Turkish Journal of Computer and Mathematics Education Vol.12 No.12 (2021), 2722-2727

Research Article

Comparative Study of Encryption Algorithms for Data Security in WoT and IoT

Baraa Mohammed Hassan [1], Haider K. Hoomod [2]

[1]Informatic Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatic, Iraq
[2]Computer Science Department, College of Education, Mustanisiryah University, Iraq
ms201910524@iips.icci.edu.iq[1],drhjnew@gmail.com[2]

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: Nowadays, both the Web of Things (WoT) and the Internet of Things (IoT) have become important areas in every aspect of our lives. This technology is supposed to link billions of devices, which leads to an enormous number of communications between devices that will produce a huge amount of sensitive information, and to protect that information from unauthorized persons to access and manipulate it. Given this, encryption algorithms are introduced as a solution to protect the security of sensitive information. In this paper, algorithms of encryption are compared for the security of data.
Keywords: WoT, Algorithms of Encryption, IoT, Security WoT, Security IoT, Encryption Algorithms Comparison.

1. Introduction

Nowadays, the internet user base is growing at a rapid rate. The internet is used by billions of people around the world to perform different activities, including browsing, online gaming, sending and receiving emails, and many other tasks. with a growing population, there is also a rapid rise in the number of people gaining access to internet networks and global information [1].

These technological advancements are laying a promising foundation for new applications and services for WoT that empower the lives of people every day. WoT has emerged as an application platform for IoT. Much like the web on the Internet the maturity of web services has pushed the web platform to host services exposed by things in the real world. Continuously constructing connections between the physical and virtual worlds are these modern WoT services and related applications [2][3].

However, WoT not only inherits from IoT its distinctive features but also many security and privacy problems. The heterogeneous and restricted nature of things, identity management (identification and authentication), protection, physical and digital access to devices, and trust are directly related to these problems. Since WoT is characterized by openness and sharing of resources, so these resources and data must be protected from malicious interferences. Accordingly, there are many encryption algorithms that have been suggested to overcome the privacy and security problem[4].

2. Literature Survey

Mingyuan Xin used Hybrid encryption algorithm which has combined AES and ECC algorithms to provide data transmission security for Internet of Things [5].

Afsoon Yousefi and Seyed Mahdi Jameii used the HAN algorithm that combines the AES algorithm for symmetric encryption with the NTRU algorithm for asymmetric encryption to reduce safety risks, enhance encryption speed, and reduce computational complexity. The purpose of this hybrid algorithm was to achieved information integrity, confidentiality, and non-repudiation in data exchange for IoT [6].

Ahmed H. Mohammed and Mohamed Mosa Jafer proposed an algorithm that relies on a lightweight encryption called (LWAES). The goals to be achieved this system first: highest speed into encrypt and decrypt by replacing the Mix Columns stage found in AES with simple SHIFT operations because the Mix Columns stage is the most requested computational stage in AES design, and thus it consumes most of the time needed for encryption and

decryption. This process took the time from the start of the sensor reading to the moment the user recalled it from 1 to 8 seconds. Second, the modified LWAES algorithm provides Security was good to a web of things, with the encryption process was faster and lightweight in the storage process [7].

Haider K. Hoomod et al used the Speck-SHA3 (SSHA) algorithm resulting from a modification to the SHA-3 algorithm by replacing the KECCAK function with another very fast algorithm SPECK, which produces a very fast algorithm with a strong security level reliable in the validation of the data produced by the sensors. Also, the extended logistic system is used to generate the initial values that the SHA3 algorithm uses to make these values unknown which the intruder cannot guess or recognize. This algorithm achieved SSHA, the speed was this algorithm much faster than the SHA-3 algorithm, with the ability to provide a good level of data security and integrity in a WoT environment compared to the level of security provided by the original SHA-3 algorithm. also, the SSHA algorithm could be used in IoT systems that need methods to quickly and securely verify data integrity [8].

B.Vinayaga Sundaram et al suggested encryption and hashing algorithms, where used RC-5, Skipjack, and AES. The purposed to be achieved confidentiality assurance where attackers cannot interpret the encrypted-text that was sent, also ensure integrity (the encrypted-text has not been changed) by being used a hashing algorithm. The algorithm is not vulnerable to brute force attacks due to its key length (128 bits), it does not have any weak keys. Confusion and diffusion are also achieved through this algorithm [9].

