RESEARCH REVIEW JOURNALS
Volume-04
Issue-03
March-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Performance Analysis of Light Weight Security Algorithms for Resource Constrained Devices

Khan Riaz

Assistant Prof., Computer Science and Engineering, Islamic University of Science and Technology, Kashmir (India)

ARTICLE DETAILS

Article History
Published Online: 13 March2019

Keywords
IoT, Light weight security, Constrained devices, sensor networks, Raspberry Pi.

***Corresponding Author**
Email:riazk3[at]gmail.com

ABSTRACT

With the advent of technologies like Internet of Things (IoT) and Machine to Machine (M2M) communication, a huge quantity of data is generated every day. Being a distributed system of constrained devices, this data needs to be communicated securely without wasting the resources of constrained devices. Therefore there is need of appropriate lightweight security protocols to avoid the security threat to future internet. In this context, a study of lightweight security algorithms is presented in this paper. The algorithms are first theoretically analyzed followed by their implementation on Cryptool and Raspberry Pi in order to check their efficacy.

1. Introduction

Internet of Things (IoT) is a novel worldview that is quickly making progress in the field of cutting-edge remote media communication [1]. IoT is a global movement that unites people, data, processes and things to build network connections that are more pertinent and useful than ever before. It is a structure of interconnected computing items, such as RFID tags, sensors, actuators, and cell phones; digital machines; and people that offer the facility of transferring data among networks without need of human-to-computer or human-to-human interactions.

As IoT is growing rapidly, it faces risks and challenges, such as how to handle huge amounts of data, processing power, deal with energy consumption, address security threats, and how to encrypt/decrypt huge data [1].

IoT helps in creating connections between dissimilar things present in heterogeneous environment. This kind of openness and very less human intervention can make IoT exposed to number of attacks like man in middle attack, Denial of Service (DoS) attack. Moreover, any device can have access the network that leads to unauthorized access. These attacks can damage device physically and network connections too. This will ultimately compromise the security and privacy of IoT.

To address these challenges when many smart devices are connected in an IoT environment, there is an increasing demand for the use of appropriate cryptographic solution into the embedded applications. However, these smart devices usually have limited resources with low computational power, low battery life, smaller size, limited memory and power supply. Hence, the conventional cryptographic primitives might not be suited for low-resource smart devices. Therefore in such applications lightweight cryptography is introduced that provides solutions suitable for constrained devices [2].

Furthermore, IoT has also exposed many security attacks that can damage the network connection due to an unauthorized access. This leads to the security parameters and network privacy being compromised. In addition, IoT utilizes the cloud computing concept, which has many security issues and challenges [2, 3]. Apart from these issues, the resource-constrained devices, which have less computational power, limited battery life, a small amount of memory, and low bandwidth, need an efficient security solution that will not crunch the resources of IoT.

Therefore this paper presents a study of the lightweight algorithms suitable for resource-constrained devices that form the bulk of the IoT setup. Algorithms including AES, Mickey 2, Grain, Rabbit and TEA were first simulated using an Open-Source Software tool viz., Cryptool and later implemented using Java programs on Raspberry pi.

The remainder of this paper is organized as follows: Section 2 presents the background and survey of the field, section 3 details the work carried out, section 4 gives the experimental results and comparison both using Cryptool and the Java platform. Finally the paper is concluded in section 5.

2. Background

In [4, 5], Cryptography is defined as an ancient art of writing secret with the knowledge of science. Cryptography was first used in writing long dates back to circa 1900 B.C. where it was used as non-standard hieroglyphs in an inscription by an Egyptian. Some specialists claim that cryptography came into existence suddenly after writing was developed, with kind of applications such as political letters to war-time battle tactics. With the development of computer communication the new forms of cryptography was discovered as surprise to many intended users. When communicating over an insecure and untrusted medium such as internet, cryptography is necessary to secure the data under transmission.

There are five primary functions of cryptography today:

i) Privacy/confidentiality: This function ensures that only intended receiver can read the message and no one else.
ii) Authentication: It helps in providing one's identity.

RRIJM 2015, All Rights Reserved