Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Exploring the Efficacy of Lightweight Encryption Techniques: A Comprehensive Review

Haider Hameed Razzaq al-Mahmood*[a,b], Saad N.Alsaad[c]

[a]*Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq : phd202130676@iips.edu.iq*
[b]*Department of Computer Science, College of Science, University of Mustansiriyah, Baghdad, Iraq : haideritsec@uomustansiriyah.edu.iq*
[c]*Computer Science Department, Mustansiriyah University, Baghdad, Iraq: dr.alsaadcs@uomustansiriyah.edu.iq*

ARTICLE INFO

Article history:
Received: 13 /9/2023
Rrevised form: 23 /11/2023
Accepted : 2 /12/2023
Available online: 30 /12/2023

Keywords:

IoT Applications

Data protection

Lightweight Stream Cipher

Lightweight encryption

ABSTRACT

With the widespread adoption of applications and IoT devices, modern society has come to rely on them in various aspects of daily life. These applications and devices cover a range of needs, including home appliances and even medical devices for body monitoring. Because a significant amount of data generated by IoT devices and applications must be transmitted over networks, particularly the Internet, there is an increased risk of cyber-attacks on this transmitted data. This data can be text, images, sound, or other forms, and it is critical to ensure its protection, especially if it contains valuable information. Extensive research has been conducted on various encryption algorithms to ensure the security of transmitted data, whether through block ciphers or stream ciphers. In addition, efforts have been made to increase encryption efficiency by securing the transmission channels. The question of this research is "what is the state of the art in the lightweight encryption in terms of strength and speed up the process?". This paper provides a comprehensive survey of research related to two main categories of lightweight encryption, and work focused on secure authentication between entities. The paper includes an analysis of the techniques used in each surveyed paper and highlights their main results.

https:// 10.29304/jqcsm.2023.15.41348

1. Introduction

Today's lifestyle depends on numerous devices and applications that generate different types of data, such as text, videos, images, sound…. etc[1-5]. These data represent a new concept of data science called "Big Data," which refers to data generated in streams with high velocity and large variety, figure (1) represents the framework for the concept of big data [6, 7]. It is worth mentioning that most of these data need to be transferred via a network, which is the Internet in its most form, bringing all threats available on the network to such data as stated in [8]. Internet represents the dominant media of the network because it facilitates connect between two to multiple nodes worldwide [9, 10], data transmitted over the Internet become prone to a different type of attack especially modification attack. As such, there is a need to prevent such attacks or at least thwart the modification attack by making the data transmitted unreadable by humans, Some practical solutions for internet threats are demonstrated in figure (2), for more information, see [11-13]. Therefore, lightweight encryption as a new concept of encryption is emerged to suit encrypts data produced by devices with some constraints features such as RAM, CPU and permanent storage capacity [14-16]. Even lightweight encryption works with some limitations, but it is still achieving good balance between the security level and the available resources in terms of calculation time and how it resists attacks[17].

∗Corresponding author Haider Hameed Razzaq al-Mahmood

Email addresses: phd202130676@iips.edu.iq

Communicated by 'sub etitor'

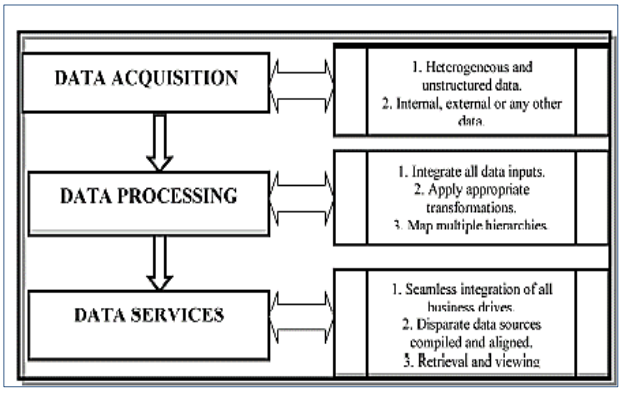

Figure 1. Framework for data mining using Big Data [6]

The two approaches of encryption algorithms are block cipher and stream cipher, block cipher algorithm divide the plain text into fixed size block before feed it to the encryption process[18]. On the other hand, stream cipher manipulate each bit of the original plaint text in real time regardless of plain text size[19], both approaches aim to encrypt data and decrypt it at the receiver end to thwart an attacker attempts to steal sensitive information. For more information, see [20].

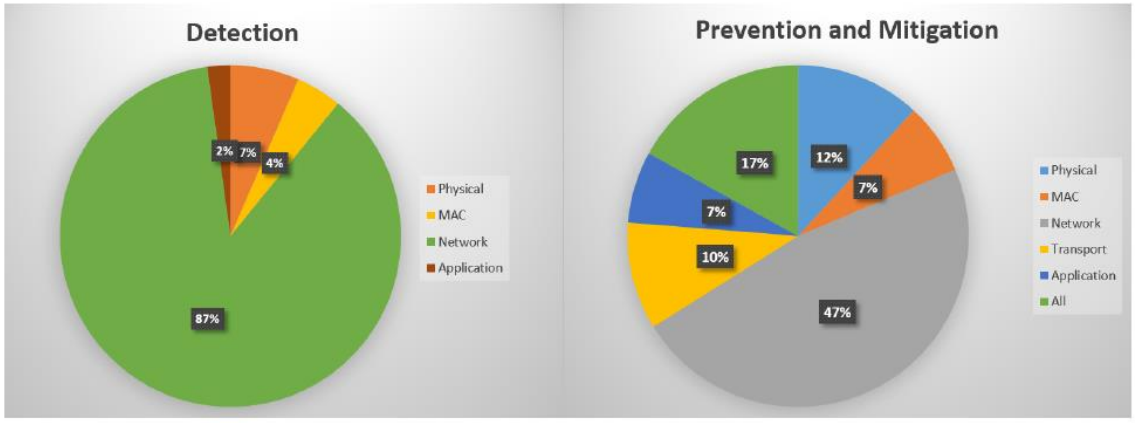

Figure 2. OSI representation for distribution of cyber security solutions [11]

Many kinds of research have been made to secure data generated by IoT or applications and transmitted, some of this research assumes that data must be manipulated as block ciphers, other papers proposed stream cipher to secure such transmitted data when applications designed to be fast in transmitting generated data[21-24]. The rest of this paper will briefly describe the recent papers up to 10 years; the description contains the major techniques adopted in such paper, significant results and in some cases the limitations if it is available in the original papers. The investigated researches are classified into two main categories: Block Cipher and Stream Cipher. Only two papers are listed under general authentication process.

