International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

A Cryptographic Approach for Securing IoT Devices

Vipul Goyal[1], Abu Zafar[2]

[1]*Student, Computer science and Engineering, ASET, Amity University, Noida, U.P., India*
[2]*Student, Computer science and Engineering, ASET, Amity University, Noida, U.P., India*

Abstract - Cryptography is a way of communication that is secure. The prefix "crypt" means "hidden" and the suffix "graphy" means "writing". In cryptography, plain text is converted to encrypted text before it is sent, and it is converted to plain text after communication on the other side. The algorithms are utilized to create cryptographic keys, for digital signatures, for verification to secure the confidentiality of information, to browse the Internet and to ensure confidential transactions such as credit and debit card transactions. The Internet of Things (IoT) is a vastly growing area in computer science as it helps exchange data by interconnecting devices over the internet, therefore, it should be secured. IoT's are making smart devices smarter and of higher quality to enhance the user experience. IoT's security challenges are more vulnerable because the devices are openly accessible to all in the network. In this paper, cryptographic methods are proposed to secure the IoT devices i.e. four of the most used encryption algorithms namely: AES (Rijndael), DES, Triple DES and Blowfish.

Key Words: Cryptography, Internet of Things

1. INTRODUCTION

These days, the figure of connected gadgets is expanding exponentially, forming the so-called Internet of Things (IoT). In the sight of IoT, every real object has virtual components, for example, a person in real has a virtual counterpart that can be located, addressed and read. It's a network of devices that are connected to the internet, thus they have their own IP addresses and can interface with one another to automate simple tasks. IoT is among the developing advances that would be the best specialists to change the current world scenarios. These devices are used in various fields, e.g. in smart homes, in public health, in smart cities, in environmental monitoring, in smart traffic systems, etc. The Internet and its users are already under attack and a growing economy full of models is undermining the moral use of the Internet: it is only aimed at developing the basic concepts of the weaknesses of the current version. This is not a good signal for IoT, which integrates many limited devices. In fact, the implementation of the IoT concept can lead to the emergence of new malicious models. The challenge is to prevent the growth of these models, or at least reduce and limit their impact.

Internet of Things is a new development and a huge set of computing components that are currently connected to each other on the Internet. IoTs are essentially distributed physical network devices that work intelligently to collect information from environmental parameters. These devices can transmit information and send messages to each other. The concepts of Internet of Things devices are like thinking out of the Box. For example, an IoT-based chair can be adapted to the size of the occupant. Based on these calculations, you can automatically increase or decrease sleep hours.

IoTs change people's lifestyles, increase productivity and reduce life stress to protect the environment. IoTs are next generation networks and a new and moderate way of the Internet to offer the ultimate in wisdom. IoT devices can collect and analyze a large amount of data, make a smart decision, and share information with devices so they can act smart.

These additional services are accompanied by their own prerequisites and limitations; therefore, several challenges have been raised:

• Network difficulties for endless number of devices to communicate with each other.

• Security challenges: The number of nodes in the network and its wide range of IoT networks for deployment and applications have become more engaging both as a target and as an attack tool.

• Power consumption faces the impossibility of implementing heavy conventional cryptographic mechanisms and security protocols on small devices with limited power sources.

Security concerns are important. The Internet of Things talks about existing cybersecurity vulnerabilities and presents new security threats. This poses the usual risks associated with sending information through the system. Each terminal (node) can be an access point and connectivity analysis will increase damage. Hacker attacks on intelligent energy systems can power millions of households and businesses, causing tremendous financial damage and threatening health and safety. IoT security breaches impact both personal data abuse and device theft. Therefore, when developing IoT applications, security is a fundamental requirement and security plays an important role in preventing unauthorized access in IoT application systems.

Cryptographic algorithms should develop security solutions that protect IoT networks and minimize security risks. However, the actual implementation of these cryptographic algorithms depends on the performance limitations of IT and IoT devices. However, choosing the right hardware, software

platform, and fundamental architecture for your application is an important step in building an IoT system. Most IoT applications include embedded systems that were used many years ago but are now becoming compatible smart devices that require network connectivity, memory usage, and scalable features. This integrated hardware system is a good example of reducing costs and energy consumption.

