ZANCO Journal of Pure and Applied Sciences

TYPE Original article
DOI http://dx.doi.org/10.21271/ZJPAS.37.5.7

OPEN ACCESS

*Corresponding author
Jawaher Abdulwahab Fadhil
jawaher.fadhil@auas.edu.krd

RECEIVED :17 /12 /2024
ACCEPTED :13/05/ 2025
PUBLISHED :31/ 10/ 2025

KEYWORDS:
Cybersecurity,
Internet of Things,
Cryptographic algorithms,
Privacy challenges,
Enhancement strategies.

Advancing IoT Security: Cryptographic Enhancements and Open Challenges

Jawaher Abdulwahab Fadhil[1,2*], Marwan Aziz Mohammed [3,4]

[1] Department of Information Technology, Technical College of Informatics, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.
[2] Department of Information Technology, Technical College of Informatics- Akre, Akre University for Applied Sciences, Duhok, Kurdistan Region, Iraq.
[3]Software Engineering Department, College of Engineering, Salahaddin University-Erbil, Kurdistan Region – F.R. Iraq
[4]Department of Computer Engineering, College of Engineering, Knowledge University, Erbil 44001, Iraq

ABSTRACT

The tremendous increase of data produced by Internet of Things (IoT) networks emphasizes how important to have robust security mechanisms in place to guarantee authenticity, integrity, and confidentiality. Due to inherent limitations of IoT devices, like limited memory, computing power, and energy consumption, they are particularly vulnerable to security threats and attacks. This paper comprehensively surveys possible cryptographic solutions to enhance IoT cybersecurity, discusses cryptographic algorithm classification, implementation problems, and performance parameters in the IoT ecosystem. This study explores common cryptographic optimization techniques using meta-heuristic algorithms (MHA), machine learning (ML), and blockchain (BC). A taxonomy of emerging technology solutions was demonstrated based on IoT security issues. Additionally, the paper explores cryptographic improvement challenges in the IoT environment with possible solutions.

1.Introduction

The Internet of Things (IoT) is a network of various embedded devices connected by sensors and communication protocols that can gather, share, and analyze data in the real world. IoT devices support smooth communication among the devices and surrounding environments without human interactions. Recently, the exponential growth in IoT applications in different sectors (e.g., healthcare, transportation, smart cities, etc.) has brought numerous advantages and conveniences for users; despite these advantages, the IoT has also introduced several security and privacy vulnerabilities (Reshi and Sholla, 2022). For example, new cyberattacks occur daily, making detecting and preventing such attacks more complicated. In 2018, it was predicted that there would be over 25.4 billion active IoT devices by 2030; these devices and the increasing number of users are also expected to generate about 73.1 Zettabytes (one Zettabyte equals one trillion gigabytes) of data by 2025. Additionally, estimated 152,200 devices will connect to the internet every minute in the same year (Thabit et al., 2023). However, IoT devices have resource limitations (e.g., low computing power, limited battery life, limited memory, and limited power supply). As a result, there are better solutions than implementing individual traditional security algorithms for IoT devices; therefore, optimizing such algorithms is essential by emerging technologies such as machine learning, BC, and optimization algorithms to enhance cyber security in different areas.

Typically, the deployment of IoT applications needs to prioritize essential security requirements, including device, data, and network security, in IoT systems. Device security uses security measures to prevent sensitive information from illegal access and malicious attacks on IoT devices, while data security protects this information from manipulations (Chanal and Kakkasageri, 2020). The process of protecting and keeping an eye on communication channels to guarantee safe data transfer between connected devices, like cloud platforms and gateways, is known as “network security” (Azrour et al., 2021). The security of IoT systems depends on a set of requirements that cooperate to protect devices, data, and services. Authentication, authorization, data integrity, confidentiality, availability, and privacy are vital requirements to improve IoT security. Authentication verifies a device or user identity before granting access to protected resources, while authorization defines access privileges to resource usage and performs specified actions. Data integrity ensures that IoT data is accurate and unreadable throughout its lifecycle, defending against unauthorized manipulation. Confidentiality refers to the protection of the privacy and security of IoT data through encryption. Availability means that services and devices can be reliably used when needed; at the software level, it means that the service is available to anyone permitted to own it, while hardware availability means that existing devices are accessible and compatible with IoT applications. Finally, privacy refers to protecting individuals’ information within the IoT ecosystem. Data privacy is a critical security requirement in IoT systems due to the passive nature of most IoT devices.

Other sections of this paper are designed as follows: Section 2 presents several previous related studies and contributions to this research. The classification of cryptographic algorithms in IoT cybersecurity, problems in applying security algorithms, common IoT security threats, and performance parameters to evaluate security level are covered in Section 3. Section 4 explores an overview of recent studies regarding related topics. Various security enhancement techniques, such as meta-heuristics algorithms, machine learning, and BC technologies, are deeply discussed in section 5, followed by the open challenges with potential solutions conducted in section 6. Figure 1 shows the taxonomy of this research.

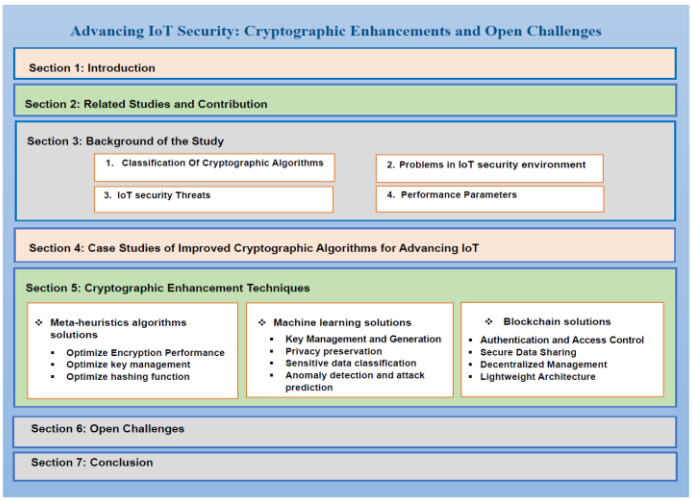

Figure 1: Paper organization and taxonomy

2. Related Studies and Contribution

Numerous papers have been presented on the security and privacy algorithm issues in IoT cybersecurity in recent years. In this section, we have briefly summarized the most relevant studies.

