Analysis of Algorithms for Effective Cryptography for Enhancement of IoT Security

Chapter · July 2022

DOI: 10.1007/978-981-16-9967-2_10

4 authors:

Valerie David
Carnegie Mellon University
3 PUBLICATIONS 6 CITATIONS
SEE PROFILE

Harini Ragu
VIT University
3 PUBLICATIONS 6 CITATIONS
SEE PROFILE

Vemu Nikhil
VIT University
1 PUBLICATION 0 CITATIONS
SEE PROFILE

Sasikumar Periyasamy
VIT University
35 PUBLICATIONS 420 CITATIONS
SEE PROFILE

Analysis of Algorithms for Effective Cryptography for Enhancement of IoT Security

Valerie David[1][0000-0002-4765-9721], Harini Ragu[2][0000-0001-5394-2227],

Vemu Nikhil[3][0000-0002-7856-2471] and Sasikumar P[4][0000-0003-3510-3694]

[1, 2, 3, 4] School of Electronics Engineering, Vellore Institute of Technology, Vellore, India

valeriedavid2101@gmail.com, hragu50@gmail.com,
nikhilvemu@gmail.com, sasikumar.p@vit.ac.in

Abstract. The Internet of Things has emerged as one of the most prevalent technologies of the current times, finding its place in a myriad of applications and is widely used for digitization and automation applications such as smart city development, automated monitoring systems, healthcare, energy management and much more. With more devices being connected to the Internet, one of the biggest challenges faced by the Internet of Things surfaces – privacy and security risks. The vulnerability of IoT devices and networks have been brought to light, presenting a threat to the integrity of data. Cryptography has proved itself as a method to secure communication channels and data, as a way to ensure IoT security. In this paper, we aim to compare cryptographic algorithms, namely – AES, DES, RSA and lightweight cryptographic algorithm Fernet, to determine which cryptographic algorithm is the most efficient and secure, and can thereby minimize the risk to data integrity and security in IoT applications.

Keywords: IoT, Security, Lightweight, Cyberattack, Cryptography, DES, AES, Fernet, RSA.

1 Introduction

The Internet of Things (IoT) is a network that connects physical entities or “things” to the Internet through a wireless network to exchange data without the need for human intervention. The Internet of Things is bringing about a transformation in our physical world by introducing a dynamic system of devices that are connected at an unparalleled scale. Technological advancements are allowing IoT to be used in many fields to enhance and automate processes, be it smart sensors that could be used in home automation or even healthcare applications to help provide remote aid and medical developments such as smart inhalers.

Although the Internet of Things has helped make lives easier by connecting devices and performing tasks that would otherwise require manual labour and human intervention, it is also susceptible to security threats, as there is a deficit of built-in security. IoT devices are often vulnerable to targeting malware and hacking, which can then set off botnet attacks at a large scale and cause a threat to the stability and efficiency of networks and the associated devices. According to reports by Kaspersky, as of early 2019, 276,000 IP addresses launched around 105 million attacks on IoT endpoints. The number of attacks of IoT devices increased by around nine times in comparison to early 2018. Since IoT connects devices through networks, continued attacks could cause a threat to developed smart cities and industries as well. These cyberattacks are known to be frequent and are expected to escalate in the near future. Hence there arises a dire need to ensure that all data exchanged over the Internet of Things can be secure and their integrity remain unharmed. Security has an important role to play in order to prevent unauthorized access and misuse of data. In order to protect the data exchanged over IoT from cyberattacks, cryptography has emerged as a method to encrypt and thereby protect data. Cryptography is the process of making data unrecognizable to users that are unauthorized, hence providing confidentiality to authorized users. Encryption and data integrity are necessary requirements for authentication, secure communication and protection of firmware. Ideally, a preferred cryptographic algorithm is one that combines high performance with low cost. However, in most cases it can be seen that there are often performance-cost trade-offs when it comes to choosing an algorithm.