Cryptography is a technique used for converting plain text to encrypted text and vice-versa. It is used for security purposes. The CIA triad is a very important terminology when we talk about security. Confidentiality means data must be kept a secret from both ends. It should not be leaked as it violates the security of the system. Integrity means ensuring the accuracy and completeness of the data. This is to protect the data from misuse or alteration by an unauthorized party. Authentication confirms that the person entering the network is valid and genuine.

The three classifications of cryptographic systems are based along the following three independent parameters- Kind of activities utilized for changing plain text to cipher text, the number of keys utilized and dealing with plain text.

All encryption algorithms depend on two general standards. The first is substitution, where each component of the plain text is assigned to a different component, and transposition, where the raw content components are arranged differently. The basic requirement is that no data is lost. Most systems, called product systems, had many stages of replacement and conversion.

If the sender and recipient have the same key, the system is called symmetric encryption with the same or private key. If the sender and recipient use different keys, the system is considered asymmetric two-key cryptography or public-key cryptography.

Block cipher encryption always processes the inputs into an element block, so an output block is generated for each input block. Current encryption processes input elements continuously and leads to a result element.

2. LITERATURE REVIEW

- In 2016, Dewanjee et al [1] have worked on a collated report on security challenges of IOTs and the Cryptographic methods used to overcome the challenges. As per a report by Cisco, stating that by 2020 there will be an enormous number of IoT devices which will take over to cover all the sectors like health services, transportation, and smart devices covering all areas of life. IoTs making Smart devices are becoming smarter and of higher Quality to enhance the user experience. IoT's security challenges are more vulnerable because the devices are openly accessible to all in the network.

- In 2018, El-hajj et al [2] have worked on analyzing the efficiency of various cryptographic algorithms in an IoT device and comparing it to the basic cost of the device. Their study provided evidence that security protocols with basic cryptographic elements (symmetric, asymmetric, hash code, and digital signature) could be entered into the system.

- In 2010, Elminaam et al [3] have worked on this article, we evaluate the performance of some symmetric encryption algorithms. The algorithms used in the study are DES, 3DES, AES, Blowfish, RC2, and RC6. Various results can be obtained from the experimental results. First, if the results are displayed in hexadecimal or 64 base code, it doesn't make much difference. Second, they found that Blowfish outperforms other popular coding algorithms and outperforms RC6 when the packet size is changed. Third, it turns out that 3DES still crashes compared to the DES algorithm. Fourth, it turns out that RC2 is time consuming compared to all other algorithms. Fifth, we believe that AES works better than RC2, DES, and 3DES. For audio and video files, you get the same results as for text and documents. As the size of the key changes, the size of the key increases and eventually the battery consumption and time will change significantly.

- In 2016, Awotunde et al [4] have worked on all strengths and weaknesses of encryption methods. The study summarizes that Blowfish algorithm uses more memory, CPU usage, and time to perform its cryptographic operations than it does because it uses a much longer key length (448 bits).

- In 2011, Roman et al [5] have worked on the theoretical ways to secure IoT devices. They have discussed the threats that have been caused to the interconnection of the devices on the internet.

- In 2016, Joshna et al [6] have worked on a comparative analysis of the symmetric key algorithms. It discusses all the details about the cryptographic algorithms with symmetric key.

3. ALGORITHMS

3.1 AES

Rijndael's proposal for AES (Advanced Encryption Standard) uses 128, 192, and 256 bits to decode a number that allows the block length and key length to be specified independently of each other. The key length determines some parameters of the AES algorithm.

The above algorithm has the following characteristics:

• Security or protection against all known attacks.

• Code speed and compactness on various platforms.

AES-128 uses a 128-bit key length to encrypt and decrypt message blocks, while AES-192 uses a 192-bit key length and AES-256 uses a 256-bit key length for encryption and decryption. Use key length. Each digit of the message uses 128, 192, and 256-bit encryption keys to encrypt and decrypt data into 128-bit blocks. The number, also known as the secret key, uses the same encryption and decryption keys, so the sender and receiver must know and use the same secret key. Governments classify information into three categories: confidential, secret, or very secret. All key lengths can be used to protect confidentiality and confidentiality levels. Key lengths of 192 or 256 bits are required for secret information.