(Singh et al., 2024) reviewed the lightweight cryptographic algorithms for IoT devices and assessed the algorithm performance based on its structures and key size. The paper also addresses IoT security measures and identifies challenges such as data integrity, user privacy, and devices' physical vulnerabilities. In addition, an improved security scheme was proposed for smart homes, and open issues were discussed. The authors highlighted the importance of utilizing lightweight security solutions in IoT environments. However, they did not discuss advanced enhancement strategies such as MHA, ML, and BC techniques, nor their significance. (Williams et al., 2022) comprehensively surveyed common IoT security threats from three main primitives: hardware, software, and data in transit. The survey explored IoT security issues based on the four-layer IoT architecture with corresponding solutions. The authors analyzed encryption methods for low-power, limited-memory devices. Furthermore, the authors identified several implementation challenges and offered possible solutions. Even the authors demonstrated the importance of emerging ML and BC solutions to ensure IoT security through data protection and threat detection against increasing IoT threats to the landscape. However, this survey needs to cover the performance parameters to evaluate these techniques and the role of MHA in assessing these methods for optimizing limited resource device security. (Sadhu et al., 2022) reviewed existing research to provide IoT applications in different sectors (e.g., smart cities, Internet of Vehicles (IoV), Internet of Medical Things (IOMT), etc.), emphasizing the limited capabilities of hardware and software in IoT devices. The paper identified active and passive attacks with their security impacts in IoT ecosystems. The study also presented various security solutions along with the pros and cons of each solution, Including physical unclonable functions (PUF), traditional cryptographic techniques, and BC. However, the authors recommended AI methods, quantum systems, and 5G as future directions to enhance IoT data integrity. (Thakor et al., 2021) provided an overview of existing lightweight cryptography algorithms (LWC) that are suitable for resource-constrained devices (e.g., sensors, smart cards, RFID tags, etc.). LWC algorithms are categorized based on their internal structure and compared in terms of hardware and software performance measures. Additionally, the study described the critical LWC standardization process presented by institutions such as NIST (National Institute of Standards and Technology) and discussed significant research challenges, such as the need for efficient S-box design and lighter key methods. Nevertheless, the authors focused on ensuring IoT security with minimal resource consumption, but they ignored the strength of emerging technologies in IoT security enhancement. (Mousavi et al., 2021b) comprehensively reviewed state-of-the-art cryptographic algorithms in IoT security and identified the most critical threats and security factors faced by IoT systems. The study compared cryptographic algorithms statistically based on their performance and security fundamentals. Moreover, the authors focused on elliptic curve cryptography (ECC) performance, considering it the most reliable cryptographic algorithm with smaller and faster key generations compared with other security algorithms and acknowledging its limitations in certain scenarios. On the other hand, the authors did not provide the role of emerging technologies in the IoT security field. (Obaidat et al., 2020) comprehensively reviewed the IoT

application areas, resent security and privacy concerns of IoT devices with limited resources, discussed the IoT security architecture with attacks taxonomy concerning each layer (perception, network, and application), as well as the study emphasized mitigation strategies from reviewed papers and explained the role of cryptographic algorithms and BC as approaches for security and privacy solutions. Moreover, the open research areas are also discussed to give researchers the most current questions related to securing the IoT ecosystem. However, the authors identified the cryptography algorithm and BC as potential solutions for resource-constrained devices but did not mention other approaches, such as MHA and ML.

Although several works reviewed cryptographic methods and addressed security and privacy issues in IoT environments, as mentioned above, they presented restricted viewpoints on a particular aspect of IoT security enhancement. Therefore, there is a need for a more detailed survey on aspects not covered in most previous studies, such as the security enhancement techniques through IoT devices and performance parameters needed to satisfy resource-constrained devices with open challenges.

The contribution of this work is to categories cryptographic algorithms and exploring hardware security solutions from reviewed papers, examining the common cybersecurity threats in IoT networks and emphasizing restrictions on applying security algorithms in limited resource devices, analyzing the performance parameters required to evaluate the efficiency of hardware security solutions, and providing cryptographic algorithm enhancement techniques with solutions and open challenges.

Table 1 presents briefly the most relevant works and contributions to this study.

Table 1: Summary of related studies and contribution

Ref.	Cryptographic Algorithms							
	Classification	Problems in Applying	Threats	Performance parameters	Enhancement Techniques			Open Challenges
					MHA	ML	BC	
(Singh et al., 2024)	√	√	-	√	-	-	-	√
(Williams et al., 2022)	√	√	√	-	-	√	√	-
(Sadhu et al., 2022)	-	-	√	-	-	√	√	√
(Thakor et al., 2021)	√	-	-	√	-	-	-	√
(Mousavi et al., 2021b)	√	√	√	√	-	-	-	-
(Obaidat et al., 2020)	-	√	√	√	-	-	√	√
Our work	√	√	√	√	√	√	√	√

3. Background of the Study

3.1. Classification Of Cryptographic Algorithms

Cryptography is the art of encrypting data using algorithms to ensure safe communication during data transmission across a network (Mehta et al., 2020). Cryptographic algorithms are essential tools to achieve security goals, such as confidentiality, integrity, and authenticity of data, especially in limited-resource IoT devices (Zhou et al., 2019, Sarker et al., 2020). Security algorithms can be categorized by their functionality in network security. First, symmetric key encryption, one key is used in data encryption and decryption. Symmetric cryptographic algorithms are more suitable for IoT applications due to their simple implementation and lower resource requirements (Newroz, 2024), such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), Blowfish, etc. However, symmetric algorithms are highly vulnerable to key distribution issues and need other methods to improve data integrity (Kureshi and Mishra, 2022). Second, asymmetric key encryption uses two separate keys to protect data. The public key encrypts the data, while the private key is used for decryption (e.g., ECC and RSA (Rivest-Shamir-

Adleman)). Public-key cryptography algorithms provide high-security performance in various applications (Arya et al., 2023). However, these algorithms have more complex implementations and a higher computation load than symmetric key encryption due to more memory and energy consumption (Makarenko et al., 2020). Third, hash functions accept an input message and generate a fixed-length sequence of characters known as “digests”. Hash function algorithms are used to check data integrity and digital signatures. Common hash functions include SHA-256 (part of the SHA-2 family), which is preferred in the IOT systems due to strong security features (Bakhsh et al., 2023), and the MD5 algorithm, which is no longer preferred due to vulnerabilities (Velmurugadass et al., 2020). Fourth, Key exchange protocols allow parties to share cryptographic keys across an unprotected channel securely. Examples include the Diffie-Hellman and it is elliptic curve variant (ECDH). However, ECDH is generally considered more efficient in establishing secure communication among IoT devices due to its ability to achieve a high level of security with shorter key sizes (Ahmed and Barukab, 2022). Finally, Digital signature Algorithms (DSAs) utilize asymmetric cryptography to generate a unique digital signature that validates both the authenticity and integrity of a message (Ali and Hasan, 2023). The most popular DSAs are RSA, and ECDSA (Elliptic Curve Digital Signature Algorithm) which enhances the efficiency of traditional DSA by using elliptic curves algorithm (Bedoui et al., 2023, Lalem et al., 2023).

Table 2 presents a comparative analysis of cryptographic algorithms based on different aspects of security features such as confidentiality, authentication, data integrity, etc.

