Available at https://www.iasj.net/iasj
Iraqi Academic Scientific Journals
Journal homepage:
https://journals.uokerbala.edu.iq/index.php/UOKJ

Research Article

Cipher algorithms challenges of IoT applications: A review

[1,]Zaid M. Jawad Kubba [2],Wisam Abed Shukur [3,]Mustafa A. Ali

[1,2,]Department of Computer, College of Education for Pure Science Ibn Al-Haitham, University of Baghdad, Iraq

[3,]College of Computer Science and Information Technology, University of Kerbala

Article Info
Article history:
Received 27 - 5 -2024
Received in revised form 21-7 -2024
Accepted 8 -9 -2024
Available online 31 -12 -2024
Keywords: Cryptography; Information Security; IoT; Cryptosystems

Abstract:

The enormous developments in the Internet and communications applications present new security challenges, such as sensitive data collection of IoT devices. Cipher algorithms play a key role in IoT applications, countless cryptosystems are presented for securing such applications. Various challenges were intensely presented due to the vast increase in the developments of IoT applications and the requirements of the cipher algorithms which are considered the main challenges for adapting lightweight cryptosystems. Thus, in this study, different cipher algorithms are reviewed and analyzed based on lightweight cryptosystems. Moreover, various features are examined and discussed through the most common cipher algorithms for designing cipher algorithms to be efficient in IoT applications. The result showed the major challenges and factors that should be undertaken when designing cryptosystems of IoT applications. The challenges are experimented with parameters such as key size, computational cost, time, etc. This work would be referenced for developing an efficient cipher algorithm for IoT applications which presents the main factors and challenges that should be considered when designing such cryptosystems.

Corresponding Author E-mail : zaidkubba@colaw.uobaghdad.edu.iq
Peer review under responsibility of Iraqi Academic Scientific Journal and University of Kerbala.

1. Introduction

In Internet of Things (IoT) is the new trend for connecting objects and appliances in real-time with remote applications in the devices and communication networks. IoT introduces new constraints and challenges that increase the requirements of robust cryptosystems[1]. In contrast, IoT is mainly based on constrained devices and they provide low computation processes [2]. This may represent the major drawback within these devices and their applications in terms of data security. IoT devices may involve very sensitive data that may be related to the physical environments corresponding to the personal information or addresses of people, discoursing this data may impact security issues [2]. In contrast, most traditional cryptosystems that apply cryptography provide solutions that focus on constructing a high layer of security, while ignoring the circumstances of constrained devices [13]. Enhancing the security of the cryptosystems requires a various procedure to support the current methods and should improve new behaviors that are resistant to most types of attacks [1]. Therefore, cipher algorithms are considered the most dependable approaches applied to protect valued and sensing data[3]. This approach is mainly based on developing robust cipher algorithms and keys that are considered efficient against different attacks, such as different sizes of keys being used for every round to have randomized round keys [4]. However, most of the recent cryptosystems are focused on the developments of encryption speed and simplicity for implementation in IoT applications. Such cryptosystems are considered less complex hardware circuitry and a distinctive feature of these cipher systems is the continued change of the keys for all bits of the plain text resulting in the creation of robust cipher text even for the plain text of repetitive blocks[5]. This paper presents a review of the security challenges of IoT applications, cipher categories, a description of cipher algorithms, and the symmetric versus asymmetric deliberating and examining various public types of lightweight cipher algorithms.

2. SECURITY CHALLENGES BASED IOT APPLICATIONS

In recent, most devices and applications have connected and managed their services through the Internet. Various IoT-based applications have been designed, such as online shopping and direct online bill payment[6].The rapid increase in IoT devices and applications presented a new challenge in terms of diverse security risks. IoT devices are based on limited resources that can handle small and lightweight applications. Constrained devices that apply for IoT systems consist of small resources such as low processor and memory that cannot implement conventional cryptosystems[7]. This is measured as a big challenge facing IoT systems which is difficult to implement conventional security on constrained devices. In contrast, the traditional cipher algorithms produce more security and do not take into account the requirements of IoT devices. Moreover, there are various challenges facing IoT security such as Encryption, Interoperability, Key Management, authentication, and mechanisms[8]. Privacy and confidentiality are considered the main security issues in IoT applications and cipher algorithms are the vital key to protect sensitive data of the sensor nodes and transmission information. Most of the Encryption algorithms implemented within the IoT systems have shown vital challenges,

and encounter various security issues of the existing network systems such as privacy interoperability and lifespan and support that arise from the utilization of billions of intelligent devices[9]. Hence, the main security challenges that should be concerned with IoT applications are confidentiality, integrity, privacy, availability, authenticity, non-repudiation, and key management[10]. The main challenges of IoT applications are shown in Figure 4 below.