A 128-bit key has 10 turns, a 192-bit key has 12 turns, and a 256-bit key has 14 turns. A round consists of several processing steps, in which a simple text input is replaced, transformed, mixed and transformed into the final output of encoded text.

3.2 DES

DES (Standard Encryption Standard) is a 64-bit symmetric block encryption algorithm. This algorithm works on 64-bit blocks of plain text. Due to the symmetry, the same key can be used for encryption and decryption. In most cases, the same algorithm is used for encryption and decryption. First, the transition is performed according to a fixed table (initial permutation), which divides a 64-bit block of plain text into two 32-bit blocks, each of which performs 16 identical operations, called rounds. The two halves are connected, and the first inversion of the permutation is performed. The purpose of the first implementation is clear. This does not affect the security of the algorithm. Therefore, small blocks of plain text and cipher text can be loaded into an 8-bit chip. Only half of the original 64-bit block is used in one run. The rounds alternate between the two halves.

3.3 Triple-DES

Triple-DES is a type of computer encryption algorithm in which each data block receives three passes. You can increase security by increasing the key length. Triple DES has been replaced by NIST, which received the above AES. Triple DES is currently considered obsolete, but some IoT products use it for compatibility and flexibility.

Triple DES is a good encryption algorithm that can be used to protect against brute force attacks. "Brute force" is a painstaking effort (as opposed to an intelligent strategy) through repeated attempts and efforts. The Brute Force attack automatically uses automated tools and then it therefore it takes guesses various combinations until a hacker breaks the key.

3.4 Blowfish

Blowfish is a block cipher and is a part of symmetric key encryption. It encrypts data in blocks of 8 bytes. The algorithm consists of two parts, a key extension part and a data encryption part. The key extension converts a key with a maximum length of 56 bytes (448 bits) into several tables with subkeys with a total of 4168 bytes.

4. REVIEW RESULTS

Table 1: Performance of Algorithm during the Encryption process

Parameters	AES	DES	Triple - DES	Blowfish
Designers	'Joan Daemen& Vincent Rijmen'	IBM	IBM	'Bruce Schneier'
Developed	1998	1977	1998	1993
Attacks	Brute force attack, Biclique attack, Related-key attacks	Brute force attack, Differential cryptanalysis, linear cryptanalysis	Chosen plain text attacks or known plain text attacks	Second order differential attack
Type of Encryption	Block Encryption	Block Encryption	Block Encryption	Block Encryption
Security	Secure	Insecure	Secure than DES	Secure
MemoryConsumptionRate (MB)	25	15	16	30
CPU Usage (%)x1000	94.8532	96.4894	85.0985	120.2343
Encryption speed (ms)	4947.7483	4747.2977	7157.5979	6471.2416
Key length in (bit)	142	132	147	448

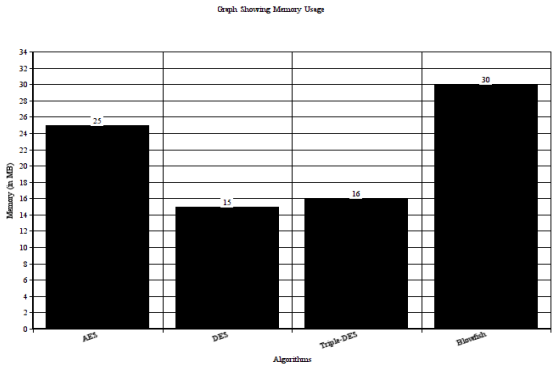

Figure 1. Graph showing Memory Usage

The graph in Figure 1 summarizes that out of the four encryption algorithms, Blowfish takes most of the memory while DES takes least of the memory.

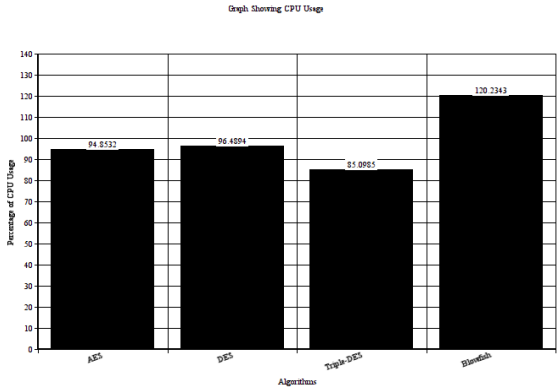

Figure 2. Graph showing CPU Usage

The graph in Figure 2 summarizes that Blowfish utilizes most of the CPU time period, and Triple-DES utilizes minimum CPU time, hence being the fastest.

