**New Hashing Algorithm and an Authentication Technique to Improve IoT Security**

Abstract

The Internet of things (IoT) is the decade's hero technology. The majority of the enterprises, market demands, and researchers worldwide shed light on this great innovation. The IoT collects and processes data from distant locations, substantially increasing the productivity of dispersed systems or people. Due to the restricted budget available for power consumption, IoT devices usually lack sophisticated data encryption and device authentication. By and large, the hardware components used in IoT devices do not have powerful resources. As a consequence, the integrity and security of the majority of IoT devices are in doubt. For instance, an adversary may include a Hardware Trojan (HT) during the manufacturing phase of IoT hardware devices in order to trigger data leakage or device failures.

Optimizing the current cryptography algorithms is one of the best solutions to enhance the security of IoT applications. This optimization should be so that the algorithm is still secure while it requires a much lower resource amount than the original version of the algorithm.

This work deals with two approaches to enhance IoT Security. The first approach presents a new hashing function suitable for all IoT devices, ranging from tiny, limited processing power that works on batteries to huge devices with continuous electrical power and heavy resources. The algorithm is based on the Secure Hash algorithm (Sha256), and it is called the Internet of Things Secure Hash Algorithm (IoSha). It comes with four levels according to robustness and power consumption. The first two levels (IoSha1 and IoSha2) are less robust and more agile than Sha256, suitable for tiny IoT devices. However, the IoSha3 algorithm is precisely equivalent to the Sha256 algorithm. In contrast, the other two levels (IoSha4 and IoSha5) are more powerful and needs more resource power, ideal for larger IoT devices with powerful resources and continuous electrical power. Six different tests are performed to ensure the proposed algorithm is secure and fulfil the requirements.

The second approach proposes a flexible technique to enhance the authentication security between IoT devices and the cloud database. This approach helps establish a direct connection between the IoT application and the cloud database. The Application Programming Interface (API) is used only at initial functions of the system like account creation, login, change password, and change role. When an account is created, a database credential will be selected upon the user's privilege level. Then it will be encrypted using the users' password as a key for Advanced Encryption Standard (AES) algorithm and stored in the database. While the users log in to their accounts, the encrypted database credential will be sent back to the client application after the account verification. Finally, the encrypted data will be decrypted using the users' password as a key for the AES algorithm from the client application. The IoT application has all the crucial information to establish a database connection with the cloud database without using API for further queries. The database credential is observed to be sure it is securely stored when an account is created. And, the transmitted packet that holds the database credential is captured and analyzed to ensure the technique's robustness. The C# language is used for software development and evaluation purpose. However, this technique can be implemented for other platforms and programming languages.