BPPA protocol for trusted authority (TA) to make it transparent and more verifiable by storing all transactions & certificates in blockchain. However, this protocol adds more computational overhead to process multiple certificates. Lie et al. [96] proposed a key management scheme using the decentralized feature of blockchain. Arora et al. [16] presented an authentication and data sharing scheme using blockchain technology. However, the protocol supports vehicle registration by centralized authority, and it cannot prevent single-point failure issues effectively. Leiding et al. [97] presented a smart contract-based protocol to provide fair and autonomous services in a centralized manner. Singh et al. [143] presented the IV-TP protocol using blockchain technology and an intelligent vehicle communication system, but this protocol cannot provide proper data security in VANET. Dorri et al. [56] proposed a vehicle networking system using blockchain to provide automotive security and general participation from manufacturers and service providers over blockchain. However, this scheme cannot prevent delay and failure in cases where central and cluster nodes get damaged. Zang et al. [164] proposed the BAVC protocol to address major issues faced by various blockchain-based VANET protocols. However, it does not ensure proper forward and backward secrecy functional requirements. Lin et al. [101] proposed the BCPPA protocol to minimize frequent interaction and private key revocation in a secured way. However, this scheme is unable to achieve the expected efficiency for signing and verifying users. We propose blockchain-based authentication in VANET with access control to ensure parallel computing and compliance with various known security challenges efficiently. Figure 7.1 depicts the architecture and various building blocks of the proposed scheme.

3.3 Summary

In this chapter, we have discussed an overview of recently proposed related works in the areas of VANET security. We analyze user authentication, blockchain-based access control, and lightweight protocols in VANET. However, it may be noted that most of the schemes recently proposed in the VANET field have been designed to address numerous security concerns, but very few schemes have concentrated on addressing all major attacks with efficiency and in compliance with the functional and general security requirements of VANET. Moreover, these are either vulnerable to various known attacks or incur high computational and communicational overheads.

Chapter 4

Anonymous Key Agreement Protocol

A modern city needs to include VANET and smart vehicles to be called a smart city. The internet-of-things (IoT) devices have become more sophisticated and dominant than ever, and the application potential is growing rapidly [83]. As the widespread use of software systems increases and becomes an integral part of our daily lives, the complexity of these systems increases the risks of widespread security concern [131]. A VANET is a wireless network formed by bringing smart vehicles and road-side fixed infrastructure for exchanging various information among multiple users to improve traffic congestion and make a responsible, reliable, and comfortable road journey. Each vehicle within 100 to 300m [163] can get the benefits of VANET if users are equipped with a biometric smart card with fine-grained access control. In fine-grained access, the user is allowed to access desired information with a unique privilege only. This access technique uses KP-ABE and the bilinear pairing cryptographic method using elliptic curve groups. Access rights of users can be provided by an efficient "fine-grained access control" for the utilization of various services. By doing so, users can be imposed with a set of access privileges. A set of attributes of the user forms the access policy, and the access policy is imposed by the policy enforcer.

In VANET, exposure of route profiles to unauthorized users and adversaries can cause traffic jams, robbery, kidnapping, and theft of personal information.

The VANET intensively uses cellular network technology as an important component. With an exponential increase in demand from users, the future generation will now occupy the place of 5G. 5G plays an important role in fulfilling the various mobility requirements of VANET and ITS. 5G enables VANET to connect devices in the milion/sqkm range with improved performance, incredible transmission speed (terabit), and reduced cost to serve a vast, transformative, and diverse automobile sector. The 5G-enabled VANET architecture is shown in Figure 4.2. 5G is a complete ad-hoc network that provides incredible speed in the range of terabit with no limitations to ITS. This 5G also provides virtual zero-distance connectivity among VANET users with maximized data throughput and input-output operations per second (IPOS) [85] in the ITS scenario. This cellular network (5G) has successfully addressed the major challenges that are not efficiently resolved in 4G [69] but it is still experiencing various security challenges for user authentication. To address these challenges and restrict information flow among legitimate users, in this Chapter, we propose an authentication and key agreement protocol incorporating fine-grained and biometrics features. Here, we consider mobile terminals (vehicles that dynamically change their locations), fixed road-side support units (RSUs for vehicles-to-vehicles communication), authentication server (AS) [88] and the VANET cloud as part of our network architecture. The AS allows access to information objects from the VANET cloud for the genuine user after a successful authentication process. The authentication server fetches the expected response, and then the response message gets encrypted by the valid authorizing key belonging to the query generator. The recipient user decrypts it if he or she has the authorization to access the information only. Figure 4.1 depicts the proposed architecture and various building blocks of the proposed scheme.

4.1 Anonymous Key Agreement Protocol

Most of the authentication mechanisms in VANET available in the literature limit the access of VANET services to a particular circle, mainly the vehicle owner. Moreover, thorough information sharing and the free flow of information among authorized users may result in the possession of critical information by other users who may fall prey to various kinds of threats. For making VANET support accessible to large sections of modern civilization, the proposed protocol will be very useful. This protocol grants permission to the real card owner to access the information object only after successful authentication. The authentication server fetches the expected

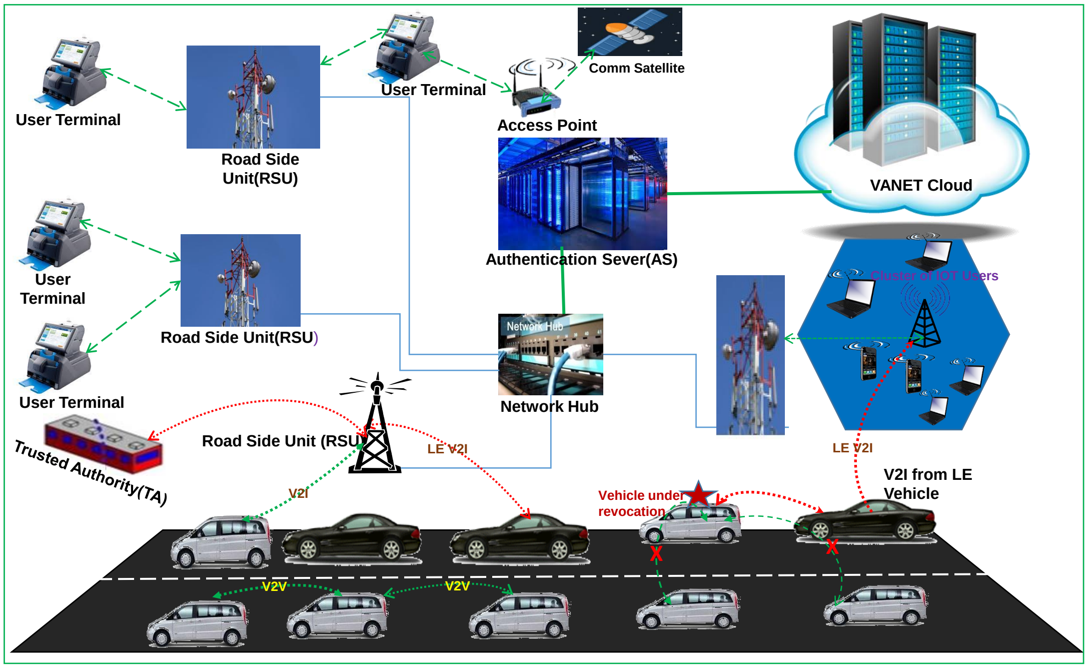

Figure 4.1: Framework/ Architecture of our proposed scheme (5G)

response, and then the response message gets encrypted by the valid authorizing key belonging to the query generator [114]. After receiving the sent response, the user can decrypt it if he or she has the authorization to access the information only.

4.1.1 Notations

In this chapter, the given notations in Table 4.1 will be used to describe our proposed protocol. One-way HA-1 [7] function for generating the hash key and AES [2], [34] have been used for encrypting and decrypting information based on symmetric key encryption and decryption processes to present our scheme.

In this proposed scheme, the user is able to access the VANET service cloud through the user terminal. A user terminal with a biometrics smart card reader gadget may be installed on vehicles, at offices or homes, or on any other mobile devices, depending on the user's choices. The user can go to any terminal to access an information object that is entitled to him or her, depending on the user's smart card. We have considered that an authentication server AS has the inbuilt functional

Table 4.1: Notations used to describe proposed scheme

Symbols	Descriptions
AS	Application server
U_i	i^{th} user
$\ominus$	Operation to discard a string from string concatenation of two or more values $(A\|\|B) \ominus B = A$
$h(\cdot)$	Secured one-way hash function
$\oplus$	Exclusive XOR operation
$A\|\|B$	String concatenation operator
$E_K(M)$	Encrypt M using key K
$D_K(M)$	Decrypt M using key K
x	AS's master secret key
P_id_i	Pseudoidentity of user U_i
r_i	Random number of 128 bits generated at the user side during registration phase
x_a	Random number of 128 bits generated at the AS side during registration phase
r_{LE}	Random number of 128 bits generated at the AS side during general authentication phase (GAP)
B_i'	Biometrics features of 1024 bits
T_{A_r}	Timestamp at the time of user registration phase at the AS side
T_l	Timestamp at the time of login at the user side
T_{LE}	Timestamp at the reception of login message at the AS side
$P_{k_{i1}}$	Keys generated by AS during registration phase for U_i
$P_{k_{i2}}$	Key generated at AS by random number generator (RNG) used for mutual authentication at general authentication phase (GAP)
P_{AS}	Key generated at the AS side during GAP
$AccP$	Access policy for fine-grained access control

capability to perform the role of legal executor (LE) who is responsible for taking any legal steps for the smooth running of the system, along with other trusted authorities (TA) or LE. AS also handles the user revocation procedure with the help of TA or LE. This Chapter also describes how the proposed protocol works to receive information objects from the VANET cloud using a biometric smart card of the user. It consists of four following major phases. A flow chart is shown in Figure 4.3.

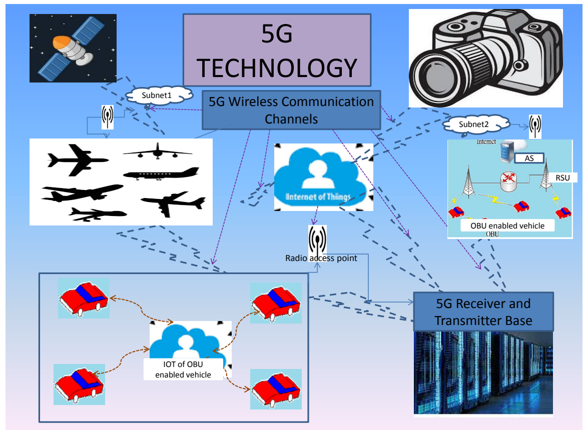

Figure 4.2: 5G-enabled VANET architecture.

4.1.2 Registration Phase

In this phase, the authentication server AS prepares a smart card for each legal user P_id_i and hands over his or her card after the successful registration phase. It is assumed that all the transactions between P_id_i and AS are transmitted through defined secured channels only. The below-mentioned operations are performed by both P_id_i and AS parties to be successfully registered with AS:

- **Step 1:** First user P_id_i selects his or her identity id_i, password pw_i, personal biometrics features B_i' and a 128 bit random number r_i.

- **Step 2:** For calculating biometrics key, the proposed protocol uses a fuzzy extractor [55], which is a nearly uniformly distributed random probabilistic generation function $G(\cdot)$. This fuzzy extractor addresses both error tolerance and non-uniformity. In a reliable way, this generates R randomly by extracting out of the given biometrics B_i' and it has a size of r bits. R can be termed as biometrics key of P_id_i and denoted as $R \in \{0,1\}^r$. A secure sketch function $G_s(\cdot)$ [6] along with a fuzzy extractor are defined to reproduce biometric keys. Fuzzy extractor also generates P as output from the given biometrics B_i'(near to original biometrics). It may be noted that R is maintained to be uniformly random for stated P. The nearness between B_i' and original biometrics is calculated as hamming distance $h_m^b(B_i', BioOri_i) \leq h_m$, where h_m is a threshold value acceptable as error tolerance. The $G_s(\cdot)$ function is used to reproduce the biometrics key for P_id_i by incorporating two inputs B_i' and

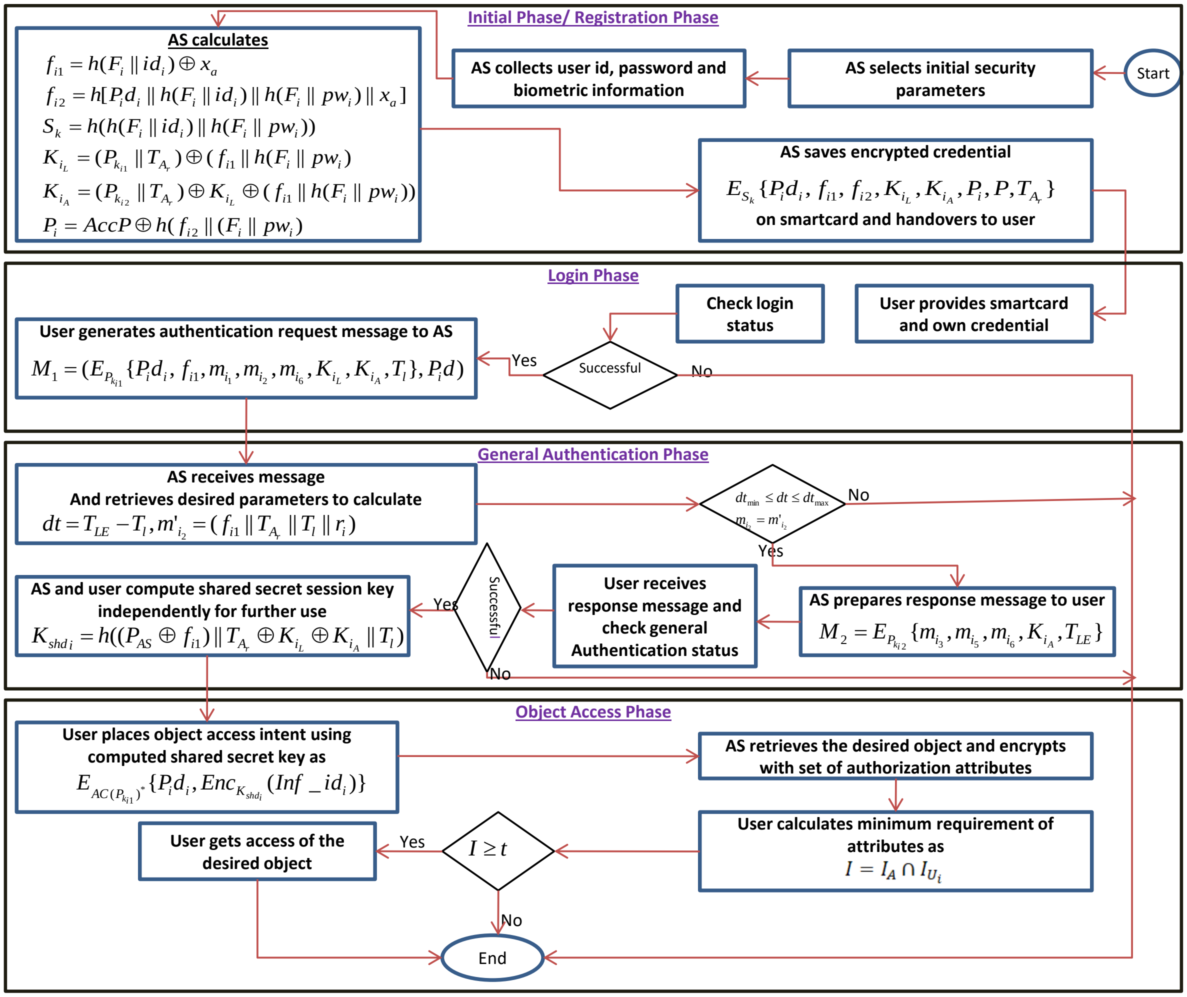

Figure 4.3: Flowchart of the proposed scheme.

P i.e. $F_i = G_s(B_i', P)$ whereas per stated definition $F_i = R$;

- **Step 3:** In this step, the user's computed values, i.e., $id_i, h(F_i||id_i), h(F_i||pw_i)$ are sent to the AS via secured channels.

- **Step 4:** After reception of $\{id_i, h(F_i||id_i), h(F_i||pw_i)\}$, AS first checks the revocation flag status of the user, and based on false status, it subsequently generates a 128-bit random number x_a, assigns pseudoidentity P_id_i to the user U_i and computes $S_k = h(h(F_i||id_i)||h(F_i||pw_i))$ and $f_{i1} = h(F_i||id_i) \oplus x_a$

- **Step 5:** Then calculates
$f_{i2} = h[P_id_i||h(F_i||id_i)||h(F_i||pw_i)||x_a]$,

- **Step 6:** AS acquires the current time stamp T_{A_r} and generates two keys $P_{k_{i1}}$ and $P_{k_{i2}}$, for the user P_id_i, each of length 160 bits, and computes $K_{i_L} = (P_{k_{i1}}||T_{A_r}) \oplus (f_{i1}||h(F_i||pw_i))$,
  $K_{i_A} = (P_{k_{i2}}||T_{A_r}) \oplus K_{i_L} \oplus (f_{i1}||h(F_i||pw_i))$,

- **Step 7:** $P_i = AccP \oplus h(f_{i2}||h(F_i||pw_i))$, where access policy belongs to anti-terrorist-squadron (ATS) before login can defined as *((Traffic Controller OR Traffic Inspector) AND (Rank Supervisor)) AND (Service Experience > 5Yrs) AND [t-out-of-n]{Driving, CCTV, Camera, GunShoot}*. However, after successful login K_{shd_i} is added as an extra component with the access policy.

- **Step 8:** Authentication server AS then saves encrypted credential $E_{S_k}\{P_id_i, f_{i1}, f_{i2}, K_{i_L}, K_{i_A}, P_i, P, T_{A_r}\}$ on the smart card belongs to user P_id_i and hands over to the user that registered with. AS stores $\{P_id_i, (P_id_i||P_{k_{i1}}) \oplus h(x), (P_id_i|| P_{k_{i2}}) \oplus h(x)\}$ the values specific to the user P_id_i in its database. The summarized registration phase is shown in Table 4.2.

4.1.3 Login Phase

For accessing VANET support through AS, P_id_i has to complete this process at its own terminal. P_id_i needs to execute the below given operations for successful login.

- **Step 1:** P_id_i places smart card and provides self-identity id_i, password pw_i along with biometrics information B_i'. Using secure sketch function $G_s(\cdot)$, F_i is retrieved as $F_i = G_s(B_i', P)$. With the help of the smart card SC and own credential user first computes $S_k = h(h(F_i||id_i)||h(F_i||pw_i))$ and then decrypts the information stored in the smart card. Retrieves x_a as follows.
  $x_a = f_{i1} \oplus h(F_i||id_i)$.
  Then smart card SC computes $f_{i2}' = h(h(F_i||id_i)||h(F_i||pw_i)||x_a)$, and checks if stored $f_{i2} \stackrel{?}{=} f_{i2}'$ matches or not. The first mismatch leads to prompt rejection of this process. Else, it is validated and ensured that the provided credential with biometrics input are right.

- **Step 2:** After success in first step, P_id_i picks up a number r_i randomly and prepares the given below two information
  $m_{i_1} = (f_{i1}||h(F_i||pw_i)) \oplus r_i$

Table 4.2: Registration phase of user with authentication server

User U_i	Authentication server AS
Input id_i, pw_i, B_i' and r_i	
User Computes	
$F_i = G_s(B_i', P)$	
$id_i, h(F_i\|\|id_i), h(F_i\|\|pw_i)$	
User Sends	
$\langle \text{id}_i, h(F_i\|\|id_i), h(F_i\|\|pw_i) \rangle$ to AS	
$\xrightarrow[\textbf{(secure channel)}]{\langle \text{id}_i, h(F_i\|\|id_i), h(F_i\|\|pw_i)\rangle}$	AS performs the following computation
	$S_k = h(h(F_i\|\|id_i)\|\|h(F_i\|\|pw_i))$
	$f_{i1} = h(F_i\|\|id_i) \oplus x_a$
	$f_{i2} = h(h(F_i\|\|id_i)\|\|h(F_i\|\|pw_i)\|\|x_a)$
	$K_{i_L} = (P_{k_{i1}}\|\|T_{A_r}) \oplus (f_{i1}\|\|h(F_i\|\|pw_i))$
	$K_{i_A} = (P_{k_{i2}}\|\|T_{A_r}) \oplus K_{i_L} \oplus (f_{i1}\|\|h(F_i\|\|pw_i))$
	$P_i = AccP \oplus h(f_{i1}\|\|h(F_i\|\|pw_i))$
	AS saves the information on smart card encrypted by S_k, $E_{S_k}\{f_{i1}, f_{i2}, K_{i_L}, K_{i_A}, P_i, P, T_{A_r}\}$
	AS stores for future computation $\{P_id_i, (P_id_i\|\|P_{k_{i1}}) \oplus h(x)$ and $(P_id_i\|\|P_{k_{i2}}) \oplus h(x)\}$ values specific to user U_i
	AS issues smart card to the user containing
	$\xleftarrow[\textbf{(secure channel)}]{E_{S_k}\{\text{f}_{i1}, f_{i2}, K_{i_L}, K_{i_A}, P_i, P, T_{A_r}\}}$
User receives smart card with secret credential	

$m_{i_2} = (f_{i1}||T_{A_r}||T_l||r_i)$

- **Step 3:** In this step, user first retrieves $P_{k_{i1}}$ to encrypt the message M_1 as follows
  $v_{p_{i1}} = P_{k_{i1}}||T_{A_r} = K_{i_L} \oplus (f_{i1}||h(F_i||pw_i))$
  $P_{k_{i1}} = v_{p_{i1}} \ominus T_{A_r}$
  and then finally sends authentication request message encrypted under $P_{k_{i1}}$ to the AS: $M_1 = (E_{P_{k_{i1}}}\{P_id_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_id_i)$ over normal (public) channels.

4.1.4 General Authentication Phase

Authentication server starts this phase by retrieving the $M_1 = (E_{P_{k_{i1}}}\{P_id_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_id_i)$ and then authenticates the user. Through successful authentication, a secret session key is settled between them for further secured communication. The AS uses the received pseudo-identity P_id_i of U_i to retrieve $P_{k_{i1}}, P_{k_{i2}}$ and T_{A_r} specific to user P_id_i.

- **Step 1:** After reception of message M_1 from P_id_i, AS calculates $dt = T_{LE} - T_l$ and Checks if $dt_{min} <= dt <= dt_{max}$. If it is found that the timestamp is within the valid limit then AS generates a reply.

- **Step 2:** Then r_i is retrieved by the authentication server as $v = (P_{k_{i1}} || T_{A_r}) \oplus K_{i_L}$ and $r_i = m_{i_1} \oplus v$.

- **Step 3:** Then calculates $(f_{i1} || T_{A_r} || T_l || r_i)$ and compares equality with m_{i_2}. Thus the equality validates truthfulness of user P_id_i. Otherwise, authentication process gets terminated by the AS.

- **Step 4:** In this step, AS generates a 160 bits key P_{AS} and embeds into m_{i_6} to mark a successful GAP phase and reuse the shared-secret key for a particular session to avoid repetitive general authentication phase and calculates the followings,
  $m_{i_3} = v \oplus r_{LE}$
  $m'_{i_5} = (P_{k_{i1}} || T_{A_r} || r_i || r_{LE} || T_{LE} || K_{i_A})$, $m_{i_5} = h(m'_{i_5})$
  $m_{i_6} = m'_{i_5} || (P_{AS} \oplus f_{i_1}) || T_{A_r}$.

- **Step 5:** AS at this step, forwards authentication answer message encrypted under $P_{k_{i2}}$ to P_id_i: $M_2 = E_{P_{k_{i2}}}\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}$ via a public channel.

- **Step 6:** First, P_id_i retrieves $P_{k_{i2}}$ to decrypt the received M_2 as follows $v_{p_{i2}} = K_{i_A} \oplus K_{i_L} = (P_{k_{i2}} || T_{A_r})$
  $P_{k_{i2}} = v_{p_{i2}} \ominus T_{A_r}$. Then user U_i retrieves the random number r_{LE} as $r_{LE} = m_{i_3} \oplus (f_{i1} || h(F_i || pw_i))$.

- **Step 7:** Then user P_id_i calculates based on his smart card information, $m''_{i_5} = (P_{k_{i1}} || T_{A_r} || r_i || r_{LE} || T_{LE} || K_{i_A})$ and $h(m''_{i_5})$ verifies its equality with m_{i_5}. The equality authenticates that the received message is generated by the AS and in turn, the AS gets authenticated by P_id_i.

- **Step 8:** Then P_id_i extracts P_{AS} from f_{i1} and m''_{i_5} as:
  $v_{pi3} = m_{i_6} \ominus m''_{i_5} \ominus T_{A_r} = (P_{AS} \oplus f_{i_1})$
  $P_{AS} = v_{pi3} \oplus f_{i_1}$.

- **Step 9:** P_id_i then computes one common shared secret key $K_{shd_i} = h((P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_l)$ and saves as one of the vital components of authorization attributes set for a defined session to mark a sign of successful general authentication process.

- **Step 10:** AS also computes shared common secret key K_{shd_i} from own side. The same common session key is agreed by user P_id_i for all future service request/ information object access from the VANET cloud via the server AS and AS uses it for decrypting the service request from user P_id_i.

4.1.5 Information Object Access Phase

Once the user P_id_i successfully completes the general authentication phase, the information object phase is initiated by the respective user at its own side.

- **Step I.** User P_id_i sends information object Inf_id_i access request as $E_{AC(P_{k_{i1}})^\star}$ $\{P_id_i, Enc_{K_{shd_i}}(Inf\_id_i)\}$ encrypted under $E_{P'_{k_1}}$ and the information object Inf_id_i encrypted by session key K_{shd_i} using AES encryption technique. Where, $(P_{k_{i1}})^\star = (P_{k_{i1}}||K_{shd_i})$

- **Step II.** AS fetches K_{shd_i} using P_id_i information and decrypts desired object Inf_id_i id applying the fetched shared secret key K_{shd_i}.

- **Step III.** The AS retrieves Inf_id_i from VANET cloud as $InfDetails\_id_i$ and encrypted with a set of authorization attributes where K_{shd_i} is treated as a special component of the authorization attributes set.

  Encryption at the AS side:

  Let U is a universal set of attributes of AS and $A = |U|$ for each attribute, $i \in \{1, 2, 3, ..., A\}$ randomly secure way user details and authorization object details are mapped e.g. details of user U_i engine number and chassis number and shared secret key K_{shd_i} securely mapped as t_1, t_2, t_3 respectively. y is chosen randomly from Z. So, the following public parameters available at AS

for general authentication and encrypting information object: $P_K = (T_1 = g^{t_1}, T_2 = g^{t_2}, ...T_A = g^{t_A}, Y = e(g,g)^y)$ And the secret key is distributed as an access policy saved on the user's respective smart card.

Let I_A and I_{user_i} be a set of attributes of AS used to encrypt $InfDetails\_id_i$ and the user trying to access $InfDetails\_id_i$ from VANET cloud respectively. Key generation policy chooses a polynomial of degree t, P_x at random such that $P_x(0) = y$. For an attribute a_{U_i}, $UK_a = g^{P_x(i)/t_a}$

- **Step IV.** Decryption by the user P_id_i: AS responses for the information object to the user as $E_{(P_{k_{i2}})^\star}\{I_A, InfDetails\_id_iY^r, \{T_j^r\}, j \in I_A\}$, where $r \in Z$ is chosen randomly by the AS and $(P_{k_{i2}})^\star = (P_{k_{i2}}||K_{shd_i})$. The decryption process is initiated by the user. User checks $|I_A \cap I_{U_i}| > t$, where t is the degree of random polynomial denoted by Px. t is decided by key the distribution centre . If the condition returns true, then $P_x(0)$ is obtained by Lagrange's interpolation. So the user can get Y^r, and finally $InfDetails\_id_i$ is retrieved. Minimum requirements for attributes and parameters are defined as the access policy of user and are saved on the user's smart card. The access policy of the user is depicted as an access tree in Figure 4.4.

  A summarized login, authentication, key establishment and object access phases is briely presented in Table 4.3.

4.1.6 An Example of Information Object Access Phase

Tracking information objects of any vehicle at any time by a user designated as anti-terrorist squadron (ATS) may be defined as an access tree as shown in Figure 4.4 which is saved on the smart card as a general logic expression. The access policy [66] of ATS is expressed as follows:

K_t *AND ((TrafficController OR TrafficInspector) AND (RankSupervisor)) AND (ServiceExperience > 5Yrs AND (⟨t-out-of-n⟩ {Driving, CCTV, Camera, GunShoot})* where $K_t = K_{shd_i}$ at session t. In Figure 4.4, $T_A(I_A) = true$ i.e., the user access policy accepts I_A ; so, $InfDetails\_id_i$ can be retrieved by the user P_id_i.

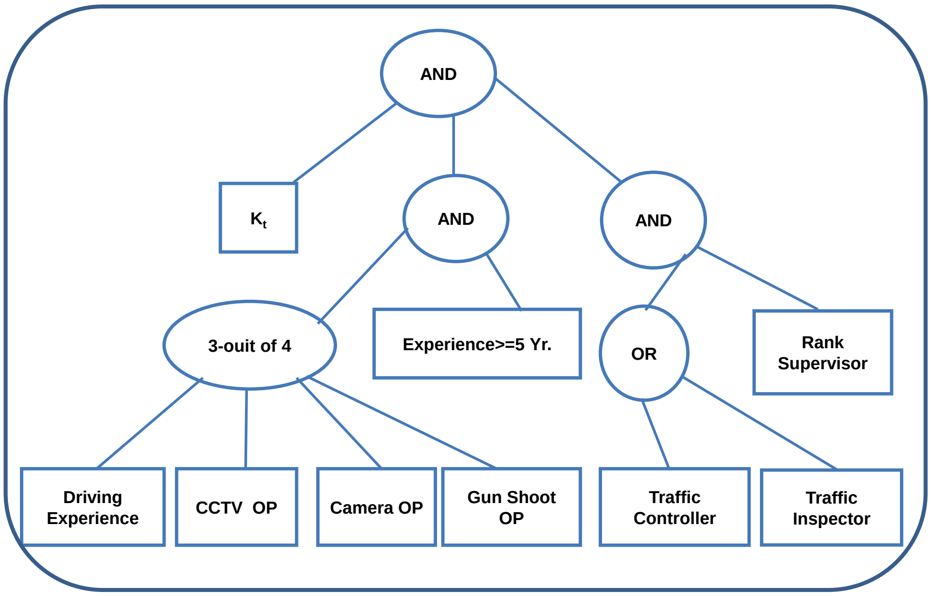

Figure 4.4: Access tree T_A for ATS user.