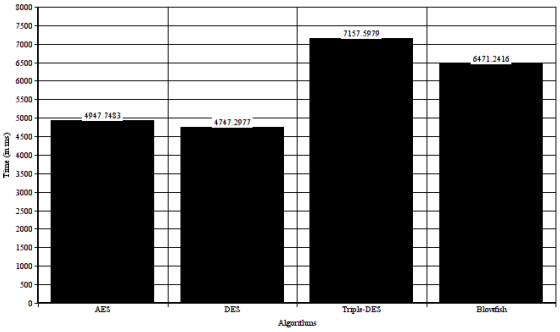

Figure 3. Graph showing the Encryption Speed of the Algorithms

The graph in Figure 3 summarizes that Triple-DES takes maximum time to encrypt, whereas DES is the fastest and takes the least time.

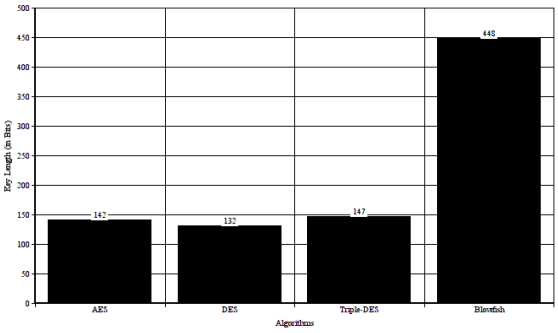

Figure 4. Graph Showing Key Length

The graph in Figure 4 summarizes that Blowfish reveals the highest Avalanche effect whereas DES reveals the least Avalanche effect. Avalanche tells us how much information is revealed.

5. CONCLUSIONS

Obviously, theoretically any key could be cracked in a brute force attack with sufficient processing power. A pragmatic approach to modern encryption is to use a key long enough that it wouldn't be compromised without extraordinary computing power, well above the value of encryption to protect content.

Cryptography can be used to protect data by controlling access to that data that has been around for a long time and as it grows, as every aspect of our human business depends on information technology. This has resulted in cryptography being required and used to protect this data from snooping eyes. Each of the encryption techniques has its own strengths and weaknesses. To apply an appropriate cryptographic algorithm to an application, someone needs to understand the performance, strength, and weakness of the algorithms.

6. REFERENCES

[1] Dewanjee, Rita & Verma, Pushpak & Vyas, Dr. (2016), "Cryptography Techniques and Internet of Things.", 3rd International conference on Electronics and Communication Systems (IEEE, ICECS'16), February 2016

[2] El-hajj, Mohammed & Maroun, Chamoun & Fadlallah, Ahmad & Serhrouchni, Ahmed. "Analysis of Cryptographic Algorithms on IoT Hardware platforms", 1-5. 10.1109/CSNET.2018.8602942. 2018 2nd Cyber Security in Networking Conference (CSNet)

[3] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader & Mohiy Mohamed Hadhoud, "Evaluating the Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213–219, May 2010

[4] J. B. Awotunde, A. O. Ameen, I. D. Oladipo, A. R. Tomori, M. Abdulraheem, "Evaluation of Four Encryption Algorithms for Viability, Reliability and Performance Estimation", NIGERIAN JOURNAL OF TECHNOLOGICAL DEVELOPMENT, VOL. 13, NO. 2, DECEMBER 2016

[5] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things", IEEE Computer, vol. 44, pp. 51 -58, 2011

[6] S, Joshna. (2016). Symmetric Key Algorithms: A Comparative Analysis. International Journal of Innovative Research in Computer and Communication Engineering. 4. 15772-15775.

[7] RIMAN, Chadi, and Pierre E. ABI-CHAR. "Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey." Information Security and Computer Fraud 3.1 (2015): 1-7.

[8] Chetan Nanjunda Mathur, Karthik Narayan, K. P. Subbalakshmi. "On the Design of Error-Correcting Ciphers", EURASIP Journal on Wireless Communications and Networking, 2007

[9] Dwi Liestyowati. "Public Key Cryptography", Journal of Physics: Conference Series, 2020