AN ABRIDGED EXAMINATION OF THE UTILISATION OF CRYPTOGRAPHY IN THE IMPLEMENTATION OF INTERNET OF THINGS (IOT) INSIDE CONTEMPORARY APPLICATIONS

Abstract

As we move towards the implementation of Industry 4.0 more and more Internet of Things (IoT) implementation are coming to the forefront. With the implementation of IoT infrastructure security has become a very important concept and in order to implement security in IoT devices cryptography Is playing a very important role. We have seen in the past that the most popular algorithms which is used till today can be divided broadly into two major categories, symmetric-key and public-key encryption. In this paper we will look into how we can increase the security of IoT devices by using various cryptographic system. We will also see the cryptographic principles like non-repudiation, confidentiality, integrity, and authentication. Cyber hygiene is the most important concept that we must keep in mind in order to secure the integrity of communication, and the protection of sensitive data are all achieved through the use of cryptography. Individuals and organisations have to put effective security measures to safeguard the information they have and secure the communications so that it's not compromised.

Keywords: Cryptography, IoT, Network Security, Cyber hygiene

Author

Indraneel Mukhopadhyay
Amity Institute of Information Technology
Amity University
Kolkata, West Bengal, India.
imukhopadhyaya@gmail.com

I. INTRODUCTION

In the digital era, network security has become an increasingly important concern for both individuals and organizations. We are in the continual danger of cyber assaults, so securing important data and communication has become a major responsibility not just for the Chief Security Officer but each and every user of the system. With the advent of the IoT devices this has become more and more important. In law man's term cryptography is "the study of secure communication via the use of codes and ciphers, is an essential component of network security. It allows safe data transfer and guarantees that sensitive information is only accessible to authorized individuals." This research paper will discuss in detail as well as propose how IoT Implementation security can be increased. We will look into the many cryptographic methods used in network security, such as symmetric-key encryption and public-key encryption, as well as their strengths and drawbacks. Finally, the paper will go through the use of cryptography in network security, such as anonymity, reliability, authentication, and non-repudiation. Individuals and organizations may adopt effective security measures to secure their information and communication by recognizing the role of cryptography in network security.

At the moment, the entire world is running towards being smart and also wants to improve the security with a nominal cost for its implementation. It's a catch22 scenario but that is what everyone wants. Network security entails protecting the system's resources. It is in charge of ensuring the security of any information transmitted from one computer to another through the Internet.

The term "cryptology" is derived from the Greek phrase crypto logos, which translates to "hidden word." Cryptography is the discipline of information security and protection. It is the process of using algorithms and mathematics to encrypt and decrypt data. It motivates the development of a secure treatment procedure. Cryptography is one of the most recent information security technologies. To ensure the integrity of the data, an authorised client must provide a client ID, secret key, or other specific information. It is used to protect increasingly safe and secure data. Non-repudiation, enigma, categorization, and validation are the four challenges associated with organised security. We may use cryptography to store or transmit sensitive information over unreliable machinery and insecure networks.

II. CRYPTOGRAPHY

Cryptography is the process of securing data by converting it into an unreadable format using mathematical formulas and secret keys. To ensure data, message, and transaction confidentiality, integrity, authentication, and non-repudiation, it uses a range of techniques and protocols.

Cryptography's main goal is to prevent unauthorised access to or disclosure of data while it is in motion or at rest. This is accomplished by converting plaintext to cipher text using secure algorithms and keys. The encrypted code in question can only be decrypted and the plaintext recovered by those who have the proper key or password.

Cryptography finds extensive utilisation across a diverse spectrum of applications, encompassing electronic mail, virtual banking, electronic commerce, and the establishment of digital signatures. Its primary objective lies in the provision of fortified communication channels and impervious transactional frameworks. Asymmetric key encryption, also known as public key encryption, digital signatures, hash algorithms, and key exchange systems represent a mere fraction of the diverse array of cryptographic techniques employed in modern information security practises.

Cryptography is a key instrument for safeguarding the security and privacy of digital communications and transactions in today's digital environment. It is also a significant area for research and development, with efforts currently underway to develop fresh cryptographic protocols and algorithms to address developing security challenges.