Password and Biometrics Update Phase

Here, the following operations should be executed through the secure channel if a user desires to update his password along with biometric components:

- **Step 1:** The user needs to insert his or her SC and provide his or her identity id_i, password pw_i and biometrics B_i'. The secured sketch function $G_s(\cdot)$ is used to retrieve F_i. With the provided information SC and own credentials, the user first computes $S_k = h(h(F_i||id_i)||h(F_i||pw_i))$ and then decrypts the information saved on SC. Retrieves x_a as follows.
  $x_a = f_{i1} \oplus h(F_i||id_i)$.
  Then smart card SC computes $f_{i2}' = h(h(F_i||id_i)||h(F_i||pw_i)||x_a)$, and checks if stored $f_{i2} \stackrel{?}{=} f_{i2}'$ matches or not. A mismatch causes prompt rejection of the password and biometrics update phase. A match ensures the genuineness of the user and smart card holder. Then AS indicates acceptance of the user request to update the credential with the given password and biometrics via secured channels if the revocation flag is false.

Table 4.3: Summarized login, authentication, key establishment and object access phases

User U_i	Authentication Server AS
Insert smart card and input id_i, pw_i , B'_i Retrieves F_i and x_a as follows: $F_i = G_s(B'_i, P)$ $x_a = f_{i1} \oplus h(F_i \Vert id_i)$ To decrypt smart card information, calculates $S_k = h(h(F_i \Vert id_i) \Vert h(F_i \Vert pw_i))$ At user terminal smart card SC computes $f'_{i2} = h(h(F_i \Vert id_i) \Vert h(F_i \Vert pw_i) \Vert x_a)$ Checks match holds or not (i) $f_{i2} \stackrel{?}{=} f'_{i2}$ An inequality leads to prompt rejection at login phase On successful match $P_i d_i$ chooses random no r_i and calculates the followings: (i) $m_{i_1} = (f_{i1} \Vert h(F_i \Vert pw_i)) \oplus r_i$ (ii) $m_{i_2} = (f_{i1} \Vert T_{A_r} \Vert T_l \Vert r_i)$ (iii) $v_{p_{i1}} = P_{k_{i1}} \Vert T_{A_r} = K_{i_L} \oplus (f_{i1} \Vert h(F_i \Vert pw_i))$ (iv) $P_{k_{i1}} = v_{p_{i1}} \ominus T_{A_r}$ (v) U_i sends an authentication request to the AS $\xrightarrow{\langle \mathrm{M}_1 = (E_{P_{k_{i1}}}\{P_i d_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_i d_i) \rangle}$ **(Public channel)**	
	Receive message $\{M_1\}$ (i) AS calculates $dt = T_{LE} - T_l$ Checks if $dt_{min} <= dt <= dt_{max}$ On validity, AS prepares M_2 (ii) $v = (P_{k_1} \Vert T_{A_r}) \oplus K_{i_L}$ and retrieves r_i as $r_i = m_{i_1} \oplus v$ (iii) $m'_{i_2} = (f_{i1} \Vert T_{A_r} \Vert T_l \Vert r_i)$ Checks for match m_{i_2} and m'_{i_2} and on matched AS further calculates (iv) $m_{i_3} = v \oplus r_{LE}$ (v) $m'_{i_5} = (P_{k_{i1}} \Vert T_{A_r} \Vert r_i \Vert r_{LE} \Vert T_{LE} \Vert K_{i_A})$, $m_{i_5} = h(m'_{i_5})$ (vi) $m_{i_6} = m_{i_5} \Vert (P_{AS} \oplus f_{i_1}) \Vert T_{A_r}$ $\xleftarrow{\langle \mathrm{M}_2 = E_{P_{k_{i2}}}\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\} \rangle}$ **(Public channel)**
Receives message $\{M_2\}$ (i)$P_i d_i$ retrives $P_{k_{i2}}$ to decrypt the received M_2 as: $v_{p_{i2}} = K_{i_A} \oplus K_{i_L} = (P_{k_{i2}} \Vert T_{A_r})$ $P_{k_{i2}} = v_{p_{i2}} \ominus T_{A_r}$ (ii) Retrieves r_{LE} as $r_{LE} = m_{i_3} \oplus (f_{i1} \Vert h(F_i \Vert pw_i))$ (iii) From smart card information, the user calculates, $m''_{i_5} = (P_{k_{i1}} \Vert T_{A_r} \Vert r_i \Vert r_{LE} \Vert T_{LE} \Vert K_{i_A})$ and $h(m''_{i_5})$ and verifies equality with m_{i_5} (iv)Retrieves P_{AS} using f_{i1} and m''_{i_5} as: $v_{p_{i3}} = m_{i_6} \ominus m''_{i_5} \ominus T_{A_r} = (P_{AS} \oplus f_{i_1})$ $P_{AS} = v_{p_{i3}} \oplus f_{i_1}$ (v) Computes shared secret key $K_{shd_i} = h((P_{AS} \oplus f_{i_1}) \Vert T_{A_r} \Vert K_{i_L} \Vert K_{i_A} \Vert T_l)$	AS computes shared secret key K_{shd_i} independently at own side
Information object access by user After successful general authentication $P_i d_i$ sends information object Inf_id_i access request as $\xrightarrow{\langle \mathrm{E}_{AC(P_{k_{i1}})^\star}\{P_i d_i,\ Enc_{K_{shd_i}}(Inf\_id_i)\} \rangle}$ **(Public channel)**	Receive message access request (i) AS fetches K_{shd_i} using $P_i d_i$ information (ii) Decrypts information object Inf_id_i (iii) Retrieves Inf_id_i from VANET cloud as $InfDetails\_id_i$ (iv) Encrypts with a set authorization attributes where K_{shd_i} special component of authorization attributes set Server sends user object details as $\xleftarrow{\langle \mathrm{E}_{(P_{k_{i2}})^\star}\{I_A, InfDetails\_id_i Y^r, \{T_j^r\}, j \in I_A\} \rangle}$ **(Public channel)**
Checks $\lvert I_A \cap I_{U_i} \rvert > t$, where t is degree of random polynomial denoted by Px On validity of check,(i) $P_x(0)$ is obtained by Lagrange's interpolation (ii) User gets Y^r (iii) Using Y^r, $InfDetails\_id_i$ retrieved	

- **Step 2:** The authentication server repeats steps three to eight mentioned in the user's registration process to update the necessary components in the database. Parallelly, required components calculated by smartcard are replaced on the user's SC at terminal side.

4.1.7 Password Update Phase

The following operations should be executed at the user's terminal in a secure environment if the user desires to update the password component.

- **Step 1:** The user needs to insert his or her SC and provide his or her identity id_i, password pw_i and biometrics B_i'. The secured sketch function $G_s(.)$ is used to retrieve F_i. With the provided information SC and own credentials, the user first computes $S_k = h(h(F_i||id_i)||h(F_i||pw_i))$ and then decrypts the information saved on SC. Retrieves x_a as follows.
  $x_a = f_{i1} \oplus h(F_i||id_i)$.
  Then smart card SC computes $f_{i2}' = h(h(F_i||id_i)||h(F_i||pw_i)||x_a)$, and checks if stored $f_{i2} \stackrel{?}{=} f_{i2}'$ matches or not. A mismatch causes prompt rejection of the password update phase. A match ensures the genuineness of user and smart card holder. Then AS check revocation flag and finally indicates acceptance of the user request to update the old password with a new password.

- **Step 2:** The authentication server repeats steps three to eight mentioned in the user's registration process to update the necessary components in the database. Parallelly, required components calculated by smart card are replaced on the user's SC at terminal side.

4.1.8 User Revocation Phase

There may be misbehaving and malicious users who report wrong and invalid information. They also do not follow the norms and regulations of VANET laid down by trusted authorities (TA) or law executors (LE). Therefore, in this undesirable scenario, the user needs to be revoked to preserve and protect the interests of VANET. The proposed scheme provides provision for user revocation in a privacy-preserving way. Based on the TA or the LE's input, the AS initiates the revocation process for user U_i. AS retrieves the desired information of user U_i from the database and marks the revocation flag true against the user. AS also updates the revocation list accordingly.

4.1.9 New User Joining Phase

The same phases are applied to a new user U_{i-new} like U_i for joining and participating in VANET. The authentication server AS needs to register and issue a fresh smart card by executing the registration process. After a successful registration process, the new user has to complete the key establishment phase through a successful log-in and the general authentication phase mentioned in sections 4.1.3 and 4.1.4 respectively. Subsequently, the new user U_{i-new} can fully participate in accessing VANET services.

4.2 Security Analysis of Proposed Scheme

The primary goal of the credential scheme is to maintain the user's privacy reliably by supporting its users to mask identifying personal attributes in transactions over a network. The sharing of information with unregistered personnel to get access to the services in any way is known as credential lending, sharing, or transfer [121]. This proposed protocol is compliant with the non-transferability of credential features. The considered set of attributes (A) are A1 (Circumvention depends on), A2 (Circumvention by), A3 (Universality depends on), A4 (Credential cloning), A5 (Unintended sharing), and A6 (VANET system value). Functional relations among attributes, non-transferability, and transferability are shown in Table 4.4.

4.2.1 Formal Security Proof by ROR Model

The formal security analysis of the proposed protocol, say V for VANET, is carried out by the widely accepted ROR model [106], [112], [72]. The ROR provides a provision to simulate real attack by an adversary $\mathcal{A}$ through which the adversary capabilities in a real attack are captured [19], [141]. Table 4.1 and Table 4.6 contain the description of the various symbols for queries and notations that are used for the semantic security proof. The adversary $\mathcal{A}$ acts to be an active participant either P_id_i or Authentication Server AS at t^{th} instance with V. We have considered all probable queries for proving formal security concerns.

Table 4.4: Comparison of credentials attributes w.r.t. transferability and non-transferability

A	Non-Transferability	Transferability
A1	Full secrecy	Accessing control open
A2	No associates	Closed associates
A3	Secrecy for all environments	Secrecy for environments
A4	Harder	Easier
A5	Impossible	Highly possible to happen
A6	Value improved	Less value addition

Definition 4.1. *The advantage function of an adversary $\mathcal{A}$ in breaking the semantic security of the proposed protocol (VANET) scheme V by guessing the correct bit b' is given by $Adv_V^{VANET} = |2Pr[b = b'] - 1|$.*

Definition 4.2. *A biometrics-based authentication protocol with a password is semantically secure if the advantage function Adv_V^{VANET} is negligibly greater than $\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\}$, where q_s, $|\mathcal{D}|$, l_b and ε_{bm} carry the same meaning as per table 4.6.*

Theorem 4.1. *If we assume that the adversary $\mathcal{A}$ runs with the complexity of a polynomial algorithm $t_{\mathcal{A}}$. The adversary executes H, S and E with maximum time complexity q_H, q_s and q_e respectively to be capable to crack the defined semantic security of the proposed protocol V. As per the definition we have,*

$$\begin{aligned} Adv_V^{VANET} &\leq \frac{q_H^2 + 28q_H}{2^{l_H}} + \frac{(q_s + q_e)^2 + 10q_s}{2^{l_r}} \\ &\quad +2\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned}$$

where q_s, q_H, l_H, l_r, $|\mathcal{D}|$, l_b and ε_{bm} carry the same meaning as per Table 4.6.

Proof. The proof can be derived by a set of five independent games and these are defined as G_{mi}, $(i = 0, 1, 2, 3, 4)$. We follow similar steps like [134], [129] to prove the theorem. In the G_{m_i}, the adversary $\mathcal{A}$ tries to guess the correct random numbers r_i through the $Test$ query. The event of occurrence is defined as S_i and the associated probability of the occurrence is written as $P_r[S_i]$.

Table 4.5: Various ROR queries with their description

Query	Description for Interpreting Query Action
Send(V, p) (S)	It allows $\mathcal{A}$ to share a plea message p to $\mathcal{V}^t$. In response, $\mathcal{V}^t$ answers to $\mathcal{A}$ as per protocol.
Execute(P_id_i, S) (E)	This makes $\mathcal{A}$ capable to listen message p transmitted among P_id_i and AS in a real operation of the scheme.
Corrupt(P_id_i, a) (C)	According to correctness of a, it helps to obtain user's credential saved in SC to mention adversary $\mathcal{A}$.
Reveal($\mathcal{V}^t$) (R)	It enables to disclose shared key K_{shd_i} generated between P_id_i and AS.
Test($\mathcal{V}^t$) (T)	By this query $\mathcal{A}$ sends a proposal to $\mathcal{V}^t$ for the present common session key K_{shd_i} and $\mathcal{V}^t$ answers probabilistically as a result of unbiased flipped coin b.

Game G_0: The first game G_{m_0} is assessed and evaluated under ideal conditions as per ROR model and definition 1. So we have,

$$Adv_V^{VANET} = |2Pr[S_0] - 1|. \tag{4.1}$$

Game G_1: In this game, the ROR queries i.e. $Send$ and $Execute$ are simulated for the proposed protocol. Table 4.7 describes the simulation of $Send$ and $Execute$ queries. In this game, the list L_H, L_A, and L_T are also considered. Under the execution of real protocol and ideal conditions, simulation of the games G_1 and G_0 are indistinguishable from each other, so, we have,

$$Pr[S_1] = Pr[S_0]. \tag{4.2}$$

Game G_2: Here, we have considered the total collision probability due to superimposition of the hash function and random key over the transmitted traffic between P_id_i and AS. As per birthday paradox theory, the at most collision probability of H given by query has $\frac{q_H^2}{2^{l_H+1}}$. Then we have,

$$|Pr[S_2] - Pr[S_1]| \leq \frac{(q_s + q_e)^2}{2^{l_r+1}} + \frac{q_H^2}{2^{l_H+1}}. \tag{4.3}$$

Table 4.6: Symbols of ROR model description

Symbols	Description and Meaning of Symbols
q_H	Total number of hash H oracle execution
q_s	Total number of *Send* query executed
q_e	Total number of *Execute* oracle query executed
l_H	Length of the hashed output string
l_r	Length of the string of random number
l_b	Length of string of user biometric key
ε_{bm}	Measure probability of false positive in biometrics [32]
$\lvert\mathcal{D}\rvert$	Size of password dictionary
L_H	Storage for output of hash H oracle query
L_A	Storage for random oracle output
L_T	Storage for message transcripts between P_id_i and AS

Table 4.7: Execution and simulation of various oracle queries

Simulation of *Hash* H for the following query operations: The availability of information about (q, H) in L_H list related to $H(q)$, is returned as hash function H. If not available, then a string $H \in \{0,1\}^{l_H}$ is selected and added (q, H) with L_H. In case availability is made by $\mathcal{A}$, (q, H) then it is added with $L_{\mathcal{A}}$ list.
Simulation of *Reveal*($\mathcal{V}^t$) query is captured as following: In case, $\mathcal{V}^t$ is implied to be in *accept*, then present common session key K_{shd_i} is generated by $\mathcal{V}^t$ and the same is returned to partner.
Test($\mathcal{V}^t$) simulation is noted as following: By *Reveal*($\mathcal{P}^t$) execution, present session key K_{shd_i} is obtained along with the flipping result b of unbiased coin. K_{shd_i} is returned if flipping results $b = 1$. In other case, returns a randomly formed string out of $\{0,1\}^*$.
Corrupt(P_id_i,*a*) simulation is noted as following: Incase, the value a resulted as 1, the query answers password (PW_i) of P_id_i. For $a = 2$, this returns biometrics key (F_i) corresponding to the biometrics B_i' of P_id_i. Incase, the value a resulted as 3, then secured information SC is returned stored in user smart card.
Execute(P_id_i, S) query simulation is performed as a successive manner by simulating *Send* query and performs all the operations required for general authentication.

Game G_3: With the assumption that H queries are accounted previous (G_2) calculation, so, it is necessary to evaluate collision probability for other left over queries. Here, we have considered the total collision probability due to superimposition of the hash function and random key already recorded with the transmitted at SC generation, SC revocation, at login time, password and biometrics change phases are considered. So, we have,

Case 1: For registration-cum-smart card generation, we have the total calculated probability is at most $(\frac{5q_H}{2^{l_H}} + \frac{q_s}{2^{l_r}})$.

Case 2: During login and GAP phases, we have total probability is at most $(\frac{6q_H}{2^{l_H}} + \frac{2q_s}{2^{l_r}})$.

Case 3: Similarly, for biometrics and password change phases contribute the total probability is at most $(\frac{3q_H}{2^{l_H}} + \frac{2q_s}{2^{l_r}})$.

Considering all the four cases, we have,

$$|Pr[S_3] - Pr[S_2]| \leq \frac{14q_H}{2^{l_H}} + \frac{5q_s}{2^{l_r}}. \tag{4.4}$$

Game G_4: In game G_4, the adversary $\mathcal{A}$ tries to reveal or disclose user's private credential. As details given [134], [129], guessing of password and biometrics has a maximum probability upto $\frac{q_s}{2^{|D|}}$ and $\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\}$ respectively. Since, games G_3 and G_4 are identical when there is an absence of guessing attack, so we have,

$$|Pr[S_4] - Pr[S_3]| \leq \max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \tag{4.5}$$

After executing all games, $\mathcal{A}$ is left with $Pr[S_4]$ probability in guessing the correct bit b. So, we have clearly,

$$Pr[S_4] = 1/2 \tag{4.6}$$

Applying the triangular inequality law, we have the following:

$$\begin{aligned} |Pr[S_0] - \frac{1}{2}| &= |Pr[S_1] - Pr[S_4]| \\ &\leq |Pr[S_1] - Pr[S_2]| + |Pr[S_2] - Pr[S_4]| \\ &\leq |Pr[S_1] - Pr[S_2]| + |Pr[S_2] - Pr[S_3]| \\ &\quad + |Pr[S_3] - Pr[S_4]| \end{aligned} \tag{4.7}$$

From Equations (4.1)-(4.7), we obtain,

$$\begin{aligned} \frac{1}{2} Adv_V^{VANET} &= |Pr[S_0] - \frac{1}{2}| \\ &\leq \frac{(q_s+q_e)^2}{2^{l_r+1}} + \frac{q_H^2}{2^{l_H+1}} + \frac{5q_s}{2^{l_r}} + \frac{14q_H}{2^{l_H}} \\ &\quad + \max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned} \tag{4.8}$$

We can obtain the following if each side of Equation (4.8) is multiplied by 2 and rearranged the expression,

$$\begin{aligned} Adv_V^{VANET} &\leq \frac{q_H^2 + 28q_H}{2^{l_H}} + \frac{(q_s+q_e)^2 + 10q_s}{2^{l_r}} \\ &\quad + 2\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned} \tag{4.9}$$

Hence, the theorem is proved. □

Table 4.8: Computation cost comparison

Phase	At	TEAM [110]	E2TEAM [130]	Ours
Smart card	AS	-	-	7h(.) + 7⊕
Registration	User	-	3h(.) + 7⊕	-
	OBU_i/UT	-	1h(.) + 1⊕	-
	AS	3h(.) + 2⊕	3h(.) + 3⊕	-
Login	OBU_i/UT	1h(.) + 1⊕	2h(.) + 1⊕	4h(.)+ 4⊕
GAS	OBU_i/UT	8h(.) + 5⊕	3h(.) + 4⊕	2h(.)+9⊕
	LE_i	8h(.) + 7⊕	7h(.) + 6⊕	-
Key Update	OBU_i/UT	6h(.) + 5⊕	4h(.) + 4⊕	-
	LE_i	5h(.) + 6⊕	4h(.) + 4⊕	-
SC update	OBU_i/UT	2h(.) + 3⊕	4h(.) + 3	9h(.) + 6⊕

4.2.2 Informal Security Proof

Most of the known security concerns are addressed by the ROR and AVISPA simulation tools. However, for a lightweight scheme, perfect forward secrecy (PPF) and key-compromised impersonation (K-CI) attacks are very crucial, and the proposed protocol should effectively withstand them. So in this section, we assess how our scheme is able to resist PPF and KCI threats.

Perfect Forward Secrecy (PPF)

PPF ensures that the leakage of current session keys at session k of one or several parties cannot affect the secrecy or acquire the session keys established by genuine parties at session $k-1$. A scheme can be resilient against PPF if it is sound and at least one component of the key or key itself is hashed by one-way secure has function [161]. In the proposed scheme, the common shared secret key K_{shd_i} is calculated as $K_{shd_i} = h((P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_l)$ independently at its own side by AS and P_id_i. The components P_{AS} and T_l get updated at each login, followed by general authentication. So, using the same theorem for soundness presented in [161], the proposed scheme is considered as sound.

Therefore, the soundness ensures that the shared secret is updated at least once for each session (Step 4 of the general authentication phase and Step 3 of the login phase), and the incorporation of a collision-resistant one-way hash function guarantees that the previous P_{AS} cannot be recomputed even if the current K_{shd_i} is compromised. Moreover, from the K_{shd_i} itself, deriving of P_{AS} as well as T_l is not possible. Therefore, the proposed scheme is compliant with PPF.

K-CI Attack

Let an adversary A_i be capable of impersonating P_id_i and intercepting the messages $M_1 = (E_{P_{k_{i1}}}\{P_id_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_id_i)$ and $M_2 = E_{P_{k_{i2}}}\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}$ during conversation between P_id_i and AS. From the available information, A_i cannot compute or gain any information regarding encryption keys $P_{k_{i1}}$ and $P_{k_{i2}}$ to decrypt messages M_1 and M_2 respectively. Further, if we assume adversary A_i gets access to the keys $P_{k_{i1}}$ and $P_{k_{i2}}$ through some means, then A_i has to retrieve P_{AS} by executing Step 8 of the general authentication phase. However, the biometric component $f_{i1} = h(F_i||id_i) \oplus x_a$ of P_id_i cannot be supplied by the adversary through any means. Therefore, it is impossible for A_i to derive P_{AS} and subsequently cannot calculate the shared secret key K_{shd_i} independently at the adversary's side to establish a legal session with the server. Thus, the proposed scheme resists K-CI attacks effectively.

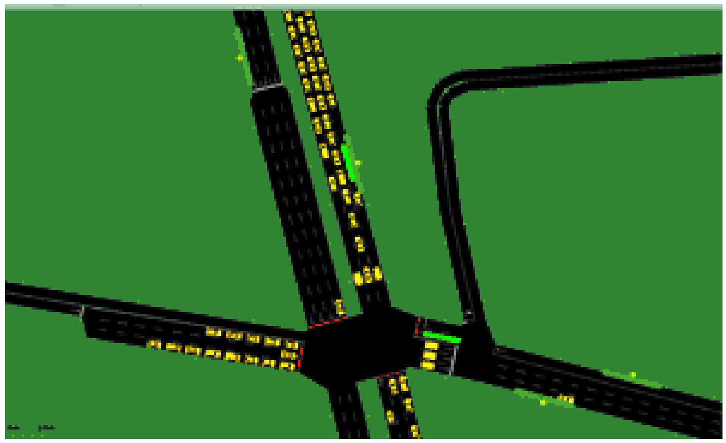

Figure 4.5: SUMO traffic deadlock simulation

4.3 Simulation of VANET Environment

4.3.1 Simulation Test-Bed

Simulation of the environment is an important aspect to investigate the feasibility of launching a protocol and to measure the effect of macro objects on the functionality of the scheme. To build the simulation test-bed, we use Veins, an open-source framework that is imported on OMNET++ (discrete event simulator) [24] and linked with traffic simulator SUMO [5], [108] via "Traffic Control Interface (TraCI)". Various modules, like the application layer, DSRC, and physical layer of OMNET++, have been incorporated to simulate realistic network behavior. Simulation of urban mobility (SUMO) is a mobility simulator to simulate the dynamic behavior of VANET protocols. The implementation of protocols has different impacts in real-time. We have used SUMO to simulate various vehicle types in a large network with multiple lane and lane changing features to study road deadlock and prediction of deadlock occurrences considering multiple micro-level affecting factors. We have also studied the impact of various similar schemes using SUMO and a snapshot is shown in Figure 4.5. Simulation environment details are given in Table 4.9

According to [122], the majority of legitimate terminals perform the desired expected operations only. The vehicles in the city center have low mobility, while rural areas observe high mobility [64].

Table 4.9: Simulation environment details

Environment/Parameter	Tool Version/Value
Traffic simulator	SUMO 0.32.0
Network simulator	OMNET++ 5.5
V2X simulator	Veins 4.7.1
Simulation area	10km x 5 km
Simulation time	1000 secs
Number of vehicles	500
Number of static terminals	500
Number of malicious terminals (%)	10, 25, 50
Network protocol	IEEE 1609.4
MAC protocol Propagation model	IEEE *02.11p Simple Path Loss
Packet size	1024 bits
Attack model	Man-In-Middle and Denial-of-Service
Action by attacker	Non-availability of Content and Content alter with delay

4.3.2 Formal Security Validation by AVISPA Tool

We have used the widely accepted AVISPA tool for formal security verification for intrusion detection and attack mitigation accuracy. We have simulated our protocol using HLPSL [4] language and our simulation results prove that the proposed scheme is secure against man-in-the-middle (MIM) attacks and replay attacks, including intrusion detections. We also implement the mandatory roles in AVISPA for user (U_i), AS, session and environment, including goals and subsequently corresponding HLPSL code presented in Figure 4.7 and Figure 4.8. We have considered six authentication goals and six secrecy goals to keep the smartcard's secret. The Figure 4.6 shows the brief simulation result by AVISPA tool from which we can conclude the proposed protocol is safe.

Table 4.10: Execution time of cryptographic operation

Operator name with description	Runtime in seconds
$T_{h(\cdot)}$: Hash function 256	11.4e-04
T_{mul}: Scalar multiplication	4.41e-04
T_{pcom}: Packet-1024 comparison	11.4e-03
T_{add}: Addition	4.0e-08
T_{ran}: Random number	2.8e-7
T_{pair}: Pairing	8.202e-03
T_{mtp}: Map-to-map	1.1025e-04

Table 4.11: Comparison of time complexity for signature verification w.r.t single and group with ECCP, DCS, LPA, NECPA, TEMCE and, AKAS schemes

Scheme name	Single user verification	Group user verification
ECCP[126]	$3T_{pair} + T_{mtp} + T_{mul}$	$3nT_{pair} + 11nT_{mul}$
DCS[10]	$5T_{pair} + 3T_{mul}$	$5nT_{pair} + 3nT_{mul}$
LPA[160]	$4T_{pair} + T_{mtp} + T_{mul}$	—-
NECPPA[132]	$3T_{pair} + T_{mtp} + T_{mul}$	$3T_{pair} + nT_{mtp} + nT_{mul}$
TEMCE[64]	$2T_{pcom}$	$2nT_{pcom}$
AKAS	$4T_{add} + 4T_{h(\cdot)}$	$4T_{add} + 4T_{h(\cdot)}$

4.3.3 Attacker Model

An adversary is a terminal with the ability to launch an attack to access an unauthorized entry into the system for their self-interest [63]. To evaluate the performance of the proposed protocol in a realistic environment, we have considered denial-of-service (DOS) attack and man-in-middle (MIM) attack scenario. DOS and MIM have a very high level of potential to cause havoc in VANET in terms of their safety and performance. Both the attacks can lead to arise traffic deadlock conditions in the time of emergency.

4.3.4 Performance Metrics

We have defined the following metrics to evaluate the efficacy and efficiency of the proposed scheme in terms of security and object access time over the VANET cloud.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/NewProtocol.if

GOAL
  As Specified
BACKEND
  CL-AtSe

STATISTICS
 Analyzed        : 15 states
 Reachable       : 15 states
 Transition      : 0.04 seconds
 Computation     : 0.001s
```

Figure 4.6: Result of AVISVA simulation

We have considered the following matrices that are used to evaluate the performance of our scheme.

1) Functional Event Availability (FEA): This metric is defined to measure the availability of a functional event in the VANET. An attacker model can inject or flood the network with garbage events, which can affect the performance of the network. High-availability detection of the true event is expected from the network, i.e., a higher FEA is desirable. The inverted FEA index can be represented as follows. $FEA = \frac{\sum(E_{to}-Eg)}{E_{to}}$, where E_{to} is the total number of events pushed into the network. E_t and E_g represent true and garbage events respectively.

2) End-to-end Signature Delay (E2SD): This metric is defined to measure the total time to verify the true signature of the genuine terminal. So, we have, $E2SD = T_{as} - T_t$, where T_t is the initiation time at terminal and T_{as} is the time of returning verified event to the terminal by the authentication server.