Dian Rachmawati et al used a hybrid cipher system is a combination between the algorithm of IDEA (International Data Encryption Algorithm) symmetry and the algorithm of knapsack asymmetry. The most prominent results achieved are: (1) It was found that the IDEA and Knapsack algorithms meet data integrity standards. The result of the message decoding test is that the encrypted text will be the same as the initial plain text (the original message). The result is that the decryption test of the encryption key will be the same as the key that was used to encrypt the messages. (2) From testing five files with different text and character lengths, the average coding time is 9.6ms. While the average decoding time is 6ms. Therefore, it can be concluded that the time to decode the message is shorter than the time to encode the message. (3) The technology of a hybrid encryption system, the message encryption using IDEA can protect the information contained in the message, and the encryption key using the knapsack algorithm can secure the key distribution [10].

Sameena Shah et al discussed potential attacks and security threats on the IoT network, and also presented solutions related to the physical security of IoT devices under a restricted environment and the need for security in the network and encryption are implemented [11].

The researchers provide the information needed to solve some of the security and privacy problems found in WoT. Luigi Catuogno and Stefano Turchi have also analyzed those problems and explained that publishing the current Security and Privacy solutions and technologies in the WoT is not an easy matter due to their potential breadth, intrinsic inhomogeneity, and the wide diversity of the entities [12].

Vithya Vijayalakshmi and Dr. L. Arockiam suggested a multi-level encryption mechanism using Merkle-Hellman and Elliptic Curve Cryptography (ECC) which encrypts the data in two steps: the first step, the data is encrypted by the Merkle-hellman cryptosystem. In the second step, the cipher text from the first step as an input to the ECC. Then sent the encrypted text generated from two algorithms to the cloud server to be stored there. The purposed to be achieved the security of the sensed data and did not enable unauthorized persons to access it, also improving the computation time [13].

Shiva Prakash and Ashish Rajput used a hybrid algorithm that included the advantage of the two algorithms: the symmetric key algorithm is AES (advanced encryption standard) and the asymmetric key algorithm is ECC (elliptic curve cryptography), in which ECC was used to generate and share keys, and AES is to encrypt and decrypt data. The purposed to be achieved data integrity and confidentiality with minimal use of system resources thus providing data security as well as the proposed hybrid algorithm provides greater security than AES and consumes less resources and time than ECC [14].

The researchers in [15] presented an analysis of the current situation and concerns related to the Internet of Things (IoT) security, as well as an overview of security principles, security challenges, and technological, proposed countermeasures, and future directions for securing the Internet of Things.

Dian Rachmawati et al used A hybrid cryptosystem method consisting of the symmetric algorithm is Tiny Encryption Algorithm (TEA) and the asymmetric algorithm is LUC, which is the file encrypt and decrypt by TEA

and the encrypting and decrypting of the TEA key by LUC. The result of this method fulfilled the requirements of the integrity side in the encryption, where the encrypted text size was increased by sixteen bytes with an increase in the length of the plain text by eight characters. Also, this system can secure the file that has the extension * .pdf, * .txt, * .rtf, * .doc, * .docx and *. otd [16].

Pavithra Kanagaraj and Manivannan Doraipandian proposed the hybrid cryptosystem, included the advantages of each (Advanced Encryption Standard (AES)) is a symmetric algorithm and (Rivest - Shamir - Adleman (RSA)) is an asymmetric algorithm to produce a hybrid algorithm. 4086 bits of paired keys are produced by RSA. In order to be provided better security for the system where it is difficult to attack, it is provided good key management, and it was also found that the calculation time that the program takes is less compared to the original algorithms [17].

M. Sri Lakshmi and V. Srikanth discussed lightweight encryption algorithms for data security in the IoT network which is still vulnerable to different types of attacks. Also explained that the traditional algorithms are not sufficient to guarantee data security in the resource-limited environment of IoT [18].