III. CRYPTOGRAPHIC PRINCIPLES

Cryptographic principles refer to the fundamental concepts and guidelines that govern the design and use of cryptographic systems. These principles are essential for ensuring the security and integrity of data and communications. Here are some key cryptographic principles:

1. **Confidentiality:** Cryptographic systems aim to provide confidentiality, ensuring that data remains private and inaccessible to unauthorized individuals or entities. Encryption is a commonly used technique to achieve confidentiality by converting plaintext into cipher text that can only be decrypted by authorized parties.

2. **Integrity:** Integrity ensures that data remains unaltered and tamper-proof during storage or transmission. Cryptographic mechanisms such as hash functions and digital signatures help verify the integrity of data by generating fixed-size hashes or digital signatures that are unique to the data and can detect any modifications.

3. **Authentication:** Authentication is a crucial process that serves to ascertain the veracity of the identities involved in communication or the trustworthiness of the origins of data. Cryptographic protocols, such as digital certificates, public key infrastructure (PKI), and authentication protocols like HMAC (Hash-based Message Authentication Code), serve the purpose of ascertaining the genuineness of entities or messages.

4. **Non-repudiation:** Non-repudiation prevents individuals from denying their involvement in a communication or transaction. Cryptographic techniques like digital signatures provide evidence of the origin and integrity of a message, making it non-repudiation.

5. **Key management:** Key management is crucial in cryptographic systems as the security of the keys directly impacts the overall security. This principle encompasses secure key generation, distribution, storage, and disposal. Effective key management includes techniques like key exchange protocols, key rotation, and secure key storage mechanisms.

6. **Availability:** Availability ensures that data and services are accessible and usable when needed. Cryptographic systems must be designed in a way that maintains the availability of data and communications, even in the presence of attacks or failures.

7. **Randomness:** Cryptographic systems often rely on random numbers for key generation, initialization vectors, and other purposes. High-quality randomness is necessary to prevent predictability and ensure the security of cryptographic algorithms.

IV. CRYPTOSYSTEM TYPES

If the keys possessed by the transmitter and receiver can be derived through a straightforward computational process from each other. In the realm of asymmetric cryptograms, it is customary to classify cryptosystems into two categories: symmetric and asymmetric. Each category employs a unique key for the purposes of encryption and decryption, contingent upon the algorithm that has been selected. In the realm of symmetric encryption, Alice and Bob possess the capability to employ a singular key (K) for the purpose of both encrypting and decrypting their communications channel, thereby rendering it inscrutable to any potential assailant.