```
role user (
Ui, AS : agent,  % Ui is the user and As is the Authentication
Server
S : symmetric_key, % S is the symmetric key between the user
and the server
H : hash_func,          % H is a cryptographic hash function
Snd, Rcv : channel(dy)
)
played_by Ui
def=
Local
State : nat,            % Transition state
Idi,Fi,Pwi:text,        % User ID,Biometric Key and Password
chosen randomly
Ri,Xa,TAr : text,       % Secret nonce
Ps : text,              % Public key of the server
C : text,               % Smart card UID
G : nat,                % Server generator nonce
P : nat,                % Random prime nonce
Sub1 : text,            % Smart card UID - Part I
Sub2 : text,            % Smart card UID - Part II
Fi2new : text,          % At login time, computed Fi2
Ciafnew : text,         % At login time, computed Ciaf
N1, N2 : nat,           % Random nonce N1 and N2
V : text,               % V corresponding to K1 computation
X : text,               % Message
Vs : text,              % Vs needs for computation at server
SKi : text,             % Session key client side
TID,Datai,Inf_Idi,Pk1,Pk2 : text, % Ticket generated by user
Mi1,Mi2,Mi3,Mi4,Mi5,Mi6 :text,
Fi1,Fi2,Ciaf,KiL,Pi,KiA : text,
Pas,Tga,Tle:text
init
State := 0
Transition  % Registration initiated by user over secure channel
0.                      State = 0 /\ Rcv(start) =|>
                        State' := 2 /\ Idi' := new() /\ Fi' :=
new()/\Pwi':=new() /\ Snd({H(Idi').H(Fi').H(Pwi')}_S)
%                       /\ witness(AS, Ui, nua)
% User receives smartcard from the server and stores it locally
2.State = 2 /\ Rcv({Fi2'.Ciaf'.KiL'.KiA'.Pi'.TAr'}_S) =|>
                        State' := 4 /\ Ri' := new()
                        /\ secret(Ri,ri, {Ui, AS})
                        /\witness( Ui,AS,xa,Xa)
                        /\witness(Ui,AS,tar,TAr)

% User enters credential Id,  Fi and  Pwi and waits for
verification after insertion of Smart card
4. State = 4 /\ Rcv(start) =|>
                        State' := 6 /\ Xa' := new()
                        /\Fi1':=xor(H(Fi).H(Idi),Xa')
                        /\Fi2new':=H(Fi1')
                        /\Ciafnew':=xor(xor(H(Pwi),Fi2new'),Xa')

% User sends verified component of smart card and gernerated
param Fi2new and Ciafnew
6. State = 6 /\  Rcv(start) =|>
                        State' := 8
/\Tga':=new()/\Mi1':=xor(Fi1.H(Pwi),Ri)
                        /\TID':=Fi2new.Ciafnew
                        /\Mi2':=(Fi1.TAr.Ri)
                        /\Snd({Mi1.Mi2.KiL.KiA.Tga'}_TID)
                        /\ secret(TID,tid,{Ui, AS})
                        /\ secret(Tga,tga,{Ui, AS})

% User receives response message from the server via
public channel
10. State = 8 /\ Rcv((Mi3'.Mi4'.Mi5'.Mi6'.Tle')) =|>
                        State' := 10 /\
SKi':=H(xor(Pas,Fi1).TAr.KiA.KiL.Tga)
                        /\Snd({Inf_Idi}_SKi')
                        /\witness(Ui, AS,cal_shared_key,Pas)
                        /\request(Ui, AS, ri,Mi2)
                        /\request(Ui,AS,tid,TID)

% User sends confirmation message to server via public
channel
12. State = 10 /\ {Inf_Idi}_SKi=X/\Rcv(start) =|>
                        State' := 12 /\ Snd({Datai}_SKi)
                        %/\request(Ui, AS, user_server_v2,
SKi)
                        %/\ request(Ui, AS, user_server_conf,
X)
end role
% Server role
role server (
                        Ui, AS : agent,
                        % Ui is the user and AS is the
Authentication Server
                        S : symmetric_key,
                        % S is the symmetric key between the
user and the server
                        H : hash_func,
                        % H is a cryptographic hash function
                        Snd, Rcv : channel(dy)
)
played_by AS
def=
local
State : nat,            % Transition state
TID,Idi,Fi,Pwi:text,    % User ID,Biometric Key and
Password chosen randomly
Nu : text,              % User identifier and validator token
AccPolicy,Inf_Idi,Pk1,Pk2 : text, % Access policy assigned by
AS abd Pi is the Encrypted Access plolicy for the Smart card
holder
Ks : text,              % Server secret key
G : nat,                % Generator of the class
Xa,Ri,Rle,Tga,Pas : text, % Random  nonce
TAr,Tle : text, % Time stamp at the time of card generation
by AS
V : text,               % V corresponding to K1 computation
at user end
K2 : text,              % K2 computation
U : text,               % Incoming user tid - ID + Ks combo
Q : nat,                % Random nonce at the server
SKi,Datai : text,       % Session key server side and Data
part
Vs : text,              % V corresponding to computation at
server
X : text,               % Message
```

Figure 4.7: Role specification in HLPSL code-page1

```
HId,HFi,HPwi:text,
Mi1,Mi2,Mi3,Mi4,Mi5,Mi6 :text,
Conf : text,                % Final confirmation message
ACK,Fi1,Fi2,Ciaf,KiL,Pi,KiA : text, % Final acknowledgment sent
to user
C : text                    % Smart card UID client
Init
                            State := 1
 transition
% Server receives request from user for authentication and new
smart card
% if the user does not exist in the database
%1.                         State = 1 /\ Rcv({H(Idi').H(Fi').H(Pwi')}_S)
=|>
1.                          State = 1 /\ Rcv({HId'.HFi'.HPwi'}_S) =|>
                            State' := 3 /\ Xa' := new() /\ TAr' :=
new()/\AccPolicy':=new()
                            /\Fi1':=xor((HFi'.HId'),Xa)
                            /\Fi2':=H(Fi1')
                            /\Ciaf':=xor(xor(HPwi',Fi2'),Xa)
                            /\KiL':=xor((Pk1.TAr'),(Fi1'.HPwi'))
                            /\KiA':=xor(xor((Pk2.TAr'),KiL'),(Fi1'.HPwi')
)
                            /\Pi':=xor(AccPolicy,H(Fi1'.HPwi'))
                            /\Snd({Fi2'.Ciaf'.KiL'.KiA'.Pi'.TAr'}_S)
                            %/\witness(AS, Ui, server_user_sid,
AccPolicy)
                            /\secret(TAr',tar,{Ui,AS})
                            /\secret(Xa',xa,{Ui,AS})
 % Server verifies whether user is properly authenticated
7. State = 3 /\ Rcv({Mi1'.Mi2'.KiL'.KiA'.Tga'}_TID) =|>
                                                   State' := 5
                            /\Pk1':=new()/\Rle':=new()/\Tle':=new()/\
Pas':=new()
                            /\V':=xor(Pk1'.TAr,KiL)
                            /\Mi3':=xor(V',Rle')
                            /\Mi4':=(Ri.Rle'.Pk1'.TAr)
                            /\Mi5':=V'.Ri.Rle'.Tle'.KiA
                            /\Mi6':=Mi5'.xor(Pas',Fi1).TAr
                            /\request(AS, Ui,xa,Xa)
                            /\request(AS, Ui,tar,TAr)
                            /\witness(AS,Ui,tid,TID)
                            /\witness(AS,Ui,ri,Mi2')
                            /\secret(Pas,cal_shared_key,{Ui,AS})
                            /\Snd({Mi3'.Mi4'.Mi5'.Mi6'.Tle'})
 % Server computes decryption key and after computation
sends response message

9. State = 5 /\Rcv(X') =|>
                            State' := 7 /\Datai':=new()/\ SKi':=
H(xor(Pas,Fi1).TAr.KiA.KiL.Tga)/\ Snd({Datai'}_SKi')

                            /\request(AS, Ui, cal_shared_key,Pas)
end role
% Session role
role session (
                            Ui, AS : agent,
                            % Ui is the user and AS is the server
                            S : symmetric_key,
                            % S is the symmetric key between the
user and the server
                            H : hash_func
                            % H is a cryptographic hash function
               )
 def=
 local
SAB, RAB, SBA, RBA : channel(dy)
Composition
user(Ui, AS, S, H, SAB, RAB) /\ server(Ui, AS, S, H, SBA, RBA)
end role
 % Environment role
role environment()
def=
const
nua, cid,ri,tga, tar,xa,tid, cal_shared_key, server_user_sid,
user_server_v2, user_server_conf, server_user_ack :
protocol_id,
                            ui, as : agent,
                            sab, suii, sias : symmetric_key,
                            h : hash_func
intruder_knowledge = {ui, as, suii, sias, h}
composition
                            session(ui, as, sab, h)
                            /\ session(ui, as, sab, h)
                            /\ session(ui, i, suii, h)
                            /\ session(i, as, sias, h)
end role