Figure 1. Security Challenges of IoT[10]

Despite IoT applications having grown speedily over the last few years, cryptosystems still face difficulty in reaching the high level of security risks. The standard security algorithms are designed to work with traditional computers and networks that are easy to implement and execute on most forms of cryptosystems. In contrast, IoT cryptosystems have no such standard solution that could work on every device because of the diverse constraints among dissimilar devices.

Thus, to provide secure communication of IoT devices with confidentiality, integrity, and authentication services, cryptosystems require multi-layers of security solutions, to protect the information from intrusions and other attacks[11]. Moreover, traditional communications could be secure at diverse layers and the current security applied in internet protocols is based on a popular broadly trusted group of cryptographic algorithms such as the AES algorithm that is utilized to provide confidentiality, the RSA algorithm utilized to generate digital signatures, and Key transport, SHA-3 algorithms generate hash values, and Diffie-Hellman algorithm that provides asymmetric shared key. This set of cipher algorithms is considered as difficult to implement in most IoT systems related to the high requirements of resources that should exist in the devices. The traditional cipher algorithms give excellent security and typically work with appliances that should have enough resources such as memory and high processing speed. Thus, Lightweight cipher algorithms are designed to use fewer resources and are appropriate for constrained devices. These algorithms such as PRESENT, LED, XTEA, and SIMON require less computational cost and low memory size, which is considered suitable for IoT devices[12]. However, Lightweight cipher algorithms suffer from the tradeoff of cost and performance and should be a concern when implemented in IoT devices. Recently, researchers enhanced and expanded the field of Lightweight cipher algorithms by mixing them with other cipher algorithms such as ElGamal and ECC to be utilized within IoT devices. This approach would give security higher than other lightweight cipher algorithms. It is designed to be implemented with constrained devices and is considered appropriate for IoT systems that comprise limited memory and processors. Recent studies about IoT network security are providing hopeful results like efficient implementations of shifting operations and adapting algorithms such as Elliptic curve cryptography (ECC) and (RSA) rather than multiplication operations

of the microprocessor that require more resources. Thus, In an IoT environment, the requirement for using the appropriate cryptosystem solution is increasing. Nonetheless, based on the limited resources such as low power computation, small memory and small size of the node devices produce limitations in implementing traditional cryptosystems. The primitives of traditional cipher algorithms may not be suitable for these constrained devices[6, 7]. Therefore, it is necessary to adapt and develop a new family of cryptosystems that are efficient for IoT applications. In addition, the current smart applications require an intelligent cipher solution that delivers adequate security performance in universal computing and also for constrained edge devices.

3. CIPHER ALGORITHMS

Cryptography is considered a mathematical or logical scheme that is mainly based on converting real data and concepts into vague data in random and reversible order. This scheme is based on reversible and utilizable operations that could work in two directions. Cryptography consists of two parameters which are the message text and the key to produce a secret text changed unpredictably using cipher algorithms [13, 14]. In general, cipher algorithms are used to achieve many goals and some of them are the following:

• Authentication: is the operation of presenting identity to a person to access special resources and information using the same keys[15].

• Confidentiality: is The eventual goal of the encryption process to confirm that only the cipher-key owner obtains the original plaintext[16].

• Data Integrity: is the process that guarantees the validity of access to the database that belongs to an exact group or person[17].

• Non-Repudiation: is the process of ensuring that both the sender and receiver acknowledge the delivery of the messages[18].

• Access Control: is the operation that confirms access only to the group with the right authentication to log into the corporate information and resources[19].

