

Hisham Raad Jafer Merzeh, Mustafa Kara, Ali Aydın, Hasan Hüseyin Balık

Secure Mutual Authentication Scheme for Iot Smart Home Environment using Biometric and Group Signature Verification Methods

Abstract: Smart equipment in smart home environments is ubiquitous and widely separated nowadays. Thus, the smart things are connected through the network to make it accessible everywhere in the world and remotely controlled. But connection to internet (public network) made the smart things vulnerable to hacking, exploitation and compromised incorrectly, and guaranteeing its security has been a broad concern. Many research and studies discuss these security problems and propose different solutions to solve these problems. However, the nature of smart devices and the lack of resources makes securing them significant challenges. Most of the existing solutions for these issues are based on single server architecture with low concern for privacy and anonymity. This paper proposes a new authentication approach for authenticating users and devices in a smart home environment. This approach is an improvement of the existing methods. In this work, we combined the group signature scheme with the biometric signature to propose an authentication mechanism based on decentralized architecture. First, we utilize the biometric data using fuzzy extractor algorithm for authentication legitimate user of the device. Then, the user device is authenticated as a group member of the smart home using group signature. The group signature is a blockchain-based scheme that allows a group member to sign their request for remote access or control. The request is received as a group request instead of a specific group member. Every group member has its group private key used for signing the request and the group public key used for request verification. Compared with existing approaches, this mutual authentication technique can provide high security, reliability in addition to the privacy and anonymity. This research integrates biometric user data, group signature, message authentication code, elliptic curve integrated encryption, and blockchain to increase the security and reliability of the authentication mechanism. We analysis the security features of our proposed scheme by comparing it with existing scheme.

Keywords: IoT, Authentication, smart home, biometric authentication, blockchain

ACCEPTANCE LETTER

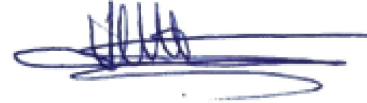
Dear Hasan Hüseyin Balık

balik@yildiz.edu.tr, Yildiz Technical University Graduate School of Science and Engineering Faculty of Electrical and Electronics Engineering Istanbul 34220, Turkey

After the three-reviewer based evaluation process, your paper titled as "Secure Mutual Authentication Scheme for IoT Smart Home Environment using Biometric and Group Signature Verification Methods" has been accepted for 'oral presentation' at ICAIAME 2022 (International Conference on Artificial Intelligence and Applied Mathematics in Engineering 2022), which will be held Baku, Azerbaijan (20-22 May 2022). Congratulations!

In the context of ICAIAME 2022, your paper may be published under the Springer Series: Engineering Cyber - Physical Systems and Critical Infrastructures and conference E-Abstract book. There are also additional opportunities for extended versions of the English or Turkish 'selected papers' to be published in TR-Index (ULAKBIM) indexed journals or international Indexed journals, if the related papers meet well enough with the scope and quality criterions of the journals project. At this point, please do not forget to submit your final paper till the mentioned submission deadline (more information are over the Web site).

Thank you very much for your great contribution to the ICAIAME 2022.



Prof. Dr. Tuncay Yiğit
Conference President

Paper Title:Secure Mutual Authentication Scheme for IoT Smart Home Environment using Biometric and Group Signature Verification Methods

Paper ID:298

Authors:Hisham Raad Jafer Merzeh, Mustafa Kara, Ali Aydın, Hasan Hüseyin Balık