Table 2: Comparison of cryptographic algorithms based on security features

Security Features	Symmetric Key Encryption	Asymmetric Key Encryption	Hash Functions	Key Exchange Protocols	Digital Signature Algorithm
Key Management	Simple, uses one key	More complex, uses key pair	No keys	Key exchange required	Key pair required
Computational Load	Lower	Higher	Lower	Higher	Higher
Confidentiality	Secure but needs key distribution	Highly secure, slower	Not applicable	Depends on key exchange	Not applicable
Authentication	Not built-in, needs extra steps	Built-in	Not applicable	Depends on key exchange	Not applicable
Data Integrity	Requires other methods	Built-in	Used for integrity checks	Depends on encryption	Yes, built-in
Key Exchange Security	Vulnerable to distribution issues	Resistant to key issues	Not applicable	Critical for security	Vulnerable to distribution issues
Usability	Easier to implement	More complex	Not applicable	Requires an additional step	More complex
Examples	AES, DES	RSA, ECC	SHA-256, MD5	Diffie-Hellman, ECDH	RSA, ECDSA

3.2. Problems in IoT security environment

The following crucial problems are being challenged when implementing the cryptographic algorithms in the IoT environment, as illustrated in Figure 2. The first challenge is Interoperability. IoT systems consist of a wide range of connected devices with different capabilities, communication protocols, and technical standards (Silva et al., 2024), which complicates the implementation of standard cryptographic solutions in a heterogeneous ecosystem. The second challenge is Scalability. The rapid growth of the IoT network raises the possibility of vulnerabilities and expands the attack surface (Babu and K.N.Veena, 2021). Therefore, safeguarding data integrity and privacy requires flexible security solutions that adapt to the constantly growing IoT networks. Third, Resource constraints. Resource constraints

are a major problem in implementing robust security algorithms in the IoT ecosystem due to many IoT devices' limited processing power, memory, and energy availability. This constraint gives rise to problems about the effectiveness of encryption and authentication strategies (Radhakrishnan et al., 2024). Finally, Key management. Key administration is another big challenge in the IoT domain. The processes involved in generating, distributing, and managing cryptographic keys for many devices can be complicated (Mirani et al., 2022). However, effective keys must be used in many protocols to improve the integrity and confidentiality of information.

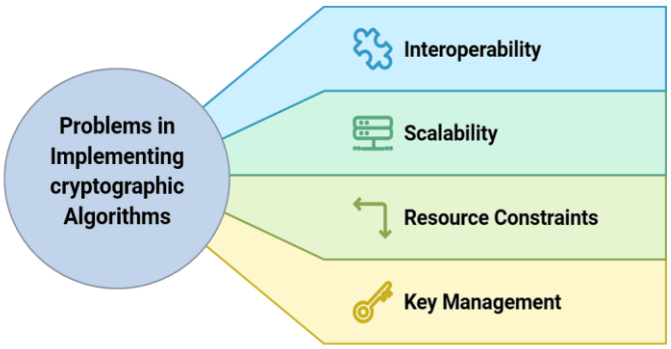

Figure 2: Problems of cryptographic algorithms in the IoT environment

3.3. IoT security Threats

Implementing strict security measures on IoT devices is necessary, but several threats affect the transmitted information and execution processes in IoT devices. Unauthorized access**,** Man-in-the-Middle (MIM), replay attack, denial of service (DoS), eavesdropping attacks, brute force attack, and physical risks are the common attacks faced by IoT devices. The unauthorized access attack covers many activities, such as phishing, hacking, and other online actions that allow unauthorized users to access databases, networks, or computer systems. MIM attacks appear when an unauthorized individual listens to a conversation between two other IoT devices and modifies the client's shared data. They may result in the injection of fake data or the loss of private information (Hamdare et al., 2023). The replay attack involves capturing, recording, and replaying IoT data from transmissions to gain unauthorized access. DoS involves overloading a targeted device with traffic in order to prevent authorized users from accessing it. Distributed DoS (DDoS) attacks are another type of DoS attack that involves several connected devices flooding a targeted server with fictitious traffic (Kumari et al., 2024). Eavesdropping attacks occur when a malicious actor tries to intercept and record communications between IoT devices to capture sensitive information exchanged during these communications(Jawed and Sajid, 2024). Brute force attack indicates a technique that involves repeatedly testing different combinations of the default password in order to obtain unauthorized access. With this method, the attacker keeps guessing until a specific password is identified. Finally, in a physical attack, an IoT device is directly accessed and manipulated in order to obtain control; this can be done by using physical tools or by making technical changes to the firmware of the device.

3.4. Performance Parameters

Security algorithms can be evaluated for effectiveness and suitability for IoT applications using various performance metrics to assess how well cryptographic algorithms meet security and privacy requirements, Figure 3 illustrates typical security metrics. The common parameters are encryption and decryption time, key generation time, response time, signature verification time, energy consumption, and memory utilization. When creating IoT systems, encryption and decryption metrics are important measures to evaluate the general performance of the system. Encryption time is the amount of time needed for cryptographic algorithms to transform readable data, or plaintext, into encrypted data, or ciphertext(Pereira et al., 2017). In contrast, decryption time indicates converting ciphertext back into plaintext. The algorithm with the lower encryption/decryption process is considered to have better security performance(Thabit et al., 2023). The time needed to generate cryptographic keys used for securing communications is Key generation time (Silva et al., 2024), Key generation speed must balance security needs with communication performance. Response time is the time required for the system to respond to an input or request after starting a cryptographic operation (Tsantikidou and

Sklavos, 2022). Lower response times in milliseconds or microseconds are critical for IoT systems, especially real-time applications such as autonomous vehicles, as delays can have a major impact on performance and safety (Radhakrishnan et al., 2024). In the IoT environment, digital signatures help ensure the authenticity and integrity of data transmission. The time required for the system to confirm the authenticity of the digital signature is known as "signature verification time". Optimal signature verification time means that system must operate fast enough to maintain overall system throughput(Arya et al., 2023). Device power usage during cryptographic operations is referred to as energy consumption. Energy consumption is particularly crucial for IoT devices that run on batteries. Optimal energy consumption is achieved when the cryptographic algorithm uses the least energy consumption to meet the

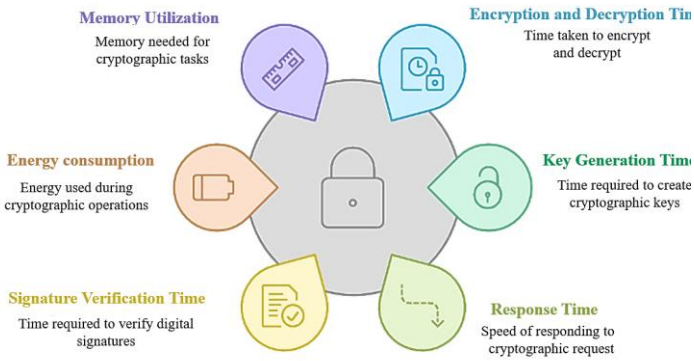

Figure 3: Performance Parameters of Cryptographic Algorithms in IoT

security goal(Hasan et al., 2021). Memory utilization pertains to the amount of memory (RAM and storage) that cryptographic algorithms utilize during operation, consisting of both static memory (code and data structures) and dynamic memory (temporary data storage during cryptographic processes). IoT devices generally cannot handle large amounts of data or complex algorithms due to hardware limitations. Efficient memory utilization can be achieved by implementing light-weight cryptographic algorithms with small key sizes (e.g., ECC) or fewer resources (e.g., ChaCha20) without compromising security level (Corthis et al., 2024, Sarker et al., 2020)

