***Article Received:** 25 December 2022 **Revised:** 12 January 2023 **Accepted:** 20 February 2023*

A Study of Data Encryption in Internet of Things Environment

Research Scholar - P Raja Lingam[1]
Department of Electronics & Communication Engineering, Dr. A. P. J. Abdul Kalam University, Indore, MP, India
rajalingam.raj@gmail.com

Research Guide - Dr Rahul Mishra[2]
Department of Electronics & Communication Engineering, Dr. A. P. J. Abdul Kalam University, Indore, MP, India
rahulmishra@aku.ac.in

Abstract

The Internet of Things (IoT) refers to a class of cutting-edge information technologies that have captured the public's imagination. We often consider sensors and stimulators to be "smart" gadgets in our surroundings. But at the same time, there are fresh concerns raised by IoT security. Smart gadgets become increasingly integrated into human life as a result of their Internet connectivity and potential for interaction with humans. It follows that security must be a first consideration while creating IoT. The Internet of Things is exceptional because of its three main characteristics: comprehensive awareness, dependable transmission, and clever processing. With the widespread nature of IoT, data transmission security has become a crucial component of overall system integrity. As a novel paradigm, the IoT may benefit from the hybrid encryption method. Strong security is produced with this sort of encryption while just a little amount of processing is required. To that end, this study proposes a hybrid encryption algorithm, the development of which has been carried out to make encryption more quickly and with less computational complexity, as well as to lessen the dangers associated with doing so. This hybrid algorithm was designed for IoT data transmission to provide privacy, authenticity, and immutability of all sent information. The proposed encryption technique was eventually tested in a MATLAB simulation to gauge its speed and security efficiency in contrast to the standard encryption approach.

Keywords—*Internet of things, security, hybrid algorithm, privacy*

INTRODUCTION

The sector of linked objects known as the Internet of Things (IoT) is rapidly expanding. All of these gadgets are constantly exchanging data with one another, so keeping that data safe is crucial. Web-enabled smart devices with embedded systems that gather, transmit, and act on data from their environs make up an IoT system. Data from the different sensors is gathered by these IoT ecosystems and sent to an IoT edge device, where it may be stored and analysed locally or in the cloud. Machine learning and artificial intelligence may benefit from the vast volumes of data collected by the many sensors. Because of the interconnected nature of the devices in an IoT network, many tasks may be automated. Smart homes and smart factories are two important applications that will have a huge impact on our daily lives. Also, it may help firms save money by reducing waste, enhancing service delivery, and optimising their workforce. In 2022, it's expected that there will be 20 billion IoT devices already in use. As a result, we can get to data whenever we want, wherever we happen to be, and on whatever device we happen to be using. Privacy protection is critical since so many of these IoT devices will be in the hands of regular people. Due to the vast amount of data generated by IoT devices, there is a greater opportunity for hackers to get access to private information. In 2016, for instance, a botnet broke into the domain name server provider Dyn and knocked off a lot of websites for a while. After breaking in using unsecured Internet of Things (IoT) gadgets, hackers launched one of the largest DDoS (distributed denial of service) assaults ever recorded. This demonstrates how, due to the interconnected nature of IoT devices, an attacker only has to exploit a single vulnerability to have access to all data. That's why encryption is such an urgent need for shielding Internet of Things networks from the myriad of potential dangers they face. When asked about the biggest challenges facing the Internet of Things (IoT), most experts point to security and privacy issues. Encryption, in its simplest definition, is the act of transforming private information into an unintelligible code. This information is encrypted using a secret key. This is encrypted and will only be legible with the correct decryption key. By doing so, we know that only the intended recipient will have access to the data. Without encryption, anybody who intercepts a communication from an Internet of Things device may access all of the data being sent.

