Chapter 17
Advanced Encryption Standard With Randomized Round Keys for Communication Security in IoT Networks

Ishpal Singh Gill
Namibia University of Science and Technology, Namibia

Dharm Singh Jat
Namibia University of Science and Technology, Namibia

ABSTRACT

Internet of things (IoT) is a rapidly emerging architecture connecting smart devices all across the world in various fields like smart homes, smart cities, health sector, security, etc. Security is a very important aspect of IoT. As more and more devices are connecting to the Internet, it becomes a lucrative target for hackers. The communication between the various devices, nodes, and between nodes and the cloud, needs to be secured. A combination of public and private key cryptography systems is used to secure the IoT networks. The Advanced Encryption Standard (AES) is used for encrypting the data in transit. However, the AES is known to be prone to brute force attacks, side channel attacks, and other forms of cryptanalysis. This chapter proposes a more secure AES algorithm with randomised round keys, which provides better security with negligible overheads, and is ideal for use in IoT networks.

INTRODUCTION

Internet of Things is rapidly emerging architecture in all fields in the world. It has tremendous benefits in the health, medical, traffic management, smart homes, smart cities (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014) etc sectors. The basic architecture of IoT is a three layered architecture, Layer 1 consists of the various smart devices, sensors etc., Layer 2 consists of the network protocols which help these devices to communicate with the Internet and the third layer is the applications and processes which are the deliverables to the end user. The IoT networks also require security for confidentiality,

DOI: 10.4018/978-1-5225-9246-4.ch017

integrity, authentication and availability. A combination of public and private cryptography is ideal for this purpose, with public key cryptography being used for providing authentication, integrity, key distribution and private key cryptography algorithms like AES being used for encryption and confidentiality of data communication. The combination is based on the utilizing the inherent strength of both types of crypto algorithms and averting the disadvantages of each. The symmetric algorithms or the private key algorithms are inherently much stronger but have the problem of key distribution and management, whereas the asymmetric algorithms or the public-private key algorithms, although not as strong as symmetric algorithms, provide for easier key management and secure distribution over networks. (Stallings, Cryptography and network security principles and practices, fourth edition, 2005, Forouzan, 2007).

The Advanced Encryption Standard (AES) is a 128 bit block cipher with key sizes of 128, 192, 256 bits (Kak, 2018). It is the FIPS standard for symmetric algorithms based on the design of the Rijndael algorithm, and is the strongest known symmetric algorithm. The only known vulnerabilities of AES are brute force and side channel attacks. A number of modifications of the AES have been attempted in order to make it more complex and secure. However, none of them address the use of randomised round keys to strengthen the security.

The only known unbreakable cipher is the One Time Pad (OTP), which uses a truly random key stream equal in length to the text size to encrypt the text. The output is a truly random encrypted text which is impossible to decrypt without the key stream and the key stream cannot be obtained through any known cryptanalysis technique. However, this system has the disadvantage of manual key distribution which involves huge administrative and logistics effort and cost (Schneier, 1996; Menezes, Oorschot, & Vanstone, 1997).

This chapter studies and analyses the various earlier usage of AES and AES modifications to secure IoT networks. A number of such modifications have tried to enhance the security of the AES algorithm. However, none address the use of randomised keys to enhance security., This chapter proposes a modified AES algorithm with randomized round keys, which will make AES more complex with randomize round keys, thus making it more difficult to break with negligible effect on efficiency, and thus ideally suited for security of IoT networks.

LITERATURE REVIEW

Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a symmetric cipher which works on 128 bit block data with three key size variants of 128, 192 and 256 bits. The encryption consists of repeated iterations of four operations performed on the data over 10, 12 and 14 rounds for the 128, 192 and 256 bit key variants respectively. The four operations are Sub Bytes, Shift Rows, Mix Columns and Add Round Key. For the 128 bit key version, the single 128 bit key is broken down into 11 keys of 128 bits. One key is used in the initially to XOR with the text/data and thereafter the balance 10 keys are used for each of the 10 rounds. The last round has three operations without the Mix Columns operation. The decryption is the exact reverse of the encryption process *(FIPS Publication 197, 2001;* Daemen & Rijmen, 1999, 2013). The AES algorithm is the strongest known symmetric algorithm. The only known attacks against AES are the brute force attack, wherein the attacker obtains the key by trying out all possible bit combinations