Lightweight cryptography, a section of classical cryptographic algorithms, is often used for IoT devices and applications. This is because lightweight algorithms consume less memory and resources for computation, and is pertinent for resource constrained conditions while delivering adequate security. In cryptography, encryption is the process of converting plaintext sent by the user into an unintelligible ciphertext whereas decryption performs the reverse operation, where the encrypted ciphertext is translated back into an intelligible plaintext. Cryptographic algorithms are largely split up into types - symmetric and asymmetric key cryptography. Symmetric Key Cryptography - This kind of encryption involves a single secret key that is used to encrypt and decrypt a message. It uses a secret key made up of various characters and it is necessary for both the authorized sender and recipient to be aware of the key in order to access the messages. Asymmetric Key Cryptography - This kind of encryption uses two keys in the process of encryption. A message that has been encrypted making use of a public key can be translated back to plaintext only by using a private key. The symmetric key cryptographic algorithms compared in this paper are AES, Fernet and DES whereas the asymmetric key algorithm is RSA.

2 Literature Review

Abu-Tair, Mamun, et al. (2020) recognized the security threats associated with IoT-enabled smart homes such as data being hacked or a large amount of data being erroneous, and have highlighted a few lightweight cryptographic algorithms such as TRIVIUM and CLEFIA that could be applied in order to prevent the same [1]. Similarly, Saraiva, Daniel AF, et al. (2019) analysed cryptographic algorithms such as AES, Twofish, SPECK128, RC6, and many more in order to find the most efficient algorithm for devices connected to the Internet that are constrained by resources. These algorithms were compared specifically to test execution times, power consumed and throughput for IoT devices using them [4]. Datta, Debajit, et al. (2020) propose a system in order to combat unprecedented cyberattacks by secure authenticated communication between devices via sound, as opposed to the conventional QR or pin-based authentication systems. The system involves encryption of a random signal before it is transmitted through sound. Many encryption algorithms were combined in order to determine what the most accurate and efficient algorithm would be [2].

Ismail, et al. (2020) identified that the MQTT (Message Queue Telemetry Transport) protocol, popularly used in IoT environments and Machine to Machine interactions owing to its small footprint and efficiency, and consuming less memory, energy and time. However, the protocol is susceptible to exploitation and hence implemented the lightweight Fernet algorithm, based on AES-128-CBC to ensure security of IoT devices and the messages sent through them [3]. Umesh V. Nikam et al. (2018) also worked towards finding methods to ensure secure communication in an IoT network through the MQTT protocol through standard techniques of cryptography such as end-to-end payload encryption and digital signature implementation [5]. Effy Raja Naru, et al. (2017) have compared various lightweight cryptographic algorithms for resource-constrained IoT devices for secure transmission of data. The comparison of algorithms was based primarily on computation and required storage space in order to protect and ensure the privacy, integrity and security of the data being transmitted [7].

Pradeep Semwal, et al. (2017) studied various cryptographic algorithms for data security applications in cloud computing. The algorithms were compared based on criteria including computation time for encryption and decryption, memory consumption and Avalanche effect. The algorithms compared in this study were DES, 3DES, RSA, AES, Blowfish, IDEA and CAST-128 [6]. Similarly, Priyadarshini Patil, et al. (2016) studied the strengths, weaknesses, performance and cost of the same cryptographic algorithms on the basis of the time it takes for the algorithm to perform encryption and decryption operations on the data, the amount of memory consumed, entropy, and the requirement of certain bits to encode data flawlessly. The comparison was implemented using Java cryptography [8]. A survey was performed on cryptographic techniques by Padmavathi, B et al. (2013) on algorithms such as AES, DES and RSA with an added LSB substitution methodology on the basis the time it takes for the algorithm to perform encryption and decryption operations on the data, and buffer size given data of multiple packet sizes. The data transmitted is in the form of images [9]. Along similar lines, Prerna Mahajan, et al. (2013) analysed encryption algorithms for security purposes. The algorithms analysed were RSA, AES and DES. The analysis was on the basis of evaluation parameters of the time it takes for the algorithm to perform encryption and decryption operations on the data packed into multiple sizes for comparison purposes [10].

3 Proposed System and Implementation

Through our work, we aim to compare a few lightweight cryptographic algorithms that can be used in resource-constrained IoT environments in order to determine which algorithm best suits the criteria of efficiency and security. The cryptographic algorithms explored within the scope of this paper are RSA, AES, Fernet and DES. Table 1 shows a comparative study between various parameters for the four cryptographic algorithms.