4. CASE Studies of Improved Cryptographic algorithms for Advancing IoT

This section presents some case studies about lightweight cryptography solutions in various IoT environments to ensure security adequate for these resource-constrained devices without loss of performance or security level. A new hybrid cryptography model based on RC4, ECC, and SHA-256 was presented by (Mousavi et al., 2021a) to safeguard the private information of IoT-based irrigation systems. The RC4 key is encrypted using the ECC technique, and the result is converted to SHA-256 for hashing and producing mysterious data to enhance data integrity. The suggested model clearly outperforms other algorithms in terms of encryption time and decryption time when compared with other models like AES and RC4 with SHA-256, RC4 and 3DES with SHA-256, etc., achieving excellent encryption efficiency. A hybrid encryption approach that combines symmetric blowfish and asymmetric ECC, has been introduced by (Zhang and Wang, 2024). A digital signature based on SHA-256 was utilized to ensure the integrity of the data, the suggested approach provided the advantage of blowfish to encrypt large volumes of data and ECC to ensure the protection of the private key, which is small and does not increase the execution time significantly. The suggested approach was evaluated against other security algorithm performances, such as AES, 3DES, DES, RSA, etc., regarding encryption time, throughput and memory consumption. The proposed solution showed a relatively low execution time (610 ms), high throughput (≈2700 kb/s), and low memory requirement (10 kb). (Rahman et al., 2022) intended to enhance traditional AES algorithms to secure an IoT-based smart home. The proposed method improved the difficulty of key generation using a Three-Dimensional Key Generation Mechanism (3DKGM), logistic map, and Exclusive OR(XOR) operation rather than the traditional two-dimensional S-box, lowering the chance of the keys being broken. Key generation time for the smoke detector and smart light was improved to

19 ms and 1516 ms for the IP Camera and IP TV. The proposed model has greatly improved the smart home system's data security, integrity, and protection through evaluation compared with similar approaches. (Satyanarayana et al., 2023) aimed to adapt the AES algorithm for low-power microcontrollers frequently encountered in IoT devices and various communication protocols in terms of computational correctness and energy consumption. The suggested method improves on the current AES encryption procedure by implementing a number of significant changes to maximize its functionality for IoT devices. Energy consumption was improved to 0.56mW, and latency(accuracy) was improved to 95.4% compared with conventional methods such as existing AES and ECC algorithms. The modified AES mitigated potential vulnerabilities such as DOS attacks and improved the overall security of IoT networks. (Corthis et al., 2024) provided a fog computing model with a hybrid mathematical model, ECC and Proxy Re-encryption (PR) to further secure data sharing in real-time healthcare services. The PR algorithm (a cryptographic technique that re-encrypts data without having access to the plaintext) is incorporated into the Enhanced Salp Swarm Algorithm (ESSA) to determine the optimal key size and parameters of the PR algorithm for IoT device verification, identification, and authentication of EHRs (Electronic Health Records). The provided method mathematical model enhanced the processing time and reliability. Also, compared to the traditional cryptographic algorithms, enhanced communication cost (4260 bits) and memory usage (680 bytes) in the context of security analysis. ElGamal-based public-key cryptosystem (PKEIE) encryption strategy was introduced by (Mohan et al., 2020) to accomplish big message encryption and guarantee data security in Internet of Things networks. The Decisional Diffie–Hellman assumption, or DDH assumption, is the foundation of the ElGamal algorithm. The proposed approach employs SHA-256 and HMAC (Hash-based Message Authentication Code) for integrity and authentication. The quality of the key used and the underlying hash function determine how strong HMAC is in ensuring the necessary security. The algorithm achieved large message encryption, and high-security level**.** (Tidrea et al., 2023) proposed hybrid cryptography Elliptic Curve Integrated Encryption Scheme (ECIES) with SHA-256 for hashing. In order to enable safe data transfer for Modbus TCP communication inside automation and SCADA systems, ECIES combines the advantages of ECC with symmetric

Table 3: Summary of improved cryptographic algorithms employed in IoT cybersecurity.

Ref.	IoT Environment	Threats	Security issue	Cryptographic Algorithms	Improved in
(Mousavi et al., 2021a)	Smart irrigation	MITM and Replay Attack	Data integrity and confidentiality.	ECC, RC4, SHA-256	Encryption and decryption time, throughput, and security.
(Zhang and Wang, 2024)	IoT Network	Brute-Force	Security and privacy of IoT data transmission.	Blowfish, ECC, SHA-256	Memory requirement, relatively execution time, and throughput.
(Rahman et al., 2022)	Smart home	Unauthorized access, Brute-Force	Enhance IoT real time applications security.	AES, SHA-256	Data security, integrity. protection of the smart-home system.
(Satyanarayana et al., 2023)	IoT Applications	Eavesdropping, Physical risk	low-power microcontrollers, and diverse communication protocols.	AES	Computational accuracy(latency), throughput and energy consumption.
(Corthis et al., 2024)	Healthcare	DDoS	Secure data sharing in the real-time services.	ECC	Processing time, reliability, communication cost, memory usage, and security measures
(Mohan et al., 2020)	IoT network	Brute-Force, Eavesdropping	Encrypting large messages, and ensuring integrity and authentication.	ElGamal, SHA-256, HMAC, DH	Sensor data integrity, authentication, and encryption.
(Tidrea et al., 2023)	IIoT	MITM, Replay Attack	Securing Automation and SCADA Systems.	ECIES, ECDSA, SHA-256	Good timing performance for the cryptographic operations (Encryption, Decryption, and key generation time).

key encryption. To guarantee that the information sent between SCADA and automation system entities is genuine and private, the ECDSA is utilized for the authentication technique and Optiga Trust X is utilized for safe key storage. The experimental findings demonstrated good timing performance for the cryptographic operations carried out on the industrial internet of things (IIoT) and successfully prevented replay and MITM threats
and MDUINO PLCs in encryption, decryption, and key generation time.

Table 3 presents the analyzed case studies and demonstrates different strategies for using lightweight cryptographic algorithms suited to IoT device limitations. These strategies include Algorithm selection: selecting the proper algorithm for specific IoT applications regarding factors such as data sensitivity, device capability and specific attacks (Rahman et al., 2022, Satyanarayana et al., 2023, Corthis et al., 2024). Hybrid cryptographic algorithms: using hybrid cryptographic algorithms and taking advantage of symmetric and asymmetric algorithm features (Mousavi et al., 2021a, Zhang and Wang, 2024). Key management: involves optimize key generation (Rahman et al., 2022), key distribution (Mohan et al., 2020), and safe key storage (Tidrea et al., 2023). Authentication scheme: consist of using DSAs (Tidrea et al., 2023) and integrated hash functions (Mohan et al., 2020) to guarantee data integrity and authentication.