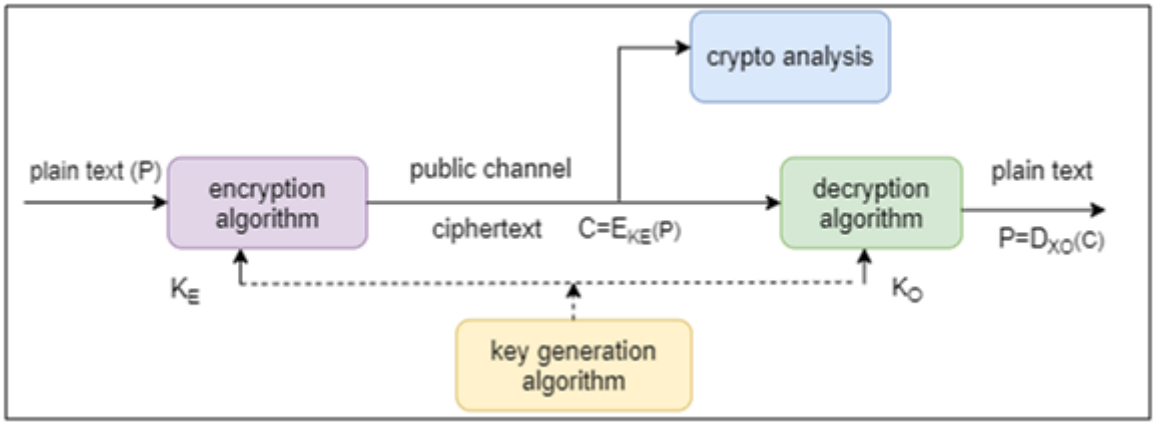

Figure 1: General secrecy system

The preservation of privacy and the establishment of authentication protocols are rendered feasible through the utilisation of cryptographic techniques within the realm of online communication and computer networks. Figure 1 elucidates the manner in which encryption methodologies employ a designated key to effectuate the metamorphosis of plaintext, denoting unencrypted communications, into cryptograms, signifying inscrutable cypher text. Once data has been subjected to encryption, it possesses the potential to be deciphered through the utilisation of a specific algorithm. Cryptanalysis is an erudite discipline that delves into the intricate art of deciphering cryptographic codes, while cryptology, on the other hand, encompasses a broader scope, encompassing not only the analysis of said codes but also the profound exploration of the techniques employed in their construction. Cryptographic algorithms are commonly referred to as cyphers, denoting their role in the realm of data encryption and decryption. In a symmetric cryptosystem, it is imperative to maintain utmost secrecy for both the enciphering and deciphering keys.

Conversely, in an asymmetric system, the disclosure of one key does not jeopardise the integrity and confidentiality of the complementary key.

1. **Asymmetric Cryptosystems**: The generation, propagation, and safeguarding of a multitude of cryptographic keys present pragmatic obstacles. In the year 1976, Diffie-Hellman presented a resolution to the predicament of key distribution. A novel cryptographic technique has been devised, employing a dual-key system wherein one key may be openly shared, while the other key necessitates utmost confidentiality for the purpose of decryption. The task of inferring the secret key from the public key, utilising the two keys that have been generated, is deemed computationally infeasible. In the event that user A aspires to establish a connection with user B, it is within A's purview to employ encryption techniques to safeguard the data by utilising B's public key, which can be readily accessed from a publicly accessible directory. Given that the exclusive possession of the secret deciphering key lies solely with individual B, it follows that the act of deciphering the encrypted text can only be accomplished by the aforementioned party. A public-key cryptosystem, also known as an asymmetric cryptosystem, is the nomenclature employed to delineate the aforementioned system. Asymmetric algorithms possess the capacity to engender what are commonly referred to as digital signatures, provided that they satisfy certain predetermined criteria.

2. **Symmetric Cryptosystems:** The cryptographic keys employed in a conventional cryptosystem, commonly referred to as a secret-key or one-key system, exhibit a notable resemblance or near equivalence to each other during both the enciphering and deciphering processes. It is imperative to maintain utmost confidentiality for both keys, as the integrity of secure communication is compromised in the event of the disclosure of either one. In the scenario where the number of users is denoted by 'n', and assuming that each pair of users necessitates a distinct key, the total number of keys can be expressed as n(n - 1)/2. It is worth noting that even for a moderate value of n, the quantity of keys can become exceedingly large. Users are mandated to engage in routine key exchanges through a deliberately unhurried and impervious channel, such as the utilisation of a private courier service. Asymmetric systems serve to mitigate the inherent challenge of key distribution that arises in cryptographic protocols. One illustrative instance of a symmetric system can be found in the Data Encryption Standard (DES), while an alternative example lies in the realm of rotor cyphers.

3. **Hash Functions:** Hash functions are mathematical algorithms that operate in a unidirectional manner, wherein they accept an input, commonly referred to as a message, and generate a predetermined and unalterable output of a consistent size, known as a hash value or message digest. Hash functions are widely employed for the purpose of ascertaining the integrity of data, given that any alteration made to the input will inevitably yield a distinct hash value. Prominent cryptographic hash functions encompass MD5, SHA-1, SHA-256, and SHA-3.

4. **Digital Signatures**: Digital signatures are cryptographic methodologies employed for the purpose of ascertaining the genuineness and uncorrupted state of a given communication or written record. They offer a means to establish a correlation between a communication and a specific entity while guaranteeing the inability to deny involvement. The utilisation

of asymmetric cryptosystems is a customary approach for the implementation of digital signatures.