Moreover, there are two types of cryptography algorithms which are symmetric and asymmetric cipher algorithms.

3.1 SYMMETRIC CIPHER ALGORITHMS

Symmetric cipher refers to algorithms that utilize the same encryption key for both the plaintext and ciphertext such as the DES algorithm[20]. The Symmetric key algorithms exchange the key between the two sides of the sender and receiver and consider the disadvantage of symmetric key algorithms. In contrast, the core advantages of symmetric key algorithms are that they do not consume too many resources with a high-speed encryption process. Symmetric Cryptography is divided into two types: block cipher and stream cipher algorithms. In the block cipher algorithm, the plaintext of any length of the message is converted into fixed blocks and each block is processed individually. Different techniques are used with block cipher algorithms that help to manage the message length when divided into blocks such as smaller or longer than the block size, then the padding approach should implemented. Block cipher is mainly based on the key length for encrypting and decrypting the message which represents the strength of the cipher algorithm and both the message and the key are applied to generate the cipher text. In contrast, In the stream cipher, the encryption process works bit by bit and encrypts together with the key stream to produce cipher text unreadable to anyone without the proper key. In general, stream cipher algorithms are

considered faster, require small resources for the encryption process, and that most chosen for converting the small message. In contrast, block cipher algorithms could be converted into stream cipher algorithms by applying various methods of operations such as counter mode which means a secure block cipher could build a fast stream cipher algorithm[21]. Such symmetric cipher algorithms that could be used in IoT applications are DES and PRESENT algorithms.

3.2 ASYMMETRIC CIPHER ALGORITHMS

Asymmetric cipher algorithms apply different keys for the plaintext and the ciphertext[22]. This approach comprises two keys: a private key and a public key. The public key is utilized to encipher plaintext and everyone may know it, whereas the private key is utilized for the deciphering process of the cipher text. Distinct from symmetric cipher algorithms, which share different keys, this is considered one of the core advantages of asymmetric ciphers. In contrast, the core disadvantage of asymmetric cipher algorithms is that consume too many resources and are not as fast as symmetric cipher algorithms. Some of the asymmetric cipher algorithms that could be used in IoT applications are RSA and Elliptic Curve Cryptography (ECC) algorithms.
The previous studies of the Symmetric and Asymmetric cryptosystems exhibited that some of the symmetric cipher algorithms are considered faster in the enciphering process compared to asymmetric cipher algorithms based on a comparative analysis of time complexity[6].

4. CHALLENGES OF CIPHER ALGORITHMS

In this section, the most common challenges related to the development and implementation of cipher algorithms for IoT applications will be presented. The current studies for developing cipher algorithms for constrained devices that consist of limited resources such as power consumption, performance speed, storage size, and data manipulation are considered critical issues. IoT applications are designed based on connecting numerous devices on a network and each device consists of different software and hardware. Most IoT appliances are computers, sensors, digital tools, and microcontrollers that transfer sensitive data via untrusted networks. Therefore, protecting data and applications is essential in IoT security which requires an efficient cryptosystem for such devices. However, Numerous cipher algorithms are designed to work with different applications and this work will be focused on the shortcomings of the most used cipher algorithms such as the cost and performance of commonly used cryptographic algorithms, including DES, AES, and RSA[23].

4.1 HARDWARE IMPLEMENTATION

One of the major issues that researchers and developers when designing and implementing cipher algorithms for IoT devices is the hardware. The storage consumption, structure size, and power consumption are the main metrics, for consideration during designing cipher algorithms. The particular type of device only gives an exact measure for any lightweight algorithm but is still not efficient for other devices. In addition, the simulation results that apply to different devices would not be enough with exact measurements and other tools for the same appliances. Thus, there is no typical comparison for measuring the efficiency of the hardware implementation based on different algorithms. In contrast, one of the main trends for developing an efficient cipher algorithm for such devices is based on considering the lowest resource consumption such as memory requirements, and smaller

block processing with smaller key sizes that are preferable for lightweight cryptosystems. However, implementation of small key length algorithms into constrained devices using read-only structures memory would enable the key schedule to use only simple operations and would be easy to break. Moreover, energy management is considered the core for hardware implementation along with the time consumption of multiple operations are also plays a key role in designing lightweight cipher algorithms[24].

