International Journal of Grid and Distributed Computing
Vol. 13, No. 2, (2020), pp. 2228-2234

Fully Homomorphic Secure Internet of Things Framework Over Untrusted Cloud

Idris Afzal Shah[1*], Adil Bashir[2] , Sheikh Moeen ul Haque[3] , Dr. Mohammad Ahsan Chishti[4], Dr. Shaima Qureshi[5]
[1,2,3]*Department of Computer Science and Engineering, School of Engineering and Technology, Islamic University of Science and Technology,Awantipora, J&K, India*
[4,5]*Department of Computer Science and Engineering, National Institute of Technology, Srinagar, J&K, India*
[1]*idrisshah@yahoo.com,*[2]*adilbashir.445@gmail.com,*[3]*sheikhmoin41@gmail.com,*
[4]*ahsan@nitsri.net,*[5]*shaima@nitsri.net*

Abstract

Leveraging the cloud support has proven critical and pivotal in storing/managing the data being generated at an exponential rate by Internet of Things (IoT) devices. The data sensed by IoT devices is private mostly and needs to be protected from unauthorized users during its transit where symmetric/ asymmetric cryptography like RSA, AES work well. However, these cryptosystems fail as they need to access plaintext for performing data analytics thus revealing data to cloud owners. The proposed model mitigates this concern by employing fully homomorphic encryption (FHE) for enciphering of data collected from the sensor for privacy preserving and providing confidentiality services before sending it to the cloud for analytics. FHE allows direct computation on encrypted data. Moreover, the model performs error detection / correction using Reed Solomon Codes (RS Codes) at edge/fog nodes and at cloud also as an additional security measure keeping in mind the sensitivity of the data obtained for IoT system. It is a unique model combining power of FHE and RS codes for IoT objects.

Keywords: *Cloud; Fully Homomorphic Encryption (FHE); IoT; Reed Solomon Codes ;Security.*

1. Introduction

Any physical object equipped with communication portion can connect to the Internet and be a part of the loT infrastructure. It includes almost everything you would consider including wearable's, bulbs, TV , etc. The number of loT-enabled devices is now 22 billion as per the Strategy Analytics Report, and the study estimates that 38.6 billion devices will be connected by 2025 and 50 billion by 2030[1]. [1]

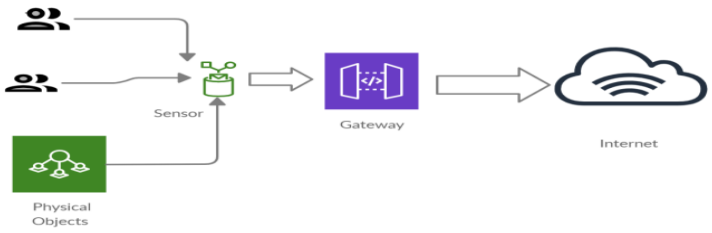

Figure 1. IoT architecture

1.1. Home Automation

ISSN: 2005-4262 IJGDC