5. **Quantum Cryptography:** Quantum cryptography is an esteemed discipline that harnesses the profound principles of quantum mechanics in order to cultivate impregnable communication protocols. It harnesses the inherent characteristics of quantum systems, such as superposition and entanglement, in order to accomplish the task of secure key distribution and the development of encryption algorithms that are impervious to quantum attacks. Quantum key distribution (QKD) exemplifies a quantum cryptographic protocol.

V. IoT ARCHITECTURE

The various IoT architectures are covered in this section. Table 1 discusses the architecture, which consists of four layers. The lowest layer of the four-layer design is reserved for all physical objects, including sensors and actuators. Sensing Layer is the name of this layer. This layer's primary objective is data collection. Internet and network gateways make up the Network Layer, which is the following layer. This layer is solely for the transfer of data. The third layer is the data processing layer, where we use various data analytics methods to the processing of the data. The Application Layer, which is in charge of intelligent application administration, is the last layer.

Table 1: IoT architecture

Layer	Component	Tasks
Application layer	3rd party specific application, consoles, websites.	Data visualization, business models, charts, and machine learning.
Middleware layer	Vendor-specific 3rd party application.	Specific information, identification, monitoring, acquiring, and taking action are transferred.
Network layer	Nodes, gateways, firmware	Send information, verify identity, keep tabs, take possession, and take action.
Perception layer	Sensors (temperature and humidity), actuators (relays, motor and humidity)	Send information, verify identity, keep tabs, take possession, and take action.

Security implementation in IoT devices is most notable from the following perspectives:

1. limited security integration due to the difficulty, if not impossibility, of integrating the vast number and variety of IoT devices into existing security infrastructure.
2. The prevalence of open-source software in IoT device firmware, which increases the likelihood of security flaws.

3. Attacks such as SQL injection, DDoS, man-in-the-middle (MITM), and network breaches frequently employ vulnerable APIs as entry points to command and control centres.

Understanding the role that various cyphers play in securing our devices and the IoT is essential.

VI. LITERATURE REVIEW OF DIFFERENT CIPHER NETWORK

There are different ciphers which we commonly use to enforce security in IoT applications. We have done a thorough study regarding the algorithm, key size and cipher used with its features which has been given in the following tables.

Table 2: Asymmetric, Elliptic Curve Cryptography

Work Suggested	Algorithm, instruments, and methods	Key dimensions, block dimensions, and rounds	Type of cypher and network	Features
ECC Based Lightweight Cybersecurity Solution For IoT Networks Utilising Multi-Access Mobile Edge Computing [11]	ECC, AES, Diffie–Hellman	256 bits and 512 bits	Asymmetric, Elliptic Curve Cryptography (ECC)	It simplified the standard algorithms, making them workable on low-power IoT nodes.
A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data [12]	ECC, SHA-512, XOR, Secret key	512 bits	Asymmetric, Elliptic Curve Cryptography (ECC)	Analysis of the data demonstrates that this strategy is effective.

Table 3: Block Cipher

Work Suggested	Algorithm, instruments, and methods	Key dimensions, block dimensions, and rounds	Type of cypher and network	Features
A New Model of Light Weight Hybrid Cryptography for Internet of Things [13]	LED, PRESENT RECTANGLE S-Box, XOR, SPECK key generation	64 bits block, 128 keys	Block cipher	Resistant to major threats

A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System [14]	PRESENT and Salsa20, XOR, Chaotic system, Pseudo-random keys	64 bits block, 128 bits key	Block cipher	It does what it's supposed to, and it does it quickly. Less processing power is required.
An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System [15]	Matrix location, XOR, Expansion function	256 bits Key. 256 block plain text. 32 rounds	Block cipher	Comparatively faster encryption and decryption times than AES, DES, and SIMON