4.2 SOFTWARE IMPLEMENTATION

The other main issue in developing and implementing the cipher algorithms for IoT applications is the primitive software such as RAM consumption, program size, and the data in bytes per round, which are considered essential measurements. The efficient framework should be evaluated based on the implementations and performance of different cipher algorithms using diverse metrics across different IoT applications. Therefore, the concern of recent studies is to reduce the computational cost of software implementation for the primitive parameters of cipher algorithms such as the number of rounds, key size, and programming code. This concern should Improve the software efficiency of cipher algorithms which are designed for resource devices[25].

4.3 KEY DISTRIBUTION

Cipher algorithms require encryption keys to encrypt and decrypt messages that transfer through IoT devices. In addition, nodes and the appliances in IoT systems should agree on key exchange in such a way as to protect the messages from adversaries and compromise the whole network. Key management is the core of cipher algorithms that protect sensitive data of different devices and applications in the communication network [26]. The generated cipher Keys should be exchanged and then stored in a manner that keeps it protected from the eavesdropper which would compromise the communication and data integrity if knows the encryption key. One of the main challenges to protect the key distribution in the network is that the entire system should comprise a refresh and update process of the keys from time to time. Such systems should implement a single key that should be utilized for all nodes and devices to make the encryption process easier for IoT applications. However, if one node becomes compromised by an attacker then all cipher algorithms in the nodes of the entire network would be broken. In contrast, having a different key for each node makes the entire key management process harder which consists of a large number of nodes and devices. Thus, still no fit size for all cipher algorithms of the key distribution in heterogeneous devices of such IoT applications.

4.4 DIGITAL SIGNATURES

Digital signatures are considered an essential component in asymmetric cipher algorithms which offer several security services such as authenticity, integrity, and non-repudiation of exchange messages in IoT applications. The cipher algorithms of IoT applications are applied to provide authentication, signature, and access control methods that could help secure sensitive data and protect them from unauthorized access. [27]. The digital signatures mechanism guarantees that the message receiver can verify the identity and prevent the eavesdropper from sending the message. Numerous digital signature algorithms have been proposed to offer practical mechanisms for reaching message integrity[28]. The Digital Signature algorithm is a mathematical scheme developed to ensure the integrity of data exchange in communication networks by giving authenticity to the received data

along with the data sender. This type of cipher algorithm is preferred for cryptosystems that require data integrity during the exchange of sensitive information between several parties. A digital signature comprises assigning a unique value that acts as a stamp on the message. This value could be generated by a hash function that converts the original message of the sender user with a key into a hash value[29]. However, digital signature verification is considered the main concern for cryptosystem developers to a void cryptoanalysis from attacking the generated hash value while transferring the data in untrusted networks. The recipient usually uses the public key to verify the message, along with generating the hash value utilizing the hash algorithm. If the two hash values for the sender and receiver are the same, it would mean that the message is truthful and no one modified it otherwise the data was changed. However, the speed and efficiency of such an algorithm are important for reaching the correct decision and giving feedback for evaluations[29].

Hence, all of the above challenges should be considered during designing and developing cipher algorithms for constrained devices of IoT applications. The analyses of these challenges would be useful for researchers in choosing appropriate cipher algorithms for real scenarios and architectures with their specific features.