2. Stream Cipher approaches

Lightweight encryption has been extensively researched by researchers to make significant improvements to balance computational cost reduction against security. Objectives are focused on either lowering the calculation time with keeping the security level or increase the security level with same level of calculation cost. Stream cipher takes significant impact in increasing speed of encryption calculation compare to block cipher. It is preferable to be utilized were enormous data transferred using resource constraint devices[25].

Frederik and Vasily in [26] divided internal states into a number of classes equal to 2κ where k represents key number of bits. The key stream generator is adapted to be updated depending on internal state.

According to [27], the major aim was to fill up the gap between block cipher and stream cipher algorithm by suggest a new stream cipher form with constant and small noise size. This approach achieved by applies a Boolean (filter) function to perform public bit permutation on a fixed key register.

In[28], a new technique presented involves an internal and external state consisting of a 43-bit LFSR, a 37-bit NFSR (total 80 bits), and a 7-bit counter respectively. The proposed approach alleged to be resistance to a classical time-memory-data tradeoff (TMDTO) attack. The proposed algorithm's strength is the reusable key by different applications in fixed size memory. While limitation mentioned by authors, if the key is lower than 17 bits, it is not resistance enough to brute force attack.

Concerning [29], only one round iteration is to produce a round function with no diffusion operation to minimize the computational calculations, leading to lower the latency and resource requirements. Also, the present scheme can implement the encryption process in parallel, while the decryption process can be done partially- parallelized.

A chaotic system in addition to Two Nonlinear Feedback Shift Registers (NFSRs) in order to generate a new stream cipher approach have been used in [30, 31], the new scheme aims to efficiently encrypt/decrypt data. The suggested method combines two systems, first is chaotic system and the second is “Nonlinear Feedback Shift Register (NFSR)” which produce a chaos based lightweight stream cipher system. Field Programmable Gate Array (FPGA) technology is utilized to quantify and integrate the chaotic system with the two NFSRs. Nist tools are used to the cipher algorithm which shows an excellent cryptographic characteristic. The results have been tested utilizing NIST SP 800-22 test tools; results showed that all fifteen tests are passed.

[32] Considered a selectively encrypt some bit streams in the middle of the coding system with a lightweight encryption manner such that the output data files are protected. The experiment results showed that the ratio (R) as 8% maxim (if more, the security level starts to be not obvious anymore) and recovery or guessing based on the cipher text is then “impossible” applied. Notice that ratio R represents the percentage of selected bits to be encrypted. Table (1) and Table (2) represent the difference between plain text and cipher text for different plaintext and keys.

Table 1. Difference ratio between Plaintext and Cipher Text with 1-b Different Plaintext [32]

Plain text sensitivity test for four kinds of data formats				
	Min	**Max**	**Mean**	**Std**
Image	49.61%	50.10%	49.73%	0.0014
Mp4 video	49.55%	50.23%	49.69%	0.0030
ASCII text	49.67%	50.41%	49.83%	0.0025
GPS log	49.22%	50.36%	49.76%	0.0041

Table 2. Difference ratio between Plaintext and Cipher Text with 1-b Different Keys [32]

Key sensitivity test for four kinds of data formats				
	Min	**Max**	**Mean**	**Std**
Image	49.11%	50.46%	49.73%	0.0024
Mp4 video	49.41%	50.53%	49.89%	0.0039
ASCII text	49.27%	50.90%	49.81%	0.0093
GPS log	49.24%	50.23%	49.39%	0.0031

Hassan *eat al* stated in [33] state a lightweight stream cipher scheme (LSC) to increase security level. The research adopts a dynamic key to achieve encryption. The proposed system involves a few numbers of simple operations to

reduce computation costs. As it was dynamic, its primitives will change in a lightweight manner with every input data block. Results showed that the proposed system is capable of attaining effectiveness and keeping its robustness well. The system uses 128-, 192-, and 256-bit keys. Algorithm in this research combined three major parts, "CR4, Pseudo-random number generator (PRNG), and Linear feedback shift register (LFSR) with 12 to 14 rounds". Figure (3) shows the diagram of the proposed dynamic key.

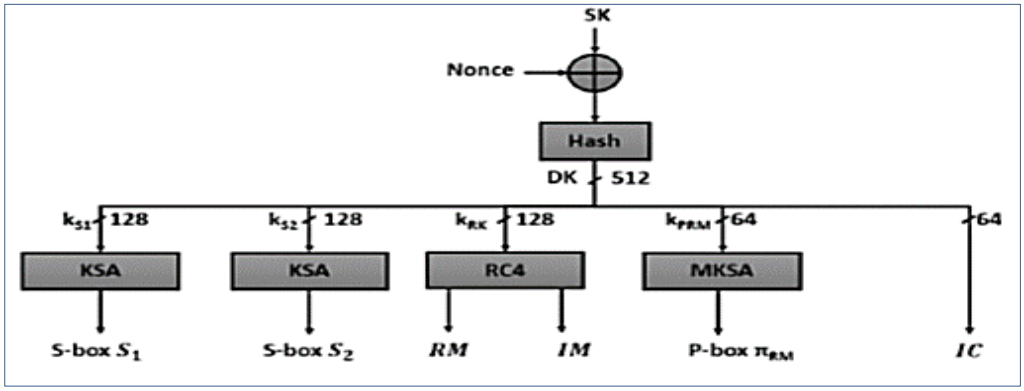

Figure 3. Proposed dynamic key derivation function and construction cipher primitives [33]

The research [34] takes in its consideration the importance of lowering computational cost but with increasing resistance to new rising cryptographic attacks. The proposed technique is "one Linear Feedback Shift Register and One Feedback with Carry Shift Register". A4 firmly ensures security to a great extent and is also easy to implement in various applications where secure communication between two parties is a priority. Each seed value is used in the "LFSR" is represented in 128 bits long; they are produced by a pseudo-random box of 256 values. To increase security, more LSFR implement required but this will increase complicity of implementation.