Goal
authentication_on xa % User nonce generated during
registration
authentication_on tar
authentication_on tid %User verifies Authentication server
authentication_on ri
authentication_on tga
authentication_on cal_shared_key
secrecy_of tar
secrecy_of tid
% Smart card must remain secret to user
secrecy_of xa
secrecy_of ri
secrecy_of cal_shared_key
secrecy_of tga
weak_authentication_on tga % Ticket identifies user issuing
request
 end goal
environment()
```

Figure 4.8: Role specification in HLPSL code-page2

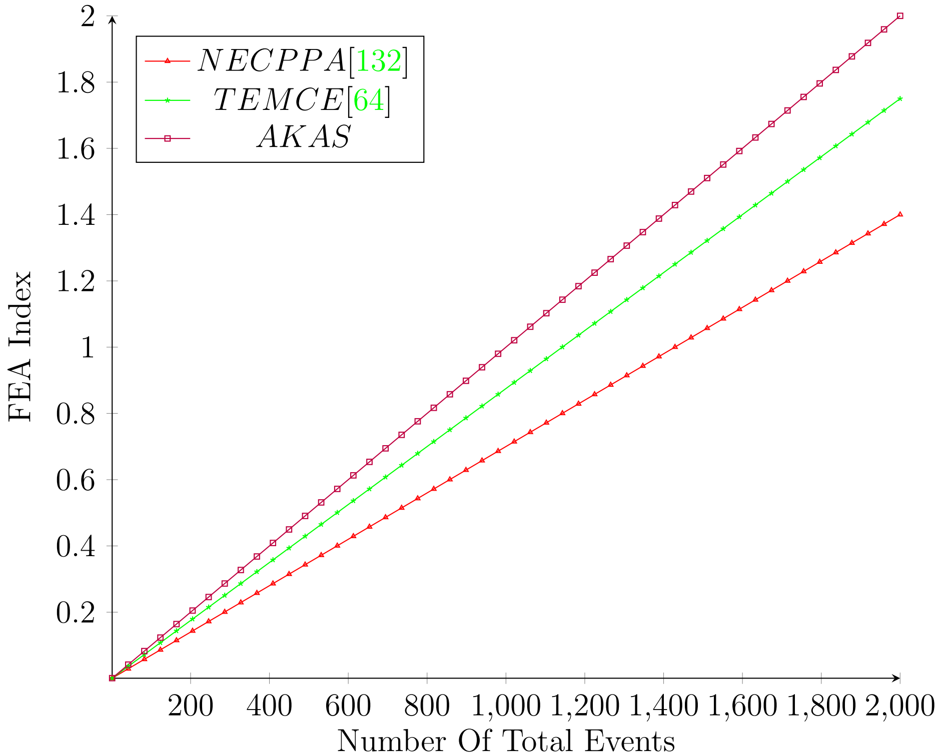

Figure 4.9: FEA index of NECPPA, TEMCE and AKAS

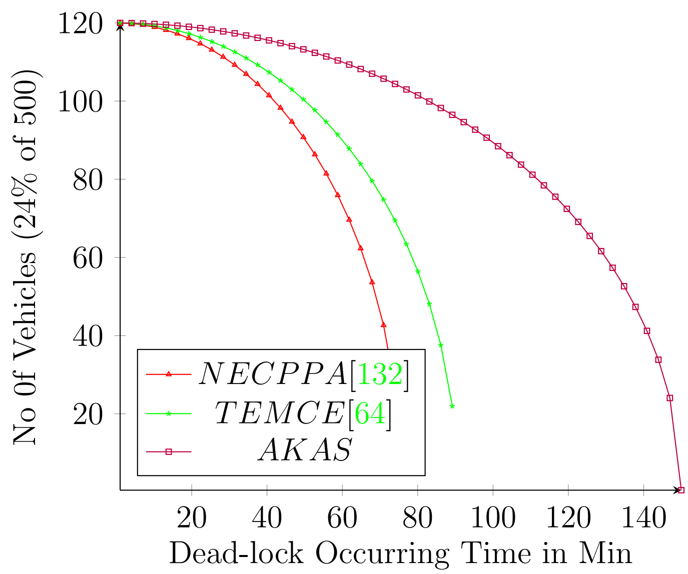

Figure 4.10: Traffic dead-lock profile w.r.t. NECPPA, TEMCE and AKAS

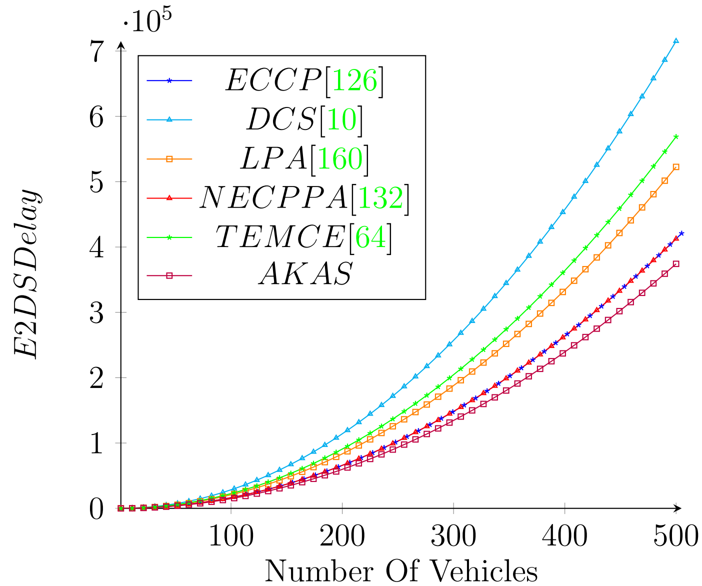

Figure 4.11: E2DS delay of ECCP, DCS, LPA, NECPPA, TEMCE and AKAS w.r.t. individual verification

3) Deadlock Factor to Traffic Jam (DFT2J): This QoS is used to measure how fast the schemes lead to traffic jams. We have defined traffic jam in the SUMO simulation, and it is assumed that a traffic jam has occurred if there 24% of vehicles are waiting at a cross-road for 60 minutes. DFT2J should be minimal to achieve higher performance from the scheme. DFT2J can be defined as,
$DFT2J = \frac{(Eg*x_n)}{(E_g+E_t)*x}$,
where x_n is the number of attempts allowed in a scheme for x number of functional events.

4) Channel Utilization: This metric is defined to measure the impact on channel utilization CH_{ut} when the user density or the density of nodes increased linearly over an ad-hoc network to communicate the AS. The channel utilization may be defined as the ratio of time the channel is utilized over the total duration. So, we have, $CH_{ut} = \frac{(2*T_t)}{(E2SD+2*T_t)}$, where $E2SD = T_{as} - T_t$ and T_t is the initiation time at terminal and T_{as} is the time of returning verified event to the terminal by authentication server.

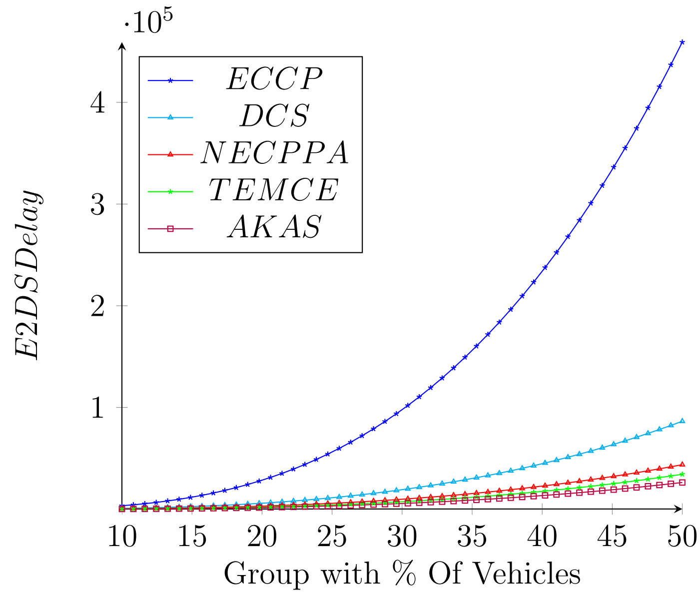

Figure 4.12: E2DS delay of ECCP, DCS, LPA, NECPPA, TEMCE and AKAS w.r.t. group verification

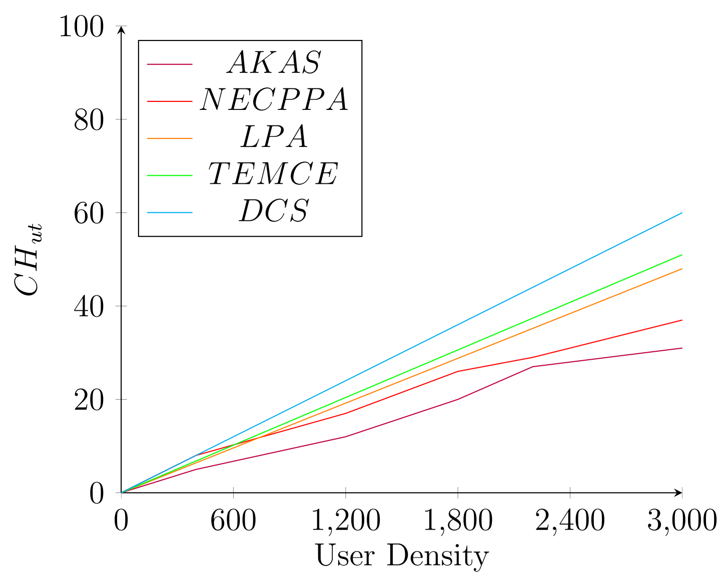

Figure 4.13: The channel utilization of the scheme

Table 4.12: Comparison of security features

Security Protocol with Attribute	TEAM [110]	E2TEAM[130]	Ours
Circumventions dependence on open accessing controls	Y	Y	N
Circumvention by close associates	Y	Y	N
Insider attack resisted	N	Y	Y
Credential cloning attack	N	N	Y
Unintended sharing attack	N	N	Y
Resisted to disclosure attack	N	Y	Y
Resisted to replay attack	N	Y	Y
Resisted to modification attack	NA	NA	Y
Resisted perfect forward secrecy	Y	Y	Y
Resisted key-compromised impersonation (K-CI) attack	N	Y	Y

4.4 Result and Discussion of Simulations

In this section, we present simulation profiles of various matrices and compare our scheme with ECCP [126], DCS [10], LPA [160], NECPPA [132] and TEMCE [64]. The running times of operators with respect to the X2 Ultra Quad-core processor are given in Table 4.10.

Table 4.11 shows the signature verification complexity for the individual user and group users. In Figure 4.9, we have demonstrated the functional availability index profile of NECPPA, TECME, and AKAS schemes. We have observed that the FEA index increases proportionately with the increase in total events.

In Figure 4.10, we have presented a deadlock tendency profile for NECPPA, TECME and AKAS. The deadlock profile has brought out that NECPPA and TECME have around 50% and 40% fast convergence towards traffic deadlock conditions compared to the AKAS protocol. A simple image of a traffic deadlock condition is shown in Figure 4.5.

In Figure 4.11 and Figure 4.12, we have presented the E2DS delay profile with respect to individual signature verification and group verification respectively. It is noted that for both individual and group verification, AKAS spends less time on signature verification. It is essential to consume less time for signature verification because this helps to prevent various attacks by giving less time to the adversary, and it also increases throughput to achieve scalability for a large network.

4.5 Performance Comparison and Cost Comparison

Here, we have compared the functionalities and performances of the proposed protocol with recent publications on authentication protocols for VANET [110] and [130]. From the results presented in Tables 4.8 and Table 4.12, we can say that the proposed protocol solves the security and functionalities limitations of the available protocols. Our proposed protocol is secured, lighter-weight, and supports additional functionalities w.r.t. those discussed protocols.

4.5.1 Comparison of Functionalities

In this section, we have compared various aspects of securities and functionalities, and details of the results are shown in Table 4.12. From this comparison, it is clear that the proposed protocol promises higher security with other requirements for VANET, compared to other relevant protocols. This protocol handles with only 22 one-way hash operations presented in Table 4.8 supporting better performance. From the channel utilization profile Figure 4.13, we can show that our protocol keeps the communication channel less busy. Therefore, it supports high levels of scalability.

4.6 Summary

In this chapter, we have presented a fine-grained access control mechanism for vehicular ad-hoc networks using biometrics. We have demonstrated that our protocol is lighter-weight as it has less computational complexity compared to many relevant and related protocols. A noted aspect of our protocol is that it is free from credential transferability problems, and a user continues to avail services with a single registration process as user credentials are permanently saved on the user's smart device. We have shown that this protocol has remarkable efficiency and is more appropriate for practical applications where there is a special requirement to support a dynamic platform with a battery-operated source as it is independent of a fixed onboard unit (OBU).

Chapter 5

Biometric-Based Authentication

A smart city should have at least two major components of many modern features to be provided with to attain the feather of a real smart city crown. One is a VANET, and the other is a smart vehicle. Government and manufacturers have brought sea changes to the automobile industry by bringing smart vehicles to the smart road [34]. Implementing a sophisticated VANET can bring countless benefits to its users. It would be an easy situation if users were issued smartcards based on their needs and interests. A user can access the VANET services based on his smart card, which belongs to him only. Moreover, a VANET has to deploy tight security measures like any other communication channel. Divulging critical information with the wrong motivation may lead to traffic jams; vehicles get tracked by adversaries. Misuse of privacy, like the current position or route profile of a vehicle, may be used for robbery, theft, and kidnapping.

The VANET is openly exposed to various security concerns, and user authentication is one of the major concerns. In this chapter, we have proposed a biometric smart card-based dynamic authentication scheme to restrict information access among various users. A typical VANET model is shown in Figure 5.1. In our scheme, we have considered three core building blocks like road side fixed infrastructure (RSU), vehicle and authentication server (AS) [84]. The user terminal is housed in every vehicle, which changes its position dynamically, and the RBU is a stationary unit stationed at roadside. RSU helps to access outside information and establishes connections among vehicles as a gateway.

5.0.1 Our Contributions

In this chapter, we propose a smart card-based dynamic lightweight authentication mechanism with a biometric feature for accessing VANET services. Our scheme has the following salient features:

- It provides smart card-based, lightweight authentication for genuine users.
- In our scheme, there is no need for any fixed on-board unit (OBU). In this scheme, any mobile portable device with a smart card reader can be used as a user terminal for login purposes. So, it is a dynamic authentication scheme.
- Our proposed scheme provides scalability as there are no limitations on the number of user terminals; only the genuine user needs to be registered once for accessing the services. No multiple registrations or session-based registrations are required.
- Only users with a valid smart card fulfilled by the biometric component can access the specific service of VANET.
- In our scheme, credentials are stored on a smart card, which is also loss-proof.

5.1 The Proposed Biometric Smart Card-based Authentication

To make VANET services reachable to a larger part of society, we studied this authentication scheme. This scheme helps genuine card holders for accessing information entitled to authorized users only. Once the validity of the smart card and the owner of the smart card are confirmed through the local terminal, an automatic general authentication process is initiated. After successful authentication, AS processes the information object. Then AS retrieves the desired information and encrypts the information object with the authorization key of the user. The received information will be decrypted by the user if and only if he or she is an authorized person for accessing that information. In this scheme, we focus mainly on the authentication process only. However, we have discussed the access control process in Chapters 4 and 7.

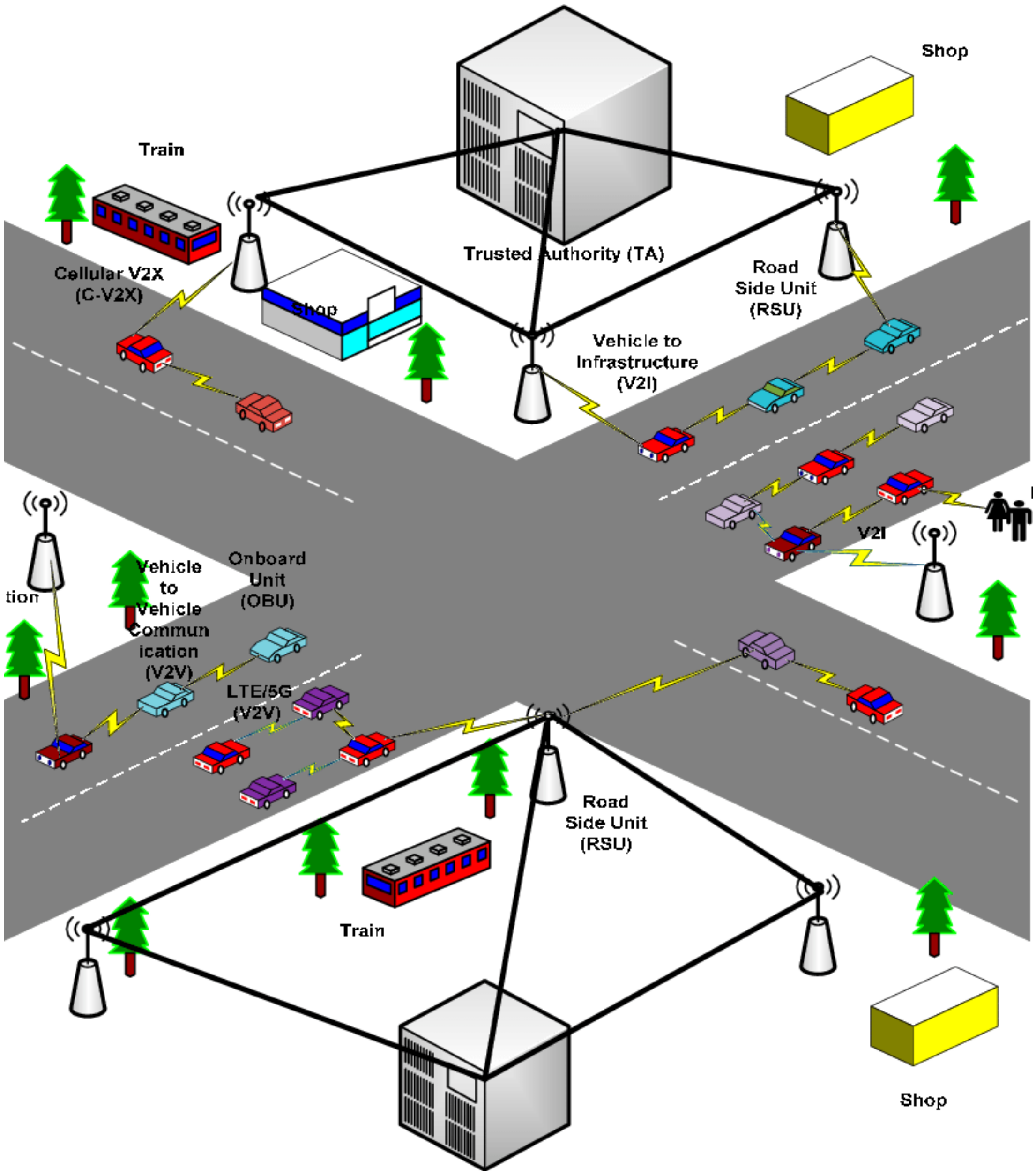

Figure 5.1: A VANET model [138]

5.1.1 Notations

We have used SHA-1 as one-way hash function, and for symmetric key encryption and decryption, we have used AES-based encryption and decryption techniques for our proposed scheme. To explain the scheme, we use various mathematical notations, and these notations are tabulated in Table 5.1.

Table 5.1: Notations used in the proposed scheme.

Symbol	Description
AS	Application server
U_j	Unique identifier of user j
$h(\cdot)$	One-way secure hash function
$A\|\|B$	Concatenates string A and B
$E_K(M)$	Symmetric key encryption under key K
$D_K(M)$	Symmetric key decryption under key K

In our scheme, users can access the VANET cloud through the user terminal. Our scheme consists of three major phases, and we have considered the authentication server AS as a legal entity LE legal executor for smooth running of the system.

5.1.2 Biometric-based Registration Phase

Through the registration phase, every legal user U_i obtains his or her smart card from the authentication server AS. In this phase, communications between user U_i and authentication server AS take place over a secure channel. The following steps should be executed for registration purposes by both U_i and AS:

- **Step 1:** User U_i chooses his/her identity id_i, password pw_i, personal biometrics features B_i and a 128 bit random number r_i.
- **Step 2:** For the biometrics component of the user credential, our proposed scheme makes use of a fuzzy extractor with a nearly uniform randomness probabilistic generator function $G(\cdot)$. It reliably extracts a uniformly random string R of length r bits from its biometric input B_i. R is the biometric key of

user U_i and defined as R$\in\{0,1\}^r$. To assist in recovering a secure sketch function $G_s(\cdot)$ and fuzzy extractor output P from biometrics $B_i^{'}$ (close to B_i) are defined. However, R remains uniformly random even given P. The closeness between $B_i^{'}$ and B_i is defined as hamming distance $h_m^b(B_i^{'}, B_i) \leq$h$_m$,where h_m is the error tolerance threshold value. The $G_s(\cdot)$ function takes $B_i^{'}$ and P as two inputs and reproduces the biometric key for user U_i i.e. (F$_i$) =G$_s(B_i^{\prime}, P)$ where by the virtue of definition $(F_i) = R$;

- **Step 3:** Then the user computes $h(F_i), h(id_i), h(pw_i)$ and sends those computed hashed values to the AS via a secure channel.
- **Step 4:** Receiving those hash values the AS then computes $f_{i1} = (h(F_i)||h(id_i))\oplus$ x_a and
- **Step 5:** Then calculates $f_{i2} = h(h(F_i)||h(id_i) \oplus x_a)$,
- **Step 6:** Compute $c_{i_{af}} = h(pw_i) \oplus f_{i2} \oplus x_a$,
- **Step 7:** Compute $K_{i_L} = (P_{k_1}||T_{A_r}) \oplus (f_{i1}||h(pw_i))$,
- **Step 8:** Compute $K_{i_A} = (P_{k_2}||T_{A_r}) \oplus K_{i_L} \oplus (f_{i1}||h(pw_i))$,
- **Step 9:** Compute $P_i = Acc\_Policy \oplus h(f_{i1}||h(pw_i))$
- **Step 10:** Authentication server (AS) then saves $\{f_{i2}, c_{i_{af}}, K_{i_L}, K_{i_A}, P_i, T_{A_r}\}$ on the smart card of user U_i and gives the smart card to the registered user.

5.1.3 Login Phase

In order to access the services from the server AS, user U_i must login to the system, and the following steps need to be executed.

- **Step 1:** The user inserts his or her smart card SC and inputs his identity id_i, password pw_i and personal biometrics information $B_i^{'}$. Using a secure sketch function $G_s(\cdot)$, F_i is retrieved. Using this information, smart card SC generates $f_{i2}^{\prime} = h(h(F_i)||h(id_i) \oplus x_a)$ and $c_{i_{af}}^{\prime} = h(pw_i) \oplus f_{i2} \oplus x_a$,
- **Step 2:** Using the generated $f_{i2}^{\prime}$ and $c_{i_{af}}^{\prime}$, U_i checks if stored $f_{i2} \stackrel{?}{=} f_{i2}^{\prime}$ and $c_{i_{af}}$ $\stackrel{?}{=} c_{i_{af}}^{\prime}$ holds or not. A mismatch results in immediate termination of the login

phase. Otherwise, it is ensured that the user has entered the correct identity, password, and biometric information.

- **Step 3:** Then User U_i chooses a random number r_i and calculates the following parameter
  $m_{i_1} = (f_{i1}||h(pw_i)) \oplus r_i$
  $m_{i_2} = (f_{i1}||T_r f||T_{ga}||r_i)$

- **Step 4:** The user then finally sends an authentication request to the AS: $M_1 = \{m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_{ga}\}$ via a public channel.

5.1.4 Authentication Phase

In this phase, AS first receives the message $M_1 = \{m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_{ga}\}$ and then mutually authenticates the user. After successful mutual authentication, the user and server establish a common secret session key, which is used for future secure communications between them.

- **Step 1:** After receiving the message M_1 from user U_i, AS calculates $dt = T_{LEC} - T_{ga}$ and Checks if $dt_{min} <= dt <= dt_{max}$. On the validity of the time stamp, AS prepares the response message.

- **Step 2:** AS then retrieves r_i
  as $v = (P_{k_1}||T_{A_r}) \oplus K_{i_L}$ and $r_i = m_{i_1} \oplus v$

- **Step 3:** Then calculates $(f_{i1}||h(pw_i))||T_{A_r}||T_0||r_i)$ and verifies equality with m_{i_2}. This equality confirms the truthfulness of user U_i. Otherwise, the authentication request is rejected by the AS.

- **Step 4:** AS then further calculates the followings
  $m_{i_3} = v \oplus r_{LE}$
  $m_{i_4} = r_i||r_{LE}||(P_{k_1}||T_{A_r})$
  $m_{i_5} = v||r_i||r_{LE}||T_{LE}||K_{i_A}$
  $m_{i_6} = m_{i_5}||(P_{AS} \oplus f_{i_1})||T_{A_r}$

- **Step 5:** AS then finally sends an authentication response message to the user U_i: $M_2 = m_{i_3}, m_{i_4}, m_{i_5}, m_{i_6}, T_{LE}$ via a public channel.

- **Step 6:** User U_i then retrieves random number r_{LE} and verifies m_{i_4}. This equality confirms the truthfulness of the AS.

- **Step 7:** In this step m_{i_5} and $((P_{k_1}||T_{A_r})||r_i||r_{LE}||T_{LE}||K_{i_A})$ equality is verified by U_i and in turn authenticates the received message from the AS and the user also mutually authenticates the server AS.

- **Step 8:** Then the user retrieves P_{AS} using f_{i1} and m_{i_5}.

- **Step 9:** User U_i computes $K_1 = h(P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_{ga})$, a shared sectet key, and subsequently sends the service request message by encrypting the information object Inf_id_i using the session secret key K_1 and the AES symmetric key encryption algorithm.

- **Step 10:** AS checks the validity of P_{AS} and also computes the shared secret key K_1 from its own side. This common secret session key is used for all future communications between the user U_i and the server AS.

Table 5.2: Comparison of transferable syndrome attributes

Attributes	Non-Transferability	Transferability
Circumvention depends on	Completely secret and secured	Unattended access control
Circumvention by	Non	Close family members, friends and drivers
Universality depends on	Biometric and secret	Secret in controlled environment
Credential cloning	Hard	Easy
Unintended sharing	Unlikely	High possibility to occur
VANET system value	Highly raised	Less impact expected

Table 5.3: Comparison of functionality features among different schemes

Security Schemes and Attributes	TEAM [110]	Enhanced Extended TEAM [130]	Ours
Circumvention depends on	Unattended access control	Unattended access control	Secret and secured
Circumvention by	Family members, friends and drivers	Family members, friends and drivers	Non
Resistance to insider attack	✖	✔	✔
Credential cloning attack	✖	✖	✔
Unintended sharing attack	✖	✖	✔
Resistance to disclosure attack	✖	✔	✔
Resistance to replay attack	✖	✔	✔
Resistance to modification attack	NA	NA	✔

Table 5.4: Comparison of computation cost

Authentication steps	At (Unit name)	TEAM [110]	Enhanced Extended TEAM [130]	Ours
Smart card provision(one time)	At security centre(AS)	-	-	4h(.) + 8$\oplus$
Registration	$User_i$	-	3h(.) + 7$\oplus$	-
	OBU_i/User's Terminal	-	1h(.) + 1$\oplus$	-
	AS	3h(.) + 2$\oplus$	3h(.) + 3$\oplus$	-
Login	OBU_i/User's Terminal	1h(.) + 1$\oplus$	2h(.) + 1$\oplus$	4h(.)+ 4$\oplus$
General Authentication	OBU_i/User's Terminal	8h(.) + 5$\oplus$	3h(.) + 4$\oplus$	1$\oplus$
	LE_i	8h(.) + 7$\oplus$	7h(.) + 6$\oplus$	1h(.) + 3$\oplus$
Key Update	OBU_i/User's Terminal	6h(.) + 5$\oplus$	4h(.) + 4$\oplus$	-
	LE_i	5h(.) + 6$\oplus$	4h(.) + 4$\oplus$	-
Smart card revocation	OBU_i/User's Terminal	-	-	4h(.) + 8$\oplus$
Password/Biometrics Change	OBU_i/User's Terminal	2h(.) + 3$\oplus$	4h(.) + 3	4h(.) + 8$\oplus$

5.1.5 Password and Biometrics Change Phase

As updating passwords and biometrics involves sensitive parameters over the smart card, So, if a user wishes to change their password and biometric component, the following steps should be executed through a secure channel:

- **Step 1:** The user inserts his or her smart card SC and inputs his identity id_i, password pw_i and personal biometrics information B'_i. Using a secure sketch function, $G_s(\cdot)$, F_i is retrieved. Using this information, smart card SC generates $f'_{i}2 = h(h(F_i)||h(id_i) \oplus x_a)$ and $c'_{i_{af}} = h(pw_i) \oplus f_{i2} \oplus x_a$,

- **Step 2:** Using the generated $f'_{i}2$ and $c'_{i_{af}}$, AS checks if stored $f_{i2} \stackrel{?}{=} f'_{i}2$ and $c_{i_{af}} \stackrel{?}{=} c'_{i_{af}}$ holds or not. On matching, AS gives a green signal to the user to provide their new password and biometrics via a secure channel. Otherwise, it results in the immediate termination of the password and biometrics update phase.

- **Step 3:** AS performs steps: 3 to step: 10 of user registration phase with a new password and biometrics.

5.1.6 Smart Card Revocation Phase

The user has to approach AS to reissue smart card and he or she has to perform the following steps successfully:

- **Step 1:** The user provides his or her credentials, i.e., identity id_i, password pw_i and personal biometrics information B'_i. Using a secure sketch function

$G_s(\cdot)$, F_i is retrieved. Then the user calculates $h(F_i')$, $h(id_i')$ and $h(pw_i')$ and send the same to AS via a secure channel.

- **Step 2:** Using the provided credential AS calculates $c'_{i_{af}}$ and checks if stored $c_{i_{af}} \stackrel{?}{=} c'_{i_{af}}$ holds or not. A mismatch results in the immediate termination of the request for the reissue of the smart card. Otherwise, it is ensured that the user is a legitimate smart card holder.

- **Step 3:** Upon successful user validity check, AS gives two options to user either to reissue smart card with the old credential saved in the AS database or reissue the smart card with a new password and biometrics. AS performs step: 4 if the user opts to have reissued smart card with an updated credential.

- **Step 4:** AS performs steps: 3 to step: 10 of user registration phase with a new password and biometrics.

5.2 Cryptanalysis of Our Proposed Scheme

The sharing of information in any form over any medium is referred to as credential lending, sharing, or transfer [146]. Cryptanalysis of TEAM and enhanced extended TEAM shows that user registration is highly interconnected with vehicle details. User credentials in these schemes have to be transferable in nature if a vehicle is considered as a shared object. So, these schemes suffer from the credential transferability syndrome problem. Our proposed scheme adheres to the non-transferability credential feature. Here, we also informally show that this scheme can prevent various known attacks effectively.

5.2.1 Insider Attack

At the time of registration, user U_i submits his credential to security center $\{F_i, id_i, pw_i\}$ which is converted into $\{h(F_i), h(id_i), h(pw_i)\}$ by security terminal. So the insider has access to the hashed value of the finger print, password, and id. Thus, insiders cannot misuse the user's credentials, and BSAS effectively prevents insider attacks effectively.

5.2.2 Resistance to Impersonation Attack

Let an adversary A_i has captured message: $\{m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_{ga}\}$ and message $\{m_{i_3}, m_{i_4}, m_{i_5}, m_{i_6}, T_{LE}\}$ during conversation between U_i and AS. From the available information, the adversary cannot retrieve the general authentication key P_{AS} from m_{i6} as he will not able to provide f_{i_1}. Thus, this scheme resists impersonation attacks.

5.2.3 Resistance to Disclosure Attack

Since an adversary cannot gain access to the general authentication key as discussed in Section 5.2. Thus, the adversary cannot initiate any process of authentication. So, VANET services, key updates, session updates, or credential parameters can not be disclosed. Similarly, in the proposed scheme, unintentional sharing of credentials is unlikely to happen through relatives, friends, or drivers. Thus, our scheme is resistant to information disclosure from any likely sources of leakage.

5.2.4 Resistance to Card-theft Attack

An adversary can get user credentials $\{f_{i2}, c_{i_{af}}, K_{i_L}, K_{i_A}, P_i, T_{A_r}\}$ if smart card is lost or theft. From the card, the adversary cannot gain any access as id and password are already in hashed form. In a hypothetical situation, id and password get communicated verbally, but the biometric component cannot be misused as biometric component is non-transferable. Thus, our proposed authentication scheme resists card theft attacks.

5.2.5 Biometric-based Authentication

At each transaction of messages, both parties calculate dt before real processing to assess the time stamp genuinity based on the definition of the too old or too fresh timestamp concept. As the adversary is unable to grab the current time stamp, the replay attack situation is completely avoided in the proposed scheme.

5.2.6 Resistance to Modification Attack

Let an adversary A_i has captured message M_1:$\{m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_{ga}\}$ and message: M_2:$\{m_{i_3}, m_{i_4}, m_{i_5}, m_{i_6}, T_{LE}\}$ during conversation between user U_i and AS.

The component m_{i_2} of M_1 and the component m_{i_5} of M_2 determine the genuinity of user and AS respectively. If any portion of the message is modified during the transition, both parties have equations to verify and discard at their ends. Thus, our proposed scheme resists modification attacks.

5.2.7 Password Guessing Attack

Due to the one-way property of the hash function $h(\cdot)$ backward calculation facility is not available, which makes it infeasible to derive any mandatory information like id, password and biometrics to gain to access the user-sensitive domain. Thus, the proposed scheme is protected from password-guessing attack.

5.2.8 Denial of Service Attack

Any mismatch in user credentials at general authentication, user is barred from the general authentication stage. Hence, it is impossible for an adversary to set up a valid session. Hence, this scheme is resistant from denial of service attack.

5.2.9 User Anonymity Attack

If an adversary possesses a smart card illegally through the wrong means, he cannot distinguish the user in the various steps of authentication. Thus, the anonymity of the user is enforced in this scheme.

5.3 Performance Comparison

In this section, we compare the functionality and performance of the proposed scheme with some very recently published authentication schemes for VANET [110] and Enhanced Extended TEAM [130]. It is noticed from the table that our proposed scheme overcomes the security and functionality weaknesses of the existing schemes. Our scheme is more secure, lightweight, and provides many extra functional features compared to those schemes.

5.3.1 Comparison of Functionality Features

Here, a detailed comparison of different security and functionality features among different schemes is tabulated in Table 5.3. Our proposed scheme is much more secure and having all required features for VANET, compared to other related schemes in the light of Table 5.3.

5.3.2 Computation Cost Comparison

Table 5.4 shows the computation cost and complexity involved at various steps of authentication in VANET. In our proposed authentication protocol, the registration phase is only one-time process. So compared to other related schemes, performance-wise, our scheme is better as it takes only 9 one-way hash functions, $h(\cdot)$ as shown in Table 5.4.

5.4 Summary

In this chapter, we have proposed a biometric smart card-based dynamic, lightweight access control scheme that is less complex and easier to manage compared to other related schemes. We have also analyzed transferability syndrome issues and presented them in Table 5.2. The special feature of our proposed biometric-based scheme is that it does not suffer from the credential transferability syndrome problem. In our scheme, users do not need to go through the user registration process each and every time, which makes transactions lighter compared to other schemes. Our scheme does not require the involvement of any on-board unit OBU during the login, and authentication phases. So, this proposed protocol is more suitable for practical applications and can perform efficiently especially for power-constraint and mobile user terminal devices, as compared to other relevant existing protocols.

Chapter 6

Rabin Cryptosystem in Authentication

In the present era, vehicular ad-hoc networks (VANETs) play an important role in modern traffic management activities. A VANET is an inherently complex cyber-physical system of systems (SOS) that can include basic stand-alone static elements to very sophisticated dynamic elements to provide data access as per real-time need. An SOS-oriented VANET architecture is shown in Figure 6.1. To ensure users' core security concerns over crucial data in transit, it essentially demands a foolproof user authentication scheme for accessing desired services from VANET clouds. Recently, various schemes have been designed to address numerous security concerns, but very few schemes have concentrated on addressing all major attacks with efficiency. A VANET can bring a favorable situation if its users are entrusted and ensured their interests in terms of security measures. A user gets the facility of VANET services under the scanner of an efficient authentication scheme only. Divulging critical information with improper intention can cause traffic jams, and subsequently, vehicles are easily exposed to adversaries [110]. Leakage of positional and route information gets exploited by robbers, thieves, and kidnappers. Therefore, the VANET is directly experiencing enormous security challenges. Beside this, user authentication has become one of the major concerns.

There is significant work already being carried out in the direction of authentication and privacy preservation using Rabin Cryptosystem security solutions. However, the basic Rabin Cryptosystem is a factoring-based efficient method, but its decryption process leads to failure as it generates 4 to 1 output. In this chapter, we propose an enhanced method, and it may be noted that the enhanced method is unique and does not lead to failure. The fundamentals of the algorithm are presented in Section 6.1.3. Rabin cryptosystem has three major steps for authentication, like key generation, encryption, and decryption. To generate keys, two prime numbers are chosen as private, and the product of prime numbers has been taken for public keys. A public key is used for encryption. To decrypt a private key, a Blim-Blum-Shub pseudo-random bit generator is used. Three major components, like vehicles with smart features, a roadside unit (RSU), and an authentication server (AS) are considered to explain the proposed scheme [84], [112]. All the vehicles have dynamic state vectors along with a user access terminal. A roadside unit (RSU) is a fixed infrastructure to perform gate-way jobs and provide links among all vehicles in a defined VANET domain.

6.1 The Proposed Authentication Scheme

In this section, we present our concept of the proposed improved and enhanced Rabin cryptosystem-based authentication mechanism. This scheme has five prominent steps that are discussed below:

6.1.1 Notations

The notations presented in Table 6.1 are used to describe our proposed protocol. One-way HA-1 [7] function for generating the hash key and AES [2], [34] have been used for encrypting and decrypting information based on symmetric key encryption and decryption processes to present our scheme.

6.1.2 Our Major Contributions

In this chapter, we have proposed an improved and enhanced Rabin cryptosystem-based authentication mechanism to authenticate users for VANET services. The proposed scheme has the following important aspects:

- We propose an improved and enhanced Rabin cryptosystem-based authentication mechanism that can address most of the known major attacks with robustness, efficiency, scalability, and dynamicism in picture.

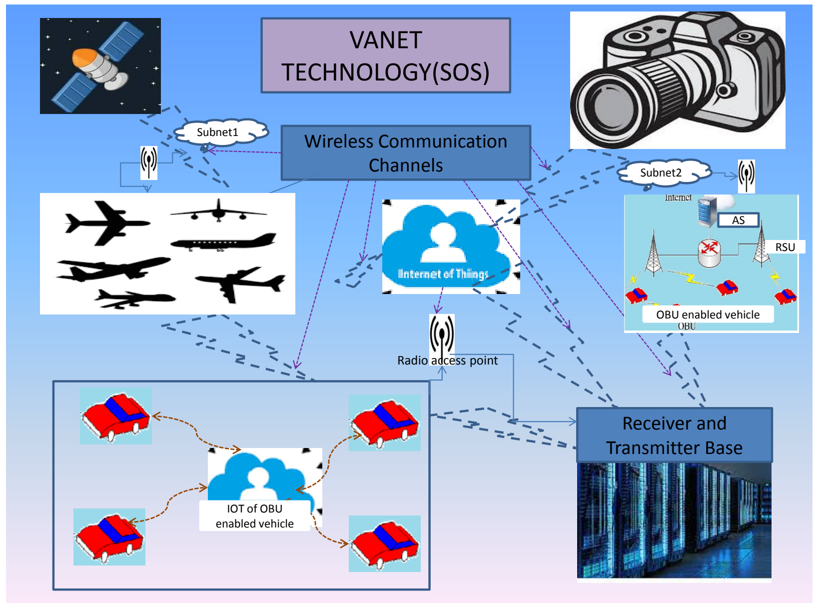

Figure 6.1: An SOS-oriented VANET architecture.

- It supports a light-weight authentication process for legitimate users.
- This proposed scheme supports scalability as it does not depend on the volume of user access points, and valid users are required to register only once to access the VANET services. Thus, session-based and duplicate registration can be avoided.
- We have carried out formal verification using the Random Oracale Model.
- We have also rigorously carried out security analysis by AVISVA.

6.1.3 Enhanced Rabin Cryptosystem

In this section, the proposed methods are elaborated in details. It may be noted that we exclude the details of the Jacobi symbol and the concept of extra redundant information from plain text. The algorithms can be explained as the following.
Procedure: $M \in (0, 2^{2n-2})$ **with** $N = p^2q$
Here, we also have considered the choice of an alternative modulus $N = p^2q$ similar to that defined by Takagi [69]. But the limit for searching space M for plaintext is defined within $M \in (0, 2^{2n-2})$.

Algorithm 1 : Procedure for generating key

Input: The input security parameter dimension n

Output: Public-key: N and Private-key: (p, q)

I: Select two distinguished prime numbers p and q so that $2^n < p, q < 2^{n+1}$, agreed upon $(p, q) \equiv 3(\mathrm{mod}\ 4)$

II: Calculate N, such that $N = pq$.

III: Return output: public-key N and private-key (p, q).

Algorithm 2 : Procedure for encrypting the plaintext

Input: The public-key N and the message M

Output: The encrypted message C

I: Randomly select an integer $M \in (0, 2^{2n-2})$

II: calculate $C \equiv M^2(\mathrm{mod} N)$

III: Return output: encrypted message C

Algorithm 3 : Procedure for decrypting the ciphertext

Input: Private-key $(p; q)$ and encrypted message C

Output: The original message M

i: calculate $m_p \equiv C^{\frac{q+1}{4}}(\mathrm{mod}\, p)$

ii: calculate $m_q \equiv C^{\frac{p+1}{4}}(\mathrm{mod}\, p)$

iii: calculate two integers r and s such that $(rp + sq = 1)$

iv: calculate $M1 \equiv rpm_q + sqm_p(\mathrm{mod}\, pq)$

v: calculate $M2 \equiv rpm_q - sqm_p(\mathrm{mod}\, pq)$

vi: calculate $M3 \equiv -M_2(\mathrm{mod}\, pq)$

vii: calculate $M4 \equiv -M_1(\mathrm{mod}\, pq)$

viii: calculate $i = 1$ to 4 calculate $W_i = C - M_i^2$ for $M_i < 2^{2n-1}$, otherwise discard.

ix: Calculate the original message $M = M_i$ when it $W_i \in \mathbb{Z}$

6.1.4 Rabin Cryptosystem Based Registration Phase

In this phase, the authentication server AS prepares a smart card for each legal user P_id_i and hands over his or her card after the successful registration phase. It is assumed that all the transactions between P_id_i and AS are transmitted through defined secured channels only at the physical station. The below-mentioned operations are performed by both P_id_i and AS parties to be successfully registered with AS:

- **Step 1:** First, user P_id_i selects own ID id_i, password pw_i, and biometric features F_i along with a 128-bit number r_i chosen randomly.
- **Step 2:** Paralally, AS selects security parameters p_i and q_i as per Algorithm I for registering P_id_i and also checks $1 \leq r_i \leq N_i - 1$.
- **Step 3:** In this step, the user's computed values, i.e., $id_i, h(F_i||id_i), h(F_i||pw_i)$ are sent to the AS via secured channels.
- **Step 4:** In this step, the authentication server checks the availability and existence of the requested user id_i for further processing.
- **Step 5:** Based on the availability of AS, it performs the computation presented in **Algorithm I**.
- **Step 6:** After reception of $\{id_i, h(F_i||id_i), h(F_i||pw_i)\}$, AS generates a 128-bit random number x_a, assigns pseudoidentity P_id_i to the user U_i and computes $S_k = h(h(F_i||id_i)||h(F_i||pw_i)) \bmod N_i$ and $f_{i1} = h(F_i||id_i) \oplus x_a$
- **Step 7:** Then calculates
  $f_{i2} = h[P_id_i||h(F_i||id_i)||h(F_i||pw_i)||x_a]$,
- **Step 8:** AS acquires the current time stamp T_{A_r} and generates two keys $P_{k_{i1}}$ and $P_{k_{i2}}$, for the user P_id_i, each of length 160-bits and computes $K_{i_L} = (P_{k_{i1}}||T_{A_r}) \oplus (f_{i1}||h(F_i||pw_i)) \bmod N_i$,
  $K_{i_A} = (P_{k_{i2}}||T_{A_r}) \oplus K_{i_L} \oplus (f_{i1}||h(F_i||pw_i)) \bmod N_i$,
- **Step 9:** Authentication server (AS) then saves encrypted credential $E_{S_k}\{P_id_i, f_{i1}, f_{i2}, K_{i_L}, K_{i_A}, P_i, P, T_{A_r})\}$ on the smart card belongs to user P_id_i and hands over to the user that registered with. AS stores $\{P_id_i, (P_id_i||P_{k_{i1}}) \oplus h(x), (P_id_i||$

$P_{k_{i2}}) \oplus h(x)\}$ the values specific to the user P_id_i in its database. It may be noted that $S_k = N_i$ and generated by **Algorithm I and encrypted as per Algorithm II**. The summarized registration phase is shown in Table 6.2.

Table 6.1: Notations used to describe proposed scheme

Symbols	Descriptions
AS	Application server
U_i	i^{th} user
$\ominus$	Operation to discard a string from string concatenation of two or more values $(A\|\|B) \ominus B = A$
$h(\cdot)$	Secured One-way hash function
$\oplus$	Exclusive XOR operation
$A\|\|B$	String concatenation operator
$E_K(M)$	Encrypt M using key K
$D_K(M)$	Decryp M using key K
x	AS's master secret key
P_id_i	Pseudoidentity of user U_i
r_i	Random number of 128 bits generated at the user side during registration phase
x_a	Random number of 128 bits generated at the AS side during registration phase
r_{LE}	Random number of 128 bits generated at the AS side during general authentication phase (GAP)
B_i'	Biometrics features of 1024 bits
T_{A_r}	Timestamp at the time of user registration phase at the AS side
T_l	Timestamp at the time of login at the user side
T_{LE}	Timestamp at the reception of login message at the AS side
$P_{k_{i1}}$	Keys generated by AS during registration phase for U_i
$P_{k_{i2}}$	Key generated at AS by random number generator (RNG) used for mutual authentication at general authentication phase (GAP)
P_{AS}	Key generated at the AS side during GAP

Table 6.2: Registration phase of user with authentication server

User U_i	Authentication Server AS
Input id_i, pw_i, F_i and r_i	AS picks up p_i and q_i and calculates N_i
	$\xleftarrow[\textbf{(secure channel)}]{N_i}$
User chooses randomly $r_i where 1 \leq r_i \leq N_i - 1$	
$id_i, h(F_i\|\|id_i), h(F_i\|\|pw_i)$	
User Sends	
$\langle id_i, h(F_i\|\|id_i), h(F_i\|\|pw_i) \rangle$ to AS	
$\xrightarrow[\textbf{(secure channel)}]{\langle id_i, h(F_i\|\|id_i), h(F_i\|\|pw_i)\rangle}$	AS performs the following computation
	$S_k = h(h(F_i\|\|id_i)\|\|h(F_i\|\|pw_i)) \bmod N_i$
	$f_{i1} = h(F_i\|\|id_i) \oplus x_a$
	$f_{i2} = h(h(F_i\|\|id_i)\|\|h(F_i\|\|pw_i)\|\|x_a)$
	$K_{i_L} = (P_{k_{i1}}\|\|T_{A_r}) \oplus (f_{i1}\|\|h(F_i\|\|pw_i)) \bmod N_i$
	$K_{i_A} = (P_{k_{i2}}\|\|T_{A_r}) \oplus K_{i_L} \oplus (f_{i1}\|\|h(F_i\|\|pw_i)) \bmod N_i$
	AS saves the information on smart card encrypted
	by S_k, $E_{S_k}\{f_{i1}, f_{i2}, K_{i_L}, K_{i_A}, T_{A_r})\}$
	AS stores for future computation
	$\{P_id_i, (P_id_i\|\|P_{k_{i1}}) \oplus h(x)$ and
	$(P_id_i\|\|P_{k_{i2}}) \oplus h(x)\}$ values specific to user U_i
	AS issues smart card to the user containing
	$\xleftarrow[\textbf{(secure channel)}]{E_{S_k}\{f_{i1}, f_{i2}, K_{i_L}, K_{i_A}, T_{A_r}\}}$
User receives smart card	
with secret credential	

6.1.5 Login Phase

To access VANET support through AS, P_id_i has to complete this process at its own terminal. P_id_i executes the following operations to login successfully.

- **Step 1:** P_id_i inserts a smart card and uses self-identity id_i, password pw_i along with biometrics information F_i. With the help of the smart card SC and own credential, the user first computes $S_k = h(h(F_i||id_i)||h(F_i||pw_i))$ and then decrypts the information stored in the smart card. It retrieves x_a as follows.
  $x_a = f_{i1} \oplus h(F_i||id_i)$.
  Then smart card SC computes $f'_{i2} = h(h(F_i||id_i)||h(F_i||pw_i)||x_a)$, and checks if stored $f_{i2} \stackrel{?}{=} f'_{i2}$ matches or not. A first mismatch leads to prompt rejection of this process. Otherwise, it is validated and ensured that the provided credentials with biometric input are correct.

- **Step 2:** After success in the first step, P_id_i picks up a number r_i randomly and prepares the given below two pieces of information

$m_{i_1} = (f_{i1}||h(F_i||pw_i)) \oplus r_i \bmod N_i$
$m_{i_2} = (f_{i1}||T_{A_r}||T_l||r_i) \bmod N_i$

- **Step 3:** In this step, the user first retrieves $P_{k_{i1}}$ to encrypt the message M_1 as follows
  $v_{p_{i1}} = P_{k_{i1}}||T_{A_r} = K_{i_L} \oplus (f_{i1}||h(F_i||pw_i))$
  $P_{k_{i1}} = v_{p_{i1}} \ominus T_{A_r}$
  and then finally sends an authentication request message encrypted under $P_{k_{i1}}$ to the AS: $M_1 = (E_{P_{k_{i1}}}\{P_id_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_id_i)$ over normal (public) channels.

6.1.6 General Authentication Phase

The authentication server starts this phase by retrieving the $M_1 = (E_{P_{k_{i1}}}\{P_id_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_id_i)$ and then authenticates the user. Through successful authentication, a secret session key is settled between them for further secured communication. AS uses the received pseudoidentity P_id_i of U_i to retrieve $P_{k_{i1}}, P_{k_{i2}}$ and T_{A_r} specific to user P_id_i.

- **Step 1:** After reception of message M_1 from P_id_i, AS calculates $dt = T_{LE} - T_l$ and checks if $dt_{min} <= dt <= dt_{max}$. If it is found that the timestamp is within a valid limit, then AS generates a reply.

- **Step 2:** Then r_i is retrieved by the authentication server as $v = (P_{k_{i1}}||T_{A_r}) \oplus K_{i_L}$ and $r_i = m_{i_1} \oplus v$.

- **Step 3:** Then calculates $(f_{i1}||T_{A_r}||T_l||r_i) \bmod N_i$ and compares equality with m_{i_2}. This equality validates the truthfulness of user P_id_i. Otherwise, the authentication process gets terminated by the AS.

- **Step 4:** In this step, AS generates a 160-bits key P_{AS} and embeds it into m_{i_6} to mark a successful GAP phase at the AS end and reuses the shared-secret key for a particular session to avoid repetitive general authentication phase, and calculates the followings,
  $m_{i_3} = v \oplus r_{LE} \bmod N_i$

$m'_{i_5} = (P_{k_{i1}}||T_{A_r}||r_i||r_{LE}||T_{LE}||K_{i_A}) \bmod N_i$, $m_{i_5} = h(m'_{i_5})$
$m_{i_6} = m'_{i_5}||(P_{AS} \oplus f_{i_1})||T_{A_r} \bmod N_i$.

- **Step 5:** AS at this step, it forwards an authentication response message encrypted under $P_{k_{i2}}$ to P_id_i: $M_2 = E_{P_{k_{i2}}}\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}$ via a public channel.

- **Step 6:** First, P_id_i retrieves $P_{k_{i2}}$ to decrypt the received M_2 as follows $v_{p_{i2}} = K_{i_A} \oplus K_{i_L} = (P_{k_{i2}}||T_{A_r})$
$P_{k_{i2}} = v_{p_{i2}} \ominus T_{A_r}$. Then user U_i retrieves random number r_{LE} as $r_{LE} = m_{i_3} \oplus (f_{i1}||h(F_i||pw_i))$.

- **Step 7:** Then user P_id_i calculates based on his smart card information, $m''_{i_5} = (P_{k_{i1}}||T_{A_r}||r_i||r_{LE}||T_{LE}||K_{i_A}) \bmod N_i$ and $h(m''_{i_5})$ verifies its equality with m_{i_5}. The equality authenticates that the received message is generated by the AS and in turn, the AS gets authenticated by P_id_i.

- **Step 8:** Then P_id_i extracts P_{AS} from f_{i1} and m''_{i_5} as:
$v_{p_{i3}} = m_{i_6} \ominus m''_{i_5} \ominus T_{A_r} = (P_{AS} \oplus f_{i_1})$
$P_{AS} = v_{p_{i3}} \oplus f_{i_1}$.

- **Step 9:** P_id_i then computes one common shared secret key $K_{shd_i} = h((P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_l)$ and saves as one of the vital components for a defined session to mark a sign of a successful general authentication process.

- **Step 10:** AS also computes the shared common secret key K_{shd_i} from its own side. The same common session key is agreed upon by user P_id_i for all future service requests and information object access from the VANET cloud via the server AS and AS uses it for decrypting the service request from user P_id_i .

The summarized steps from login to the general authentication phase are briefly presented in Table 6.2.

6.2 Threat and Security Analysis

The primary goal of a credential scheme is to maintain users' privacy reliably by supporting its users to mask identifying personal attributes in transactions over a

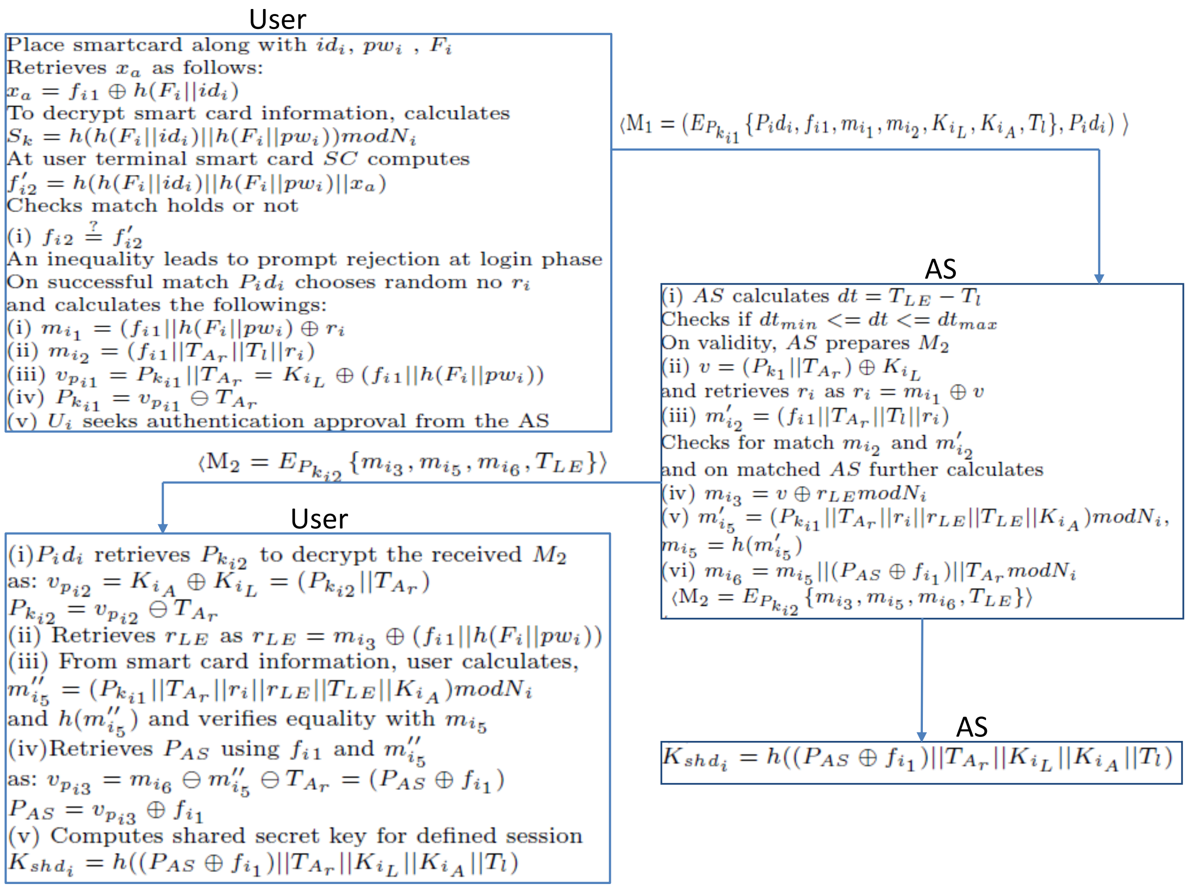

Figure 6.2: Overal processes in Rabin cryptosytem-based authentication scheme

network. The sharing of information with unregistered personnel to get access to the services in any way is known as credential lending, sharing, or transfer [34]. This proposed protocol is compliant with the non-transferability of credential features. The considered set of attributes (A) are A1 (Circumvention depends on), A2 (Circumvention by), A3 (Universality depends on), A4 (Credential cloning), A5 (Unintended sharing) and A6 (VANET system value). Functional relations among attributes, non-transferability, and transferability are shown in Table 6.3.

6.2.1 Formal Security Proof by ROR Model

The formal security analysis of the proposed protocol, say V for VANET is carried out by the widely accepted ROR model [106], [112], [72]. The ROR provides a

Table 6.3: Comparison sharable credentials

A	Non-sharable	Sharable
A1	Full secrecy	Accessing control open
A2	No associates	Closed associates
A3	Secrecy for all environments	Secrecy for environments
A4	Harder	Easier
A5	Impossible	Highly possible to happen
A6	Value improved	Less value addition

provision to simulate real attack by an adversary $\mathcal{A}$ through which the adversary capabilities in a real attack are captured [19], [141]. Table 6.4 and 6.5 contain descriptions of the various symbols for queries and notations that are used in the semantic security proof. The adversary $\mathcal{A}$ acts to be an active participant either P_id_i or authentication server AS at t^{th} instance with V. We have considered all probable queries for proving formal security concerns.

Table 6.4: Various ROR queries with their description

Query	Description for Interpreting Query
Send(V, p) (S)	It allows $\mathcal{A}$ to share plea message p to $\mathcal{V}^t$. In response $\mathcal{V}^t$ answers to $\mathcal{A}$ as per protocol.
Execute(P_id_i, S) (E)	This makes $\mathcal{A}$ capable to listen message p transmitted among P_id_i and AS in a real operation of the scheme.
Corrupt(P_id_i, a) (C)	According to correctness of a, it helps to obtain user's credential saved in SC to mentioned adversary $\mathcal{A}$.
Reveal$(\mathcal{V}^t)$ (R)	It enables to disclose shared key K_{shd_i} generated between P_id_i and AS.
Test$(\mathcal{V}^t)$ (T)	By this query $\mathcal{A}$ sends a proposal to $\mathcal{V}^t$ for the present common session key K_{shd_i} and $\mathcal{V}^t$ answers probabilistically as result of unbiased flipped coin b.

Definition 6.1. *The advantage function of an adversary $\mathcal{A}$ in breaking the semantic*

Table 6.5: Symbols of ROR model description

Symbols	Description and Meaning of Symbols
q_H	Total number of hash H oracle execution
q_s	Total number of *Send* query executed
q_e	Total number of *Execute* oracle query executed
l_H	Length of the hashed output string
l_r	Length of random number
l_b	Length biometric key
ε_{bm}	Measure of false positive in biometric input [33]
$\|\mathcal{D}\|$	Size of password dictionary
L_H	Storage for output of hash H oracle query
L_A	Storage for random oracle output
L_T	Storage for message transcripts between P_id_i and AS

security of the proposed protocol (VANET) scheme V with assumption of the exact bit b' can be written as $Adv_V^{VANET} = |2Prb[b = b'] - 1|$.

Definition 6.2. *A biometrics-based scheme to authenticate a user using a password can be semantic-secured if the advantage Adv_V^{VANET} is slightly larger than $\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\}$, where q_s, $|\mathcal{D}|$, $l_b$and ε_{bm} carry the same meaning as per Table 6.5.*

Theorem 6.1. *If we assume that the adversary $\mathcal{A}$ runs with the complexity of a polynomial algorithm $t_{\mathcal{A}}$. The adversary executes H, S and E with maximum time complexity q_H, q_s and q_e respectively to be capable to crack the defined semantically secured of our protocol V. As per definition, we have,*

$$\begin{aligned} Adv_V^{VANET} \quad &\leq \quad \frac{q_H^2 + 28q_H}{2^{l_H}} + \frac{(q_s + q_e)^2 + 10q_s}{2^{l_r}} \\ &\quad +2\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned}$$

where q_s, q_H, l_H, l_r, $|\mathcal{D}|$, l_b and ε_{bm} carry the same meaning as per Table 6.5.

Proof: The proof can be derived from a set of five independent games, and these are defined as G_{mi}, $(i = 0, 1, 2, 3, 4)$. We follow the similar steps as [134], [129] to prove the theorem. In the G_{m_i}, the attacker $\mathcal{A}$ cracks to assume the exact random numbers r_i by the $Test$-query. The event of occurrence is defined as S_i and the associated probability of occurrence is written as $Prb[S_i]$.

Game G_0: The first game G_{m_0} is assessed and evaluated under ideal conditions as per the ROR model and definition 1. Therefore, we can write,

$$Adv_V^{VANET} = |2Prb[S_0] - 1|. \tag{6.1}$$

Table 6.6: Execution and simulation of various oracle queries

Simulation of *Hash* H for following queries operation: The availability of information about (q, H) in L_H list related to $H(q)$, is returned as hash function H. If not available, then a string $H \in \{0,1\}^{l_H}$ is selected and added (q, H) with L_H. In case availability is made by $\mathcal{A}$, (q, H) then it is added with $L_{\mathcal{A}}$ list.
Simulation of *Reveal*($\mathcal{V}^t$) query is captured as following: Incase, $\mathcal{V}^t$ is implied to be in *accept*, then present common session key K_{shd_i} is generated by $\mathcal{V}^t$ and the same is returned to partner.
Test($\mathcal{V}^t$) simulation is noted as following: By *Reveal*($\mathcal{P}^t$) execution, present session key K_{shd_i} is obtained along with the flipping result b of unbiased coin. K_{shd_i} is returned if flipping results $b = 1$. In other case, returns a randomly formed string out of $\{0,1\}^*$.
