I.J. Wireless and Microwave Technologies, **2021, 4, 41-45**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.04.05

Resource Efficient Security Mechanism for Cloud of Things

Adil Bashir and Sahil Sholla
Department of Computer Science & Engineering, Islamic University of Science and Technology, Kashmir, India
Email：adilbashir.445@gmail.com

Received: 30 May 2021; Revised: 09 June 2021; Accepted: 27 June 2021; Published: 08 August 2021

Abstract: Cloud of Things (CoT) relates to the convergence between Cloud Computing (CC) and the Internet of Things (IoT) and has significantly transformed the way services are delivered in the ubiquitous realm of devices. This integration has become essential because of the huge data being generated by IoT devices, requiring an infrastructure for storage and processing. Such infrastructure is provided by Cloud Computing services with massive space for data storage and exceptional platform to process complex data. IoT networks are vulnerable to multiple security breaches because of the growing usage of IoT devices in user personal systems. This leads to security and privacy threats that need to be addressed. IoT consists of resource limited devices which have feeble computing power, battery source and storage capacity. This paper addresses security issue by proposing usage of obfuscation and encryption techniques to scramble the data at IoT devices which is later on stored in encrypted form at the cloud server. The data at IoT devices is classified into highly critical or less critical and accordingly the appropriate technique between encryption and obfuscation is applied. The proposed mechanism is evaluated in terms of processing time for cryptographic operations at IoT devices. Evaluation results depict that the proposed mechanism is 1.17 times faster than [22] in terms of encryption and decryption times.

Index Terms: Cloud Computing, Cloud of Things, Encryption, Obfuscation, Internet of Things.

1. Introduction

Cloud Computing and Internet of Things have recognized an individualistic transformation. Although some mutual favors have been listed in the literature as a consequence of their merger and are anticipated in future. In particular, the Cloud provides a versatile tool for managing and designing IoT services, and even some applications that manipulate the stuff or the information that they generate [1]. From the other side, the Cloud takes advantage of IoT by extending its purview to cope with issues in the actual environment in the most suitable and efficient manner, and to introduce new services in various real-life scenarios. IoT finds applications in many fields such as smart Buildings, smart cities, smart agriculture etc [2]. Typically IoT is described by tiny devices in the modern world, widely distributed with finite storage and processing capabilities focusing on issues such as efficiency, output, and privacy protection [3, 4]. And from the other hand, cloud computing, having huge potential in terms of storing and processing power, is a highly developed technology which helps the IoT to partially solve its problems. Consequently, the current as well as future internet should be transformed by a new IT paradigm that combines these two complementary technologies.

Security is among the big concern that needs to be kept in mind while exchanging information in the Cloud-IoT environment [5]. The various security attacks by insiders and outsiders to IoT is because of its wireless nature. The on-going contact among the IoT devices or the IoT network and Cloud interface can be disrupted by an intruder [6-9]. Infected Cloud-IoT connectivity adversely affects secure and effective Cloud data storage. Meanwhile, Cloud usage to enable IoT data storage poses privacy issues by requiring all users to access information globally. There is a requirement of secure communication between IoT gadgets and Cloud framework, what is significant to protect person privacy and security within the CoT setting. The existing security mechanisms for CoT environment are complex and consume significant resources which is not feasible for IoT devices. IoT environment is characterized by constrained resources which are to be used efficiently in order to keep the devices functional for longer period of time. The work done in this paper address the security issue in Cloud-IoT environments by proposing an Authenticated-Encryption mechanism in order to safeguard sensitive data from attackers and requiring less time for cryptographic operations.