As asserted by [2], it is claimed to be succeeded to reducing the volume of data transmission between a server and an IoT device, focusing on the bandwidth, transmission security, and system resources of the IoT device. The reduction is achieved by data compression and replacing the SSL/TLS cryptographic protocol (but kept for device management when need only) with lightweight cryptography based on the Vernam cipher principle. This cipher uses the one-time pad method; the original message is encrypted with XOR and a key. For encryption to be secure, the key must meet some necessary conditions. Using a nonstandard compression result in reduce size to 20% of their original size. Eliminating the SSL/TSL protocol from the data transfer process led to reducing the total amount of data transferred to less than 10% of the original value. The main part of the savings is data related to building an encrypted. The presented solution focuses on the transmission of short messages, which in the original JSON form, have a size of 100 bytes (up to 500 characters). The presented solution is limited to the transmission of short messages, which, in the original JSON form, have a size of 100 bytes (up to 500 characters).

[35] Suggested two function, first is the round and the second is to update encryption primitive, the results are promising enhancement, it reaches three times compared to Advanced Encryption Standard (AES) when applied on Raspberry Pi (RPI4).

3. Block Cipher approaches

Symmetric key based authentication with integrated key management proposed by [36, 37]. AES 128 CBC (Cipher Block Chaining) mode uses with exchanged symmetric key. This method is payload embedded, thus minimizing the handshaking overhead negotiation and challenge-response processes proposed (3 handshake way). Latency overhead achieved up to exceed 5% when packet loss is (0-20) % is produced as results; also, it is found that the message size increment in secure CoAP is less than 2%. Figure (4) shows the security threat and the proposed engineering to process such a threat.

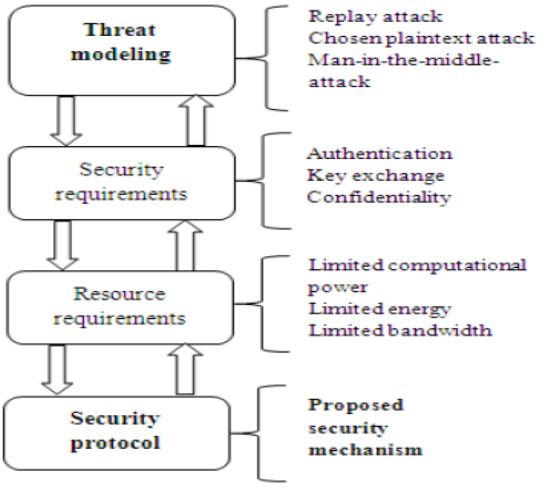

Figure 4. Security threat model and security engineering [36]

According to[38], an explanation for the idea of lightweight ABE scheme based on elliptic curve cryptography was made. This paper showed a given an elliptic curve cryptography (ECC) scheme defined by a set of secure parameters called (q, a, b, G, p). For the attributes set ω, the secret key is constructed by secret sharing based on Lagrange interpolation. As a result, for this method, When the size of the encryption attributes set (k) < =10, the proposed scheme has a prominent advantage in lightweight over the existing CP-ABE schemes. Another result was when k > 10, only the cipher-text size in the scheme is longer than that of the scheme with constant size cipher-text. It is assumed that the rest metrics are much lower compared others. It worth to mention that proposed system is suffering from flexibility poorness in revoking attributes, Scalability and Generality. The researchers addressed some limitations corresponding to the proposed system; the weaknesses can be addressed as weak Flexibility Repealing Attribute, poor in generality and scalability.

Partitions the responsibility of secure communication represent the core of [39]. Secure session performed at the application layer and transfer full of application layer over a secure channel. An advantage for suggested project is consistent performance even in lousy condition and performs full session establish in just two steps compared to six steps in standard DTLS. Implementing Less as CoAP handshake is demonstrated clearly in figure (5).

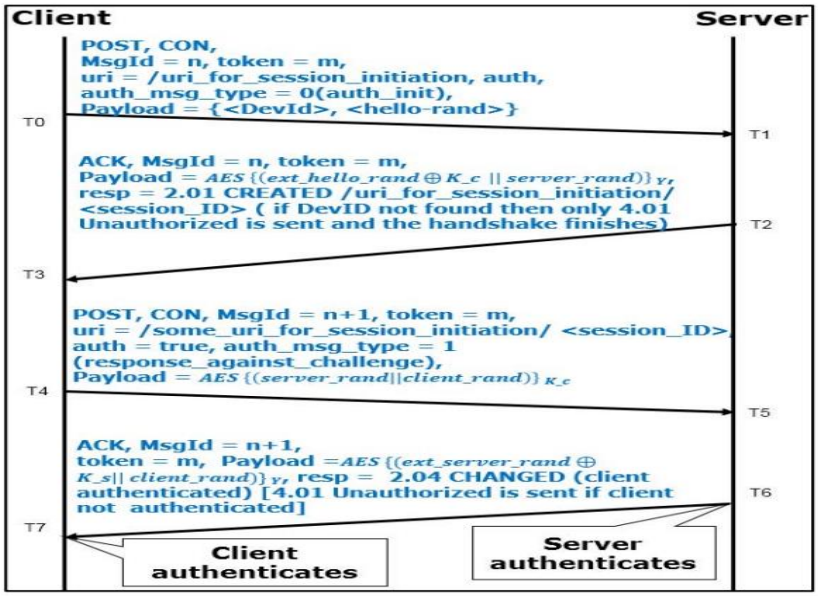

Figure 5. Implementing LESS as CoAP handshakes using the confirmable (CON) message type [39].

A "Hybrid Lightweight Algorithm" (HLA) demonstrated in details in [40], a combination of lightweight symmetry/asymmetry based on levels of hierarchy is presented. It is considered an improved version of conventional algorithms as they reduce the code length, number of rounds, key size, and block size. This research focused on low-constrained devices to implement suggested algorithm.