Corrupt(P_id_i,*a*) simulation is noted as following: Incase, the value a resulted as 1, the query answers password (PW_i) of P_id_i. For $a = 2$, this returns biometrics key (F_i) corresponding to the biometrics B_i' of P_id_i. Incase, the value a resulted as 3, then secured information SC is returned stored in user smart card.
Execute(P_id_i, S) query simulation is performed as successive manner by simulating *Send* query and performs all the operation required for general authentication.

Game G_1: In this game, the ROR queries i.e. $Send$ and $Execute$ are simulated for the proposed protocol. Table 6.6 describes the simulation of $Send$ and $Execute$

queries. In this game, the lists L_H, L_A, and L_T are also considered. Under the execution of real protocol and ideal conditions, simulation of the games G_1 and G_0 are indistinguishable from each other, so, we have,

$$Prb[S_1] = Prb[S_0]. \tag{6.2}$$

Game G_2: Here, we have considered the total collision probability due to the superposition of hash function and random key over the transmitted traffic between $P_i d_i$ and AS. As per birthday paradox theory, the at most collision probability of H given by query has $\frac{q_H^2}{2^{l_H+1}}$. Then we have,

$$|Prb[S_2] - Prb[S_1]| \leq \frac{(q_s + q_e)^2}{2^{l_r+1}} + \frac{q_H^2}{2^{l_H+1}}. \tag{6.3}$$

Game G_3: With the assumption that H queries are accounted for in the previous (G_2) calculation. So, it is necessary to evaluate the collision probability for other left-over queries. Here, we have considered the total collision probability due to the superposition of the hash function and random key already recorded with the transmitted at SC generation, SC revocation, at login time, password and biometrics change phases are considered. So, we have,

Case 1: For registration-cum-smartcard generation, we have the maximum computed probability $(\frac{5q_H}{2^{l_H}} + \frac{q_s}{2^{l_r}})$.

Case 2: During the login and GAP phases, we have total probability is at most $(\frac{6q_H}{2^{l_H}} + \frac{2q_s}{2^{l_r}})$.

Case 3: Similarly, for biometrics and password change phases, the total probability is at most $(\frac{3q_H}{2^{l_H}} + \frac{2q_s}{2^{l_r}})$.

Considering all the four cases, we have,

$$|Prb[S_3] - Prb[S_2]| \leq \frac{14q_H}{2^{l_H}} + \frac{5q_s}{2^{l_r}}. \tag{6.4}$$

Game G_4: In game G_4, the adversary $\mathcal{A}$ tries to reveal or disclose the user's private credential. As details given [134], [129], guessing of password and biometrics has maximum probability upto $\frac{q_s}{2^{|D|}}$ and $\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\}$ respectively. Since games G_3 and G_4 are identical when there is an absence of a guessing attack, so we have,

$$|Prb[S_4] - Prb[S_3]| \leq \max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \tag{6.5}$$

After executing all games, $\mathcal{A}$ is left with $Prb[S_4]$ probability in guessing the correct bit b. So, we have clearly,

$$Prb[S_4] = 1/2 \tag{6.6}$$

Applying the triangular inequality law, we have the following:

$$\begin{aligned} |Prb[S_0] - \frac{1}{2}| &= |Prb[S_1] - Prb[S_4]| \\ &\leq |Prb[S_1] - Prb[S_2]| + |Prb[S_2] - Prb[S_4]| \\ &\leq |Prb[S_1] - Prb[S_2]| + |Prb[S_2] - Prb[S_3]| \\ &\quad +|Prb[S_3] - Prb[S_4]| \end{aligned} \tag{6.7}$$

From Equations (6.1)-(6.7), we obtain,

$$\begin{aligned} \frac{1}{2}Adv_V^{VANET} &= |Prb[S_0] - \frac{1}{2}| \\ &\leq \frac{(q_s + q_e)^2}{2^{l_r+1}} + \frac{q_H^2}{2^{l_H+1}} + \frac{5q_s}{2^{l_r}} + \frac{14q_H}{2^{l_H}} \\ &\quad + \max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned} \tag{6.8}$$

We can obtain the following if each side of Equation (6.8) is multiplied by 2 and rearranged the expression,

$$\begin{aligned} Adv_V^{VANET} &\leq \frac{q_H^2 + 28q_H}{2^{l_H}} + \frac{(q_s + q_e)^2 + 10q_s}{2^{l_r}} \\ &\quad +2\max\{q_s(\frac{1}{2^{|\mathcal{D}|}}, \frac{1}{2^{l_b}}, \varepsilon_{bm})\} \end{aligned} \tag{6.9}$$

Hence, the theorem is proved.

6.3 Informal Security Scrutiny of Our Proposed Scheme

The primary goal of a credential scheme is to preserve a user's privacy by allowing its user to mask identifying personal attributes in transactions over a network. If a user is registered for a particular service from a service providing body (VANET) then the user has to share credentials with unregistered personnel to get access to

Table 6.7: Computation cost comparison

Phase	At	TEAM [110]	E2TEAM [130]	Ours
Smart card	AS	-	-	$7h(\cdot) + 7\oplus$
Registration	User	-	$3h(\cdot) + 7\oplus$	-
	OBU_i/UT	-	$1h(\cdot) + 1\oplus$	-
	AS	$3h(\cdot) + 2\oplus$	$3h(\cdot) + 3\oplus$	-
Login	OBU_i/UT	$1h(\cdot) + 1\oplus$	$2h(\cdot) + 1\oplus$	$4h(\cdot) + 4\oplus$
GAS	OBU_i/UT	$8h(\cdot) + 5\oplus$	$3h(\cdot) + 4\oplus$	$2h(\cdot) + 9\oplus$
	LE_i	$8h(\cdot) + 7\oplus$	$7h(\cdot) + 6\oplus$	-
Key Update	OBU_i/UT	$6h(\cdot) + 5\oplus$	$4h(\cdot) + 4\oplus$	-
	LE_i	$5h(\cdot) + 6\oplus$	$4h(\cdot) + 4\oplus$	-
SC update	OBU_i/UT	$2h(\cdot) + 3\oplus$	$4h(\cdot) + 3$	$9h(\cdot) + 6\oplus$

Table 6.8: Execution time of cryptographic operation

Operator Name with Description	Runtime in Seconds
$T_{h(\cdot)}$: Hash function 256	11.4e-04
T_{mul}: Scalar multiplication	4.41e-04
T_{pcom}: Packet-1024 comparison	11.4e-03
T_{add}: Addition	4.0e-08
T_{ran}: Random number	2.8e-7
T_{pair}: Pairing	8.202e-03
T_{mtm}: Map-to-map	1.1025e-04

the service. This divulging of user information over any medium causes credential lending, sharing, or transfer [34]. After cryptanalysis, it shows that the user registration and vehicle details are highly dependent on each other in ETEAM and TEAM. In this scenario, a credential lending problem will occur if a vehicle is treated as a common object among users. So, the mentioned schemes are conditioned to suffer from the credential transferability syndrome problem. The proposed scheme has a non-transferability credential-compliant feature. The following sub-section normally reveals that the proposed scheme can tolerate numerous other documented attacks.

6.3.1 Insider Attack

During the registration process, the user U_i gives his credential to the approved security corner (F_i, id_i, pw_i) which is re-written into $(h(F_i), h(id_i), h(pw_i))$ by the

Table 6.9: Comparison of time complexity of for signature verification w.r.t single and group with ECCP, DCS, LPA, NECPA , TEMCE, and Rab_CBA schemes

Scheme name	Single User Verification	Group User Verification
ECCP[126]	$3T_{pair} + T_{mtp} + T_{mul}$	$3nT_{pair} + 11nT_{mul}$
DCS[10]	$5T_{pair} + 3T_{mul}$	$5nT_{pair} + 3nT_{mul}$
LPA[160]	$4T_{pair} + T_{mtp} + T_{mul}$	—-
NECPPA[132]	$3T_{pair} + T_{mtp} + T_{mul}$	$3T_{pair} + nT_{mtp} + nT_{mul}$
TEMCE[64]	$2T_{pcom}$	$2nT_{pcom}$
Rab_CBA	$4T_{add} + 4T_{h.}$	$4T_{add} + 4T_{h.}$

security terminal. The security terminal submits a hashed credential to AS via a secure channel. So, insiders have the visibility of hashed information of id, password and fingerprint only. Thus, the internal operators do not get direct access to the user's credentials, and subsequently, AS can stop insider attacks efficiently and effectively.

6.3.2 Avoidance of Impersonation Attacks

If we assume that an adversary A_i has got the information :$\{m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_{ga}\}$ and $\{m_{i_3}, m_{i_4}, m_{i_5}, m_{i_6}, T_{LE}\}$ during communication between U_i and authentication server. From the retrieved information, unwanted entity can not calculate key P_{AS} from m_{i6} as he is unable to generate or provide f_{i_1}. Therefore, the proposed scheme avoids impersonation attacks.

6.3.3 Avoidance of Disclosure Attack

As the unwanted user does not have general authentication key information as mentioned in step 6.2. Therefore, an adversary will be unable to start the authentication phase, and subsequently, VANET services, key updating, session updating, or secured values will not be revealed. Our scheme also protects relatives, friends, or drivers from disclosing secured information. So, the proposed scheme prevents all possible leak-gate.

6.3.4 Avoidance of Card Lost/Theft Attack

If we assume that an adversary has got user credential $\{f_{i2}, c_{i_{af}}, K_{i_L}, K_{i_A}, P_i, T_{A_r})\}$ in case a smart card is gone out of the hand. From the lost card, the adversary is unable to retrieve *id* and *password* because all information is already stored as hashed from. In another situation, if user credential (*id* and *password*) are shared verbally, then adversary cannot misuse biometrics as it is non-transferable. Therefore, this scheme avoids card lost or theft attacks.

6.3.5 Resistance to Replay Attack

Freshness of message is measured based on dt for all conversations between legitimate sender and receiver for assessing the genuineness of the timestamp, considering too fresh and too old timestamp definition. As each message has a current timestamp as an important component of the message exchanged between AS and user during authentication, the adversary cannot calculate the current timestamp for verifying its authenticity. Therefore, the replay attack condition can be completely avoided in our scheme.

6.3.6 Avoidance of Modification Attack

If an adversary A_i is able to capture the messages M_1:$\{m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_{ga}\}$ and M_2:$\{m_{i_3}, m_{i_4}, m_{i_5}, m_{i_6}, T_{LE}\}$ when user U_i and AS communicate each other. The part m_{i_2} of M_1 and the part m_{i_5} of M_2 judge the user's and AS's validity, respectively. Both parties can check and reject if any part of the message gets modified during conversation based on the available equations at both ends. Therefore, this scheme prevents modification attacks.

6.3.7 Password Guessing Attack

In a hypothetical situation, let us assume that the sensitive information of user U_i has reached an adversary. User credentials, i.e., password and biometrics cannot be calculated in a backward way to obtain the user's sensitive information because the one-way hash function $h(\cdot)$ is not feasible to perform the desired operations. Thus, our scheme is password guessing attack proof.

6.3.8 Denial-of-Service Attack (DoS)

In the proposed scheme, general authentication is initiated automatically once the user finishes login successfully. So, if any user provides the wrong credential, it will be retrieved and rejected to perform the general authentication phase. Therefore, an adversary cannot build a valid session. So, our scheme prevents denial-of-service (DOS) attacks effectively.

6.3.9 Users Anonymity Attack

The credentials like id, password and biometrics of user U_i are never available in the form of plain text, as credentials are always masked by different operations like xor, $concat$, and $hash$ at various stages of the scheme. The user cannot be distinguished at various stages of authentication if an unwanted user gets the smart card in wrong manner. Therefore, user anonymity is ensured in the proposed scheme.

6.3.10 Attacker Model

An adversary is a terminal with the ability to launch an attack to access an unauthorized entry from the system for their self-interest [63]. To evaluate the performance of the proposed protocol in a realistic environment, we have considered the denial-of-service (DOS) attack and the man-in-the-middle (MIM) attack scenarios. DOS and MIM have a very high level of potential to cause havoc in VANET in terms of its safety and performance. Both attacks can lead to cause traffic deadlock condition during an emergency.

Table 6.10: Comparison of security features

Security Protocol with Attribute	TEAM [110]	E2TEAM[130]	Ours
Circumventions dependence on open accessing controls	Y	Y	N
Circumvention by close associates	Y	Y	N
Insider attack resisted	N	Y	Y
Credential cloning attack	N	N	Y
Unintended sharing attack	N	N	Y
Resisted to disclosure attack	N	Y	Y
Resisted to replay attack	N	Y	Y
Resisted to modification attack	NA	NA	Y

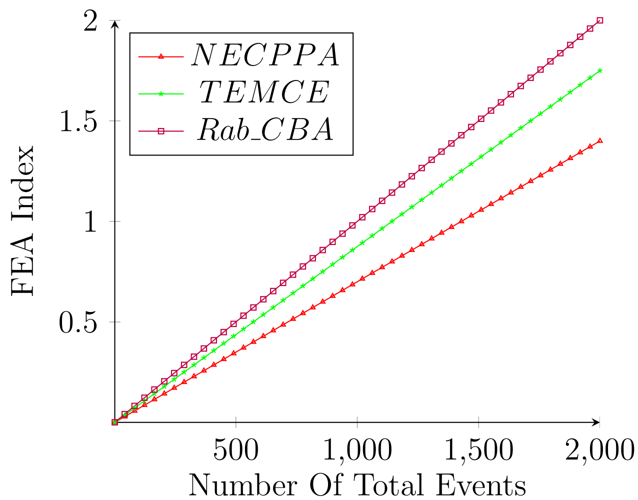

Figure 6.3: FEA index of NECPPA, TEMCE and Rab_CBA

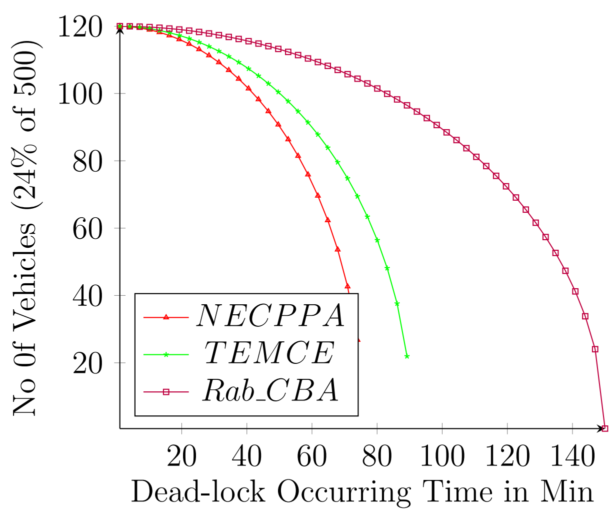

Figure 6.4: Traffic dead-lock profile w.r.t. NECPPA, TEMCE and Rab_CBA

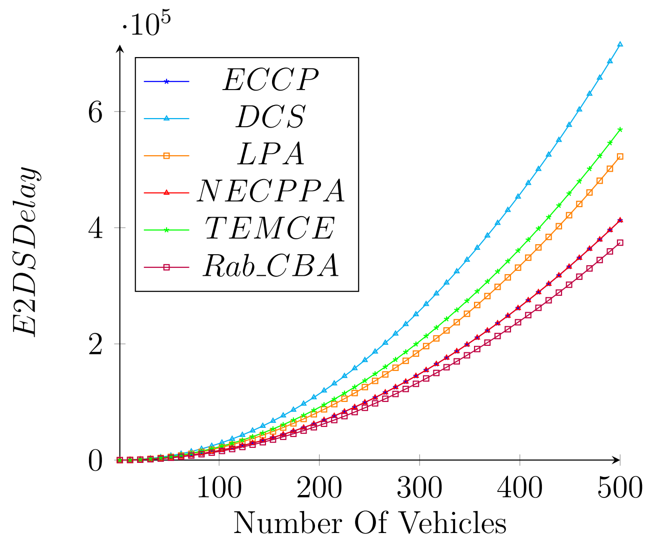

Figure 6.5: E2DS delay of ECCP, DCS, LPA, NECPPA, TEMCE and Rab_CBA w.r.t. individual verification

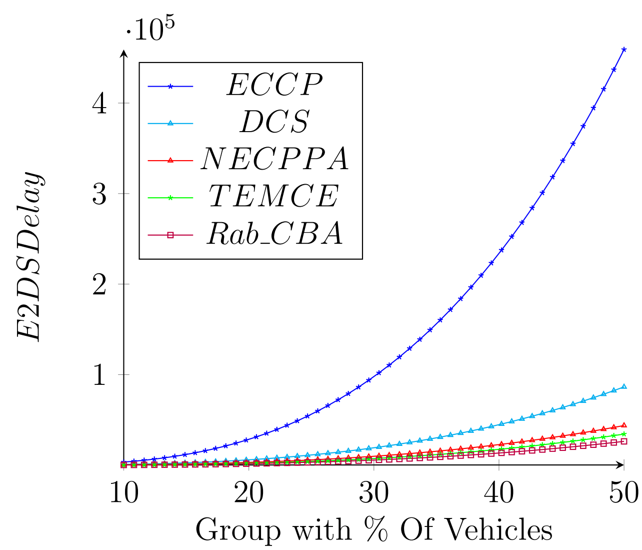

Figure 6.6: E2DS delay of ECCP, DCS, LPA, NECPPA, TEMCE and Rab_CBA w.r.t. group verification

6.4 Result and Discussion of Simulations

In this section, we present the simulation profiles of various matrices and compare our scheme with ECCP [126], DCS [10], LPA [160], NECPPA [132] and TEMCE [64]. The running times of operators with respect to the X2 Ultra Quad-core processor are given in Table 6.8. Table 6.9 shows the signature verification complexity for individual users and group users. In figure 6.3, we have demonstrated the functional availability index profile of NECPPA, TECME and Rab_CBA schemes. We have observed that the FEA index increases proportionately with the increase in total events.

In figure 6.4, we have presented a deadlock tendency profile for NECPPA, TECME and Rab_CBA. The deadlock profile has brought out that NECPPA and TECME have around 50% and 40% fast convergence towards traffic deadlock conditions compared to Rab_CBA protocol. In Figures 6.5 and Figure 6.6, we have presented the E2DS delay profile with respect to individual signature verification and group verification, respectively. It is noted that for both individual as well as group verification, Rab_CBA spends less time for signature verification.

6.5 Performance Comparison and Cost Comparison

Here, we have compared the functionalities and performances of the proposed protocol with recent publications on authentication protocols for VANET[110] and [130]. From the results presented in tables Table 6.7 and Table 6.10, we can say that the proposed protocol solves the security and functionalities limitations of the published protocols. Our proposed protocol is secure, lighter-weight, and supports additional functionalities w.r.t. those discussed protocols.

6.5.1 Comparison of Functionalities

In this section, we have compared various aspects of securities and functionalities, and details of the results are shown in Table 6.10. From this comparison, it is clear that the proposed protocol promises higher security with other requirements for VANET compared to other relevant protocols. This protocol handles with only 22 one-way hash operations presented in Table 6.7 supporting better performance.

6.6 Summary

In this chapter, we have presented an enhanced Rabin cryptosystem method, and it may be noted that the enhanced method is unique and does not lead to decryption failure. Additionally, the biometrics feature is also used for vehicular ad-hoc networks. We have demonstrated that our protocol is lighter-weight as it has less computational complexity compared to many relevant and related protocols. A noted aspect of our protocol is that it is free from credential transferability problems, and a user continues to avail services with a single registration process as user credentials are permanently saved on the user's smart device. We have shown that this protocol has remarkable efficiency and is more appropriate for practical applications where there is a special requirement to support a dynamic platform with limited-power sources, as it is independent of a fixed onboard unit (OBU).

Chapter 7

Blockchain and Fine-grained Access Control

Autonomous smart vehicles have become an integral feature of modern cities. The vehicular ad-hoc network (VANET) is the main pillar of intelligent transport systems (ITS) for safe and comfortable journeys over the road. Government bodies and manufacturing sectors are playing vital roles in implementing ITS features [146]. A system of systems (SOS) of VANET and ITS has a collection of heterogeneously complex cyber and functionally independent systems interconnected over a vast geographical area [165]. Performances and functionalities are aggregated to achieve higher-level, unified goals. The main goal of VANET is to ensure proper security and authentication in real-time for better utilization of various VANET resources and to prevent unauthorized access by attackers. An SOS of VANET and ITS system model for the proposed scheme is depicted in Figure 7.2.

With rapid technological growth, researchers have brought out numerous schemes and protocols for VANET to increase efficiency and effectiveness. However, most of the work was done for peer-to-peer delivery to prevent dynamic attacks in centralized form [114]. Recently, blockchain-based VANET has become an interesting field of research, and researchers have also found great potential to add more functional values to ITS and VANET [133]. Parallelism and decentralization are the main working principles in blockchain technology.

Most of the research work for blockchain-based VANET has been concentrated on blockchain design. Therefore, there is a need to exploit the possible extent to utilize the benefits of parallel computing and the authentication process of VANET.

In this chapter, we propose lightweight blockchain-based secure authentication and fine-grained access control for VANET using the promising features of blockchain technology. VANET authentication and a proper algorithm are used to measure the trustworthiness of messages and nodes after successful authentication by the respective RSU. So, a suitable blockchain should be designed to realize the real decentralization of VANET features.

7.0.1 Overview of Blockchain

Recently, several studies have been incorporated to address security and privacy issues in VANET. However, the majority of the work could not use the full potential of blockchain to the maximum extent possible. Lu et al. [105] proposed the BPPA protocol for trusted authority (TA) to make it transparent and more verifiable by storing all transactions & certificates in blockchain. However, this protocol adds more computational overhead to process multiple certificates. Lie et al. [96] proposed a key management scheme using the decentralized feature of blockchain. Arora et al. [16] presented an authentication and data sharing scheme using blockchain technology. However, the protocol supports vehicle registration by a centralized authority, and it cannot effectively prevent single-point failure issues. Leiding et al. [97] presented a smart contract-based protocol to provide fair and autonomous services in a centralized manner. Singh et al. [143] presented the IV-TP protocol using blockchain technology and an intelligent vehicle communication system, but this protocol cannot provide proper data security in VANET. Dorri et al. [56] proposed a vehicle networking system using blockchain to provide automotive security and general participation from manufacturers and service providers over blockchain. However, this scheme cannot prevent delay and failure in cases where central and cluster nodes get damaged. Zang et al. [164] proposed the BAVC protocol to address major issues faced by various blockchain-based VANET protocols. However, it does not ensure proper forward and backward secrecy functional requirements. Lin et al. [101] proposed the BCPPA protocol to minimize frequent interaction and private key revocation in a secured way. However, this scheme is unable to achieve the expected efficiency for signing and verifying users. We propose blockchain-based authentication in VANET with access control to ensure parallel computing and compliance with various known security challenges efficiently. Figure

7.1 depicts the architecture and various building blocks of the proposed scheme.

Table 7.1: Comparison of functionality features

Protocol	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8	ϕ_9	ϕ_{10}
Hao *et al.* [74]	✓	✓	✓	**X**	**X**	**X**	**X**	✓	✓	**X**
Lu *et al.* [104]	✓	✓	**X**	✓	**X**	**X**	**X**	**X**	✓	**X**
Lie *et al.* [96]	✓	✓	✓	✓	**X**	**X**	✓	✓	✓	**X**
Dorri *et al.* [56]	✓	✓	✓	✓	✓	**X**	✓	✓	✓	**X**
Feng *et al.* [65]	✓	✓	✓	✓	✓	✓	**X**	**X**	**X**	**X**
Zang *et al.* [164]	✓	✓	✓	✓	✓	✓	✓	✓	✓	**X**
Lu *et al.* [105]	**X**	**X**	✓	✓	✓	✓	✓	✓	**X**	**X**
Keyur *et al.* [105]	✓	✓	✓	✓	✓	✓	**X**	✓	✓	**X**
Proposed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

ϕ_1 : provides mutual authentication; ϕ_2 : flawless password change phase; ϕ_3 : resists server spoofing attack; ϕ_4 : resists man-in-the-middle attack/replay attack; ϕ_5 : resists privileged-insider attack; ϕ_6 : strong user anonymity; ϕ_7 : resists session-specific temporary information attack; ϕ_8 : resists DoS attack; ϕ_9 : resists key-compromised impersonation (K-CI) attack; ϕ_{10} : perfect forward-backward secrecy;

7.0.2 Our Contributions

Here, we propose lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users. The major contributions of the proposed scheme are as follows:

- We have proposed lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users that is able to address major security threats more efficiently with high scalability.
- We have defined a framework with edge computing and mobile edge computing to offload computation-intensive tasks as well as optimize data processing before sending it to a blockchain-based VANET network.
- In LBAFA, we have incorporated blockchain technology to introduce decentralization and parallel computing over the traditional centralized VANET.

- We have used ECC to optimize the computation cost and CP-ABE to impose access control over the data in a fine-grained manner based on user attributes.
- We have done rigorous security analysis using BAN logic and Proverif tools.

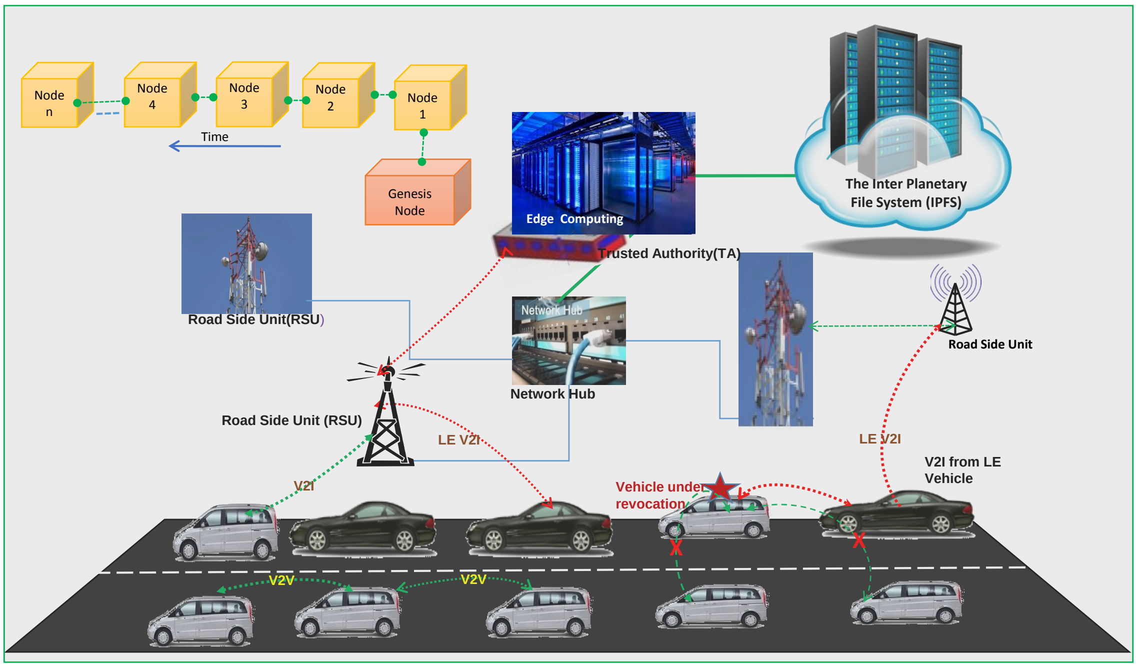

Figure 7.1: Proposed VANET architecture with blockchain.

7.1 Proposed Architecture and SOS Overview

The main components of the proposed blockchain-enabled VANET are shown in Figure 7.1. The architecture mainly consists of seven elements: edge computing (EC), mobile edge computing (MEC), inter-planetary file system (IPFS), vehicle, mobile law executor (MLE), roadside unit (RSU), and trusted authority (TA). The features and functionality are explained below in detail.

7.1.1 System Model and Components

In the proposed scheme, seven entities are involved, and the entities have various roles and functionalities. In Figure 7.1 different communication setups among net-

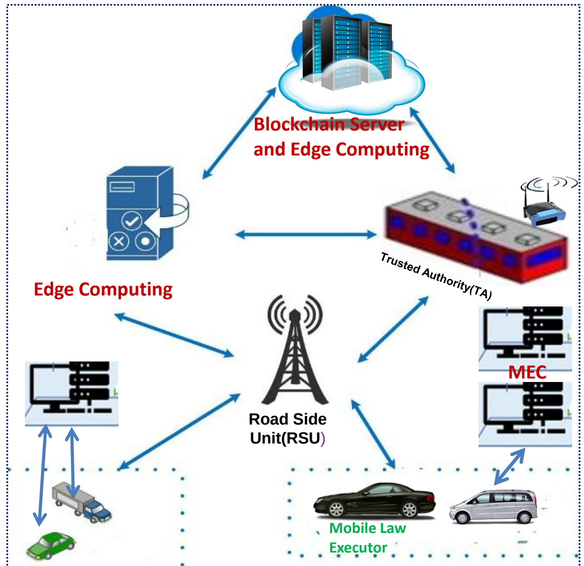

Figure 7.2: VANET and ITS system model.

work entities are depicted.

Edge Computing

The edge computing component provides an important function to achieve parallelism in a decentralized way and offloading of complex work and computation. Because of limited resources, RSUs may experience network performance and computation delays if all transactions in the consensus work of the blockchain are executed by the RSUs. Therefore, this proposed scheme achieved parallel computation and fast processing by offloading the intensive, time-consuming computation work to edge computing.

Mobile Edge Computing

A high volume of transactional data is produced in the VANET environment. The network performance will be affected, and a high delay will also be added if all the blockchain consensus processing is executed by RSUs. Therefore, our scheme offers the functionality to offload intensive computational jobs to dynamic MEC, and the final result is shared with RSU. Thus, this also prevents the effects of RSU failure issues.

IPFS

IPFS is a distributed global data storage solution for large-scale persistent data storage. It is a peer-to-peer (P2P) decentralized file system to communicate static and mobile edge computing features of a blockchain-based VANET system. This file system can combine block exchange incentives (BCE), distributed hash tables (DHT), and self-certified namespaces. It inherently can avoid single-point failure issues [158].

Vehicle

Vehicles are considered data producers and consumers. Due to resource limitations, vehicles share transactional data with IPFS through RSU.

Mobile Law Executor

Mobile law executors are trustworthy vehicles (TV). The MLEs are generally considered to be trustworthy by default. An MLE can be defined as authorized public transportation or police vehicles that are equipped with MEC and mobile TA-enabled features. The MLE helps TA to authenticate vehicles other than LE that can participate in the blockchain network after successful authentication.

RSU

RSU is a roadside static unit deployed along the roadside, and it is equipped with a high-end processing system and networking setup. RSUs are considered nodes of the blockchain and are used as proxy nodes for vehicles to share data in IPFS. Most of the high computation extensive processing is executed by edge computing and MEC for the respective RSU.

Law Executor and Trusted Authority

The major responsibility of trusted authorities (TA) cum *LE* is to perform registration of RSUs and vehicles within a defined area. It also carries out various computation-intensive data processing tasks with the help of edge computing. Whereas, the mobile law executor is responsible for authorizing vehicles and RSUs for a small area of coverage.

7.1.2 Elliptic Curve Cryptography

We have used numerous mathematical notations in this chapter to explain the proposed protocol, and details are described in Table 7.2. The collision-resistant SHA-1 [7] is used as one-way hash function.

Let us assume p is prime order, where $p > 3$ and F_p is a finite field. Then the non-singular elliptic curve E can be defined by equation
$y^2 = (x^3 + ax + b) \bmod p$, where $a, b \in F_p$
satisfying $(4a^3 + 27b^2) \bmod p \neq 0$ with the following properties.
(i) It forms a cyclic abelian group G with $E_p(a, b)$ and $\bmod p$ additive operations.
(ii) If G is generator and $P \subset G$ having order n
Let Z is a set of natural number of order n
$Z = 1, 2, 3, ..., n - 1$
$H(\cdot)$ is defined as a collision-resistant one-way hash function.
$H : 0, 1 \rightarrow Z$

7.2 The Proposed Blockchain Based Authentication Scheme

In this section, we present our concept of proposed ECC-based authentication and CP-ABE fine-grained access control for participating in blockchain. This scheme includes five major steps that are presented below:

7.2.1 Vehicle Registration Phase

The interested new and legal vehicle gets registered by the trusted authority (TA) in a secure way. The following steps are carried out by the TA as well as the legitimate party for participating in blockchain transactions and successful registration.

- **i:** Vehicle selects Sk_{v_i}, identity Id_{v_i}, biometric features F_i and a 128 bit random number x_a and sends to TA as $H(Sk_{v_i})$, $H(Id_{v_i})$, $H(F_i)$, $H(x_a)$.

- **ii:** Trusted authority computes the public key $Pk_{v_i} = Sk_{v_i} \cdot P$ and pseudo-identity & credential $PId_{v_i} = Id_{v_i} \cdot P$, $PF_i = F_i \cdot P$. TA further calculates

Table 7.2: Mathematical notations and other symbols used to explain the protocol.

Symbol	Description
$H(\cdot)$	Collision-resistant one way hash function
F_p	Finite field of order
Z	Set of natural number
E	Elliptic curve
G	Cyclic abelian group
TA	Trusted authority
Sk_{v_i}	Secret key of vehicle i
Pk_{v_i}	Public key of vehicle i
Id_{v_i}	Identity vehicle i
PId_{v_i}	Pseudo-identity of vehicle i
Sk_{RSU_i}	Secret key of RSU_i
Id_{RSU_i}	Identity of RSU i
Pk_{RSU_i}	Public key of RSU_i
PId_{RSU_i}	Pseudo-identity of RSU_i
Trs_i	Timestamp of RSU_i
$Rpos_i$	Positional information of RSU_i
$Rpos_i$	Reputation index of vehicle i
Pk_{vx}	Public key for broadcast message
Sk_{RSU_i}	Secret key for broadcast message
SCE_i	Event shared by vehicle i

the following
$S_k = h(h(F_i||Id_{v_i})||h(F_i||pw_i)) \bmod p$
$f_{i1} = h(F_i||Id_{v_i}) \oplus x_a$
$f_{i2} = h(h(F_i||Id_{v_i})||h(F_i||pw_i)||x_a)$
$K_{i_L} = (P_{k_{i1}}||T_{A_r}) \oplus (f_{i1}||h(F_i||pw_i)) \bmod p$
$K_{i_A} = (P_{k_{i2}}||T_{A_r}) \oplus K_{i_L} \oplus (f_{i1}||h(F_i||pw_i)) \bmod p$
TA shares to other RSUs and stores the following information for future computation $\{PId_{v_i}, (PId_{v_i}||P_{k_{i1}}) \oplus h(x_a)\}$ and $\{(PId_{v_i}||P_{k_{i2}}) \oplus h(x_a)\}$ values specific to the vehicle PId_{v_i}

- **iii:** After successful registration, TA decides the list of access attributes Ap_{v_i}

and stores details of the vehicle's parameter record, including reputation status as $VR_i =< PId_{v_i}, E_{S_k}\{f_{i1}, f_{i2}, K_{i_L}, K_{i_A}, T_{A_r}, Ap_{v_i})\}, Rpt_i >$ and the same record is stored in the memory chip of the vehicle.

- **iv:** The trusted authority updates the blockchain to activate the newly added vehicle for participating in the blockchain transactions, and subsequently, registration parameters are shared with the vehicle for future requirements.

7.2.2 RSU Registration Phase

In the proposed scheme, RSU is considered as a real blockchain node that is less attack-prone and works as a proxy node for the vehicles within its range. However, for successful registration, the following computations are carried out by TA.

- **i:** Vehicle selects Sk_{RSU_i} and identity Id_{RSU_i} and sends to TA as $H(Sk_{RSU_i})$, $H(Id_{RSU_i})$.
- **ii:** TA computes the public key $Pk_{RSU_i} = Sk_{RSU_i} \cdot P$ and the pseudo-identity $PId_{RSU_i} = Id_{RSU_i} \cdot P$
- **iii:** After successful registration, TA stores details of RSU including its positional information, as $SRUR_i =< PId_{RSU_i}, Pk_{RSU_i}, Trs_i, Rpos_i >$ and updates the blockchain with the newly added RSU_i as new blockchain node.

7.2.3 RSU Authentication Phase

RSU_i initiates the authentication process by sending message M_{RSU-TA}. M_{RSU-TA} and this is prepared as follows:

- **Step i:** The RSU_i acquires authentication code Aut_i and its current timestamp $Trsu_{ij}$ & culculates $Aut_{iH} = H(Aut_i)||PId_{RSU_i}||Trs_i)$ and sends it TA_i as $M_{RSU-TA} =< Aut_{iH}, PId_{RSU_i}, Trsu_{ij}, Aut_i >$

- **RSU authentication:** TA_i retrieves RSU_i information using PId_{RSU_i}. First, the TA_i acquires the current timestamp T_{TA} and performs the following: TA_i calculates with retrieved information $Aut'_{iH} = H(Aut_i)||PId_{RSU_i}||Tru_{ij})$ $dt = T_{TA} - Trsu_{ij}$

and check if $Aut'_{iH} \stackrel{?}{=} Aut_{iH}$ & $dt_{min} <= dt <= dt_{max}$ hold. If it passes the check, TA_i accepts the authentication code Aut_i and allows PId_{RSU_i} to participate in transactions.

7.2.4 Vehicle Authentication Phase

- **Step i:** We assume that RSUs are legal entities and can authenticate with the help of TA with minimum communication. Initially, the following are calculated to initiate authentication by RSU on behalf of TA:
  (i) $m_{i_1} = (f_{i1}||h(F_i||pw_i) \oplus r_i$
  (ii) $m_{i_2} = (f_{i1}||T_{A_r}||T_l||r_i)$
  (iii) $v_{p_{i1}} = P_{k_{i1}}||T_{A_r} = K_{i_L} \oplus (f_{i1}||h(F_i||pw_i))$
  (iv) $P_{k_{i1}} = v_{p_{i1}} \ominus T_{A_r}$

  PId_{v_i} requests authentication from the RSU by sending
  $M_1 = (E_{P_{k_{i1}}}\{PId_{v_i}, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, PId_{v_i})$

- **Step ii:** RSU Receives message $\{M_1\}$ and calculates the following
  (i) AS calculates $dt = T_{LE} - T_l$
  Checks if $dt_{min} <= dt <= dt_{max}$
  On timestamp validity, RSU calculates further to form M_2
  (ii) $v = (P_{k_1}||T_{A_r}) \oplus K_{i_L}$
  and retrieves r_i as $r_i = m_{i_1} \oplus v$
  (iii) $m'_{i_2} = (f_{i1}||T_{A_r}||T_l||r_i)$
  check if $m_{i_2} \stackrel{?}{=} m'_{i_2}$
  and on matched RSU further calculates
  (iv) $m_{i_3} = v \oplus r_{LE}\ mod\ p$
  (v) $m'_{i_5} = (P_{k_{i1}}||T_{A_r}||r_i||r_{LE}||T_{LE}||K_{i_A})\ mod\ p$
  $m_{i_5} = h(m'_{i_5})$
  (vi) $m_{i_6} = m_{i_5}||(P_{AS} \oplus f_{i_1})||T_{A_r}\ mod\ p$
  and preapres response message to vehicle
  $M_2 = E_{P_{k_{i2}}}\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}$

- **Step iii:** The vehicle receives the message $\{M_2\}$ and calculates
  (i) PId_{v_i} retrieves $P_{k_{i2}}$ to decrypt the received M_2

as: $v_{p_{i2}} = K_{i_A} \oplus K_{i_L} = (P_{k_{i2}}||T_{A_r})$
$P_{k_{i2}} = v_{p_{i2}} \ominus T_{A_r}$
(ii) Retrieves r_{LE} as $r_{LE} = m_{i_3} \oplus (f_{i1}||h(F_i||pw_i))$
(iii) From smart card information, the user calculates,
$m''_{i_5} = (P_{k_{i1}}||T_{A_r}||r_i||r_{LE}||T_{LE}||K_{i_A}) \mod p$ and $h(m''_{i_5})$ and verifies equality with m_{i_5}
(iv) Retrieves P_{AS} using f_{i1} and m''_{i_5}
as: $v_{p_{i3}} = m_{i_6} \ominus m''_{i_5} \ominus T_{A_r} = (P_{AS} \oplus f_{i_1})$
$P_{AS} = v_{p_{i3}} \oplus f_{i_1}$
(v) Computes the shared secret key for a defined session
$K_{shd_i} = h((P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_l)$

- **Step iv:** Finally, RSU computes the shared secret key K_{shd_i} independently and passes it to TA for communication over blockchain participation

7.2.5 Participation in Blockchain Using CP-ABE

- **Initial Setup Phase:** We assume that RSUs are legal entities and can authenticate with the help of TA in coordination with edge computing (EC) and blockchain with minimum communication. For any event, it has two levels of encryption: one by vehicle (DG) and another by RSU. Similarly, the original event is decrypted by RSU and the vehicle (DR). RSU computes the following with the help of EC. It selects $s,\ \alpha\ \&\ \beta$ randomly and computes public parameters. $P_\alpha = \alpha \cdot G$ $P_\beta = \beta \cdot G$ $P_s = s \cdot G$ $T_i = t_i \cdot G$ for all $a_i \in A$, Where $\{A\}$ is global attribute set. Finally, RSU prepares the system master public key parameters $P_{kp} = (A, P_s, T_i, H, G)$ and master secret key parameters $SM_{kp} = (\alpha, s, \{t_i \in Z_p : i \in A_p\})$

- **Encryption Step by Data Generator (DG):** The following computation is done to encrypt message m. Let us assume each DG maintains two attributes $At_{ri}, At_{rj} \in A_r$ of RSU and $T_{ir}, T_{jr} \in Z_p$. DG uses its shared secret key K_{shd_i} generated after successful authentication by TA.
$C_{sh} = K_{shd_i} \cdot G$
$C_n = q_n(0).G, -> (k_x, k_y)$
$C_i = (T_{ir} + T_{jr})/T_iT_j \cdot G$

$D_i = (T_{ir} + T_{jr})/T_iT_j$
$C_1 = C_{sh} + C_n + D_i \cdot P_s$
$C_m = E_{k_x}(m) \& C_s = H(m, k_y)$
Cipher text $CT_{DG} = (C_1, C_i, C_m, C_s)$

- **Decryption Step RSU:** To decrypt the public key and master key, RSUs are considered. RSU calculates the shared secret key K'_{shd_i} and further calculates.
  $C_n = C_1 - (s.C_i - C'_{sh})$
  $= C_{sh} + q_n(0).G + D_i \cdot s \cdot G - (s.(T_{ir} + T_{jr})/T_iT_j \cdot G + C'_{sh})$
  $= q_n(0).G$
  Therefore, $q_n(0) \cdot G- > (k_x, k_y)$ and RSU gets (k_x, k_y) and subsequently retrieve m.

- **Encryption Step by RSU:** First, the original message m is retrieved by RSU. Then the following computation is done by RSU to re-encrypt with coordination with TA and EC and made it available as a transaction in the blockchain. RSU randomly selects a polynomial q_x for each node x in the users access tree τ corresponding to access policy ψ. Let d_x denote the degree of the q_x and th_x threshold value of the node. So, we have $d_x = th_x - 1$. The root node value is set $q_r(0) = a$ by RSU. a is chosen randomly, where $a \in Z_p$. RSU also selects others dR points randomly to build the polynomial qR uniquely with completeness. For other nodes x (leaf nodes and non-leaf nodes), RSU sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses other dx points randomly to define properly and uniquely the polynomial q_x for the access tree τ. Let ω be a set of leaf nodes of the access tree τ. RSU carries out encryption under the access policy ψ. The following is calculated.
  $Y = a.P_s- > (a_x, a_y)$, where $Y \neq O$
  $C_m = E_{a_x}(m) \& C_{sint} = H(m, a_y)$
  $C_2 = q_x(0) \cdot T_i, i \in \omega$
  Cipher text $CT_{RSU} = (\tau, C_m, C_{sint}, C_2)$

- **Key Generation Step:** In this step, the RSU receives the list of attributes λ from DR whose identity is PId_{v_i} considering its own master key SM_{kp} and generates decryption keys. First, it checks the validity of λ and further calculates D_i for each attribute $i \in \lambda$ as
  $D_i = H(PId_{v_i}).s.(t_i)^{-1} : i \in \lambda.$

- **Decryption Step by Data Receiver:** This step is executed by DR, by considering $CT_{RSU} = (\tau, C_m, C_{sint}, C_2)$ and D_i. To decrypt the public key, master key, and set of user attributes, $\{\lambda\}$ are considered. If $\tau(\lambda) = 1$ i.e. if λ attribute set is accepted by access tree then polynomial is calculated by the language interpolation formula, and finally a is retrieved. The polynomial is computed recursively as

$$\begin{aligned} f(x) &= \sum_{v \in ch_x} D_j \prod_{i=m, j \neq m}^{d_x} \frac{(x_m - x)}{(x_m - x_j)} \\ f(0) &= \sum_{v \in ch_x} D_j \prod_{i=m, j \neq m}^{d_x} \frac{(x_m - 0)}{(x_m - x_j)} \\ f(0) &= a \end{aligned}$$

Where, D_j langrage coefficient, $j, m = index(v)$, $m \neq j$ for all $v \in ch_x$

Therefore, the evaluation of root node of the access tree is $q_r(0) = a\ y.G- > (a_x, a_y)$. The original message can be retrieved from c_m using a_x and message integrity is ensured by retrieving a_y.

- **Proof of Correctness:** The function $decryptnodeKey(T_{RSU}, D_i, x)$ is used recursively by this algorithm, and it takes CT_{RSU} and D_i. For leaf node x and $i = attr(x)$, the function $decryptnodeKey()$ is evaluated as

$$\begin{aligned} decryptnodeKey(T_{RSU}, D_i, x) &= \begin{cases} \frac{D_i.C_2}{H(PId_{v_i})} & \text{for } \forall i \in \lambda \\ Null & Otherwise \end{cases} \\ &= \frac{H(PId_{v_i}) \cdot s \cdot (t_i)^{-1} \cdot q_x(0) \cdot T_i}{H(PId_{v_i})} \\ &= s \cdot (t_i)^{-1} \cdot q_x(0) \cdot t_i \cdot G \\ &= q_x(0) \cdot s \cdot G \end{aligned}$$

For non-leaf node x, the decryptnodeKey() is computed recursively for its all child node using the language interpolation formula as follows:

$$decryptnodeKey(T_{RSU}, D_m, x) = \sum_{v \in ch_n} D_j(0) \cdot decryptnodeKey(T_{RSU}, D_m, v)$$

Where, D_j langrage coefficient, $j, m = index(v)$, $m \neq j$ for all $v \in ch_x$.

$$\begin{aligned} decryptnodeKey(T_{RSU}, D_m, x) &= \sum_{v \in ch_n} D_m(0) \cdot q_v(0) \cdot s \cdot G \\ &= \sum_{v \in ch_n} D_m(0) \cdot q_{parent(v)}(index(v)) \cdot s \cdot G \\ &= \sum_{v \in ch_n} D_m(0) \cdot q_x(m) \cdot s \cdot G \\ &= q_x(0) \cdot s \cdot G \end{aligned}$$

Therefore, the function $decryptnodeKey(T_{RSU}, D_i, x)$ results the same as $(q_x(0) \cdot s \cdot G)$ irrespective of leaf node or non-leaf node. Similarly, the computation can be done for the root as $decryptnodeKey(T_{RSU}, D_i, root) = q_{root}(0) \cdot s \cdot G$ or $Y = a.P_s$, finally $Y- > (a_x, a_y)$ & $m = Dec_{a_x}(C_m), C'_{sint} = H(m, a_y)$. The eqality of C_{sint} and C'_{sint} proves the integrity of the decrypted message. Therefore, the three main security requirements like confidentiality, integrity and authenticity are ensured by the proposed scheme.

Table 7.3: Notations and their meaning in BAN logic

Notations	Meanings and Description
$Q \overset{K}{\leftrightarrow} R$	The key K is shared only between Q and S and userd for communication
$Q \overset{S}{\rightleftharpoons} R$	The secret S is known only to Q and R and principals trusted by them
$Q\| \equiv S$	Q Believes that the statement S is true
$Q \triangleleft S$	Q sees the statement S
$\#(S)$	S is considered to be fresh
$Q\|\| \sim S$	Once, S was said by Q
$Q \Rightarrow S$	Q has control over S
$\langle S \rangle_T$	Formula S and T get combined together
K_i	Session key between user $P_i d_i$ and AS

7.2.6 Formal security analysis by BAN Logic

Logical flaws in a protocol can be unearthed by BAN logic during the mutual authentication of two communicating parties over a network. The derivation of BAN logic

Table 7.4: Notations used to describe proposed scheme

Symbols	Descriptions
AS	Authentication server
U_i	i^{th} user
$\ominus$	Operation to discard a string from string concatenation of two or more values $(A\|\|B) \ominus B = A$
$h(\cdot)$	Secured one-way hash function
$\oplus$	Exclusive XOR operation
$A\|\|B$	String concatenation operator
$E_K(M)$	Encrypt M using key K
$D_K(M)$	Decryp M using key K
x	AS's master secret key
P_id_i	Pseudoidentity of user U_i
r_i	Random number of 128 bits generated at the user side during registration phase
x_a	Random number of 128 bits generated at the AS side during registration phase
r_{LE}	Random number of 128 bits generated at the AS side during general authentication phase (GAP)
B_i'	Biometrics features of 1024 bits
T_{A_r}	Timestamp at the time of user registration phase at the AS side
T_l	Timestamp at the time of login at the user side
T_{LE}	Timestamp at the reception of login message at the AS side
$P_{k_{i1}}$	Keys generated by AS during registration phase for U_i
$P_{k_{i2}}$	Key generated at AS by random number generator (RNG) used for mutual authentication at general authentication phase (GAP)
P_{AS}	Key generated at the AS side during GAP

shows that our proposed scheme satisfies the authentication goals. The notations of BAN logic and the contextual meaning are briefly written in Table 7.3.

The logical postulates of BAN logic are expressed in terms of a set of rules as briefly presented below [109], [147].

- **Rule1(RL1):** Rule for meaning of message. $\frac{Q\mid\equiv R\overset{K}{\rightleftharpoons}Q, Q\triangleleft\langle S\rangle_K}{Q\mid\equiv R\mid\sim S}$.
- **Rule2(RL2):** Rule for nonce verification. $\frac{Q\mid\equiv\#(S), Q\mid\equiv R\mid\sim S}{Q\mid\equiv R\mid\equiv S}$.
- **Rule3(RL3):** Rule for freshness conjunctenation. $\frac{Q\mid\equiv\#(S)}{Q\mid\equiv\#(S,T)}$.
- **Rule4(RL4):** Rule for jurisdiction control. $\frac{Q\mid\equiv R\Rightarrow S, Q\mid\equiv R\mid\equiv S}{Q\mid\equiv S}$
- **Rule5(RL5):** Rule for simplification (Additional Rule). $\frac{Q\mid\equiv\#(S,T)}{Q\mid\equiv S}$, $\frac{Q\triangleleft S,T)}{Q\triangleleft S}$, $\frac{Q\mid\equiv R\mid\sim(S,T)}{Q\equiv R\mid\sim S}$

As per the proposed protocols, the following goals must be satisfied to verify its authentication proof.

Goal 1: $AS| \equiv \{P_i d_i \overset{K_{shd_i}}{\longleftrightarrow} AS\}$

Goal 2: $P_i d_i| \equiv \{P_i d_i \overset{K_{shd_i}}{\longleftrightarrow} AS\}$

Goal 3: $P_i d_i| \equiv AS| \equiv \{Access\_Policy\}$

In this protocol scheme, the following generic messages are exchanged between user $P_i d_i$ and authentication server AS.

M1: $P_i d_i \rightarrow AS$:$(E_{P_{k_{i1}}}\{P_i d_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, P_i d_i)$

M2: $AS \rightarrow P_i d_i$:$E_{P_{k_{i2}}}\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}$

The messages M1 and M2 are idealized and reproduced as below.

M1(Idealized): $\{P_i d_i, f_{i1}, m_{i_1}, m_{i_2}, K_{i_L}, K_{i_A}, T_l\}, \{P_i d_i \overset{E_{P_{k_{i1}}}}{\longleftrightarrow} AS\}$,

M2(Idealized): $\{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}, \{AS \overset{E_{P_{k_{i2}}}}{\longleftrightarrow} P_i d_i\}$,

Where,

$$m_{i_1} = (f_{i_1}||h(pw_i)) \oplus r_i \tag{7.1}$$

$$m_{i_2} = (f_{i_1}||T_{A_r}||T_l||r_i) \tag{7.2}$$

$$m_{i_3} = v \oplus r_{LE} = (P_{k_{i1}}||T_{A_r}) \oplus K_{i_L} \oplus r_{LE} \tag{7.3}$$

$$m_{i_5} = v = (P_{k_{i1}}||T_{A_r}) \oplus K_{i_L}||r_i||r_{LE}||T_{LE}||K_{i_A} \tag{7.4}$$

$$m_{i_6} = m_{i_5}||(P_{AS} \oplus f_{i_1})||T_{A_r} \tag{7.5}$$

$$K_{shd_i} = h(P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_l) \tag{7.6}$$

The following assumptions can be made as per the proposed protocol scheme.

1. $P_i d_i| \equiv \#T_l$
2. $AS| \equiv \#T_{LE}$
3. $AS| \equiv P_i d_i \Rightarrow (id_i, F_i, pw_i)$
4. $P_i d_i| \equiv AS \Rightarrow (T_{A_r}, K_{i_L}, K_{i_A})$
5. $P_i d_i| \equiv F_i$
6. $P_i d_i| \equiv id_i$

7. $P_id_i| \equiv pw_i$
8. $P_id_i| \equiv P_id_i \stackrel{K_{i_L},K_{i_A},P_{AS}}{\rightleftharpoons} AS$
9. $AS| \equiv P_id_i \stackrel{K_{i_L},K_{i_A},P_{AS}}{\rightleftharpoons} AS$
10. $P_id_i| \equiv AS \Rightarrow (K_{i_L}, K_{i_A}, T_l))$
11. $P_id_i| \equiv P_id_i \stackrel{m_{i_1},m_{i_2}}{\rightleftharpoons} AS$
12. $AS| \equiv P_id_i \stackrel{m_{i_1},m_{i_2}}{\rightleftharpoons} AS$
13. $P_id_i| \equiv K_{i_L}$
14. $P_id_i| \equiv K_{i_A}$
15. $P_id_i| \equiv T_{LE}$
16. $P_id_i| \equiv P_{AS}$
17. $P_id_i| \equiv T_{A_r}$
18. $P_id_i| \equiv AS \Rightarrow Access\_Policy$
19. $P_id_i| \equiv U_i \stackrel{Access\_Policy}{\rightleftharpoons} AS$
20. $P_id_i \triangleleft \{Access\_Policy\}_{Biometric}$
21. $P_id_i| \equiv \#(Access\_Policy)$

We show the derivation of goals using fundamental postulates of BAN logic, assumptions based on proposed protocols, and idealized forms of messages exchanged among parties

Derivation of Goal 1

- D1: $AS \triangleleft \{T_l, m_{i_1}, m_{i_2}, \{P_id_i \stackrel{E_{P_{k_{i1}}}}{\longleftrightarrow} AS\},$
  $\{P_id_i \stackrel{E_{P_{k_{i2}}}}{\longleftrightarrow} AS\}\}$

- D2: Using RL5, $AS \triangleleft \{\{P_id_i \stackrel{E_{P_{k_{i1}}}}{\longleftrightarrow} AS\}, \{U_i \stackrel{E_{P_{k_{i2}}}}{\longleftrightarrow} AS\}\}$

- D3: $AS| \equiv \#(T_l)$

- D4: From assumption (9) and (RL1) $AS| \equiv P_i d_i| \sim (K_{i_L}, K_{i_A}, P_{AS})$
- D5: Using (RL2), D3 and D4 $AS| \equiv U_i| \equiv (K_{i_L}, K_{i_A}, P_{AS})$
- D6: From assumption (9) and (17) $P_i d_i| \equiv AS \Rightarrow T_{A_r}$
  $P_i d_i| \equiv AS| \equiv T_{A_r}$ As per (RL4) $P_i d_i| \equiv T_{A_r}$
- D7: From D1 and (RL5) $AS \lhd m_{i_1}$ and $AS \lhd m_{i_2}$
- D8: From D1 and applying (RL5) $AS \lhd T_l$ and $AS \lhd f_{i_i}$
- D9: $AS| \equiv P_i d_i \sim (f_{i_i}, T_l)$
- D10: From D3 and D9 we get $AS| \equiv P_i d_i| \equiv (f_{i_i}, T_l)$
- D11: Combination of D5, D6 and D10 result in $AS| \equiv U_i \xleftrightarrow{K_{shd_i}} AS$ **Goal 1** as $K_{shd_i} = h((P_{AS} \oplus f_{i_1})||T_{A_r}||K_{i_L}||K_{i_A}||T_l)$

Derivation of Goal 2

- D12: $P_i d_i \sim \{m_{i_3}, m_{i_5}, m_{i_6}, T_{LE}\}_{rLE}$
- D13: From D12, using (RL5) $P_i d_i| \sim m_{i_5}$
- D14: From equation (6) $U_i \lhd \{P_{AS}, f_{i_1}, T_{A_r}\}$
- D15: Using assumption (8) and D14 $P_i d_i| \sim AS\{P_{AS}, f_{i_1}, T_{A_r}\}$
- D16: From assumption (2) and D15 we get, $P_i d_i| \equiv AS \equiv \{P_{AS}, f_{i_1}, T_{A_r}\}$
- D17: From Assumption (8) $P_i d_i| \equiv \{P_i d_i \xleftrightarrow{K_{i_L}} AS, P_i d_i \xleftrightarrow{K_{i_A}} AS\}$
- D18: Using D1, D3 and D17 $P_i d_i| \equiv AS| \equiv \{K_{i_L}, K_{i_A}\}$
- D19: Combination of D10, D16 and D18 using (RL5) $P_i d_i| \equiv P_i d_i \xleftrightarrow{K_{shd_i}} AS$ **Goal 2**

Derivation of Goal 3

- D20: From assumption (18) and (19) $P_i d_i| \equiv AS| \sim (Access\_Policy)$
- D21: (RL2) and assumption (21) produce together $P_i d_i| \equiv AS| \equiv (Access\_Policy)$ **Goal 3**

7.2.7 Formal Secrity Verification by ProVerif Tool

We have used ProVerif [22] to carry out formal security verification for the proposed scheme. This is used mainly for authentication phase and proving session key secrecy and its background design uses applied pi calculus [91]. The details the tools and its implementation are available in [92]. ProVerif is an automatic tool for cryptographic protocol that can collaborate with verifier tool in the formal model (i.e. Dolev-Yao threat model). This protocol verifier works based on a representation of the protocol using Horn clauses. This can examine hash functions, public-key cryptography (encryption or signatures), many classes of cryptographic primitives, and Diffie-Hellman key agreements using rewrite rules or as equations. It can also examine parallel unbounded number of sessions of the protocol and an unbounded message spaces. In case, the tool cannot execute a property, it can reconstruct an attack, that is, an execution trace of the protocol is reconstructed that can falsify the desired property. ProVerif has the capability to prove the following cryptographic properties:

- Secrecy (the secret is unreachable to the adversary)
- Authentication and, more generally, correspondence properties
- Strong secrecy (the adversary unable to see the difference at changes of secret)
- Equivalences between processes that differ only by terms

In Figure 7.3, we present the proverif code for declaring environment variables as well as the proverif code for primitive functions, destruct primitives, equations, queries, and events are provided in the same figure. We provide the code for the user and PId_{v_i} and trusted authority in Figure 7.4. The execution of code ProVerif 1.93 is provided in Table 7.5. The analysis of the result shows that the proposed protocol is free from various security attacks and vehicle theft attacks, with the following outcomes.

- RESULT inj-event(User_Approval_Trmtd_By_As(ID)) ==>
  inj-event(User_Login_Terminated(ID)) is true.
- RESULT inj-event(User_Approved(ID_1180)) ==>
  inj-event(User_Login_Start(ID_1180)) is true.