Sumit Singh Dhanda et al presented a comprehensive study on lightweight encryption algorithms as a solution to the resource-limited devices security problem of the Internet of Things and also discussed 21 lightweight block algorithms, 19 lightweight stream algorithms, 9 lightweight hash functions, and 5 different types of curve coding Elliptical (ECC)[19].

3. The Overview of Architectures

The WoT's basic architecture is split into four layers as shown in figure (1). Layer one is the access layer is considered the most important because it provides a means of connecting devices to the web by providing a web application programming interface. Layer two is a find layer that defines the criteria for easy device use by customers and other applications. It allows devices findable on the web by search engines and other web indexes.

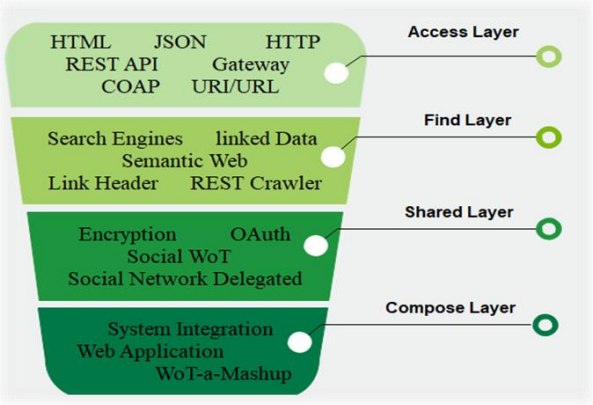

Figure. 1 Layered Architecture WoT

Layer three is the shared layer that defines the secure and efficient sharing of data created by WoT devices across the web. Lastly the compared layer simplifies creating applications that include WoT and web services and also responsible for making use of the tools [20]. As well as, the infrastructure of the IoT consists of three layers, as shown in figure (2). The physical layer or layer of perception which is primarily concerned with identifying the objects and collecting the data and this layer contains **N**ear **F**ield **C**ommunication(NFC), **G**lobal Positioning **S**ystem(GPS), **W**ireless **S**ensor **N**etwork(WSN), **R**adio-**F**requency **Id**entification (RFID), and so on. In addition, this layer transforms the data into digital signals obtained from sensors and then used for data transmission.

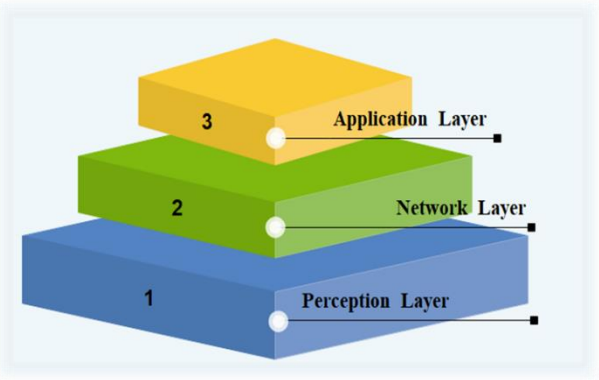

Figure. 2 Layered Architecture IoT

The network layer that sensibility the data from devices IoT and transfers it into the cloud. Which huge amount of the data would be transferred to the next layer through the network. Transmission in this layer involves WIFI, 4G,3G, ZigBee, Bluetooth, infrared technology, UMB, and other types of transmission. Finally, the application layer deals with data representation and provides an interface for the user, by sending commands over the network, to monitor or even control variables [20,21,10].

4. Cryptography for WoT and IoT

Cryptography involves hidden words or the study of data concealment and verification which includes the use of algorithms, protocols, and strategies to prevent access to sensitive information by unauthorized persons while enabling verification of all components in the communication. In other words, it is a way to protect data by converting it into encrypted text [23][24].

Each of the WoT and IoT layers has its own set of procedures and security principles. Algorithms for cryptography are basically utilized to secure the data. This technology encrypts data necessary to secure it for the encrypted text during data transmission on the network. Cryptography can be divided into two types: symmetric and asymmetric algorithms. The symmetric encryption process is a process where the same key is used for every encrypting and decrypting process, this method is characterized by speed and less complexity. But the security is less because it uses the same key in both processes. Also, in the encryption process of asymmetric which uses private and public keys into the encrypt/decrypt process, respectively, this method is slow and complex, but it provides a high level of security [22].