Secure and lightweight for cloud healthcare environments based on the internet of things argued in [41]. The proposed system applied mutual authentication mechanism, maintaining integrity while transmitting data and protecting against replay attack. The authentication must be established between node sensor and cloud service before beginning transmitting-receiving. The elliptic group is utilized to prove the integrity of transmitted data between the body sensor and the body sensor network administrator.

As observed in [42], the research aimed to design cipher approach that differ from AES in its structure to optimize delay time when working with constraint devices, the research uses dynamic key rather than static key such as AES uses. The relation between the dynamic keys is made independent to strength the algorithm and resist being invertible. The suggested system can deal with any type of data messages, for instance text data, video, audio or image. Figure (6) demonstrates the throughput ratio between the suggested cipher variants and AES-CTR.

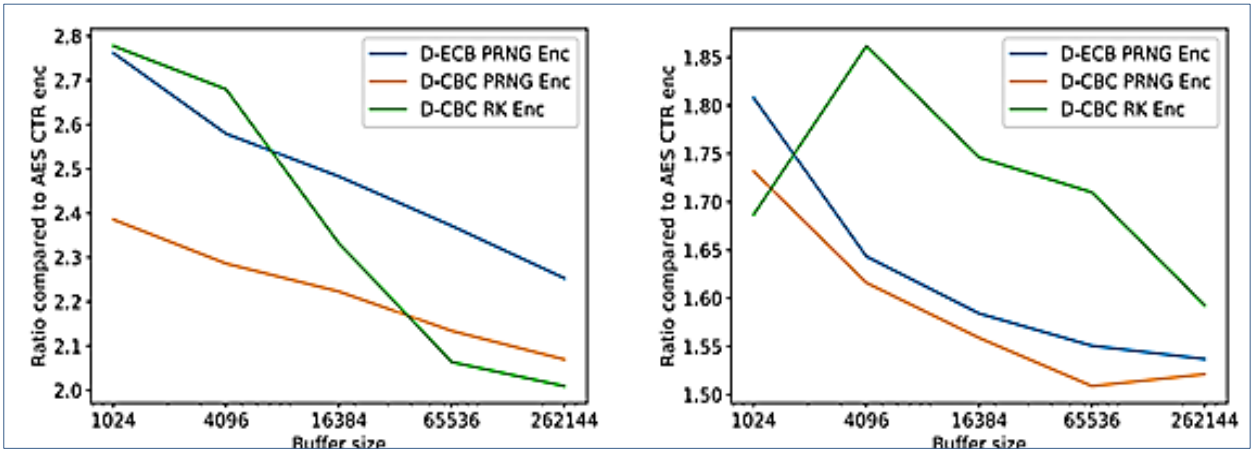

Figure 6: Pain of adopted approach with comparison to AES, N=246 (a) Raspberry Pi0 & (b) raspberry Pi3 [42]

An efficient fix to the key policy attribute-based encryption {KP-ABE) vulnerability proposed in [43]. Also the suggested algorithm claimed to extend KP-ABE into a hierarchical KP-ABE (H-KP-ABE) scheme. In this research, an extra pseudorandom number generator is added by replacing the function index with a new function index that generates sequence numbers based on a random salt of k bits. The proposed scheme solved the generality problem that original scheme limited to.

The right choosing of plain-ciphered block and the numbers of rounds that configure the system was the main focus by [44], these two parameters are principal keys that manage the flexibility of trading off between performance Vs security level. Technically the research focus on three steps, firstly each end (sender & receiver generate a number which will be used later as key. Number of permutation round must be made secondly. Finally, the algorithm rotates randomly the information obtained from previous round. Figure (7) demonstrate the classification of lightweight encryption as suggested by [44].

Results showing significant increase as plain data block gets bigger reaching up to 10 MS for 25000kB of plain data block.

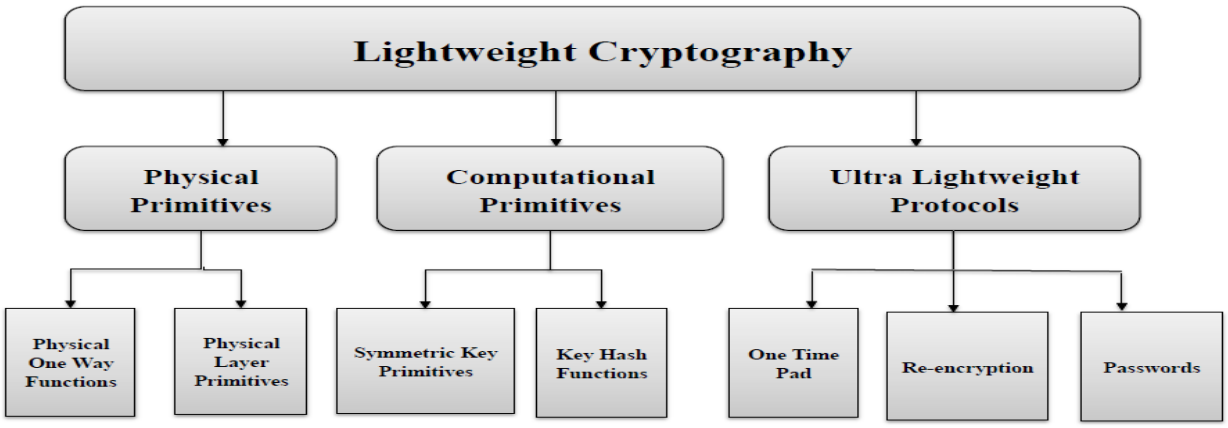

Figure 7: Lightweight Cryptography classes [44]

Flexible design for lightweight cryptographic approach introduced by [4]. The algorithm depends on selecting encryption parameters automatically in order to control the complexity of the encryption process. Additionally, a new key management and authentication approach makes communication more secure when exchanging keys and data over various nodes. Cooja simulator with Contiki OS utilized to evaluate the proposed scheme. The results showed a significant improvement regarding delay time, encryption times, and power consumption compared to other different cryptosystems of fixed encryption parameters. The results showed a linear relation between calculation time (encryption time) regarding to the increase in data block size and a number of rounds, as stated in figure (8). It is worth to mention that the results obtained by Cooja simulator without approved by real devices.