Table 1. Comparison of Algorithms

Factors	**RSA**	**DES**	**Fernet**	**AES**
Cipher Type	Asymmetric	Symmetric	Symmetric	Symmetric
Key Length (bits)	>1024	56	256	128/ 192/ 256
Block Size (bits)	>=521	64	128	128
Speed	Slowest	Slow	Very fast	Fast
Scalability	Not scalable	Scalable	Scalable	Not scalable
Power Consumption	High	Low	Low	Low
Security	Least secure	Medium	Excellent	Excellent

4 Results

The algorithms are evaluated based on five evaluation parameters namely: encryption time, decryption time, throughput of encryption, key lengths and average entropy per byte. The comparison is performed against multiple packet sizes for each algorithm.

Table 2. Comparison of Parameters

S. No.	**Algorithm**	**Packet Size (KB)**	**Encryption time (sec)**	**Decryption time (Sec)**	**Throughput (KB/sec)**
1	RSA	118	10.0	5.0	11.8
	DES		3.2	1.2	36.88
	Fernet		0.066	0.065	1787.8
	AES		1.7	1.2	69
2	RSA	153	7.3	4.9	20.9

	DES		3.0	1.0	51
	Fernet		0.066	0.066	2318.18
	AES		1.6	1.1	95.63
3	RSA	196	8.5	5.9	23.058
	DES		2.0	1.4	98
	Fernet		0.066	0.063	2969.7
	AES		1.7	1.24	115.29
4	RSA	312	7.8	5.1	40
	DES		3.0	1.6	104
	Fernet		0.076	0.070	4105.26
	AES		1.8	1.3	173.33
5	RSA	868	8.2	5.1	105.85
	DES		4.0	1.8	217
	Fernet		0.077	0.079	11272.72
	AES		2.0	1.2	434

On analysing Table 2 and Fig. 1., Fig. 2. and Fig. 3., it can be concluded that the Fernet algorithm takes the least amount of time for both encryption and decryption of data of all packet sizes, followed by AES and DES. The RSA algorithm takes the most time for both encryption and decryption. Hence, Fernet has the highest encryption throughput for all packet sizes whereas RSA has the least.

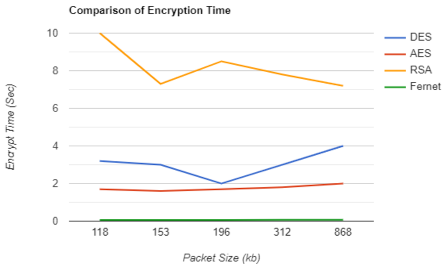

Fig. 1. Time for Encryption of all the algorithms

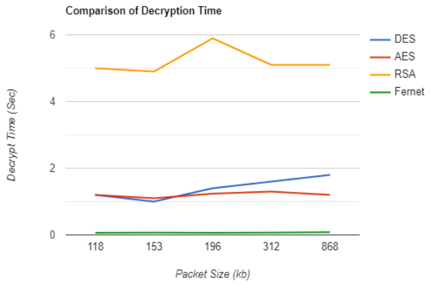

Fig. 2. Time for Decryption of all the algorithms

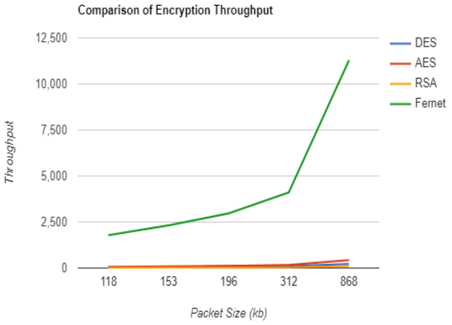

Fig. 3. Comparison of encryption throughput

Table 3. Comparison of Key Lengths

Algorithm	**RSA**	**DES**	**Fernet**	**AES**
Key Length (bits)	1024	56	256	128

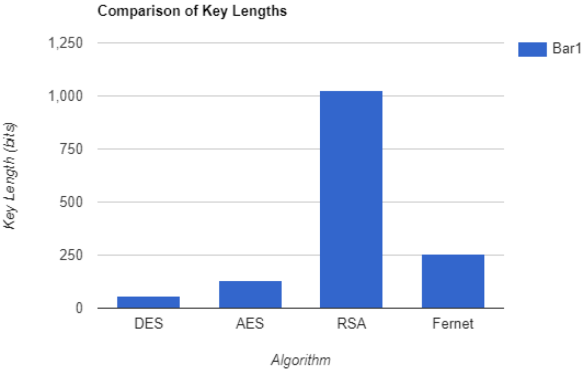

Fig. 4. Comparison of Key Lengths

Table 3 and Fig. 4 show that RSA has the largest key size, followed by Fernet, AES and DES. However, RSA is an asymmetric algorithm, which means that its key size of 1024-bit is analogous to an 80-bit key length for a symmetric algorithm, when algorithm strength is compared. This means that among the algorithms compared, Fernet is considered the strongest depending on the key size.