5. Comparison for Various Encryption Algorithms

The table 1 gives the comparison between encryption algorithms previously discussed in literature survey with respect to structure, block size, key size, round, and features.

The Table (1) Comparative of The Algorithms

REF. NO	ALGORITHMS	ARCHITECTURE	BLOCK SIZE	KEY SIZE	ROUNDS	FEATURES
[6]	AES	Substitution-Permutation Network	128 bits	128,192, 256 bits	10, 12, 14	It is the best in encryption performance and security, thus excellent Security.

[5]	ECC	Public Key Algorithm	variable	Variable and More than symmetric	1	Faster speed, higher security, low requirements for bandwidth and smaller storage space.
[9]	RC-5	Feistel Network	32,64, 128 bits	0 to 2048 bits	0 to 255	Good security but it uses more CPU power.
[10]	IDEA	Lai–Massey scheme	64-bit	128-bit	8	The fastest in encrypt time, speed, and flexibility.
[16]	TEA	Feistel network	64 bits	128 bits	variable	Fast speed and most efficient
[17]	RSA	Public Key Algorithm	128 bits	1,024 to 4,096	1	Low Speed and excellent Security
[8]	SPECK	Feistel network	32-128	64-256	22- 34	Fast speed, good security

6. Outcomes and Discussion

This section explains the performance analysis based on the results of different researchers and deals with the security aspects in developing an encryption algorithm based on the evaluation criteria. As some researchers focus heavily on surveying encryption algorithms and evaluating their performance, in general, block cipher performance depends on block size and key size. The large block size will make the algorithm faster because a large portion of the data will be encrypted in one execution cycle. Likewise, a small block of data requires more execution cycles which increases the total execution time. On the other hand, large key size will affect the performance of the algorithm because all the main bits participate in the implementation of the algorithm that makes the performance slower. But at the same time, it provides more security of the algorithm and thus provides more protection against the cryptanalyst. Therefore, from the above table, the results show that the AES, IDEA, SPECK, TEA algorithms are the fastest in encryption time, speed, and flexibility. The results also prove that the SPECK and AES algorithms are the best in security, flexibility, stronger encryption performance, and the most efficient in comparison with other's algorithms.

7. Conclusion

IoT and WoT are two of the most important modern technologies for future systems everywhere. Data that was done Created by these two technologies must be protected. Hence, different types of encryption algorithms are used to transmit data securely. Each algorithm has various performances based on its block size, key size, rounds, and also its architecture (structure). The encryption algorithms used for IoT and WoT devices should have different considerations, taking into account the limited resources of these devices to improve device performance in addition to maintaining security as a priority.

References

1. V. K. Solanki and R. K. and L. H. Son, Smart Innovation of Web of Things(book). CRC Press, 2020.
2. S. S. Mathew, Y. Atif, and M. El-Barachi, “From the Internet of Things to the web of things-enabling by sensing as-A service,” Proc. 2016 12th Int. Conf. Innov. Inf. Technol. IIT 2016, pp. 218–223, 2017, doi: 10.1109/INNOVATIONS.2016.7880055.

