Abstract

Over last few years, with the massive growth of smartphone technology and mobile internet, the use of various Online Social Networks (OSNs) has increased rapidly. This ever-growing use of OSNs leverage cyber-attackers to exploit various security threats. Hence, the design of security protocol, authentication, and access control mechanism is highly essential for OSN applications. This thesis covers: 1) privacy preservation in location sharing, 2) mitigation of DDoS attack, and 3) mitigation of Phishing Attack resisting protocols for mobile-based OSN applications.

In the first study, a privacy-preserving, secure, and efficient location-sharing scheme for mOSNs is described, which is efficient and flexible for location updates, sharing, and queries of social friends and strangers. The security of the proposed scheme is validated using BAN logic-based proof, informal security analysis, and ProVerif 1.93 simulation tool.

The second study is on a multi-faceted, secure, and lightweight authentication scheme that resists DDoS attacks in mobile OSN environments. After a predefined threshold, the scheme discards further login attempts blocking an adversary who intends to overload the server. Using NS3 simulator, the impact of DDoS attacks on network throughput and delay is shown. Using the CIC DoS dataset, and machine learning algorithms, the performance is demonstrated in a practical DDoS attack detection scenario achieving 97.05% attack detection accuracy.

The final study describes a secure, lightweight cryptography-based authentication scheme (ASPA-mOSN) for resisting phishing attacks in OSNs. In OSN, phishers steal sensitive information by sending fraudulent communications. For resisting these attacks, secure authentication using only the password and biometrics is done. The security of this scheme is explained with an informal and formal Real-Or-Random (ROR) model. Finally, the security, and functionality of this scheme are compared with other existing related schemes showing the scheme outperforms.