Sooner Lightweight Cryptosystem: Towards Privacy Preservation of Resource-Constrained Devices

Abraham Ayegba Alfa[0000-0001-5926-9520][1], John Kolo Alhassan[2], Olayemi Mikail Olaniyi[3], Morufu Olalere[4]

abraham.alfa@st.futminna.edu.ng,
{jkalhassan,mikail.olaniyi,lerejide}@futminna.edu.ng

Abstract. The use of cryptosystem became popular because of the increased need for exchanges across untrusted medium especially Internet-enabled networks. On the basis of application, several forms of cryptosystems have been developed for purpose of authentication, confidentiality, integrity, and non-repudiation. Cryptosystems make use of encryption schemes that convert plaintext to ciphertext in diverse areas of applications. The vast progressions in the Internet of Things (IoT) technology and resource-constrained devices have given rise to massive deployment of sensor devices and growth of services targeted at lightweight devices. Though, these devices support a number of services, they require strong lightweight encryption approaches for privacy protection of data. Existing lightweight cryptosystems fall short on the expected privacy levels and applicability in emerging resource-constrained environment. This paper develops a mathematical model for a sooner lightweight cryptographic scheme based on reduced and hardened ciphertext block sizes, hash sizes and key sizes of traditional cryptosystems and Blockchain technology. Thereafter, the hardening procedure offered by the RSA homomorphic encryption was applied for the purpose of generating stronger, secure and lightweight AES, and SHA-3 in order to deal with untrusted channels exchanges. The proposed Sooner is recommended for adoption in public Blockchain-based smart systems and applications for the purpose of data privacy at 95% likelihood.

Keywords: Lightweight, encryption, block size, key size, Blockchain technology, Internet of Things, resource-constrained devices, Hashes, data transmission, hardening, Homomorphism.

1 Introduction

There is need to address the various problems faced by users when generating, storing and transmitting data across the cloud-based services. There are high demands to secure cloud infrastructure stack at network, host, application and data levels. A number of data security problems have been reported in [1] including: data privacy, confidentiality and authentication. In cloud services such as traditional smart rice farming that is built on cloud utilizes plaintext data format for generation, transmission and storage. Recently, users are capable of applying encryption and decryption algorithms for the purpose of providing protection for data for varying processing