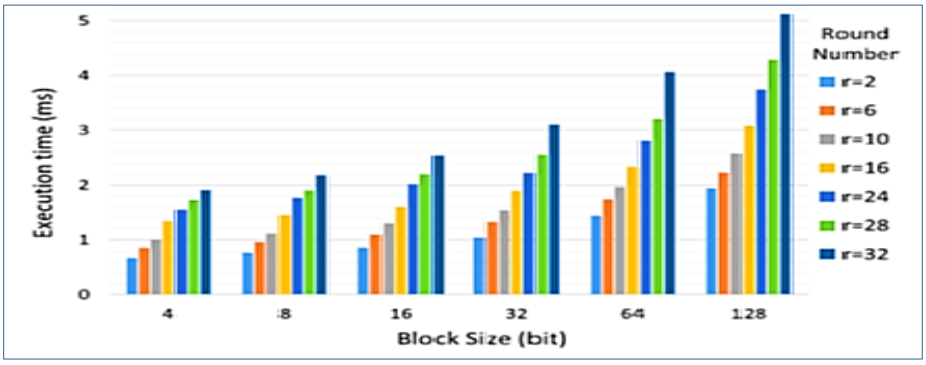

Figure 8. Relation between the encryption time, data block size, and number of rounds [4].

Mohammed et al [45], introduced algorithm is a symmetric key block cipher inspired by a combination of feistily and SP architectural methods to improve the complexity of the encryption. It is a 16 bytes (128-bit) block cipher/ key size for encrypt the data. Encryption algorithms are usually configured to take 10 to 20 rounds on average to keep the encryption process strong[26]. The solution achieved High security strength highly flexible. Lowers computational complexity and decreases the power of processing AES, HIGHT, DES, on the other hand, consists (“12, 32, 32, and 20”) rounds of encryption respectively. While mathematical operations number per round and S boxes used in NLCA is higher, the whole complexity is smaller. The NLCA algorithm offers data size consistency compared to most other schemes such "AES" and "RC6″ where block length is fixed. The data processing time also faster than other algorithms with secure key generation. It introduces mixed operations in multiple algebraic classes, including XOR and Addition operations, to generate difficulty for attackers.

The solution is limited to only five rounds to maximize energy efficiency results, as each round requires crypto mathematical operations involving 4 bits of data to work, which is considered a limitation to such a solution. Table (3) & table (4) demonstrates example of the encryption/decryption process using four rounds. For more information, see [45].

Table 3. NLCA adopting four rounds of encryption [45]

State	Value P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
Original	0A	0B	0C	0D	0F	01	02	03	04	05	06	07	08	09	1A	2B
key	01	02	04	05	06	AA	BB	CC	44	DD	EE	88	09	04	05	06
Key cipher	4F	29	4C	71	D3	AB	29	D0	AB	79	AC	69	A2	73	AC	7B
Round 1	BA	DD	BF	83	AF	5B	FA	9A	2B	59	27	2P	P8	DF	A9	A5
Round 2	C3	0F	2C	B1	41	5P	2E	1D	F8	A1	E9	F0	01	0D	FA	04
Round 3	D7	89	7F	27	39	A9	1C	1D	A0	EB	00	D4	15	8B	A2	92
Round 4	64	25	AF	99	81	32	9A	53	A6	0D	A2	84	FD	67	53	50
Encrypted	64	25	AF	99	81	32	9A	53	A6	0D	A2	84	FD	67	53	50

Table 4. NLCA adopting four rounds of encryption [45]

State	Value P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
Key cipher	4F	29	4C	71	D3	AB	29	D0	AB	79	AC	69	A2	73	AC	7B
Encrypted	64	25	AF	99	81	32	9A	53	A6	0D	A2	84	FD	67	53	50
Round 4	64	25	AF	99	81	32	9A	53	A6	0D	A2	84	FD	67	53	50
Round 3	D7	89	7F	27	39	A9	1C	1D	A0	EB	00	D4	15	8B	A2	92
Round 2	C3	0F	2C	B1	41	5P	2E	1D	F8	A1	E9	F0	01	0D	FA	04
Round 1	BA	DD	BF	83	AF	5B	FA	9A	2B	59	27	2P	P8	DF	A9	A5
Original	0A	0B	0C	0D	0F	01	02	03	04	05	06	07	08	09	1A	2B

Mohammad et al worked on a light encryption algorithm to secure medical images using two permutations as stated by [5]. The encryption technique uses three stages to encrypt the image considering 256 bits key value for logical operation. The selected image size was 256 bits, transformed to 4-sub-binary image each of 16 sub-blocks (16 bits for each sub). Then 256 chosen key is applied to encrypt the image.

According to [46] a pliable lightweight cryptosystem system using simple/strong transposition/substitution process to low processing capabilities associated with IoT especially devices memory to encrypt and decrypt data. The flexibility in present system derived from utilizing a variable block size when implemented on various IoT devices. Additionally, the DeoxyriboNucleic Acid (DNA) sequence is adopted to produce random keys that used to encrypt data. The observed results of suggested system showed promising results for devices with low memory, reaching over 50% compared to other lightweight encryption systems. Figure (9) clarify the graphical chart view for the relationship between the data size and proposed encryption versus AES calculation as time listed in table (5).

Table 5: the encryption time of the proposed and AES cryptographic systems [46]

Data	Data Size (byte)	Encryption time (msec)	
		Proposed	AES
Data 1	49152	139	750
Data 2	709200	531	1910
Data 3	889200	911	1323
Data 4	950878	1030	1890

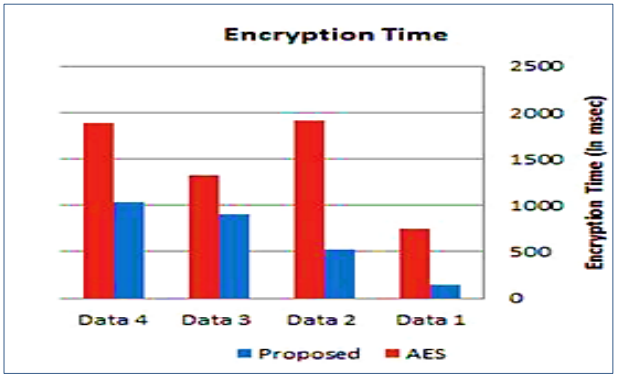

Figure 9. The graphical chart of encryption time value in table (5) [46].