5. CIPHER ALGORITHMS-BASED IOT APPLICATIONS

Lightweight cipher algorithms are mainly based on the cryptography field that focuses on fast performance and efficient encryption techniques for constrained devices of IoT applications. These algorithms are considered as the replacement of the traditional computationally expensive cipher algorithms that require high resource requirements. In contrast, Lightweight cipher algorithms are designed to be lighter based on their key length, storage requirements, and execution time along with reaching an adequate level of security[24]. These types of cipher algorithms are considered the most suitable for constrained devices and more applicable for IoT systems which are lesser resources for utilized compared to heavyweight traditional cryptosystems[30]. Lightweight cryptosystems are developed to fit the resource limitations of such IoT devices, for the important specification of key size, block size, code functions, clock cycles, and other properties. The target of developing a lightweight cipher algorithm is to compromise various parameters such as low resource requirements, computational cost, performance, and robustness of the cryptosystem. Thus, the main requirements for designing an efficient cryptosystem of IoT applications are based on lightweight algorithms that are intended to utilize smaller block sizes (32, 48, or 64 bits) than a traditional cipher algorithm, which has a larger block size (128 or 256 bits). Lightweight cipher algorithms are compromises on properties of hardware implementation that are evaluated by essential measures such as chip size, memory size, and power consumption. Different structures of Lightweight cipher algorithms should be considered when developing an efficient cipher algorithm as shown in the following table 1.

Table 1. The Structures of Different Lightweight Cipher Algorithms			
Acronyms	Cipher Structure	Lightweight Cipher Algorithms	Explanation of Cipher Structure
SPN	Substitution Permutation Networks	AES, PRESENT, I-PRESENT, GIFT, Midori, SKINNY, Zorro, Prince, Pride, EPCBC, LED, Picaro, Crypton, Rectangle, Iceberg, Noekeon, Puffin-2, 3Way, Kalyna, Kuznyechik, SAFER, SHARK, Square,	In substitution box(S-Box) replaces symbols or groups of symbols, while the permutation box(P-Box) rearranges their orders and then forms them into the next round
FN	Feistel networks	LBlock, DESL, DESLX, TEA	The data block is splatted into two equivalent parts and then run encryption in multiple rounds
GFN	General Feistel Network	CLEFIA, TWINE,Piccolo,	Divides input data into sub chunks (k) and runs a standard Feistel function for each two sub chunks, then executes a cyclic shift of (k) subblocks [12]
ARX	Add-Rotate-XO	Speck, SIMON, HIGHT, IDEA	ARX involves three operations 1-Add modification on the finite field 2-Rotate circular shift 3- XOR function encryption-decryption using addition, rotation, and XOR functions, in comparison with SPN and Feistel ciphers although ARX is fast it is limited in security
NLFSR	NonLinear-Feedback Shift Register	KeeLoq, Halka, KATAN/KTANTAN	builds blocks of stream ciphers
Hybrid	Hybrid	Hummingbird, Hummingbird-2, PRESENT-GRP	Mix of any three types of(SPN, FN, GFN, ARX, NLFSR)

Table 2. Comparison of the most known lightweight cipher algorithms

Cipher Algorithm	Structure	Year	Block Size (bits)	Key Size (bits)	Rounds	Throughput At 100Khz (Kbps)	Describe & Environment	Ref.
AES	SPN	2001	128	128	10	56.64	classic algorithm standardized by NIST is not proper for extremely constrained devices like RFID tags and sensor networks	13
				192	12			
				256	14			
I-PRESENT	SPN	2014	64	80	30	12.4	Encryption-Decryption is done in the same circuit	14
				128		12.12		
GIFT	SPN	2017	64	128	28		improved version of PRESENT	15
			128		40			
CLEFIA	GFN	2007	128	128	18	39	High-performance high security towards a variety of attacks, used in ultra-small applications	16
Rectangle	SPN	2015	64	80	25	246	ultra-lightweight very good security and performance, suitable to use with a variety of application	17
				128				
LBlock	FN	2011	64	80	32	200	enough security against various attacks, use in RFID tags, sensor networks, microcontrollers…	18
SPECK	ARX	2013	48	96	23	4.2	Released by the National Security Agency (NSA)	19
			64	128	27			
Halka	NLFSR	2014	64	80	24		High level of security, 7% smaller and 3 times faster than PRESENT	20

In addition, to achieve an efficient cryptosystem for IoT applications, it is necessary to develop a cipher algorithm consisting of tradeoffs among both security and performance[31].Thus, in this work a comparison of the most known lightweight cipher algorithms is conducted based on some major features such as block size, key size, and rounds with a Throughput measurement of each algorithm as shown in Table 2.