The following are examples of widely used forms of encryption:
1. RSA
2. Advanced Encryption Standard (AES)
3. Two fish
Server-side data encryption protects data privacy and confidentiality. Therefore, it safeguards and isolates information from users, corporations, and anybody else who could be associated with or have access to the information. People and businesses may rest easy knowing their private information is protected in this way. For this reason, encryption has to be included in every device connected to the Internet of Things. Internet of Things (IoT) can only reach its full potential if it is secure. Machine learning algorithms and other patterns may then be applied to this data. This facilitates the discovery of patterns and the execution of research, etc. On the other hand, the whole IoT infrastructure becomes very susceptible if all this information can be accessed. Machine learning data sets may be incredibly huge while yet being private thanks to encryption.
Security Issues:

1. Data Confidentiality: Users are concerned about their data's security and only want the appropriate parties to have access to it. This means preventing unauthorised individuals from gaining access to and making use of data.
2. Data Authenticity: The identity of the communicating node must be verified for security reasons.
3. Data Integrity: This is a critical security need since it ensures that messages are delivered unaltered from their original state.
4. Data Authorization: Data dissemination must be restricted to authorised sensors, therefore security is paramount.
5. Non- repudiation: The system controls how messages are resent from one node to another. A node shouldn't prevent a retransmission from asserting that the original message was transmitted.
6. Data Freshness: It controls the distribution and storage of incoming data from sensor nodes.

LITERATURE REVIEW

S. Rameezraja et al (2022), We have analysed the strengths and limitations of each encryption technique used in our IoT application by comparing the time and throughput at which they operate. Based on the findings of the experiments, the DES and 3DES algorithms need the least amount of time to encrypt a file, whereas Blowfish has the greatest throughput.

In this research, by Dana Khwailleh et al. (2022), a dynamic algorithm is introduced to identify the significance of data acquired and to use the appropriate security method for each kind of data collected. This was achieved via a hybrid approach that mixes block cyphers and stream cyphers to increase security. Following data categorization using machine learning classifiers, the less crucial data is encrypted with a stream cypher (SC) based on the rivest cypher 4 algorithm, while the more crucial data is encrypted with a block cypher (BC) based on the advanced encryption standard algorithm. The suggested solution offers faster encryption with less CPU time by using a hybrid system, which was evaluated through simulation to ensure its efficacy.

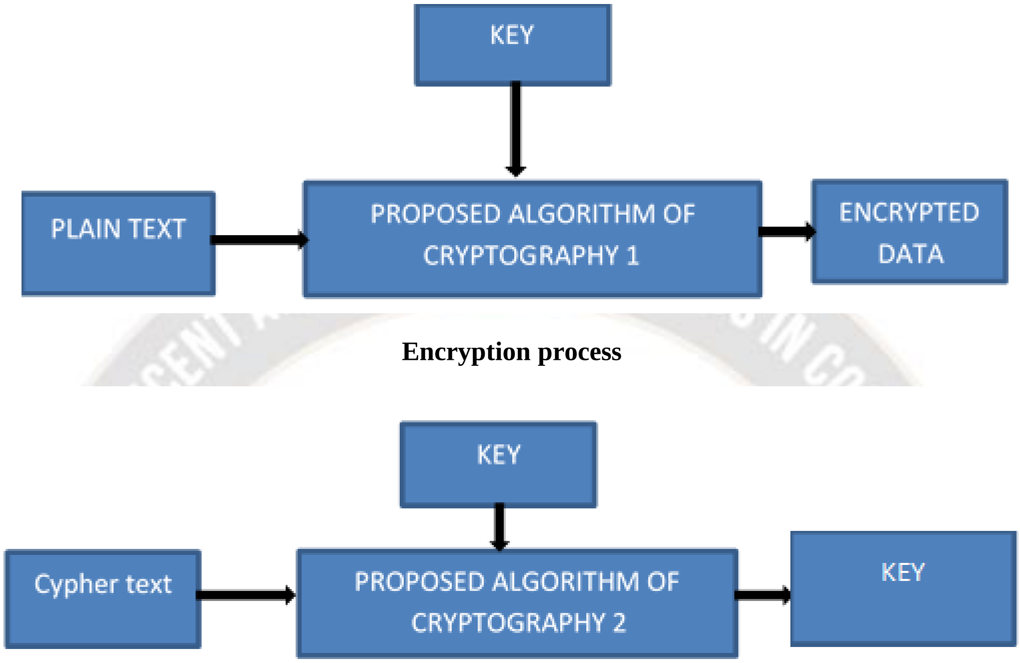
To the Editors: Haiyun Ma et al (2020), In this study, they examine the efficacy of several forms of private data encryption. We build a model of a data-encryption system based on the stream-cipher technique. The private data is sent to the relay node over encrypted subspace. They are encrypted, then split up and reorganised. The lengthy private data is chopped up into manageable chunks. They undergo a religious transformation and are eventually readmitted to society. In order to safeguard the confidentiality of the encoded data, we use a stream cypher and a dual-key method to perform a freely nondestructive transformation between the plaintext and the ciphertext. The experimental findings demonstrate that the suggested technique is faster than the state-of-the-art methods in both the encryption and decryption processes, with superior ciphertext conversion output effect and reduced vulnerability to network assaults. In comparison to other approaches, encrypting and decrypting messages takes less time. The suggested technique results in a 14% savings in the cost of calculations. Additionally, it offers better security and increases the security and integrity of the privacy information gathering process.