A new method of adopting a block cipher algorithm to encrypt and employ defined trust ends to light generate authenticating-verification factor claimed by [1]. This research aimed to address distributing lightweight encryption, speed of authentication and authorization, and dynamic sleep period based on battery energy level. This paper utilized "Cipher Block Chaining-Message Authentication Code (CCM)" and saving power relying on achieved sleep mode which is proportional to the remaining power in the power supply.

4. Lightweight encryption-based authentication

Authentication is one of the vital step in the identification process,[47], it is the procces that prove "who is the user"? and "is the user really who he/she represents himself/herself?". Authentication concept is widely adopted by many commercial applications such as social media account rather than registration with online services. Wang *et al* in [48] stated that the main three authentication system is 1- password base, 2- biometric base and 3- distributed system base. All of these types are prone to attacks. For more information, see [48]

Yao et al [49] suggested a multicast authentication scheme based on the improved and the original Nyberg's fast one-way accumulator the improved one is used to embed both the secret information (i.e., the shared keys) and multicast data into the accumulated value, and the accumulated value MACs can be served as the signature of the multicast. The major results can be briefed as the receiver authenticates the multicast data immediately, and the authentication scheme doesn't depend on time factor (data can be sent at any time). Also lowers computation overhead and verify Robustness resists node compromising ability to tolerate packet loss. Table (6) shows the proportional relationship between the length of signature r and the increment of the accumulated, indicating a weakens as the proposed method is not fit for the multicast to large number of receivers compared to suitability to be used for small scale applications.

Table 6: The relations among N, minimum q, r and pf [49]

d	N	Minimum q(bits)	Minimum r(bytes)	P_F
2	4	40	26	3.29467E-06
3	8	80	40	1.00566E-05
4	16	160	72	2.1099E-05
5	32	320	132	3.04606E-05

Researchers in [50] succeeded in building upon the Hypertext key-value store by modifying the existing components to provide transactional guarantees. Warp consists of three components: the coordinator, clients, and storage servers. The coordinator maintains the meta-state for the system, specifically, the partitioning of the key space across storage servers. It showed reducing the number of transactions to the minimum necessary to enforce serializability; Acyclic transactions achieve scalability by arranging servers into data dependent and dynamically determined chains and allowing multiple overlap transactions to proceed in multiple overlapping transactions. Additionally, experiments showed that Warp achieves 4 × higher throughputs than Senoia's mini-transactions on the standard TPC-C benchmark with no aborts. Also, the system reaches 75% of the throughput of the non-transactional key-value store it builds upon. Figure (10) presents the overall transactional throughput for Warp; MiniDex, and HyperDex.

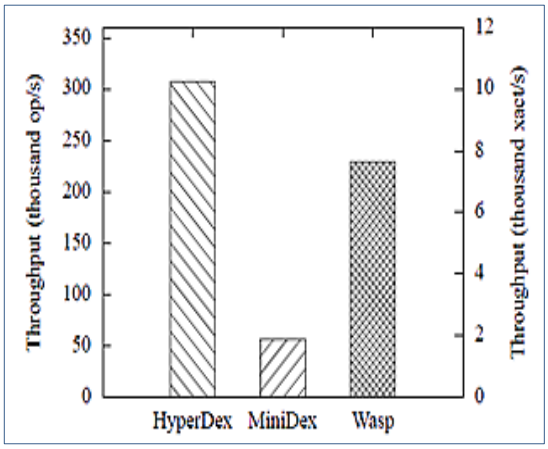

Figure 10. HyperDex, MiniDex, and Warp overall transactional throughput [50]

Tables (7, 8 and 9), give high abstract for each investigated research in the current paper to help other researchers benefit from the technique adopted by each reference

Table 7. Stream cipher-based techniques for investigated research

Stream Cipher Category	Reference Number	Technique
Stream Cipher	[26]	Internal states are partitioned into 2^k equalized classes where k refers to the number of bits assigned to that key.
Stream Cipher	[27]	Suggest applies a Boolean (filter) function to perform public bit permutation on a fixed key register.
Stream Cipher	[28]	Presented an internal and external state consisting of a 43-bit LFSR and a 37-bit NFSR (total 80 bits) and a 7-bit counter respectively.
Stream cipher	[29]	proposed only one round iteration to produce round function with no diffusion operation
Stream Cipher	[30]	Utilized a chaotic system in addition to two Nonlinear Feedback Shift Registers (NFSRs). Nist tools are used to shows a good cryptographic characteristic.
Stream Cipher	[32]	Suggested a lightweight encryption method to encrypt some selected bit stream which lay in the middle of the coding system to produce protected output data.
Stream Cipher	[33]	The proposed system involves a few numbers of simple dynamic operations. The system uses 128-, 192-, and 256-bit keys.
Stream Cipher	[34]	The proposed technique is “one Linear Feedback Shift Register and One Feedback with Carry Shift Register”. Each

		seed value long is 128 bits; they produced by pseudo-random box of 256 values.
Stream Cipher	[2]	Compressing data and substitute cryptographic algorithm used by SSL/TLS by another lightweight cryptography algorithm depending on the Vernam cipher.
Stream Cipher	[35]	Utilizing two functions, one for round and the other function for updating the cryptosystem primitives