Table 2 above shows the security analysis of lightweight cipher algorithms that are based on enough security margin against various known attacks, such as differential and correlation cryptanalysis. The analysis based on these
major features that should be considered when designing and developing cipher algorithms which are usually need more round operations eve sufficient diffusion property. There are different indicators are utilized to guide the design of lightweight cipher algorithms, such as block size, key size, rounds, and high throughput.

6. Result and analysis

Some considerations should be considered when designing an efficient cipher algorithm as the following:

- The main variables of a cipher algorithm should be considered such as block size, key length, rounds, and throughput. In contrast, the internal structure of the algorithm may cause security issues such as brute-force key attacks.
- The cipher algorithms would be preferred built upon parameters that are widely utilized and thoroughly analyzed.
- The structure of cipher algorithms should be based on simple function and alterations operations with simplified layers that decrease the ROM requirements.
- The design should compromise productive components to measure the performance such as data-dependent bits, shift registers, low cost, and other elements.
- The structure of cipher algorithms should consist of a simple key schedule that could derive subkeys rapidly.
- The entire design of cipher algorithms should compromise on basic operations with a substantial number of rounds.
- The proposed cipher algorithms should consider the operations and the available resources for which devices and platforms are designed.
- The cipher algorithms that work with constrained devices should be equipped with a symmetric key algorithm for attaining the security of end-to-end and consumes fewer resources of IoT applications.

  Thus, to design efficient cipher algorithms for IoT applications, it is necessary to consider the tradeoff between both security and performance

6. CONCLUSION

The significant change in the usage of internet and the form amount of computing devices presents many challenges in terms of the security of their resources, as well as the connection data that are transmitted in untrusted networks. IoT applications are considered the most concern for cryptosystem developers which consist of various platforms and limitations that should be studied well before designing such systems. This paper presented a broad description of the most important challenges of cipher algorithms that should be considered for de-

veloping an efficient lightweight cryptosystem. These challenges are studied and explored in order to help researchers enhance the performance of the current cipher algorithms of constrained devices. Therefore, several limitations of cipher algorithms-based IoT applications are discussed in this paper such as hardware and software implementation, Key size, block size, rounds, throughput, and others. Moreover, the security analysis shows that the cipher algorithms should have enough security margin against various known attacks, such as differential and correlation cryptanalysis. Moreover, cipher algorithms should achieve a trade-off between high diffusivity and available hardware resources. The recently used cipher algorithms are not all applicable to IoT applications due to their complexity, computational cost, and performance. The design requirements and different essentials, issues, and trends in cryptosystem security are expressed in this paper to give a valued solid idea for designing an efficient cipher algorithm for IoT applications. Thus, to use IoT devices and applications with all their technological advantages, an efficient cipher algorithm is required to tradeoff between the performance and computational cost.

REFERENCES

1. HUSSEIN, W.A., Z.M.J. KUBBA, and A. AWAD, *Towards Designing intelligent intrusion detection systems.* Journal Of AL-Turath University College, 2023. 2(36).
2. Jamshed, M.A., et al., *Challenges, applications, and future of wireless sensors in Internet of Things: A review*. IEEE Sensors Journal, 2022. 22(6): p. 5482-5494.
3. Urooj, S., et al., *Cryptographic data security for reliable wireless sensor network.* Alexandria Engineering Journal, 2023. 72: p. 37-50.
4. Jat, D.S. and I.S. Gill. *Enhanced Advanced Encryption Standard with Randomised Round Keys*. in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. 2020. IEEE.
5. Qassir, S.A., M.T. Gaata, and A.T. Sadiq, *Modern and Lightweight Component-based Symmetric Cipher Algorithms.* ARO-The Scientific Journal of Koya University, 2022. 10(2): p. 152-168.
6. Hasan, M.K., et al., *Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications.* Complexity, 2021. 2021: p. 1-13.
7. Kubba, Z.M.J. and W.A. Shukur. *An enhanced LED cipher algorithm performance for data security in IoT systems*. in *AIP Conference Proceedings*. 2023. AIP Publishing.
8. Mohanty, J., et al., *IoT security, challenges, and solutions: a review.* Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2, 2021: p. 493-504.
9. Thabit, F., et al., *A comprehensive literature survey of cryptography algorithms for improving the iot security.* Internet of Things, 2023: p. 100759.
10. Khan, Y., et al., *Architectural threats to security and privacy: a challenge for internet of things (IoT) applications*. Electronics, 2022. 12(1): p. 88.
11. Bary, T.A.A.A.A., B.M. Elomda, and H.A. Hassan, *Multiple Layer Public Blockchain Approach for Internet of Things (IoT) Systems (January 2024)*. IEEE Access, 2024.
12. Panahi, P., et al., *Performance evaluation of lightweight encryption algorithms for IoT-based applications.* Arabian Journal for Science and Engineering, 2021. 46(4): p. 4015-4037.
13. Salami, Y., V. Khajevand, and E. Zeinali, *Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges.* Journal of Computer & Robotics, 2023. 16(2): p. 46-56.
14. Shukur, W.A., Z.M.J. Kubba, and S.S. Ahmed, *Novel Standard Polynomial as New Mathematical Basis for Digital Information*

