ABSTRACT

The motivation behind our research is the need to counter the ever-evolving security attacks, especially during the authentication process in a system. As part of this thesis work, an innovative authentication framework has been designed to counter security threats across diverse systems and scenarios. In one of the solutions, a novel one-time password authentication system has been developed based on QR code and a multi-dimensional hash chain. An OTP will be generated at the client end based on a challenge thrown by the server. This challenge is represented in the geometrical coordinate system as a random path originating from the origin and leading to a point located within a multi-dimensional hypercube. Another solution introduces a unique one-time QR code-based mechanism. This method leverages context-aware authentication by embedding dynamic information within the QR code, which varies with each login attempt. Based on the encoded data, users generate a one-time password derived from their original password. Our next solution is designed for ATM kiosks where the prominent mode of authentication is an ATM card and its associated PIN. This method suffers from some difficulties, such as carrying an additional ATM card during use, manufacturing and securely shipping the ATM card to the end user, being prone to ATM card skimming, etc. To handle these challenges, we have designed a solution to authenticate in ATM networks using NFC and blockchain. The communication range for data exchange between two NFC devices is very small, making it a good choice for exchanging sensitive data. In another research, we have used the context of users and devices during authentication to detect anomalies and security-related attacks. In our research, in particular, DoS/DDoS attacks & brute-force techniques have been analyzed in detail. Extensive simulations were conducted on the CIC-IDS2017 dataset using the Weka tool. The performance metrics of recall, precision, accuracy, f-score, and model-built time were computed for the four machine-learning classifiers—J48, Random Forest, Multi-Layer Perceptron, and Bayes Net—for different combinations of data splits and groups of data features.