Table 8. Block cipher-based techniques for investigated researches

Block Cipher Category	Reference Number	Technique
Block Cipher	[36]	symmetric key is used with AES 128 CBC (Cipher Block Chaining) mode
Authentication	[38]	Proposed Elliptic curve cryptography (ECC).
Block cipher		The security level based on the Elliptic Curve Decisional Diffie–Hellman (ECDDH) assumption rather than bilinear Diffie–Hellman.
Block Cipher	[39]	The secure communication responsibility is partitioned and performed at the application layer and the transport-layer.
Asymmetric authentication	[41]	Suggested a system consist of four parities, body sensor; personal reader; medical reader and medical cloud server.
Block cipher		The elliptic group utilized to proof the integrity of transmitted data between body sensor and body sensor network administrator.
Block cipher	[42]	The research uses dynamic key rather than static key such as AES uses. The relation between the dynamic keys is made to be independent and resist being
Dynamic Key		invertible.
Block Cipher based	[43]	An extra pseudorandom number generator is added by replacing the function index with a new function index that generates sequence numbers based on a
authentication		random salt of k bits.
Block Cipher	[44]	The research focus on three steps: Generates a number which will be used later as key. Number of permutation round must be made secondly. Rotates randomly the information obtained from previous round
Symmetric based		
Authentication		
Block Cipher	[4]	Selecting encryption parameters automatically. A new key management and authentication approach created make communication more securely when exchange keys and data over various nodes. Cooja simulator with Contiki OS utilized to evaluate the proposed scheme.
Block Cipher	[45]	Uses symmetric key block cipher inspired by a combination of Feistily and SP architectural methods It is a 16 bytes (128-bit) block cipher/ key size for encrypt the data.
Block Cipher	[5]	The encryption technique uses Three stages used to encrypt the medical image. A key of 256 bits implemented for logical operation. Image block size was 256 bits quantized into 4-sub-binary image, each sub of 16 bits

		Finally, a new key 256 bit long is applied to encrypt the image data.
Block Cipher	[46]	The Deoxyribonucleic Acid (DNA) sequence is adopted to produce random keys that are used to encrypt data.
Block Cipher based authentication	[1]	Utilized "Cipher Block Chaining-Message Authentication Code (CCM)" and saving power relying on achieved sleep mode which proportional to remaining power in the power supply.

Table 9. Authentication-based techniques for investigated research

Authentication Category	Reference Number	Technique
Dynamic, authentication	[49]	Adopted absorbency property utilized by original Nyberg's fast one-way accumulator
Multi key	[50]	Guarantee transactions by modifying HyperDex key-value store existing components.

5. Conclusion

Extensive research has been done in the field of lightweight ciphers, focusing on two main categories: Block ciphers and stream ciphers. The goal of both categories is to minimize computation time while improving the robustness of key generation algorithms. While many works acknowledged the limitations of the lightweight cipher techniques used, others did not look for the limitations of lightweight cipher techniques, and others did not address this aspect. Tables (7, 8 and 9) provide a brief summary of the abstract of each research paper highlighting the technique used. Most of the work focused on specific applications. However, none of the papers reviewed explicitly stated whether or not they addressed raw data at the bit level, as the encryption process considered time consuming, it would be beneficial to address how to reduce time consumption for preprocessing time depending on the way the suggested algorithm read and manipulate plain text before implementing encryption process. The main finding from the papers reviewed is that none of them provided a clear explanation of the method used to read the original data before performing computations. This means that there is no definitive and efficient approach to loading and processing the data. This observation can serve as a starting point to address the critical problem of reducing overall processing time, especially in the context of lightweight encryption.

6. References

[1] P. Sudhakaran, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," *International Journal of Communication Systems*, vol. 35, no. 2, p. e4198, 2022.

[2] I. Sokol, P. Hubinský, and Ľ. Chovanec, "Lightweight cryptography for the encryption of data communication of iot devices," *Electronics*, vol. 10, no. 21, p. 2567, 2021.

[3] A. Nasif, Z. A. Othman, and N. S. Sani, "The Deep Learning Solutions on Lossless Compression Methods for Alleviating Data Load on IoT Nodes in Smart Cities," *Sensors (Basel)*, vol. 21, no. 12, Jun 20 2021, doi: 10.3390/s21124223.

[4] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 115, p. 102448, 2021.

[5] M. K. Hasan *et al.*, "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731-47742, 2021.

[6] R. Sowmya and K. Suneetha, "Data mining with big data," in *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, 2017: IEEE, pp. 246-250.

[7] A. Ramola, A. K. Shakya, and D. Van Pham, "Study of statistical methods for texture analysis and their modern evolutions," *Engineering Reports*, vol. 2, no. 4, 2020, doi: 10.1002/eng2.12149.

[8] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," *Digital Communications and Networks*, vol. 9, no. 1, pp. 101-110, 2023.

[9] V. D. Soni, "IOT connected with e-learning," *International Journal on Integrated Education*, vol. 2, no. 5, pp. 273-277, 2019.

[10] S. M. Hadi, A. H. Alsaeedi, R. R. Nuiaa, S. Manickam, and A. S. D. Alfoudi, "Dynamic Evolving Cauchy Possibilistic Clustering Based on the Self-Similarity Principle (DECS) for Enhancing Intrusion Detection System," *International Journal of Intelligent Engineering & Systems*, vol. 15, no. 5, 2022.

[11] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616-644, 2019.

[12] W. Gao, L. Hu, and P. Zhang, "Feature redundancy term variation for mutual information-based feature selection," *Applied Intelligence*, vol. 50, pp. 1272-1288, 2020.

[13] S. M. Hadi *et al.*, "Trigonometric words ranking model for spam message classification," *IET Networks*, 2022, doi: 10.1049/ntw2.12063.

[14] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," National Institute of Standards and Technology, 2016.

[15] A. H. Alsaeedi *et al.*, "Hybrid Extend Particle Swarm Optimization (EPSO) model for Enhancing the performance of MANET Routing Protocols," *Journal of Al-Qadisiyah for computer science and mathematics*, vol. 15, no. 1, pp. Page 127-136, 2023.

[16] Y. Dai, Z. Hu, S. Zhang, and L. Liu, "A survey of detection-based video multi-object tracking," *Displays*, vol. 75, 2022, doi: 10.1016/j.displa.2022.102317.

[17] A. Cheema *et al.*, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review," *Security and Communication Networks*, vol. 2022, pp. 1-15, 2022, doi: 10.1155/2022/8379532.

[18] Z. Bao, C. Guo, J. Guo, and L. Song, "TNT: how to tweak a block cipher," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2020: Springer, pp. 641-673.