Encryption Process. Advances in Decision Sciences, 2023. 27(3): p. 72-85.
15. Saqib, M. and A.H. Moon, *A systematic security assessment and review of Internet of things in the context of authentication.* Computers & Security, 2023. 125: p. 103053.
16. Sharma, K., et al., *RSA based encryption approach for preserving confidentiality of big data*. Journal of King Saud University-Computer and Information Sciences, 2022. 34(5): p. 2088-2097.
17. Gangwani, P., et al., *IoT Device Identity Management and Blockchain for Security and Data Integrity*. International Journal of Computer Applications, 2023. 184(42): p. 49-55.
18. Chen, F., et al., *TrustBuilder: A non-repudiation scheme for IoT cloud applications.* Computers & Security, 2022. 116: p. 102664.
19. Sun, S., et al., *Blockchain-based IoT access control system: towards security, lightweight, and cross-domain.* IEEE Access, 2021. 9: p. 36868-36878.
20. Pitale, R.R., et al. *Cryptographic algorithm development and application for encryption and decryption*. in *Proceedings of the 5th International Conference on Information Management & Machine Intelligence*. 2023.
21. Noura, H., et al., *Lesca: Lightweight stream cipher algorithm for emerging systems.* Ad Hoc Networks, 2023. 138: p. 102999.
22. Banoth, R. and R. Regar, *Asymmetric Key Cryptography*, in *Classical and Modern Cryptography for Beginners*. 2023, Springer. p. 109-165.
23. Radhi, S.M. and R. Ogla, *In-Depth Assessment of Cryptographic Algorithms Namely DES, 3DES, AES, RSA, and Blowfish.* Iraqi Journal of Computers, Communications, Control and Systems Engineering, 2023. 23(3): p. 125-138.
24. Shamala, L.M., et al. *Lightweight cryptography algorithms for internet of things enabled networks: An overview*. in *Journal of Physics: Conference Series*. 2021. IOP Publishing.
25. Al_Azzawi, R.M.A. and S.S. AL-DABBAGH, *Software Implementation Solutions of A Lightweight Block Cipher to Secure Restricted IoT Environment: A Review.* AL-Rafidain Journal of Computer Sciences and Mathematics, 2022. 16(2): p. 77-88.
26. Dammak, M., et al., *Decentralized lightweight group key management for dynamic access control in IoT environments.* IEEE Transactions on Network and Service Management, 2020. 17(3): p. 1742-1757.
27. Lalem, F., et al., *A novel digital signature scheme for advanced asymmetric encryption techniques.* Applied Sciences, 2023. 13(8): p. 5172.
28. Kavin, B.P. and S. Ganapathy, *A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves.* Int. Arab J. Inf. Technol., 2021. 18(2): p. 180-190.
29. Vandervelden, T., et al., *SHA 3 and Keccak variants computation speeds on constrained devices.* Future Generation Computer Systems, 2022. 128: p. 28-35.
30. Pandey, S. and B. Bhushan, *Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks.* Wireless Networks, 2024: p. 1-40.
31. Yasmin, N. and R. Gupta, *Modified lightweight GIFT cipher for security enhancement in resource-constrained IoT devices.* International Journal of Information Technology, 2024. 16(4): p. 2647-2659.