Table 4. Comparison of Entropy per byte

Algorithm	RSA	DES	Fernet	AES
Avg. Entropy/byte	3.0958	2.9477	3.47248	3.84024

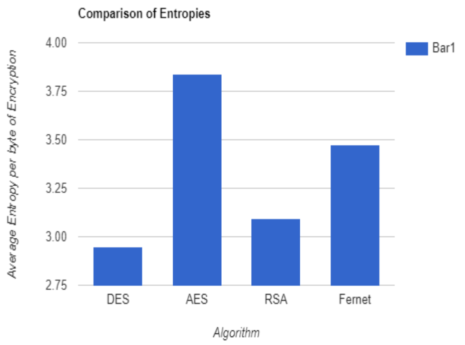

Fig. 5. Comparison of average entropy per byte

On analysing Table 4 and Fig. 5, it can be seen that AES has the highest entropy per byte, followed by Fernet, RSA and lastly, DES. This shows that each time the algorithm is run, AES tends to produce a more randomized key, hence making it more difficult to crack, in comparison to the other algorithms compared within the study.

5 Conclusion

Through this paper, we have aimed to find a solution to the security challenges faced by IoT applications. Cryptographic algorithms, including the lightweight Fernet algorithm, have been compared based on evaluation parameters of the time it takes for the algorithm to perform encryption and decryption operations on the data, throughput of encryption, key length and average entropy per byte in order to determine the most secure and efficient algorithm which can alleviate the risk to data security in IoT applications.

Since Fernet is a lightweight algorithm, it emerges as the most efficient algorithm, with the least encryption and decryption time and the highest encryption throughput. AES has the highest average entropy per byte, which means that it is the most secure algorithm among the algorithms compared, followed by the Fernet algorithm. As IoT devices require cryptographic security provided by lightweight sources in order to reduce latency as well as the consumption of resources, yet maintain the authenticity of data, which can be determined by the difficulty in cracking the key, it can be concluded that out of the algorithms compared, the Fernet algorithm emerges as a better fit for security applications in IoT.

In the future, more lightweight cryptographic algorithms can be compared for IoT device security and authentication, in order to determine the strongest algorithm that can be used.

References

1. Abu-Tair, Mamun, et al. "Towards Secure and Privacy-Preserving IoT Enabled Smart Home: Architecture and Experimental Study." *Sensors* 20.21 (2020): 6131.
2. Datta, Debajit, et al. "An efficient sound and data steganography based secure authentication system." *CMC-Computers Materials & Continua* 67 (2020): 723-751.
3. Ismail, EL GAABOURI, Asaad CHAHBOUN, and Naoufal RAISSOUNI. "FERNET SYMMETRIC ENCRYPTION METHOD to GATHER MQTT E2E SECURE COMMUNICATIONS for IoT DEVICES." (2020).
4. Saraiva, Daniel AF, et al. "Prisec: Comparison of symmetric key algorithms for iot devices." *Sensors* 19.19 (2019): 4312
5. Nikam, Umesh V., Harshal D. Misalkar, and Anup W. Burange. "Securing MQTT protocol in IoT by payload Encryption Technique & Digital Signature." (2018)
6. Semwal, Pradeep, and Mahesh Kumar Sharma. "Comparative study of different cryptographic algorithms for data security in cloud computing." *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017.
7. Naru, Effy Raja, Hemraj Saini, and Mukesh Sharma. "A recent review on lightweight cryptography in IoT." *2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC)*. IEEE, 2017.
8. Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." *Procedia Computer Science* 78 (2016): 617-624
9. Padmavathi, B., and S. Ranjitha Kumari. "A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution." *IJSR, India* (2013).
10. Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." *Global Journal of Computer Science and Technology* (2013)
11. Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." *International Journal of Computer Applications* 67.19 (2013)