5. Cryptographic Enhancements Techniques

5.1. Meta-heuristics algorithms solution

MH algorithms are problem-solving frameworks that guide searching for the best solutions in complex structures, the common optimization algorithm is Particle Swarm Optimization(PSO) (Alizadehsani et al., 2023). MH algorithms are ideal for dynamic environments like IoT because they can analyze a large number of options and modify their strategies in response to input. Table 4 illustrates various studies that utilized MH techniques to significantly enhance cryptographic performance in IoT security. The integration of MH algorithms has the following benefits:

5.1.1. Optimize Encryption Performance:

applying optimization algorithms helps enhance cryptographic algorithm parameters to achieve better performance, particularly for IoT devices, which often have limited processing power. (M et al., 2023) intended to enhance data encryption algorithms and attack detection rates in IoT cities. The authors proposed Hybrid Convolutional Neural Networks (HCNN) for attack identification, Entropy-Hummingbird Optimization Algorithm (EHOA) for feature selection, and the Krill Herd-Advanced Encryption Standard (KH-AES) algorithm for security optimization. The proposed method evaluated data sharing security, feature selection, and attack identification. The proposed system produced better outcomes and increased the security level to 96% compared with other security approaches. Similarly, (Duraisamy et al., 2021) intended to enhance confidentiality and data integrity in IoT cities. An optimized deep learning modified neural network approach was used for classification to identify attacks more efficiently, and an AES algorithm enhanced by the KH optimization algorithm was used for secure data exchange, which gained lower encryption and decryption time compared with other encryption algorithms such as DES, 3DES, and AES. The proposed method increased the security level to 96%. (Jawed and Sajid, 2024) introduced a faster and more secure encryption technique based on Harris Hawks optimization (HHO) that incorporates filter-based feature selection to improve secure data transmission between IIoT and cloud computing against eavesdropping attacks. The suggested method obtained a faster encryption process and higher security level compared with other standard encryption algorithms since only the sensitive portion of generated data was encrypted before sending to the cloud.

5.1.2. Optimize key management:

This process includes two main approaches first optimal key generation: MHA help generate keys that are both robust against attacks and suitable for resource- constrained IoT environments. For instance, using genetic algorithms can help generate cryptographic keys that are more random and less predictable (Guruprakash and Koppu,

2020), making it harder for attackers to guess them. Second optimal key selection: techniques that adapt to complex optimization landscapes make it possible to find cryptographic
keys that are highly secured and use the least amount of computing power while still meeting a number of criteria, such as performance, randomness, and strength. (Prabhakaran and Kulandasamy, 2021) utilized the crossover-based mine blast optimization algorithm (CMBA) to determine the optimal key for the AES algorithm to protect patient's health data in IoT health applications. This method identifies an optimal key that decreases the chances of unauthorized access and computational time. The suggested framework greatly enhanced medical data confidentiality and data privacy in cloud storage against threads (e.g., on-the-fly attacks). Multiple homomorphic encryptions (MHE) methods with Sailfish Optimization (SFO) enhance medical data transmission privacy in E-health IoT systems are suggested by (Alzubi et al., 2022). This method improves the exploration of the search area to select the best key from a random key sequence generator, resulting in a robust encryption key and a high-security level in the cloud.

5.1.3. Optimize hashing function: Indicates techniques used for performing improved hashing algorithms to increase data security in an IoT setting, consisting of device identities, reducing cyber threats, and data integrity conferring. (Al Shahrani et al., 2022) presented an authentication model, including DDTHA (Discrete Decision Tree Hashing Algorithm) with ACO is designed to optimize the hashing algorithm with digital certificates. The designed model optimized the hashing algorithm alongside digital certificates customized for healthcare applications. (Kalyani and Chaudhari, 2020) presented a security optimization approach to enhance the secure communication between cloud computing platforms and IoT devices. The authors employed the Step Size Firefly (SFF) optimization algorithm and the Optimal Homomorphic Encryption (OHE) algorithm to enhance key authentication and optimization in the encryption process. The presented method demonstrates that the suggested security model for IoT achieves a longer key breaking time and decreases computational duration, offering a higher level of security for IoT applications.

Table 4: Summary of MH techniques for optimizing cryptographic algorithm.

Ref.	Environment	Security Algorithm	MHA	Security purpose	Optimize	Outcome
(M et al., 2023)	IoT	AES	KH	secure data exchanges	Encryption Performance	High security level, lower encryption and decryption time.
(Duraisamy et al., 2021)	Smart cities	AES	KH	secure data exchanges	Encryption Performance	Enhanced confidentiality and integrity
(Jawed and Sajid, 2024)	IIoT	HHO (used for encryption)	HHO	secure communication	Encryption performance and key generation.	Cryptographic key fitness, encryption and decryption time.
(Alzubi et al., 2022)	Healthcare	MHE	SFO	Medical data privacy	key selection, encryption performance.	Robust key, increase security level.
(Kalyani and Chaudhari, 2020)	IoT	OHE	SFF	Key Authentication	key selection	increase key breaking time and decrease computational time.
(Prabhakaran and Kulandasamy, 2021)	Healthcare	AES	CMBA	Data storage	key selection, encryption performance.	Increase key breaking time and decrease encryption and decryption time.
(Al Shahrani et al., 2022)	Healthcare	DDTHA	ACO	Data Integrity, Authentication	hashing function	Enhanced data confidentiality, Minimize the computational load.

5.2. Machine learning solutions

ML uses statistical methods to assist devices in learning from experience, identifying patterns and abnormalities in large datasets, and enabling security analysts. ML models can detect unusual activity using real-time data in an IoT environment, the IoT provides data to ML, while ML senses the data intelligently (El-Sofany et al., 2024). For instance, ML algorithms assist in providing appropriate solutions for resource limitation and anomaly detection in cryptographic protocols by analyzing a large volume of data to detect unusual patterns (Ozkan-Okay et al., 2024). Employing ML techniques offers an effective approach for safeguarding IoT devices against cyber threats. Table 5 summarizes ML techniques for optimizing cryptographic algorithms in various studies, which include the following methods:

5.2.1. Key Management and Generation: This process indicates improving key generation processes by predicting optimal parameters based on historical data and securely distributing keys among devices. For example, ML models can analyze previous security breaches to generate keys that are less susceptible to attacks. (Saini and Sehrawat, 2024) offered a creative and expandable information security approach that uses contemporary technologies to improve data safety. The suggested technique turns the MNIST dataset into a source for key creation by fusing modern cryptography techniques' advantages with the autoencoder model's feature extraction powers. Applying symmetric (AES and DES) and asymmetric (RSA and ElGamal) encryption with modifiable block cipher properties and using SHA-512 for hashing, this tow-layered encryption system demonstrates enhanced performance when compared with existing systems, including AES, DES, RSA and ElGamal.

5.2.2. Privacy preservation: Refers to safeguarding personal and sensitive data collected and processed by IoT devices by applying ML models to analyze data without exposing individual or sensitive details. (Ranjan and Kumar, 2024) proposed a hybrid encryption (AES and Blowfish) and BC technology to securely transmit medical data collected from IoT sensors to a personal digital assistant (PDA) for processing. A hybrid deep learning model including Long Short-Term Memory and Convolutional Neural Networks (LSTM and CNN) was utilized for generating robust encryption keys and key selection optimized with the Self-Improved Lion Optimization Algorithm (SI-LA) . The proposed algorithm offered lower encryption and decryption times, faster key generation, and rapid response to user queries, increasing the speed of executed tasks. (Aiyshwariya Devi and Arunachalam, 2023) presented a malware detection and prevention system with a deep learning model (Deep LSTM) enhancing detection capabilities and an Improved Elliptic Curve Cryptography (IECC) algorithm for secure data transmission in IoT networks. The Deep LSTM classifier processes preprocessed data to accurately predict various attack types (e.g., anomalies, DOS, etc.).The IECC algorithm key generation and selection is optimized through a hybrid optimization technique called the "Mayfly-Black Widow Optimization Algorithm (MA-BW)". The proposed system achieved 95% accuracy, 92% precision, and a 5% error rate in malware detection, demonstrating significant improvements over traditional methods.