3. H. Najm, H. K. Hoomod, and R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System," pp. 184–199.
4. S. E. L. Jaouhari, A. Bouabdallah, and J. Bonnin, "Security issues of the Web of Things," pp. 1–42, 2017.
5. M. Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System," Proc. - 2015 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2015, pp. 62–65, 2015, doi: 10.1109/CyberC.2015.9.
6. A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," IEEE Int. Conf. IoT its Appl. ICIOT 2017, pp. 3–7, 2017, doi: 10.1109/ICIOTA.2017.8073627.
7. A. H. Mohammed and M. M. Jafer, "Secure web of things based on a lightweight Algorithm," 1st Int. Sci. Conf. Comput. Appl. Sci. CAS 2019, no. 2016, pp. 216–221, 2019, doi: 10.1109/CAS47993.2019.9075831.
8. H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "Modify Speck-SHA3 (SSHA) for Data Integrity in Wot Networking Based on 4-D Chaotic System," Period. Eng. Nat. Sci., vol. 8, no. 4, pp. 2379–2388, 2020, doi: 10.21533/pen.v8i4.1743.
9. B. Vinayaga Sundaram, M. Ramnath, M. Prasanth, and J. Varsha Sundaram, "Encryption and hash based security in Internet of Things," 2015 3rd Int. Conf. Signal Process. Commun. Networking, ICSCN 2015, pp. 1–6, 2015, doi: 10.1109/ICSCN.2015.7219926.
10. D. Rachmawati, M. S. Lydia, and W. A. Siregar, "Hybrid Cryptosystem Implementation Using IDEA and Knapsack Algorithm for Message Security," J. Phys. Conf. Ser., vol. 1090, no. 1, 2018, doi: 10.1088/1742-6596/1090/1/012030.
11. S. Shah, S. S. A. Simnani, and M. T. Banday, "A Study of Security Attacks on Internet of Things and Its Possible Solutions," 2018 Int. Conf. Autom. Comput. Eng. ICACE 2018, pp. 203–209, 2018, doi: 10.1109/ICACE.2018.8687091.
12. L. Catuogno and S. Turchi, "The Dark Side of the Interconnection: Security and Privacy in the Web of Things," Proc. - 2015 9th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2015, pp. 205–212, 2015, doi: 10.1109/IMIS.2015.86.
13. A. V. Vijayalakshmi, "Enhancing the Security of Iot Data Using Multilevel Encryption," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 9, pp. 841–845, 2017, doi: 10.26483/ijarcs.v8i9.4959.
14. S. Prakash and A. Rajput, "Hybrid cryptography for secure data communication in wireless sensor networks," Adv. Intell. Syst. Comput., vol. 696, no. January, pp. 589–599, 2018, doi: 10.1007/978-981-10-7386-1_50.
15. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.
16. D. Rachmawati, A. Sharif, Jaysilen, and M. A. Budiman, "Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm," IOP Conf. Ser. Mater. Sci. Eng., vol. 300, no. 1, 2018, doi: 10.1088/1757-899X/300/1/012042.
17. T. Sengodan and M. Murugappan, Advance in Electrical and Computer Technologies. Springer US, 2020.
18. M. Sri Lakshmi and V. Srikanth, "A study on light weight cryptography algorithms for data security in IOT," Int. J. Eng. Technol., vol. 7, pp. 887–890, 2018, doi: 10.14419/ijet.v7i2.7.11088.
19. S. S. Dhanda, B. Singh, and P. Jindal, Lightweight Cryptography: A Solution to Secure IoT, vol. 112, no. 3. Springer US, 2020.
20. N. Kumar and S. Ahmad, "Security Threats in Layered Architecture of Web of Things," Proc. 4th Int. Conf. Inven. Syst. Control. ICISC 2020, no. Icisc, pp. 745–750, 2020, doi: 10.1109/ICISC47916.2020.9171223.
21. B. Dhanalaxmi and G. A. Naidu, "A survey on design and analysis of robust IoT architecture," IEEE Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2017 - Proc., no. Icimia, pp. 375–378, 2017, doi: 10.1109/ICIMIA.2017.7975639.
22. K. N. Pallavi, V. Ravi Kumar, and S. Srikrishna, "Comparative study of various lightweight cryptographic algorithms for data security between IoT and cloud," Proc. 5th Int. Conf. Commun. Electron. Syst. ICCES 2020, no. Icces, pp. 589–593, 2020, doi: 10.1109/ICCES48766.2020.09137984.
23. S. K. Ghosh, S. Rana, A. Pansari, J. Hazra, and S. Biswas, "Hybrid Cryptography Algorithm for Secure and Low Cost Communication," 2020 Int. Conf. Comput. Sci. Eng. Appl. ICCSEA 2020, pp. 4–8, 2020, doi: 10.1109/ICCSEA49143.2020.9132862.
24. H. Najm, H. K. Hoomod, and R. Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa (20)," Periodicals of Engineering and Natural Sciences, vol. 8, no. 3. pp. 1829–1835, 2020, doi: 10.21533/pen.v8i3.1619.