[19] O. Kuznetsov, O. Potii, A. Perepelitsyn, D. Ivanenko, and N. Poluyanenko, "Lightweight stream ciphers for green IT engineering," *Green IT Engineering: Social, Business and Industrial Applications*, pp. 113-137, 2019.

[20] R. Rahim and A. Ikhwan, "Cryptography technique with modular multiplication block cipher and playfair cipher," *Int. J. Sci. Res. Sci. Technol*, vol. 2, no. 6, pp. 71-78, 2016.

[21] A. Bassel, A. B. Abdulkareem, Z. A. A. Alyasseri, N. S. Sani, and H. J. Mohammed, "Automatic Malignant and Benign Skin Cancer Classification Using a Hybrid Deep Learning Approach," *Diagnostics (Basel)*, vol. 12, no. 10, Oct 12 2022, doi: 10.3390/diagnostics12102472.

[22] A. S. Alfoudi *et al.*, "Hyper clustering model for dynamic network intrusion detection," *IET Communications*, 2022.

[23] S. M. Ali, A. H. Alsaeedi, D. Al-Shammary, H. H. Alsaeedi, and H. W. Abid, "Efficient intelligent system for diagnosis pneumonia (SARSCOVID19) in X-ray images empowered with initial clustering," *Indones. J. Electr. Eng. Comput. Sci*, vol. 22, no. 1, pp. 241-251, 2021.

[24] E. Refaee *et al.*, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-12, 2022, doi: 10.1155/2022/5665408.

[25] L. Jiao, Y. Hao, and D. Feng, "Stream cipher designs: a review," *Science China Information Sciences*, vol. 63, pp. 1-25, 2020.

[26] F. Armknecht and V. Mikhalev, "On lightweight stream ciphers with shorter internal states," in *Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers 22*, 2015: Springer, pp. 451-470.

[27] P. Méaux, A. Journault, F.-X. Standaert, and C. Carlet, "Towards stream ciphers for efficient FHE with low-noise ciphertexts," in *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I 35*, 2016: Springer, pp. 311-343.

[28] V. Amin Ghafari and H. Hu, "Fruit-80: a secure ultra-lightweight stream cipher for constrained environments," *Entropy*, vol. 20, no. 3, p. 180, 2018.

[29] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, "One round cipher algorithm for multimedia IoT devices," *Multimedia tools and applications*, vol. 77, pp. 18383-18413, 2018.

[30] L. Ding, C. Liu, Y. Zhang, and Q. Ding, "A new lightweight stream cipher based on chaos," *Symmetry*, vol. 11, no. 7, p. 853, 2019.

[31] A. F. Mohamed Nafuri, N. S. Sani, N. F. A. Zainudin, A. H. A. Rahman, and M. Aliff, "Clustering Analysis for Classifying Student Academic Performance in Higher Education," *Applied Sciences*, vol. 12, no. 19, 2022, doi: 10.3390/app12199467.

[32] H. Qiu, M. Qiu, M. Liu, and Z. Ming, "Lightweight selective encryption for social data protection based on EBCOT coding," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, pp. 205-214, 2019.

[33] H. Noura, R. Couturier, C. Pham, and A. Chehab, "Lightweight stream cipher scheme for resource-constrained IoT devices," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2019: IEEE, pp. 1-8.

[34] N. A. Mohandas, A. Swathi, R. Abhijith, A. Nazar, and G. Sharath, "A4: A lightweight stream cipher," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020: IEEE, pp. 573-577.

[35] H. Noura, O. Salman, R. Couturier, and A. Chehab, "Lesca: Lightweight stream cipher algorithm for emerging systems," *Ad Hoc Networks*, vol. 138, p. 102999, 2023.

[36] A. Ukil, S. Bandyopadhyay, A. Bhattacharyya, and A. Pal, "Lightweight security scheme for vehicle tracking system using CoAP," in *Proceedings of the International Workshop on Adaptive Security*, 2013, pp. 1-8.

[37] R. R. Nuiaa, S. Manickam, and A. S. D. Alfoudi, "Dynamic Evolving Cauchy Possibilistic Clustering Based on the Self-Similarity Principle (DECS) for Enhancing Intrusion Detection System," 2022.

[38] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Generation Computer Systems*, vol. 49, pp. 104-112, 2015.

[39] A. Bhattacharyya, T. Bose, S. Bandyopadhyay, A. Ukil, and A. Pal, "LESS: Lightweight establishment of secure session: A cross-layer approach using CoAP and DTLS-PSK channel encryption," in *2015 IEEE 29th international conference on advanced information networking and applications workshops*, 2015: IEEE, pp. 682-687.

[40] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-18, 2017.

[41] Y.-Y. Deng, C.-L. Chen, W.-J. Tsaur, Y.-W. Tang, and J.-H. Chen, "Internet of Things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system," *Sensors*, vol. 17, no. 12, p. 2919, 2017.

[42] H. N. Noura, A. Chehab, and R. Couturier, "Efficient & secure cipher scheme with dynamic key-dependent mode of operation," *Signal processing: Image communication*, vol. 78, pp. 448-464, 2019.

[43] S.-Y. Tan, K.-W. Yeow, and S. O. Hwang, "Enhancement of a lightweight attribute-based encryption scheme for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6384-6395, 2019.

[44] S. Medileh *et al.*, "A flexible encryption technique for the internet of things environment," *Ad Hoc Networks*, vol. 106, p. 102240, 2020.

[45] F. Thabit, S. Alhomdy, A. H. Al-Ahdal, and S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91-99, 2021.

[46] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, "Lightweight cryptography system for IoT devices using DNA," *Computers and Electrical Engineering*, vol. 95, p. 107418, 2021.

[47] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A review on authentication methods," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 5, pp. 95-107, 2013.

[48] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *Journal of Network and Computer Applications*, vol. 188, p. 103080, 2021.
[49] X. Yao, X. Zhou, and X. Du, "A lightweight dynamic multicast authentication scheme," in *9th International Conference on Communications and Networking in China*, 2014: IEEE, pp. 595-600.
[50] R. Escriva, B. Wong, and E. G. Sirer, "Warp: Lightweight multi-key transactions for key-value stores," *arXiv preprint arXiv:1509.07815*, 2015.