5.2.3. Sensitive data classification: Identifying and categorizing data that requires protection due to its confidential or personal nature. ML models are trained to detect patterns and classify data based on its sensitivity level, such as health records or financial details, enabling the system to apply appropriate security measures. (Alzubi et al., 2022) designed a novel named PPEDL-MDTC (privacy-preserving encryption with Deep Learning-based medical data transmission and classification) to ensure privacy and security in the transmission and classification of medical data. The model incorporates multi-key homomorphic encryption enhanced with sailfish optimization (MHE-SFO) for secure encryption. Additionally, a method that combines cross-entropy and artificial butterfly optimization achieves feature selection, and an optimized deep neural network (ODNN) with hyperparameters refined using chemical reaction optimization (CRO) manages data classification. This model demonstrates superior accuracy (0.9813 and 0.9650) on activity recognition and sleep stage datasets,

outperforming existing methods. (Annamalai et al., 2023) introduced a framework called SMOEGE-HDL, which stands for SMO with EGE and a Hybrid Deep-Learning. The proposed SMOEGE-HDL model merges encryption and classification techniques to safeguard IoT data. During the encryption process, the EGE technique is enhanced by using SMO to generate more secure optimal keys, whereas, in the classification process, the HDL model, including CNN-LSTM techniques with Nadam optimizer, is used to ensure accurate data categorization. The SMOEGE-HDL model was validated from different perspectives, achieving 98.50% accuracy compared with existing techniques, resulting in more reliable and secure IoT applications.

5.2.4. Anomaly detection and attack prediction: Anomaly detection involves identifying unusual or unexpected behaviors in data patterns generated by IoT devices (Aiyshwariya Devi and Arunachalam, 2023). (Kathamuthu et al., 2022) introduced a new framework known as the "Deep Q-learning-based neural Network with Privacy Preservation Method (DQ-NNPP)" to improve data security and privacy in IoT healthcare. The model employs a systematic approach using ML and cryptographic techniques to authenticate users and detect anomalies. Data encrypted using an asymmetric Ciphertext-Policy Attribute-Based Privacy Preservation (CPABPP) algorithm, which includes a key generation process based on ciphertext-policy attribute-based encryption (CP-ABE). By integrating deep Q-learning with a privacy preservation approach, the framework reduces encryption and decryption times while minimizing network traffic. Performance analysis shows that DQ-NNPP is more accurate (93.74%), more sensitive (92%), and more specific (92.1%) than other models.

5.2.5. Access control: ensures that only authorized devices, users, or applications can

Table 5: Summary of ML techniques for optimizing cryptographic algorithm.

Ref.	IOT Application	Security Algorithm	Security issue	ML technique	Optimize	Outcome
(Ranjan and Kumar, 2024)	E-health	AES and Blowfish	Security of patient information, prevent unauthorized access.	LSTM and CNN	Key generation, Privacy prevention	Fast and efficient encryption operations, key generation, response time, and lower computational time.
(Saini and Sehrawat, 2024)	Not specified	(AES + DES) and (RSA + ElGamal), hash-128.	Secure data transmission, ensuring efficient and reliable decryption.	Autoencoder -based key generation.	Key Management and Generation	efficiency encryption and decryption process, enhance secure communication.
(Alzubi et al., 2022)	E-health	MHE-SFO	secure transmission of medical data	CNN	Data classification	superior accuracy on activity recognition
(Annamalai et al., 2023)	IoT-Cloud	SMOEGE	Protect user information saved in the cloud from untrusted administrators	CNN-LSTM	Data classification	superior accuracy in sensitive data classification.
(Kathamuthu et al., 2022)	Healthcare	CPABPP	secure medical systems, detect anomalies.	DQ-NNPP	Prediction	High accuracy in anomaly detection, decrease encryption and decryption times and network traffic.
(Zhou et al., 2021)	IoT Mobile application	CP-ABPRE	Secure EI model sharing, detect malicious edge nodes.	Not specified	Access control, Anomaly detection	low-latency data processing at the network's edge.
(Aiyshwariya Devi and Arunachalam, 2023)	IoT network	IECC	malware detection and prevention	LSTM	Prediction, Privacy preservation	High accuracy in malware detection reduces execution time and memory usage.

interact with ML models deployed on IoT edge devices, protecting data privacy and security within a distributed, often vulnerable, environment. (Zhou et al., 2021) proposed a secure and privacy-preserving scheme for sharing ML models in edge-enabled IoT environments called Edge Intelligence (EI).The trained ML model has been encrypted using Ciphertext Policy Attribute-Based Proxy Re-encryption (CP-ABPRE) to address secure sharing among IoT devices while embedding accountability mechanisms to trace malicious or negligent edge nodes. According to experimental analysis, the suggested plan preserved user privacy while meeting the need for low-latency data processing at the network's edge.

5.3. Blockchain solutions

BC technology enables a shared and decentralized ledger to securely document transactions across different systems. Each transaction is grouped into blocks and linked to previous ones, creating a "chain" almost impossible to alter. In the sequential chain, each block connects with the previous block with a unique encrypted hash function, creating a continuous data sequence (Giannoutakis et al., 2020). Since a constant data sequence is generated, changing or deleting any previously recorded transactions is very difficult.

Combining IoT and BC technology creates opportunities for secure and transparent data sharing and addresses various challenges associated with IoT systems. BC enables decentralized storage of IoT data, enhances transparency and trust by reducing the risk of data modification or unauthorized access, and ensures resistance to tampering and accessibility only for authorized users (Ahakonye et al., 2024). BC and IoT can be used for several applications, such as managing supply chains, smart contracts, and energy management. For instance, in supply chain management, BC can help monitor the movement of products from the producer to the consumer, guaranteeing their authenticity and integrity (Khan et al., 2023).

Table 6 presents different studies that used the advantages of BC technology for enhancing security algorithms across the following approaches:

5.3.1. Authentication and Access Control: The process of verifying the identities of users and devices in an IoT network; BC technology offers secure and decentralized solutions for handling digital identities, increasing trust and security in the authentication mechanisms. (Velliangiri et al., 2022) developed a lightweight authentication mechanism based on ECC to secure data exchange in Industry 4.0, particularly in-vehicle networks. The author demonstrated the security and performance evaluation of the employed protocol using AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. The security evaluation of the proposed protocol showed a lower communication cost of 834 bits and computation costs of 7.96 seconds, which indicates the strength of security against significant attacks, including MIM, DoS, and spoofing, compared with existing authentication mechanisms. (Velmurugadass et al., 2020) constructed a BC architecture for evidence collection and provenance preservation in the IaaS (Infrastructure as a Service) cloud utilizing the IoT. The authors developed a cloud-based Software Defined Network (SDN) comprising mobile IoT nodes, an open flow switch, and BC controllers to monitor data activities securely. The framework employed the Elliptic Curve Integrated Encryption Scheme (ECIES) for encrypting data packets sent to the cloud, while SHA-256 was used for hashing to ensure data integrity. Users were registered with an Authentication Server (AS) and received a secret key generated through Harmony Search Optimization (HSO). The system allows authorized investigators to collect, analyze, and report on evidence through a Logical Graph of Evidence (LGoE). The suggested system successfully addressed secure evidence management in cloud environments and security issues in IoT environments by improving performance metrics like response time, accuracy, and throughput.