RESEARCH METHODOLOGY

Method for encrypting data using a combination of binary-bit sequencing and several stages:

The user supplies the symmetric key for this novel symmetric cryptography algorithm [1]. Using the planned algorithm, the same key will be used to encrypt the supplied data. By manipulating the binary bit sequence of the plain text, we are able to replace it with the encryption text. The user-supplied key must be an integer between 0 and 255. Figure 1 shows a simplified schematic of the whole process of symmetric cryptography. The most compelling arguments in favour of symmetric-key encryption include:

1. The procedure is simple and quick.
2. In other words, the key is what provides the security.
3. The sender and the receivers may use the same encryption and decryption methods and keys.


KEY
PLAIN TEXT
PROPOSED ALGORITHM OF CRYPTOGRAPHY 1
ENCRYPTED DATA
KEY
Cypher text
PROPOSED ALGORITHM OF CRYPTOGRAPHY 2
KEY

Encryption process

Decryption process

Fig 1. Sequencing binary digits and a multi-stage encryption algorithm: a block diagram

Proposed Encryption Algorithm:

In order to begin replacing the plain text, we must first establish certain character values. Characters defined as 2n/2. The value of N represents a binary bit string.

1: First, you need to read the user's plaintext message.

2: Second, switch out the regular characters with their ASCII equivalents.

3: Gather a private key from the user, step 3.

4: Using the user-supplied key, perform an XOR operation on the ASCII values.

5: Changing the binary n-bit sequence into a numerical value.

6: Transform the incoming n-bit sequence into a binary sequence with twice as many bits.

7: Decimalize the binary sequence of length n/2.

8: Inserting the appropriate characters from the character table into all of the decimal places.

9: Send the encrypted message.

Security concerns become more important as IoT applications grow in popularity. To keep information sent between IoT gadgets secure, encryption methods have become more important. In the study, we compare many popular techniques to guarantee this. Symmetric key encryption and asymmetric key encryption are two of the many forms of cryptography. Symmetric key encryption relies on the idea of a secret or private key that is utilized during transmission. The same key is used to decode the message at the receiving end [5]. With asymmetric key encryption, each recipient has their own unique set of keys public and private keys. To encode data, a public key is utilized, and only the recipient in possession of the corresponding private key may decode the message.

Hybrid Encryption in Cloud Computing

With cloud computing, users' data is not stored on their local machine but rather on distant servers in the cloud [9]. As an added bonus, it offers a number of security models to keep sensitive data safe from prying eyes. Hybrid encryption is one of several variants that combine different methods of encryption. There hasn't been anything quite like a hybrid

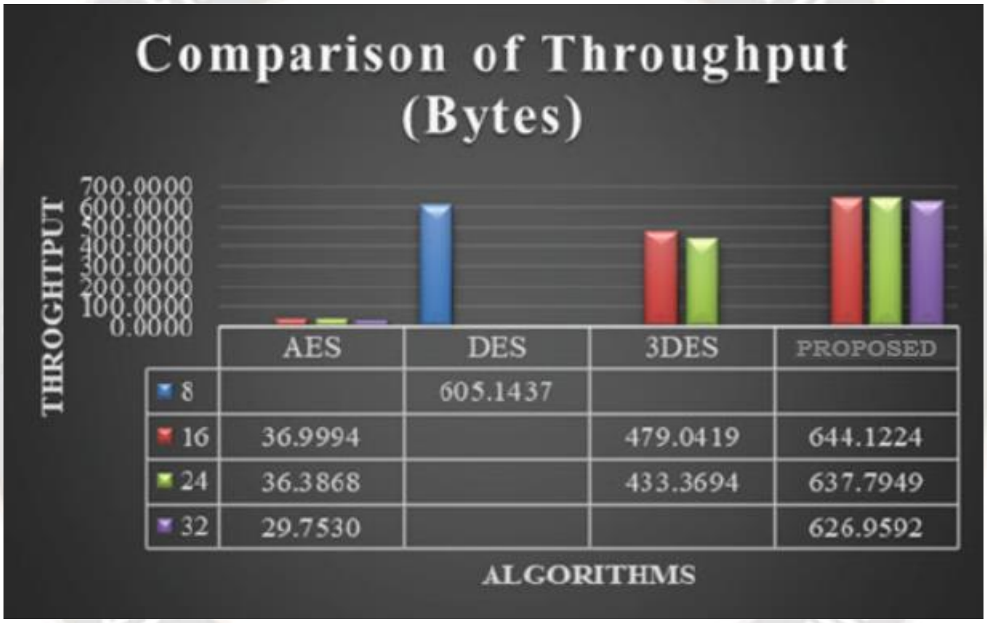
***Article Received:** 25 December 2022 **Revised:** 12 January 2023 **Accepted:** 20 February 2023*