```
(* -------------communication channels------------*)
free public ch: channel. (* ---public channel--- *)
free secured ch: channel [private]. (*secured
channel*)
free secured ch1: channel [private]. (* secured
channel *)
(* -------- shared keys---------- *)
free Ku shared:bitstring [private]. (* common
shared key for user calculated its own side *)
free Ks shared:bitstring [private]. (* common
shared key for server calculated its own side *)
(* ----------Servers secret parameters ---------- *)
free Acess Policy:bitstring [private].
free Auth key:bitstring [private]. (*Server
Authentication Key for authenticating particular
user*)
free Pk1:bitstring [private].
free Pk2:bitstring [private].
free r LE:bitstring [private].
free P as:bitstring [private]. (*AccessPloicy from
authentication server*)
(*--------- constants----------- *)
const ID:bitstring [private].
const PW:bitstring [private].
const BiometricFi:bitstring [private].
const Xa:bitstring [private].
(*------------Vehicle's parameter -----------*)
free Fi2:bitstring.
free Ci af:bitstring.
free Ki L:bitstring.
free Ki A:bitstring.
free Pi:bitstring.(*Encoded Access ploicy of
user*)
free T Ar: bitstring.(*Timestamp at the time of
smart card preparation*
```

```
(* ---------- functions and equations------------------)
fun hash(bitstring):bitstring. (* hash function *)
fun Fuzzy Extractor(bitstring):bitstring. (* Fuzzy
extractor function *)
fun xor(bitstring,bitstring):bitstring. (* XOR
operation *)
fun concat(bitstring,bitstring):bitstring. (* string
concatenation *)
fun
vehdatagen(bitstring,bitstring,bitstring,bitstring,bit
string,bitstring)
:bitstring. (* string concatenation *)
equation forall x:bitstring,y:bitstring;
xor(xor(x,y),y) = x.
(* ---------------Security goals verication----------- *)
query attacker(Ku shared).
query attacker(Pas).
query attacker(r_LE).
query attacker(Pk1).
query attacker(Pk2).
query attacker(Acess Policy).
query ID: bitstring; inj-event(User
Approved(ID))==>inj-
event(User Login Start(ID)).
query Id:bitstring; inj-
event(User Approval Trmtd By As(ID)) ==>inj-
event(User Login Terminated(ID)).
(*-------------------- event ------------------*)
event User Login Start(bitstring). (* User starts
login event *)
event User Login Terminated(bitstring). (* User
fails to login at user terminal *)
event User Approved(bitstring). (* User's
approval through authentication process *)
event User Approval Trmtd By As(bitstring). (*
User's approval through authentication process *)
```

Figure 7.3: Proverif code for environment, function, destruct primitive, equations, queries and events.

- RESULT not attacker(Acess_Policy[]) is true.
- RESULT not attacker(Pk2[]) is true.
- RESULT not attacker(Pk1[]) is true.
- RESULT not attacker(r_LE[]) is true.
- RESULT not attacker(P_as[]) is true.
- RESULT not attacker(Ku_shared[]) is true.