5.3.2. Secure Data Sharing: Includes implementing BC technology to maintain secure data communication between IoT devices through cryptographic hashes and immutable records. (Ali et al., 2022) presented an approach to enhance

security and privacy in healthcare systems by integrating the IIoT and BC technology. The authors proposed a secure, searchable encryption (SSE) mechanism that utilizes BC and a hybrid deep neural network (HDNN) to address vulnerability access to patient health records (PHR) from the IoMT database. The proposed HDNN, which consists of the CNN-LSTM model, was implemented to train and test datasets for accurate intrusion detection. BC was introduced as a distributed database with homomorphic encryption to ensure a secure search and keyword-based access to the database. An attribute-based signature (ABS) model has also been introduced for fine-grained access control. The proposed approach improved security and efficiency in handling PHR, ensuring transparency and cost-effectiveness in managing healthcare data.

5.3.3. Decentralized Management: Describes a system where control is spread across a network rather than concentrated in one central authority. BC technology supports data storage and decision-making in a decentralized manner, thereby minimizing risks related to central points of failure. (Gajendran et al., 2024) utilized Extended Elliptic Curve Cryptography (E_ECurCrypt) to encrypt IoMT data, processed through a BC-powered federated Q-learning model, to analyze potential attacks and improve privacy protection. The encrypted data is securely stored using decentralized BC technology, validated by a Delegated Proof of Stake (Del_PoS) consensus algorithm. The results demonstrate that the proposed system achieved high-performance metrics, including 99.23%

Table 6. Summary of BC techniques for optimizing cryptographic algorithms.

Ref.	IOT Application	Security Algorithm	Security issue	BC technique	Authentication Validation	Optimize	Outcome
(Gajendran et al., 2024)	IoMT	E_ECurCrypt	Security of healthcare services	Decentralized (BC -powered federated Q-learning)	Del_PoS	Confidentiality and medical data security	Secure data storage, high accuracy and encryption performance.
(Velmurugadass et al., 2020)	IoT network and cloud	ECIES	Provenance preservation in IaaS cloud, Weak authentication, MITM attack	Centralized in IaaS cloud	Not used	Robust user authentication, secure data monitoring.	Better performance in accuracy, response time, increasing throughput.
(Mohammed and Wahab, 2024)	IoT network	OUH	data breaches, unauthorized access in supply chains	Decentralized-IoT network	PoSS	data reliability and Authenticity.	Minimize computational power, secure data storage and analysis.
(Ali et al., 2022)	IoMT	EHE	Patient data privacy and security in the PHR system.	Decentralized (BC as distributed database with HDNN model)	ABS	Secure healthcare data management and searchable mechanism	Ensuring transparency and cost-effectiveness in managing healthcare data
(Ngabo et al., 2021)	Healthcare	ECC	Enormous data generation, and security threats in the fog computing layers.	Public-permissioned BC	ECCDSA	Secure medical data mining, resolve latency issues in fog layer.	Ensures immutable security, reduced latency, and transaction transparency.
(Badr et al., 2023)	IoMT	GIFT with CSKey	malicious intent and privacy breaches against HER and PHI	Decentralized	within the BC	Authenticity of medical data during storage	Lightweight, fast, reliable and memory-efficient cryptosystem.
(Velliangiri et al., 2022)	IoV	ECC	privacy prevention against multiple attackers.	Decentralized	AVISPA	secure authentication, Secure data exchange between end devices	Decrease computational cost, verification cost, and resource utilization

accuracy and 59080.506 average throughputs, outperforming existing methods. The proposed methods overcome the challenges of traditional healthcare systems, e.g. data encryption and vulnerability to attack, by using a decentralized BC integrated with a ML model. (Ngabo et al., 2021) focused on enhancing medical data security within a fog computing architecture. The authors address vulnerabilities and cyber threats that affect different layers of fog computing, including the edge layer (where data is sensed), the fog layer (where data is processed), and the cloud layer (where data is stored). The paper introduces a public-permissioned BC security mechanism utilizing the adoption of an ECC digital signature algorithm. The distributed ledger database solution enhances medical data security and privacy in IoT environments, reducing latency and transaction transparency.

5.3.4. Lightweight Architecture: Refers to the Design of lightweight security solutions optimized for resource-constrained IoT devices; lightweight BC implementations ensure resource-efficient security measures, making them suitable for environments where efficiency is critical (Mohammed and Wahab, 2024) suggested an innovative method that used a lightweight BC framework to provide decentralized administration and offer security to IoT devices. The IoT data was stored in a distributed ledger and subjected to the proof of secret sharing (PoSS) method to improve data authenticity and dependability. Okamoto Uchiyama (OU), a homomorphic encryption technique, improves data security by encrypting data inside these ledgers. Combining BC with IoT and Okamoto Uchiyama homomorphic encryption creates a safe route for information exchange between diverse IoT devices. The suggested method is appropriate for low-power Internet of Things devices as it expedites each process and lowers the overall computing power needed. (Badr et al., 2023) presented a novel lightweight encryption method to protect medical data transmitted by portable medical devices without exhausting their limited resources in healthcare applications. The proposed method develops an efficient, lightweight block cipher cryptographic system based on GIFT, known for its efficiency and low resource consumption. It enhances this system with chaotic key generation techniques from Chaos Theory (CSKey) to improve security level. The proposed method achieved a high entropy score of 7.9917 for medical images, indicating a strong level of randomness. The average encoding time was recorded at 3.8952 seconds, while the average decoding time was 3.0584 seconds.

The global taxonomy of solutions provided by integrated technologies involving MHA, ML, and BC approaches was emphasized in Figure 4.