Table 4: Block cipher, Substitution–per-Mutation Network

Work Suggested	Algorithm, instruments, and methods	Key dimensions, block dimensions, and rounds	Type of cypher and network	Features
SAT_Jo: An Enhanced Lightweight Block Cipher for the Internet of Things [16]	PRESENT, DES, S-Box	64 bits block, 80-bit key, 31 rounds	Block cipher, Substitution–per-Mutation Network (SPN)	With this method, the trade-offs between speed, power consumption, and safety in the Internet of Things can be minimised.
An efficient ASIC Implementation of QARMA Lightweight Algorithm [17]	QARMA, ASIC, CMOS 55 nm, S-Box, Boolean, Permutation, Mix-Columns	64 blocks, 27 rounds	Block cipher, Substitution–per-Mutation Network (SPN)	This method resulted in a 54% reduction in area while simultaneously boosting the frequency 25-fold.

Table 5: Stream Cipher

Work Suggested	Algorithm, instruments, and methods	Key dimensions, block dimensions, and rounds	Type of cypher and network	Features
Lightweight Stream Cipher Scheme for Resource-Constrained IoT Devices [18]	CR4, PRNG, Dynamic key, XorShift64, LFSR, XOR	Secret keys 128, 192, 256 nonce and dynamic key 512 bits, 12 to 14 rounds	Stream cipher	Very common Low processing and energy requirements. Not susceptible to brute-force, arithmetic, or statistical attacks
A4: A Lightweight Stream Cipher [19]	LFSR, FCSR, XOR, Boolean	126 bits Key	Stream cipher	Protection against all possible assaults, including those based on brute force, differentials, and algebra.
A New Lightweight Stream Cipher Based on Chaos [20]	NFSR	80 bits Key	Stream cipher	This algorithm defies statistical attacks

Table 6: Substitution–per-Mutation Network

Work Suggested	Algorithm, instruments, and methods	Key dimensions, block dimensions, and rounds	Type of cypher and network	Features
One round cipher algorithm for multimedia IoT devices [21]	KSA, RC4, SHA-512	One round	Substitution–per-Mutation Network (SPN)	Tested for sensitivity, statistical significance, and visual degeneration and found

				wanting
A Modified Lightweight PRESENT Cipher For IoT Security [22]	PRESENT, TEA, S-Box, P-Layer	64 bits plain text, 80 bits key, 25 rounds	Substitution–per-Mutation Network (SPN)	Enhancements in gate value performance

VII. CONCLUSION

Cryptography protects buyers by enabling the encryption of information and the validation of various clients. This innovation allows the receiver of electronic communication to check the sender, ensures that a message can be read clearly by the desired individual, and guarantees the beneficiary that a message wasn't modified in transit. Cryptography attack techniques like cryptanalysis and brute force assaults are used.

The matter of network security poses a formidable challenge. Diverse perspectives abound when it comes to the conceptualization of "security" and the thresholds for tolerable levels of risk. The crux of cultivating a robust system lies in the meticulous delineation of the parameters that encompass security within the confines of your esteemed organisation. The dissection of activities and frameworks into their elemental components facilitates the evaluation of potential conflicts with existing security measures and practises. The matter of security is a collective concern, necessitating the collaborative efforts of all individuals. It is only through the amalgamation of diligent cooperation, a discerning mind-set, and the implementation of reliable protocols that the attainment of security becomes feasible.

VIII. FUTURE SCOPE

Finally, we know that the future will be organized all over. As a result, "System Security" is gaining importance all over. So, with everyone's help and consistent practice, will it be possible? Science and technology, presumably, develop step by step. We must apply advances in growing disciplines of Science and Technology to envision profoundly secure and trustworthy practices so that we can trouble the bad guys, who must separate our layers of security precaution. Various new and sophisticated encryption approaches provide security and aid in the development of a secure system. In many aspects, quantum cryptography is superior to traditional cryptography. The Heisenberg uncertainty principle underpins quantum cryptography. Steganography is one of the most important methods for concealing information. Steganography conceals the presence of a message by routing data via various transporters. It will almost certainly prevent the mysterious message from being discovered.