```
let User=
(* User Smart Card Request Starts*)
let hasedBio=hash(BiometricFi) in
let hasedID=hash(ID) in
let hasedPW=hash(PW) in
out(secured ch,(hasedBio,hasedID,hasedPW));
(* User Smart Card Request Ends*)
in(secured ch1,(Fi2:bitstring,Ci af:bitstring));
new ri:bitstring;(*nonce chosen by user*)
new Tga:bitstring;(*Timestamp at user side->server
side for general authentication*)
let 1=xor(concat(hash(BiometricFi),hash(ID)),Xa)
in
let mi1=xor(concat(1,hash(PW)),ri) in
let mi2=concat(1,concat(T Ar,concat(Tga,ri))) in
let
2=hash(xor(concat(hash(BiometricFi),hash(ID)),Xa
))
in
let Ci af drvd=xor(xor(hash(BiometricFi),Fi2),Xa)
in
if (2=Fi2)
(Ci af drvd=Ci af) then
event User Login Start(ID);
out(public ch,(mi1,mi2,Ki L,Ki A,Tga));
in(public ch,(mi3:bitstring,mi4:bitstring,
mi5:bitstring, mi6:bitstring, T le:bitstring));
!(
let v1=concat(concat(concat(Pk1,T Ar),concat(ri,r
LE)),
concat(T le,Ki A)) in
if v1=mi5 then
let H1=hash(xor(P as,1)) in
let v2=concat(concat(T Ar,Ki L),concat(Ki A,Tga))
in
let Ku shared=concat(H1,v2)
else
(*event User Approval Trmtd By As(ID)*)
event User Login Terminated(ID) ).
```

```
let AuthenServer=
(* User Smart Card Preparation Starts*)
in(secured
ch,(hasedBio:bitstring,hasedID:bitstring,hasedPW:bitstring));
let Fi1=xor(concat(hash(BiometricFi),hash(ID)),Xa)
in
let Fi2=hash(xor(concat(hash(BiometricFi),hash(ID)),Xa))
in
let Ci af=xor(xor(hash(BiometricFi),Fi2),Xa) in
let Ki L=xor(concat(Pk1,T Ar),concat(Fi1,hasedPW))
in
let Ki A=xor(xor(concat(Pk2,T Ar),Ki L),concat(Fi1,hasedPW))
in
let P i= xor(Acess Policy,hash(concat(Fi1,hash(PW))))  in
let SMCRD=smartcardgen(Fi2,Ci af,Ki L,Ki A,P i,T Ar) in
out(secured ch1,(Fi2,Ci af));
(* User Vehicle Data Preparation Ends*)
in(public ch,(mi1:bitstring,mi2:bitstring,Ki L:bitstring,Ki
A:bitstring, Tga:bitstring));
new dt min, dt max,T_le:bitstring;
let dt=xor(T le,Tga) in
if (dt min  dtkdt  dt max) then
let v=xor(concat(Pk1,T Ar),Ki L) in
let r i=xor(mi1,v) in let
1=xor(concat(hash(BiometricFi),hash(ID)),Xa) in
let mi2 calted=concat(concat(concat(1,hash(PW)),concat(T
Ar,Tga)), r i) in
if mi2 calted=mi2 then
let mi3=xor(v,r LE) in
let mi4= concat(concat(r i,r LE),concat(Pk1,T Ar))  in
let mi5= concat(v,concat(concat(r i,r LE),concat(T le,Ki A)))  in
let mi6= concat(concat(mi5,xor(P as,1)),Ki A) in
out(public ch,(mi3,mi4,mi5,mi6,T le));
let H1=hash(xor(P as,1)) in
let v2=concat(concat(T Ar,Ki L),concat(Ki A,Tga))  in
let Ku shared=concat(H1,v2)   in
event User Approved(ID)  else
event User Approval Trmtd By As(ID)
(*event User Login Terminated(ID)*).
```

Figure 7.4: Proverif code for user and PId_{v_i} and trusted authority.

From the above analysis, we may state that the proposed protocol scheme satisfies the various secrecy goals and properties.

7.3 Result and Discussion of Simulations

7.3.1 Computation cost comparison and performance analysis

Here, we have analyzed the computation complexity of various recently proposed protocols in the blockchain-based VANET domain. Initially, we have executed the

```
RESULT inj-event(User
Approval Trmtd By As(ID))
==>inj-event(User Login
Terminated(ID)) is true.
File "/root/Desktop/Paper/fine
grain/update.pv",
line 50, character 7 - line 50,
character 9:
Warning: identier ID rebound.
{ Query inj-event(User
Approved(ID 1180))
==>inj-event(User Login
Start(ID 1180))
Completing...
Starting query inj-event(User
Approved(ID 1180))
==>inj-event(User Login
Start(ID 1180))
RESULT inj-event(User
Approved(ID 1180))
==>inj-event(User Login
Start(ID 1180)) is true.
{ Query not attacker(Acess
Policy[])
Completing...
Starting query not
attacker(Acess Policy[])
```