encryption system that combines RSA and Diffie Hellman to provide data security for cloud services before. The goal of this amalgamation is to maximise the benefits of both public key cryptography (key management) and secret key cryptography (encoding, decoding process speed). Diffie-Hellman is an old method of encryption used for IPsec.

To achieve even more impressive results, hybrid cryptographic approaches incorporate the combination of symmetric and asymmetric methods. The processes of scrambling and decrypting are integral to any and all cryptographic methods. The first step in encryption is to transform data into a format that is incomprehensible to humans. The information decoding method is used to extract primary data from the graphic. Since both asymmetric and symmetric processes are used in this inquiry, encryption and decryption must be conducted twice.

RESULT

Numerous tests on various encryption techniques have been conducted. To prevent any setup mistake or early bias, all encryption algorithms have skipped the first run. The suggested algorithm's time consumption is less for shorter key lengths (128 bits, 192 bits), but it is quite large for longer key lengths. Our testing shows that using a 256-bit key length is suboptimal for the suggested technique. The DES algorithm demonstrated, in comparison to AES, that the whole encryption process may be completed in less time.



	AES	DES	3DES	PROPOSED
8		605.1437		
16	36.9994		479.0419	644.1224
24	36.3868		433.3694	637.7949
32	29.7530			626.9592

Fig. 2 Comparison plot of different encryption algorithms for throughput

3DES has the same time requirement as DES. In all these algorithms, when the individual time requirementis studied, it has been found that the “Key Generation Time” has been the largest time need as compared with “Encryption Time” and “Decryption Time.” The "Decryption Time" criteria is the quickest to meet out of the three. The experiment also shown that there is a general tendency toward longer encryption times as key lengths have become longer. Apart from the time required, the throughput of each method has also been evaluated. Using the formula Throughput = (Total Plaintext Bits/Encryption Time), we were able to determine the throughput. The computation requires the ciphertext, which was created from the plain text using the encryption techniques. Algorithm throughputs are displayed in Fig. 2.

Comparing the AES to the suggested method, it is clear that the latter has the maximum throughput.

CONCLUSION

In this article, we have covered such topics as the algorithm of IOT, its applications, security models, methodologies, and frameworks, and encryption algorithms investigated in the context of IOT by previous researchers. We have also looked at the recommended approach for the IoT's hybrid encryption algorithm. In order to better protect IoT, we have proposed a hybrid encryption algorithm. One approach proposed for IOT enhancement is the HAN algorithm, which is a hybrid of the AES symmetric encryption algorithm and the NTRU asymmetric encryption algorithm. This algorithm provides

***Article Received:** 25 December 2022 **Revised:** 12 January 2023 **Accepted:** 20 February 2023*

sufficient security for IoT while still being fast enough to generate keys, encryption data, and decrypt data. The multinomial employment in encryption, decryption, and digital signature to create a proper message ensures the security of this algorithm. This algorithm requires less memory than others because to its simpler financial model. The use of this algorithm makes stronger encryption for the Internet of Things (IoT) possible by allowing for attacks to be determined in advance.

REFERENCES

[1] W. Bruce D, GR. Milne, Y. G. Andonova, and F M. Hajjat. "Internet of Things: Convenience vs. privacy and secrecy." Business Horizons 58, no.6, Science Direct, pp. 615-624, 2015.

[2] R. Davice, ”The Internet of Things Opportunties and challeng”, European, p.p.1-8, 2015.

