World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:05, 2022

A New Block Cipher for Resource-Constrained Internet of Things Devices

Authors : Muhammad Rana, Quazi Mamun, Rafiqul Islam

Abstract : In the Internet of Things (IoT), many devices are connected and accumulate a sheer amount of data. These Internet-driven raw data need to be transferred securely to the end-users via dependable networks. Consequently, the challenges of IoT security in various IoT domains are paramount. Cryptography is being applied to secure the networks for authentication, confidentiality, data integrity and access control. However, due to the resource constraint properties of IoT devices, the conventional cipher may not be suitable in all IoT networks. This paper designs a robust and effective lightweight cipher to secure the IoT environment and meet the resource-constrained nature of IoT devices. We also propose a symmetric and block-cipher based lightweight cryptographic algorithm. The proposed algorithm increases the complexity of the block cipher, maintaining the lowest computational requirements possible. The proposed algorithm efficiently constructs the key register updating technique, reduces the number of encryption rounds, and adds a new layer between the encryption and decryption processes.

Keywords : internet of things, cryptography block cipher, S-box, key management, security, network
Conference Title : ICNSS 2022 : International Conference on Networking Systems and Security
Conference Location : Berlin, Germany
Conference Dates : May 23-24, 2022