REFERENCES

[1] Dorothy E. Denning, Peter J. Denning, "Data Security", ACM Computing Surveys, Volume 11Issue 3pp 227–249 https://doi.org/10.1145/356778.356782

[2] Joshi, Mukund and Renuka Avinash Karkade. "Network Security with Cryptography Prof." (2015). https://www.semanticscholar.org/paper/Network-Security-with-Cryptography-Prof-Joshi-Karkade/486b32d22ceea364263cccca0bfae26a427f3f0b
[3] Mukhopadhyay, I. , Chakraborty, M. and Chakrabarti, S. (2011) A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems. Journal of Information Security, 2, 28-38. doi: 10.4236/jis.2011.21003
[4] Murat Fiskiran, Ruby B. Lee, "Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments", http://palms.ee.princeton.edu/PALMSopen/fiskiran02workload-with-reference.pdf
[5] Coron, J. S., "What is cryptography?", IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73. https://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf
[6] Salomon, D., "Coding for Data and Computer Communications", New York, NY: Spring Science and Business Media. 2005.
[7] Shannon, E. C.," Communication theory of secrecy system", Bell System Technical Journal, Vol.28, No.4, 1949, pp.656- 715.
[8] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, **11,** pp. 305-330, https://doi.org/10.1145/356789.356793
[9] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, **21,** pp. 120-126, https://doi.org/10.1145/359340.359342
[10] I Mukhopadhyay et.at. "The Future of the Internet of Things (IoT) and IoT Authentication", 2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), 978-1-6654-7512-9/23/ ©2023 IEEE, DOI: 10.1109/IEMECON56962.2023.10092285
[11] E. Gyamfi, J. A. Ansere and L. Xu, "ECC Based Lightweight Cybersecurity Solution For IoT Networks Utilising Multi-Access Mobile Edge Computing," 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 2019, pp. 149-154, doi: 10.1109/FMEC.2019.8795315.
[12] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739.
[13] V. Prakash, A. V. Singh and S. Kumar Khatri, "A New Model of Light Weight Hybrid Cryptography for Internet of Things," 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2019, pp. 282-285, doi: 10.1109/ICECA.2019.8821924.
[14] Z. M. Jawad Kubba and H. K. Hoomod, "A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System," 2019 First International Conference of Computer and Applied Sciences (CAS), Baghdad, Iraq, 2019, pp. 199-203, doi: 10.1109/CAS47993.2019.9075488.
[15] R. R. K. Chaudhary and K. Chatterjee, "An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System," 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2020, pp. 991-995, doi: 10.1109/SPIN48934.2020.9071421.
[16] M. J. R. Shantha and L. Arockiam, "SAT_Jo: An Enhanced Lightweight Block Cipher for the Internet of Things," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 1146-1150, doi: 10.1109/ICCONS.2018.8663068.
[17] C. Zhao, Y. Yan and W. Li, "An efficient ASIC Implementation of QARMA Lightweight Algorithm," 2019 IEEE 13th International Conference on ASIC (ASICON), Chongqing, China, 2019, pp. 1-4, doi: 10.1109/ASICON47005.2019.8983618.
[18] H. Noura, R. Couturier, C. Pham and A. Chehab, "Lightweight Stream Cipher Scheme for Resource-Constrained IoT Devices," 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 2019, pp. 1-8, doi: 10.1109/WiMOB.2019.8923144.
[19] N. A. Mohandas, A. Swathi, A. R., A. Nazar and G. Sharath, "A4: A Lightweight Stream Cipher," 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 573-577, doi: 10.1109/ICCES48766.2020.9138048.
[20] L. Ding, C. Liu, Y. Zhang, Q. Ding, A new lightweight stream cipher based on chaos, Symmetry 11 (7) (2019) http://dx.doi.org/10.3390/ sym11070853, MDPI.
[21] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, M.M. Mansour, One round cipher algorithm for multimedia IoT devices, Multimedia Tools Appl. (2018) http://dx.doi.org/10.1007/s11042-018-5660-y
[22] R. Chatterjee and R. Chakraborty, "A Modified Lightweight PRESENT Cipher For IoT Security," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-6, doi: 10.1109/ICCSEA49143.2020.9132950.