[3] G. Price, “The Internet of Things 2015”, State of THE Market: Internet of Things 2015, Verison wireless company p. p1-24, 2015.

[4] X. Xingmei, Zh. Jing, W. He, “Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things”, 3rd International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, IEEE, p.p.825-828, 2013.

[5] Y. Challal, E. Natalizio, S. Sen, and A. Maria Vegni “Internet of Things security and privacy: Design methods and optimization”, Add Hoc Network, vol.32, Science Direct, p.p1-2, 2015.

[6] Ch. Qiang, G. Quan, B. Yu, L. Yang, “Research on Security Issues of the Internet of Things”, International Journal of Future Generation Communication and Networking (IJFGCN), vol.6, NO.6, IEEE, pp 1-10, 2013.

[7] R. Weber, “Internet of Things New security and privacy challenges”, Computer and Low Security Review, vol.26, issue1, Science Direct, p.p. 23-30, 2010.

[8] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, A. Bouabdallah” A systemic approach for IoT security’, International Conference on Distributed Computing in Sensor Systems (DCOSS), Cambridge, MA, IEEE, p.p.351-355, 2013.

[9] F. Olivier, G. Carlos, N. Florent “New Security Architecture for IoT Network”, Procedia Computer Science, vol.52, Science Direct, p.p1028- 1033, 2015.

[10] M. Xin, H. China “A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System”, International Conference on Cyber-Enabled Disributed Computing and Knowledge Discovery, Xian, IEEE, p.p.62-65, 2015.

[11] H. Shafagh, A. Hithnawi” Poster Abstract: Security Comes First, A Publickey Cryptography Framework for the Internet of Things’, International Conference on Distributed Computing In Sensor Systems (DCOSS), Marina Del Rey, CA, IEEE, p.p.135-136, 2014

[12] A. F. Skarmeta, J. L. Hernandez, M. V. Moreno” A decentralized approach for Security and Privacy challenges in the Internet of Things”, IEEE Word Forum on Internet of Things (WF-IOT), Seoul, IEEE, p.p.67-72, 2014.

[13] N. Hong, Z. Xuefeng, “A Security Framework for internet of thingsbased on SM2 cipher algorithm”, Fifth International Conference on Computer Science and Network Technology, Shiyang, Hubia, China, IEEE, p.p13-16, 2013.

[14] R. Arbia, Ya. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah. "A systemic approach for IoT security." In 2013¬ IEEE International Conference on Distributed Computing in Sensor Systems, p.p. 351-355. IEEE, 2013.

[15] L. Yuan Zeng, “A Security Framework for Internet of Things Based on 4G communication,-2nd International Conference On computer Science And Network Technology, Chanchun, China, IEEE, p.p1715-1718, 2012.

[16] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, “Proposed embeded seurity framework for internet of things”, 2nd International Conference on Information Theory and Aerospace & Elentronic Systems Technology, Chennai, IEEE, p.p.1-5, 2011.

[17] K. Nur Prasetyo ST, Y. Purwanto, and D. Darlis. "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA."In Information and Communication Technology (ICoICT), 2014 2nd International Conference, Bandung, p.p. 75-79. IEEE, 2014.

[18] SB. Vinayaga, M. Ramnath, M. Prasanth, and V. Sundaram. "Encryption and hash based security in Internet of Things." In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference, Chennai, p.p. 1-6. IEEE, 2015.

[19] P. Xu, Li. Min, and He. Yu-Jie. "A hybrid encryption algorithm in the application of equipment information management based on Internet of things." In 3rd

International Conference on Multimedia Technology (ICMT-13). Atlantis Press, 2013.

[20] X. Yi Chen, Zh. Gang Jin, “Research on Key Technology and Applications for Internet of Things”, Physics Procedia, vol33, Science Direct, p.p 561-566, 2012.

[21] R. Wuling, and Zh. Miao. "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication.” In Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on Sanya, p.p. 221-225. IEEE, 2010.

[22] Kureshi, Rameezraja & Mishra, Bhupesh. (2022). A Comparative Study of Data Encryption Techniques for Data Security in the IoT Device. 10.1007/978-981-16-7637-6_40.

[23] Khwailleh, Dana & Albalas, Firas. (2022). A dynamic data encryption method based on addressing the data importance on the internet of things. International Journal of Electrical and Computer Engineering (IJECE). 12. 2139. 10.11591/ijece.v12i2.pp2139-2146.