```
RESULT not attacker(Acess
Policy[]) is true.
{ Query not attacker(Pk2[])
Completing…
Starting query not attacker(Pk2[])
RESULT not attacker(Pk2[]) is
true.
{ Query not attacker(Pk1[])
Completing...
Starting query not attacker(Pk1[])
RESULT not attacker(Pk1[]) is
true.
{ Query not attacker(r LE[])
Completing...
Starting query not attacker(r LE[])
RESULT not attacker(r LE[]) is
true.
{ Query not attacker(P as[])
Completing...
Starting query not attacker(P as[])
RESULT not attacker(P as[]) is
true.
{ Query not attacker(Ku shared[])
Completing...
Starting query not attacker(Ku
shared[])
RESULT not attacker(Ku
shared[]) is true.
```

Figure 7.5: ProVerif simulation results for the given queries.

various major time-consuming cryptographic operations on the "11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz" system with 16.0 GB RAM and the runtimes are recorded in Table 7.5. We have also compared the performances of various recent approaches with the proposed scheme. Table 7.6 presents the cost comparison matrix of ECPP, DAIA, ZHOU, EAAP and BAVC against LBAFA scheme. Figure 7.7 shows the verification delays against a group of vehicles. From the comparison matrix and Figure 7.7, it shows that the proposed scheme is more secure and less affected by the increase in vehicle numbers compared to other related schemes and achieves parallelism and scalability effectively. The availability of various event parameters is presented in Figure 7.6.

7.4 Summary

In this chapter, we have proposed a lightweight blockchain-based authentication scheme (LBAFA) with fine-grained access control for secured message delivery on

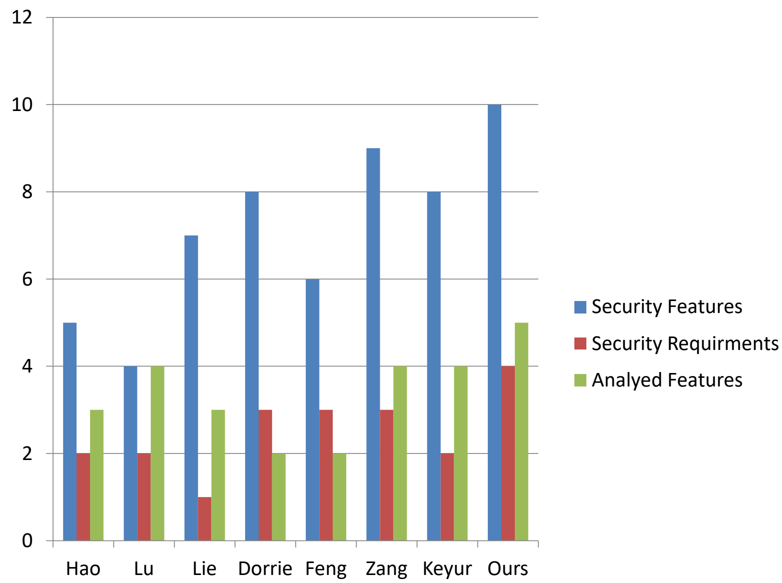

Figure 7.6: Various aspect of security features.

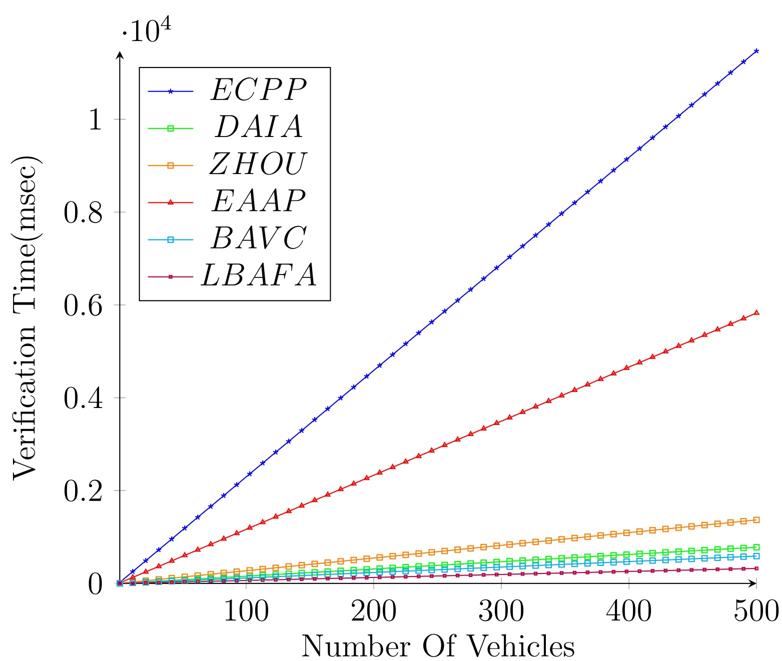

Figure 7.7: Signature verification delay of ECPP, DAIA, ZHOU, EAAP, BAVC and LBAFA scheme w.r.t. group of vehicles

Table 7.5: Run time of cryptographic operations

Operator name with description	Run Time (in second)
$T_{h(\cdot)}$: Hash function 256	1.14e-05
$T_{ecc-mul}$: ECC point multiplication	0.3841e-03
$T_{ecc-add}$: ECC point addition	1.80e-06
$T_{blp-mul}$: Bilinear point multiplication	1.311e-03
$T_{blp-add}$: Bilinear point addition	6.90e-06
T_{pcom}: String comparison	1.255e-05
T_{blp}: Bilinear pairing	3.5e-03
T_{ran}: Random number	2.8e-7
T_{con}: String concatenation	1.202e-06

Table 7.6: Comparison of time complexity for signature verification w.r.t single and group for ECPP, DAIA, ZHOU, EAAP, BAVC and LBAFA scheme

Scheme name	Single user verification	Group user verification
ECPP[125]	$3T_{blp} + 11T_{blp-mul}$	$3T_{blp} + (10+n)T_{blp-mul}$
DAIA[103]	$2T_{h(.)} + T_{ecc-add} + 4T_{ecc-mul}$	$n(2T_{h(.)} + T_{ecc-add} + 4T_{ecc-mul})$
ZHOU[167]	$4T_{h(.)} + 2T_{ecc-add} + 7T_{ecc-mul}$	$n(4T_{h(.)} + 2T_{ecc-add} + 7T_{ecc-mul})$
EAAP[18]	$2T_{h(.)} + 3T_{blp} + T_{blp-mul}$	$n(2T_{h(.)} + 3T_{blp} + T_{blp-mul})$
BAVC[164]	$2T_{h(.)} + 2T_{ecc-add} + 3T_{ecc-mul}$	$n(2T_{h(.)} + 2T_{ecc-add} + 3T_{ecc-mul})$
LBAFA	$T_{h(.)} + T_{ecc-add} + T_{ecc-mul} + 2T_{pcom}$	$n(T_{h(.)} + T_{ecc-add} + T_{ecc-mul} + 2T_{pcom})$

VANET. We have incorporated CP-ABE to suit the blockchain environment. The proposed scheme can offer decentralization and parallel computing using a suitable blockchain-enabled VANET framework using EC and MEC features. The notable feature of LBAFA is that it achieves scalability effectively. The incorporation of ECC helps to mask the real identity of the vehicle in a blockchain-based VANET scenario. The validation of the genuine vehicle by RSU at the entry of the blockchain prevents malicious users from participating and flooding the network with malicious intent. The result shows that our scheme is less complex and more efficient with the help of edge computing and mobile edge computing and can be more useful, especially for blockchain-based VANET for a safe and smooth journey as compared to other existing protocols.

Chapter 8

Conclusion and Future Works

In this chapter, the major contributions of the thesis have been summarized. It also briefly provides the roadmap and direction for future research that can be carried out to extend further the research framework proposed by us.

In this thesis, we have figured out the relevant security challenges in vehicular ad-hoc network (VANET). The VANET has become the most challenging and emerging field of research due to its larger scope still left for designing the ideal user authentication protocols, access control with proper user access control protocols, which can meet all the security requirements and realize all the functionality requirements. We have focused on and investigated possible solutions for those challenges. Several lightweight, efficient and concise secure authentication protocols proposed to ensure privacy and security. These schemes include single pass key based and dynamic password based authentication, multi-factor authentication and secure biometric-based authentication for user authentication in VANET networks. ECC concept is used to optimize the computation cost and CP-ABE to impose access control over the data in fine-grained manner based on user attributes along with hash functions. Further, we have explored to study the relevant user access control schemes, which make use of identity-based signature, group-id and user access with fine-grained feature. In this thesis, we focus on exploring novel security in the area of design and analysis of access control schemes, scalable user authentication, lightweight blockchain-based authentication and suitable key agreement with fine-grained access control for VANET.

A new node installation in VANET is necessary due to its dynamic topology, where some nodes may join after weeks or months of active participation, or some node may be first-timer participants. Therefore, to stop adversary nodes from participating in the existing VANET, access control should be incorporated to manage node deployment. In this scenario, the law executor can authenticate its neighbouring nodes to certify that these nodes are eligible to access the existing VANET; and only after successful authentication the new nodes can establish secured session with its neighbouring nodes to safeguard the communications among them. We have studied biometric-based and Rabin cryptosystem-based authentication with efficient and effective access control schemes.

Designing access privileges and access structures using access tree is necessary to authorize legitimate users for the rightful information and allied resources for various services. This could be provided with the support of efficient user access control protocols. An ideal user access control mechanism generally consists of user authentication (to perform identity verification), user authorization (to provide access), and user accountability (controlling and monitoring VANET activities) to control and monitor user access and avoid different kinds of attacks. We also brought out a new user access control protocol using blockchain technology suitable for vehicular ad-hoc networks.

We have performed formal security analysis using the real-oracle random (ROR) model and BAN logic. The formal security under the ROR model reveals that our proposed schemes are safe and secure.

We also have simulated our scheme using widely-accepted AVISPA (automated validation of internet security protocols and applications) tools, simulation of urban mobility (SUMO), and OMNET++. AVISPA tool can ensure that a protocol is secure against possible passive and active attacks like replay and man-in-the-middle (MIM) attacks. Using the AVISPA model verifiers, we prove that our proposed schemes are secure against possible passive and active attacks.

In addition, analysis and simulation results show that our scheme is secured against various well-known attacks. Further, we have compared the security and efficiency of our schemes with the existing schemes available in the literature and found that our proposed protocols are more secure, lighter, 5G-friendly, scalable, and even faster than the other related schemes.

8.1 Contributions

We have summarized the contributions of the thesis in the next few subsections.

8.1.1 Anonymous Key Agreement Scheme for Secure Vehicular Ad-hoc Networks

In the first contribution (**Chapter 4**), we propose a lightweight anonymous key agreement scheme (AKAS) for secure vehicular ad-hoc networks with fine-grained authentication feature. Here, we focus to address the challenges related to the restriction of unauthenticated user access and proper key agreement with fine-grained access control specifically for vehicle-to-vehicle (V2V) communication in VANET. In the proposed scheme, registered and authorized users can access services/information as per access privilege only. We have performed formal security analysis using the ROR model. Moreover, we have simulated our scheme using AVISPA tools, SUMO, and OMNET++. Analysis and simulation results show that our scheme is secured against various well-known attacks. Further, we have compared the security and efficiency of our scheme with the existing schemes available in the literature and found that our proposed protocol is more secure, lighter, 5G-friendly, scalable, and even faster than the other related schemes.

8.1.2 Biometric-based Authentication Protocol for VANET

In the second contribution (**Chapter 5**), we propose a dynamic, lightweight biometric-based authentication protocol for vehicle-to-vehicle (V2V) communication networks where user, after successful registration, can directly login from any local mobile terminal and access his or her services or information directly from the authentication servers. We have done the security analysis of our scheme and proved that it provides user anonymity, location privacy, mutual authentication to prevent spoofing attacks, and resistance against forgery, modification, and replay attacks. We also compare the efficiency of our scheme with other related schemes and show that our authentication scheme is more secure and performs faster than other schemes available in the literature. In addition, our proposed scheme provides scalability, as there are no limitations on the number of user terminals. In this scheme, the genuine user needs to be registered only once for accessing the services. No multiple registrations or session-based registrations are required.

8.1.3 Rabin Cryptosystem-based Authentication Mechanism for VANET

In our third contribution (**Chapter 6**), we propose an improved and enhanced Rabin cryptosystem-based authentication mechanism to address all known major attacks with robustness, efficiency, scalability, and dynamism in mind. There are significant works already carried out in the direction of authentication and privacy preservation using Rabin cryptosystem security solutions. However, the basic Rabin cryptosystem is a factoring-based efficient method, and its decryption process leads to failure as it generates 4 to 1 output. It may be noted that our proposed enhanced method is unique and does not lead to failure. We have rigorously carried out security analysis by AVISVA and Proverif Tools. The analysis has shown that our scheme guarantees positional privacy, user anonymity, and mutual authentication to prevent spoofing attacks, password guessing attacks, insider privilege attacks, and temporal session attacks. The comparison of the protocol with the available relevant schemes reveals that the proposed protocol is more efficient in terms of efficacy. It supports a lightweight authentication process for legitimate users. This proposed scheme supports scalability as it does not depend on the volume of user access points, and a valid user requires registering one time for accessing the VANET services. Thus, session-based and duplicate registration can be avoided by the proposed scheme.

8.1.4 Lightweight Blockchain-based Secure Authentication and Fine-grained Access Control in VANET

In our fourth contribution (**Chapter 7**), we have focused on the design of a lightweight blockchain-based secure authentication mechanism. Recently, several studies have been incorporated to address security and privacy issues in VANET. However, the majority of the work could not use the full potential of blockchain to the maximum extent possible. Lu et al. [105] proposed the BPPA protocol for trusted authority (TA) to make it transparent and more verifiable by storing all transactions & certificates in blockchain. However, this protocol adds more computational overhead to process multiple certificates. We propose lightweight blockchain-based secure authentication and fine-grained access control (LBAFA) for VANET users. In the proposed blockchain-based authentication scheme, we ensure access control, parallel computing, and compliance with various known security challenges efficiently. We have defined a framework with edge computing and mobile edge computing to offload computation-intensive tasks as well as optimize data processing before sending it to the blockchain-based VANET network. We have done security analysis using the Proverif tool and formally proved security strength using BAN logic. The security analysis shows that the proposed scheme resists various known security threats. Moreover, the performance analysis proves that our scheme is faster and more efficient compared to the other relevant protocols available. In addition, in the proposed scheme (LBAFA), we have incorporated blockchain technology to introduce decentralization and parallel computing over traditional centralized VANET. We have also used ECC to optimize the computation cost and CP-ABE to impose access control over the data in a fine-grained manner based on user attributes.

8.2 Future Research Directions

In this section, we give our suggestions and directions for possible future research.

For future research, we have suggestions to carry forward the proposed user authentication and access control framework by including retina/iris detection-based user authentication. Most of the VANET research related to authentication makes use of thumb impressions. But due to the ongoing COVID scenario, we need to focus on untouchable biometric features to work with. A single node, say a vehicle, can be used by several users, i.e., a node can be shareable, where as biometric is non-shareable. Therefore, dynamic nodes always have a primary concern related to resource constraints and user management in VANET before accessing real-time data from the VANET domain. These systems may be vulnerable to various attacks if a proper biometric feature is not considered in the robust design, as user authentication in VANET becomes inherently more secure and reliable than the usual password-based user authentication protocols. Using fingerprints, faces, irises, hand geometry, and palm prints can have the following major advantages over traditional password-based mechanisms. However, key extracted from biometric features that can be captured from a distance following social distancing norms could be better ideas.

- Biometric features keys can not be theft or forgotten.

- Biometric-based key is very difficult to clone.
- Biometric features are extremely hard to forge or redistribute.
- Biometric key can not be predicted easily.

Although considerable progress and research have been carried out in blockchain technology-based authentication, the trust and reputation management fields still face several challenges that can be addressed in future research. The following future scopes are discussed below.

- Trust Bootstrapping: Most of the recently proposed trust management solutions can assume an arbitrary initial trust values may be 0 or 0.5 [80] when a new node is installed. Alishev et al. [13] propose the Analytical Hierarchy Process (AHP) to compute the initial trust value. However, more research is needed to calculate the accurate initial trust value for newly installed or encountered nodes. One possible solution could be a hybrid mechanism considering socialistic factors, history, and cooperation behavior among nodes that can leverage bootstrapping the trust value for newly available neighbors.
- Lifetime of Trust Value/Decay: The lifetime of trust values for encountered nodes can be maintained, and it poses another important challenge in VANET. Owing to the dynamic characteristics of VANET, there is a need to study and develop a life cycle for trust value and decay.
- Incentives and Audit: An efficient incentive mechanism needs to be developed to stimulate nodes in VANET to participate in the combined trust evaluation process.
- Reputation Propagation: There should be an online reputation propagation model for users to behave strategically to keep a good reputation for the future. Therefore, there is still scope left for designing a better reputation propagation model.

In the future, we would like to focus on exploring blockchain technology-based solutions for unmanned aerial vehicle (UAV)-assisted communication for future battle field scenarios where the above-mentioned features may help for novel design. Vehicle networks in smart cities are very hard to implement and develop due to the complexity of the different technologies that may intertwine to provide results and various real-life scalability issues they have to work and deliver [14]. The internet of vehicles (IoV) is considered as decentralized technology that can expand from the pre-existing VANETs [62] for aiming at vast area level of coverage.

So, mainly, our future interests are to concentrate on testing various schemes on how to implement these smart systems in future battlefield scenarios and how to operate them efficiently. After certain years, with this knowledge and research results at hand, a large-scale implementation in large areas might be possible with the correct standards and regulations in place. The reputation features-based systems in the IoV network can usually be used to incentivize the data dissemination process [113]. In this design, a lot of machine learning (ML) and artificial intelligence (AI) are used. We are interested in building our research interest to explore the impact of ML and AI systems to study node behavior in the network to incentivize and disseminate these reputation-based systems in VANET as well as IoV.

Bibliography

[1] https://omnetsimulator.com/. Accessed on Mar 2024.

[2] Advanced Encryption Standard (AES). FIPS PUB 197, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[3] Automated Validation of Internet Security Protocols and Applications. http://www.avispa-project.org/. Accessed on January 2011.

[4] Automated validation of internet security protocols and applications, avispa web tool. http://www.avispa-project.org/web-interface/expert.php/. Accessed on January 2013.

[5] CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-Ready RF Transceiver. Available from: http://www.ti.com/product/cc2420. Accessed on September 2011.

[6] Fuzzy Extractors: How to Generate Strong keys from Biometrics and Other Noisy. http://www.iacr.org/archieve/eurocrypt2004/30270518/DRS-ec2004-final.pdf.

[7] Secure hash standard. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995.

[8] SUMO User Documentation. https://www.civil.iitb.ac.in/. Accessed on Mar 2024.

[9] A. Studer, E. Shi, F. Bai, C. Chen, A. Perrig. Tracking together efficient authentication, revocation and privacy in vanets. In *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad hoc Communication and Networks(SECON'09)*, pages 1–9. IEEE Computer Society, 2009.

[10] A. Wasef, Y. Jiang, and X. Shen. DCS: an efficient distributed-certificate-service scheme for vehicular networks. *IEEE Trans. Vehicle Technology*, 59(2):533549, 2010.

[11] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A Survey. *Computer Networks*, 38(4):393–422, 2002.

[12] S. Alazzawi, M. Hummel, P. Kordt, T. Sickenberger, C. Wieseotte, and O. Wohak. Simulating the impact of shared, autonomous vehicles on urban mobility-a case study of milan. *EPiC Series in Engineering*, 2:94–110, 2018.

[13] D. Alishev, R. Hussain, W. Nawaz, and J. Lee. Social-aware bootstrapping and trust establishing mechanism for vehicular social networks. In *2017 IEEE 85th vehicular technology conference (VTC Spring)*, pages 1–5. IEEE, 2017.

[14] P. Alvares, L. Silva, and N. Magaia. Blockchain-based solutions for uav-assisted connected vehicle networks in smart cities: A review, open issues, and future perspectives. In *Telecom*, volume 2, pages 108–140. MDPI, 2021.

[15] R. Amin and G. P. Biswas. A secure lightweight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad-Hoc Networks*, 36:58–80, 2016.

[16] A. Arora and S. K. Yadav. Block chain based security mechanism for internet of vehicles (iov). In *Proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT)*, pages 26–27, 2018.

[17] J. P. Aumasson, L. Henzen, W. Meier, and M. N. Plasencia. Quark: A Lightweight Hash. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES 2010), LNCS*, volume 6225, pages 1–15, 2010.

[18] M. Azees, P. Vijayakumar, and L. J. Deboarh. Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 18(9):2467–2476, 2017.

[19] Bellare, Mihir, Rogaway, and Phillip. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS'93)*, pages 62–73, Fairfax, Virginia, USA, 1993.

[20] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE symposium on security and privacy (SP'07)*, 2007.

[21] U. Bhanja. An attack resistance model for trustworthiness evaluation in vanet. In *2020 IEEE 17th India Council International Conference (INDICON)*, pages 1–7. IEEE, 2020.

[22] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre. Proverif 2.00: automatic cryptographic protocol verifier, user manual and tutorial. *Version from*, pages 05–16, 2018.

[23] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen. An efficient message authentication scheme for vehicular communications. *IEEE Transaction on Vehicular Technology*, 57(6):3357–3368, 2008.

[24] D. Carman, P. Kruus, and B. Matt. Constraints and Approaches for Distributed Sensor Network Security. dated September 1, 2000. NAI Labs Technical Report No. 00-010.

[25] H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. In *IEEE Symposium on Security and Privacy*, pages 197–213, Berkeley, California, 2003.

[26] S. Chatterjee, A. K. Das, and J. K. Sing. An Enhanced Access Control Scheme in Wireless Sensor Networks. *Ad Hoc & Sensor Wireless Networks*. In press, 2013.

[27] T.-H. Chen and W.-K. Shih. A Robust Mutual Authentication Protocol for Wireless Sensor Networks. *ETRI Journal*, 32(5):704–712, Oct. 2010.

[28] Y. Choi, J. Nam, Y. Lee, S. Jung, and D. Won. Cryptanalysis of advanced biometric based user authentication scheme for wireless sensor networks. *Springer*, 30:1367–1375, 2015.

[29] D. Chowdhury, L. Santen, and A. Schadschneider. Statistical physics of vehicular traffic and some related systems. *Physics Reports*, 329(4-6):199–329, 2000.

[30] Y. F. Chung, H. H. Lee, F. Lai, and T. S. Chen. Access control in user hierarchy based on elliptic curve cryptosystem. *Information Sciences*, 178(1):230–243, 2008.

[31] D. Chaum, and E. V. Heyst. Group signatures. In *Workshop on the Theory and Application of Crytographic Techniques*, pages 257–265, 1991.

[32] P. U. D. Stebila and S. Chang. Multi-factor password-authenticated key exchange, 2008. Cryptology eprint archive, report 2008/214, http://eprint.iacr.org/2008/214.

[33] D. von Oheimb. The high-level protocol specification language hlpsl developed in the eu project avispa. In *In Proceedings of 3rd APPSEM II Workshop on Applied Semantics (APPSEM 2005)*, pages 1–17, Frauenchiemsee, Germany, 2005.

[34] J. Daemen and V. Rijmen. *The Design of Rijndael, AES The Advanced Encryption Standard*. pages 31-79, Springer-Verlag, 2002.

[35] A. Das, N. Paul, and L. Tripathy. Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. *Information Sciences*, 209:80–92, 2012.

[36] A. K. Das. A Key Reshuffling Scheme for Wireless Sensor Networks. In *1st International Conference on Information Systems Security (ICISS 2005)*, volume 3803, pages 205–216, 2005.

[37] A. K. Das. A Key Pre-Distribution Scheme Using Deployment Knowledges For Security In Static Sensor Networks. In *First International Conference on Emerging Applications of Information Technology (EAIT 2006)*, pages 343–347, 2006.

[38] A. K. Das. An Identity-Based Random Key Pre-Distribution Scheme for Direct Key Establishment to Prevent Attacks in Wireless Sensor Networks. *International Journal of Network Security*, 6(2):134–144, 2008.

[39] A. K. Das. An Improved Efficient Key Distribution Mechanism for Large-Scale Heterogeneous Mobile Sensor Networks. *International Journal of Information Processing*, 2(3):21–32, 2008.

[40] A. K. Das. An Unconditionally Secure Location-Aware Key Management Scheme for Static Sensor Networks. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(3):333–355, 2008.

[41] A. K. Das. ECPKS: An Improved Location-Aware Key Management Scheme in Static Sensor Networks. *International Journal of Network Security*, 7(3):358–369, 2008.

[42] A. K. Das. A Location-Adaptive Key Establishment Scheme for Large-Scale Distributed Sensor Networks. *Journal of Computers*, 4(9):896–904, 2009.

[43] A. K. Das. A Survey on Analytic Studies of Key Distribution Mechanisms in Wireless Sensor Networks. *Journal of Information Assurance and Security*, 5(5):526–553, 2010.

[44] A. K. Das. An Efficient Random Key Distribution Scheme for Large-Scale Distributed Sensor Networks. *Security and Communication Networks*, 4(2):162–180, 2011.

[45] A. K. Das. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. *International Journal of Information Security*, 11(3):189–211, 2012.

[46] A. K. Das. Improving Identity-based Random Key Establishment Scheme for Large-scale Hierarchical Wireless Sensor Networks. *International Journal of Network Security*, 14(1):1–21, January 2012.

[47] A. K. Das. A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. *Networking Science*, 2(1-2):12–27, 2013.

[48] A. K. Das, A. Das, S. Mohapatra, and S. Vavilapalli. Key Forwarding: A Location-Adaptive Key-Establishment Scheme for Wireless Sensor Networks. In *7th International Workshop on Distributed Computing (IWDC 2005) (now, known as International Conference on Distributed Computing and Networking, ICDCN)*, volume 3741, pages 404–409, 2005.

[49] A. K. Das and I.Sengupta. A Location-Based Key Establishment Scheme for Static Wireless Sensor Networks with Multiple Base Stations. *Journal of Information Assurance and Security*, 5(4):426–436, 2010.

[50] A. K. Das and I. Sengupta. A Key Establishment Scheme for Large-Scale Mobile Wireless Sensor Networks. In *4th International Conference on Distributed Com-*

puting and Information Technology (ICDCIT 2007), Lecture Notes in Computer Science (LNCS), volume 4882, pages 79–88, 2007.

[51] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, 35(5):1646–1656, 2012.

[52] A. K. Das, M. Wazid, A. R. Yannam, J. Rodrigues, and Y. Park. Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access*, 7:55382–55397, 2019.

[53] D.Basin, S.Modersheim, and L.Vigano. OFMC: A symbolic model checker for security protocols. *International Journal of Information Security*, 4(3):181–208, 2005.

[54] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[55] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances In Cryptology-EUROCRYPT 2004: International Conference On The Theory And Applications Of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23*, pages 523–540. Springer, 2004.

[56] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak. Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, 55(12):119–125, 2017.

[57] J. R. Douceur. The Sybil Attack. In *The First International Workshop on Peer-to-Peer Systems (IPTPS '02),Lecture Notes in Computer Science, Springer-verlag*, volume 2429, pages 251–260, 2002.

[58] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In *ACM Conference on Computer and Communications Security (CCS'03)*, pages 42–51, Washington DC, USA, October 27-31 2003.

[59] M. Eltoweissy, M. Moharram, and R. Mukkamala. Dynamic key management in sensor networks. *IEEE Communications Magazine*, 44(4):122–130, April 2006.

[60] L. Eschenauer and V. D. Gligor. A Key Management Scheme for Distributed Sensor Networks. In *9th ACM Conference on Computer and Communication Security*, pages 41–47, November 2002.

[61] A. A. et al. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In *17th International Conference on Computer Aided Verification (CAV'05), LNCS 3576.*, pages 281–285, 2005.

[62] E. C. Eze, S. Zhang, and E. Liu. Vehicular ad hoc networks (vanets): Current state, challenges, potentials and way forward. In *2014 20th international conference on automation and computing*, pages 176–181. IEEE, 2014.

[63] F. Ahmad, V. N. L. Franqueira, and A. Adnane. A systematic approach for cyber security in vehicular networks. *IEEE Computer Communication*, 4:38–62, Dec 2016.

[64] F. Ahmad, V. N. L. Franqueira, and A. Adnane. TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks. *IEEE Access*, 6, 2018. DOI: 10.1109/ACCESS.2018.2837887.

[65] Q. Feng, D. He, S. Zeadally, and K. Liang. Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics*, 16(6):4146–4155, 2019.

[66] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext policy attribute based encryption. In *Automata, Languages and Programming: 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II 35*, pages 579–591. Springer, 2008.

[67] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pages 89–98, 2006.

[68] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan. CP-ABE with constant-size keys for lightweight devices. *IEEE transactions on information forensics and security*, 462:763–771, 2014.

[69] A. Gupta and R. K. Jha. A Survey of 5G network: Architecture and emerging technologies. *IEEE Special Section on Recent Advances in Software Defined Networking for 5G Networks*, 3:1206 – 1232, Aug 2015. DOI: 10.1109/ACCESS.2015.2461602.

[70] W. K. H, Y. Zheng, J. Cao, and S. Wang. A dynamic user authentication scheme for wireless sensor networks. *IEEE International Conference*, 1:8–20, 2006.

[71] H. Liu and X. Luo and H. Liu and X. Xia. Merkle tree: A fundamental component of blockchains. In *In 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, pages 556–561, 2021.

[72] H. Yang, Y. Zhang, Y. Zhou, X. Fu, H. Liu, and A. V. Vasilakos. Provably secure three-party authenticated key agreement protocol using smart cards. *Computer Networks*, 58:29–38, 2014.

[73] W. Han. Weakness of a Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, 2011. http://eprint.iacr.org/2011/293.

[74] Y. Hao, Y. Cheng, C. Zhou, and W. Song. A distributed key management framework with cooperative message authentication in vanets. *IEEE Journal on selected areas in communications*, 29(3):616–629, 2011.

[75] D. He, N. Kumar, and N. Chilamkurt. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Sciences*, 321:263–277, 2013.

[76] D. He, B. X. S. Zeadally, and X. Huang. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks. *IEEE Transactions on Information Forensics and Security*, 10:2681–2691, 2015.

[77] Y. Hu, A. Perrig, and D. Johnson. Pachet leashes: a defense against wormhole attacks in wireless networks. In *IEEE INFOCOM'03*, 2003.

[78] H.-F. Huang. A novel access control protocol for secure sensor networks. *Computer Standards & Interfaces*, 31:272–276, 2009.

[79] H.-F. Huang. A New Design of Access Control in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, 2011. Article ID 412146, 7 pages doi:10.1155/2011/412146.

[80] R. Hussain, J. Lee, and S. Zeadally. Trust in vanet: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems*, 22(5):2553–2571, 2020.

[81] M. Ilyas and I. Mahgoub. *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. CRC, 2005.

[82] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets. *Future Generation Computer Systems*, 84:216–227, 2018.

[83] A. H. S. J. Johansson and A. Gurtov. Implementation and Evaluation of the ACE DTLS Framework Over Internet of Things Devices. In *IEEE 2nd International Conference on Signal, Control and Communication (SCC)*, pages 175–181. IEEE Computer Society, 2021. doi:10.1109/SCC53769.2021.9768365.

[84] J. P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy*, 3:49–55, 2004.

[85] D. Johnson and A. Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, Dept. of C & O, University of Waterloo, Canada, August 23, 1999.

[86] M. K. Khan and K. Alghathbar. Cryptanalysis and security improvements of two-factor user authentication in wireless wensor wetworks. *Sensors*, 10:2450–2459, 2010.

[87] H.-S. Kim and S.-W. Lee. Enhanced novel access control protocol over wireless sensor networks. *IEEE Transactions on Consumer Electronics*, 55(2):492–498, 2009.

[88] N. Koblitz. Elliptic Curves Cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[89] S. Kraus, K. Sycara, and A. Evenchik. Reaching agreements through argumentation: a logical model and implementation. *Artificial Intelligence*, 104(1-2):1–69, 1998.

[90] D. R. Krause, R. B. Handfield, and T. V. Scannell. An empirical investigation of supplier development: reactive and strategic processes. *Journal of operations management*, 17(1):39–58, 1998.

[91] R. Küsters and T. Truderung. Reducing protocol analysis with xor to the xor-free case in the horn theory based approach. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 129–138, 2008.

[92] R. Küsters and T. Truderung. Using proverif to analyze protocols with diffie-hellman exponentiation. In *2009 22nd IEEE Computer Security Foundations Symposium*, pages 157–171. IEEE, 2009.

[93] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[94] C. C. Lee and Y. M. Lai. Toward a secure batch verification with group testing for VANET. *Wireless networks*, 19:1441–1449, 2015.

[95] M. Lee and T. Atkison. Vanet applications: Past, present, and future. *Vehicular Communications*, 28:100310, 2021.

[96] A. Lei, C. Ogah, P. Asuquo, H. Cruickshank, and Z. Sun. A secure key management scheme for heterogeneous secure vehicular communication systems. *ZTE Communications*, 21:1, 2016.

[97] B. Leiding, P. Memarmoshrefi, and D. Hogrefe. Self-managed and blockchain-based vehicular ad-hoc networks. In *Proceedings of the 2016 ACM international joint conference on pervasive and ubiquitous computing: adjunct*, pages 137–140, 2016.

[98] C. T. Li, C. Y. Weng, and C. C. Lee. An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. *Sensors*, 13:9589–9603, 2013.

[99] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu. Fadb: A fine-grained access control scheme for vanet data based on blockchain. *IEEE Access*, 8:85190–85203, 2020.

[100] H. Liao and Y. Shen. On the Elliptic Curve Digital Signature Algorithm. *Tunghai Science*, 8:109–126, 2006.

[101] C. Lin, D. He, X. Huang, N. Kumar, , and K. K. R. Choo. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 22:7408–7420, 2020.

[102] D. Liu and P. Ning. Establishing Pairwise Keys in Distributed Sensor Networks. In *Proceedings of 10th ACM Conference on Computer and Communications Security (CCS)*, pages 52–61, Washington DC, Oct 27-31 2003.

[103] Y.-N. Liu, S.-Z. Lv, M. Xie, Z.-B. Chen, and P. Wang. Dynamic anonymous identity authentication (daia) scheme for vanet. *International Journal of Communication Systems*, 32(5):e3892, 2019.

[104] R. Lu, X. Lin, X. Liang, and X. Shen. A dynamic privacy-preserving key management scheme for location-based services in vanets. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):127–139, 2011.

[105] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu. A blockchain-based privacy-preserving authentication scheme for vanets. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12):2792–2801, 2019.

[106] M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05), Lecture Notes in Computer Science*, volume 3386, pages 65–84, Les Diablerets, Switzerland, 2005.

[107] M. Ali, L. Tang Jung, A. Hassan Sodhro, A. Ali Laghari, S. Birahim Belhaouari, and Z. Gillani. A confidentiality-based data classification-as-a-service (c2aas) for cloud security. *Alexandria Engineering Journal*, 64:749–760, 2022.

[108] J. E. M. Behrisch, Bieker and D. Krajzewicz. SUMO- Simulation of urban mobility: An overview. In *In Proceedings of 3rd Int. Conference Adv. System Simulation*, pages 55–60, 2011.

[109] M. A. M. Burrows and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

[110] M. C. Chuang and J. F. Lee. Team: Trust-extended authentication mechanism for vehicular ad-hoc networks. *IEEE System Journal*, 8(3):749–758, 2014.

[111] M. Li, W.Lou, and K. Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1):51–58, 2010.

[112] M. Wazid, A. K. Das, S. Kumari, and X. Li, and F. Wu. Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. *Security and Communication Networks*, 9(13):1983–2001, 2016.

[113] N. Magaia and Z. Sheng. Refiov: A novel reputation framework for information-centric vehicular applications. *IEEE Transactions on Vehicular Technology*, 68(2):1810–1823, 2018.

[114] MD. Ismail, S. Chatterjee, and J.K. Sing. Secure biometric-based authentication protocol for vehicular ad-hoc network. In *18th IEEE International Symposium on*

Smart Electronic Systems (iSES)(Formerly iNiS), pages 229–234. IEEE Computer Society, 2018.

[115] T. S. Messerges, E. A. Dabbish, and R. H. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5):541–552, 2002.

[116] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: Analysis and defenses. In *Proceedings of third IEEE International Conference on Information Processing in Sensor Networks (IPSN 2004)*, pages 259–268, 26-27 April 2004.

[117] R. W. D. Nickalls. A new approach to solving the cubic: Cardan's solution revealed. *The Mathematical Gazette*, 77(480):354–359, 1993.

[118] S. Nishad and T. Pandey. Realistic simulation of vehicularnetwork in urban and semi-urban area of india. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 6(9):438–447, 2018.

[119] D. V. Oheimb. The high-level protocol specification language hlpsl developed in the eu project avispa. Proceedings of APPSEM Workshop (2005).

[120] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux. Secure vehicle communication systems: design and architecture. *IEEE Communication Magazine*, 46(11):100–109, 2008.

[121] S. Pape. *Authentication in insecure environment*. Total pages 362 Springer-Wiesbaden, Sep 2014.

[122] B. Parno and A. Perrig. Challenge in securing vehicular networks. In *In Proceedings Workshop Hot Topics Network (HOTNETs)*, pages 1–6, 2005.

[123] B. Parno, A. Perrig, and V. Gligor. Distributed Detection of Node Replication Attacks in Sensor Networks. In *IEEE Symposium on Security and Privacy*, pages 49– 63, 8-11 May 2005.

[124] Q. Fan, J. Chen, M. Shojafar, S. Kumari and D. He. A symmetric authenticated key exchange protocol with perfect forward secrecy for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 18(9):6424–6434, Sep 2022. doi: 10.1109/TII.2022.3145584.

[125] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In *The 27th IEEE International Conference on Computer Communications(INFOCOM 2008)*. IEEE Computer Society, 2008.

[126] R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In *IEEE 27th Conference on Computer Communications*, pages 1229–1237, 2008.

[127] M. Raya and J. P. Hubaux. Securing vehicular ad-hoc networks. *Journal of computer security*, 15:39–68, 2007.

[128] S. Ruj. Attribute based access control in clouds: A survey. *IEEE*, 14, 2014.

[129] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos. Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment. *IEEE Transactions on Dependable and Secure Computing*, 15(5):824 – 839, 2016. DOI: 10.1109/TDSC.2016.2616876.

[130] S. Kumari and M. Karuppiah and X. Li and A. K. Das and V. Odelu. An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks. *Security and Communication Networks*, 9(17):4255–4271, 2016.

[131] S. Mcmurray, and A. Hassan Sodhro. A Study on ML-Based Software Defect Detection for Security Traceability in Smart Healthcare Applications. In *IEEE 2nd International Conference on Signal, Control and Communication (SCC)*, pages 1–84. MDPI, 2023. https://doi.org/10.3390/s23073470.

[132] S. Morteza Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Computer Networks, ELSEVIER*, 134:78–92, Jan 2018.

[133] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[134] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo. Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. *IEEE Internet of Things Journal*, 5(4):2884 – 2895, 2017. DOI: 10.1109/JIOT.2017.2714179.

[135] M. A. Saleem, X. Li, M. F. Ayub, S. Shamshad, F. Wu, and H. Abbas. An efficient and physically secure privacy-preserving key-agreement protocol for vehicular ad-hoc network. *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[136] C. P. Schnorr. Efficient identification and signatures for smart cards. In *Advances in Cryptology (Crypto 89), Lecture Notes in Computer Science, Springer-verlag*, volume 435, pages 339–351, 1990.

[137] J. Shao, X. Lin, R. Lu, and C. Zuo. A threshold anonymous authentication protocol for VANETs. *IEEE Transactions on vehicular technology*, 65:1711–1720, 2015.

[138] M. S. Sheikh, Liang, and Wang. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors*, 19:3589, 08 2019.

[139] J. Shen, S. Moh, and I. Chung. Comment: "Enhanced novel access control protocol over wireless sensor networks". *IEEE Transactions on Consumer Electronics*, 56(3):2019–2021, 2010.

[140] W. Shi and P. Gong. A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. *International Journal of Distributed Sensor Networks*, 9:730–831, 2013.

[141] V. Shoup. Sequences of games: A tool for taming complexity in security proofs. Cryptology eprint archieve, report 2004/332, available at http://eprint.iacr.org/2004/332, 2004.

[142] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam. A new type of blockchain for secure message exchange in VANET. *Digital communications and networks*, 6:177–186, 2020.

[143] M. Singh and S. Kim. Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain. *arXiv preprint arXiv:1707.07442*, 2017.

[144] W. Stallings. *Cryptography and Network Security: Principles and Practices.* pages 328-345, Pearson Education, 3rd edition, 2004.

[145] D. S. Standard. FIPS PUB 186-3, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, June 2009.

[146] M. Stanislav. *Two-Factor Authentication* . IT Governance Publishing, Apr 2015.

[147] F. Syverson and I. Cervesato. The Logic of authentication protocols. In *Revised Versions of Lectures Given During the IFIP WG 1.7 International School on Foundations of Security Analysis and Design on Foundations of Security Analysis and Design: Tutorial Lectures (FOSAD'00)*, pages 63–137, Berlin, Heidelberg, 2001.

[148] H.-R. Tseng, R.-H. Jan, and W. Yangand. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks. In *IEEE GLOBECOM 2007 proceedings*, pages 986–990, 2007.

[149] M. Turkanovi, B. Brumen, , and M. Holbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad-Hoc Networks*, 20:96–112, 2014.

[150] M. Turkanovic and M. Holbl. An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *ElektronikairElektrotechnika*, 19:109–116, 2013.

[151] A. Varga and R. Hornig. An overview of the omnet++ simulation environment. In *1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, 2010.

[152] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. TinyPK: securing sensor networks with public key technology. In *Proceedings of the 2nd ACM Workshop on Security of ad hoc and Sensor Networks, SASN 2004*, pages 59–64, Washington, DC, USA, October 2004.

[153] K. Wong, Y. Zheng, J. Cao, and S. Wang. A dynamic user authentication scheme for wireless sensor networks. In *Proceedings of IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing, IEEE Computer Society*, pages 244–251, 2006.

[154] A. Wood and J. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, 2002.

[155] J. Wu and D. R. Stinson. Three Improved Algorithms for Multipath Key Establishment in Sensor Networks Using Protocols for Secure Message Transmission. *IEEE Transactions on Dependable and Secure Computing*, 8(6):929–937, 2011.

[156] X. Li, Q. Wen, W. Li, H. Zhang, and Z. Jin. A biometric-based password authentication with key exchange scheme using mobile device for multi-server environment. In *Applied Mathematics & Information Sciences*, 2015.

[157] X. Liu, Z. Fang, and L. Shi. Securing vehicular ad-hoc networks. In *2nd IEEE International Conference on Pervasive Computing and Application(ICPCA)*, pages 424–429. IEEE Computer Society, 2007.

[158] R. Xu, D. Nagothu, and Y. Chen. Econledger: A proof-of-enf consensus based lightweight distributed ledger for iovt networks. *Future Internet*, 13(10):248, 2021.

[159] K. Xue, C. Ma, P. Hong, and R. Ding. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, 36:316–323, 2013.

[160] X. Xue and J. Ding. LPA: a new location-based privacy-preserving authentication protocol in VANET. *Security Communication Networks*, 5(1):6978, 2012.

[161] Y. Zhang, D. He, P. Vijayakumar, M. Luo and X. Huang. Sapfs: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for industrial internet of things. *IEEE Internet of Things Journal*, 10(11):9716–9726, 1 June 2023. doi: 10.1109/JIOT.2023.3234178.

[162] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, , and H. W. Wei. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*, 11:4767–4779, 2011.

[163] Z. Shi, C. Beard, and K. Mitchell. Analytical models for understanding space, backoff and flow correlation in csma wireless networks. *Wireless networks*, 19(3):393–409, 2013.

[164] M. Zang, Y. Zhu, R. Lan, Y. Liu, and X. Luo. Bavc: Efficient blockchain-based authentication scheme for vehicular secure communication. In *2021 13th International Conference on Advanced Computational Intelligence (ICACI)*, pages 346–350. IEEE, 2021.

[165] L. Zhang. Modeling large scale complex cyber physical control systems based on system of systems engineering approach. In *20th International Conference on Automation and Computing*, pages 55–60, Cranfield, UK, 2014. doi: 10.1109/IConAC.2014.6935460.

[166] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Digital communications and networks*, 462:262–277, 2018.

[167] Y. Zhou, S. Liu, M. Xiao, S. Deng, and X. Wang. An efficient v2i authentication scheme for vanets. *Mobile Information Systems*, 2018:1–11, 2018.

[168] Y. Zhou, Y. Zhang, and Y. Fang. Access control in wireless sensor networks. *Ad Hoc Networks*, 5:3–13, 2007.

[169] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang. Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks. *IEEE Transactions on Mobile Computing*, 9(7):913–926, 2010.

Md. Ismail
18/04/2024

Jamuna Kanta Sing, Ph.D.
Professor
Dept. of Computer Science & Engineering
Jadavpur University, Kolkata-700032

डॉ. शांतनु चटर्जी/Dr. SANTANU CHATTERJEE
वैज्ञानिक / Scientist
अनुसंधान केंद्र इमारत/Research Centre Imarat
डॉ. ए पी जे अब्दुल कलाम प्रक्षेपास्त्र सम्मिश्र / Dr. APJ Abdul Kalam Missile Complex
डी आर डी ओ, रक्षा मंत्रालय, भारत सरकार, हैदराबाद
DRDO, Ministry of Defence, Govt. of India, Hyd-69