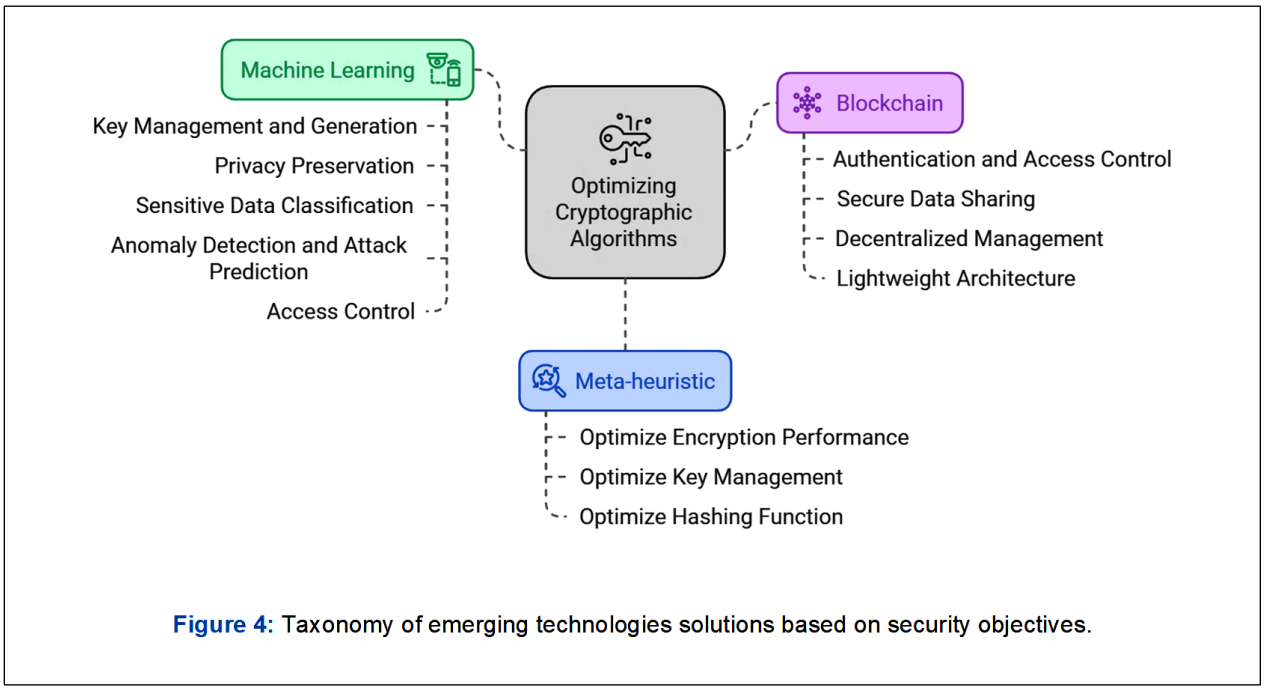

Figure 4: Taxonomy of emerging technologies solutions based on security objectives.

6. Open Challenges

Improving the security and privacy algorithms in IoT systems involves many important security issues. These issues arise from the distinct features of IoT settings, where many heterogeneous devices connect and exchange information. Based on previous case studies in this research, some of the research challenges with open research areas are discussed below:

6.1. End- to -End Security Solutions: In IoT systems, developing complete end-to-end security solutions that safeguard data at every stage of its lifecycle is a major problem, especially for sensitive applications such as healthcare and industrial IoT(Abdlrazaq et al., 2023). For instance, protecting patient data requires robust mechanisms to ensure that information is secure at every stage, from collection to transmission and storage (Corthis et al., 2024, Gajendran et al., 2024). Existing algorithms frequently need to meet the requirement of providing this level of security (Mousavi et al., 2021a, Satyanarayana et al., 2023). Also, developing more effective methods that can handle the unique requirements of IoT environments to mitigate risks associated with data breaches (Saleh et al., 2022).

6.2. Dynamic Encryption Models: Dynamic encryption utilizes algorithms that adjust encryption keys or methods in real-time, depending on specific conditions or factors, to respond to the constantly changing environment of IoT networks. Dynamic encryption models should be bio-inspired to improve their flexibility and responsiveness to threats (Alzubi et al., 2022). For example, developing intelligent security systems can learn from past incidents and adapt their defenses accordingly (Gajendran et al., 2024, Aiyshwariya Devi and Arunachalam, 2023). However, implementing dynamic encryption models presents several challenges that make it a current research focus. For example, problems in accurate keys are updated (Tidrea et al., 2023), and these algorithms often require more processing power and memory (Kathamuthu et al., 2022), which can result in latency and slow down data transmission (Annamalai et al., 2023).

6.3. Complexity in Integration: The combination of multiple cryptographic techniques with ML methods introduces many complexities that complicate the implementation and ongoing maintenance processes in IoT security networks (Bharati and Podder, n.d.). For instance, integrating ML methods, such as autoencoder neural networks in (Saini and Sehrawat, 2024) and LSTM and CNN in (Ranjan and Kumar, 2024), with multiple cryptographic algorithms (such as AES combined with DES, Blowfish, etc.), demands

substantial computational resources, raising concerns about the efficiency of these systems, particularly with the large datasets common in IoT applications(Aiyshwariya Devi and Arunachalam, 2023). However, implementing simplified systems, such as developing lightweight ML models or alternative training approaches, can minimize computational requirements in IoT security systems (Aouedi et al., 2024).

6.4. Real-time Implementation: Implementing traditional encryption methods like AES (Rahman et al., 2022, Satyanarayana et al., 2023) and ECC (Corthis et al., 2024), in real-time shows vulnerability in various IoT applications due to challenges related to resources, standardization (Tidrea et al., 2023), and varying environments, raising questions about how well they secure sensitive data. In a dynamic environment where manufacturers frequently develop their own security protocols, the lack of widely accepted cryptographic standards results in incompatibility and potential vulnerabilities(Obaidat et al., 2020, Aslan et al., 2023). However, post-quantum cryptography, using robust key management with appropriately integrated technologies like BC (Velliangiri et al., 2022), ML (Ranjan and Kumar, 2024), and meta-heuristics (Prabhakaran and Kulandasamy, 2021), provides powerful solutions to enhance data security in IoT environments against emerging threats and vulnerabilities. However, creating a global standardized framework that combines BC, ML, and meta-heuristics techniques is still a significant challenge.

6.5. Centralized data management: BC offers a decentralized approach to improve IoT device security by lowering single points of failure and making it more difficult for hackers to breach the system. Many IoT systems still use centralized procedures for data processing and key management (Velmurugadass et al., 2020, Laturkar and Laturkar, 2023), depending on centralized data management can create several vulnerabilities in IoT security, such as single-point failure problems, lack of transparency, and privacy breaches (Cherbal et al., 2024). However, centralized data management risk can be addressed by integrating decentralized methods for key generation and distribution to eliminate a single point of failure (Ali et al., 2022). Another approach is Enabling devices to train ML models locally while sharing only model updates; federated learning can reduce reliance on central servers and enhance security (Gajendran et al., 2024). Developing comprehensive data management policies that define how data is collected, processed, and secured across various layers of the IoT architecture needs to be explored (Mahmood and Al Dabagh, 2023).

7. Conclusion

The security of IoT systems is still an active area of concern for researchers, It requires further investigation and innovative solutions, particularly with the growth of IoT applications, dynamic nature, combining with emerging technologies, and the continuous evolution of new attacks and threats. This paper presents the most enhancement techniques for improving the security and privacy algorithms in IoT cybersecurity. Cryptographic algorithms were categorized and compared based on different security features; the paper also discussed the common parameters required to evaluate cryptographic algorithm performance in IoT systems. Several case studies presented the most common techniques used to improve the efficiency of cryptographic algorithms with emerging technologies, including MHA, ML methods, and BC technology, providing an in-depth understanding of current research and analyzing available enhancement approaches in the field. Also, a global taxonomy of solutions in every specific category is provided based on security objectives. Finally, open research challenges were examined with suggested solutions. In the future, this study intends to investigate how to improve IoT cybersecurity by integrating other strategies, such as quantum computing and the role of federated learning, to enhance IoT security in terms of scalability, privacy protection, and resilience to complex attacks.

Reference

Abdlrazaq, A. A., Azzez, S. N., Anwer, & M.A. And Hassen, S. I. 2023. Proposed Solutions for the Main Challenges and Security Issues in IoT Smart Home Technology. *Zanco Journal of Pure and Applied Sciences,* 35**,** 84-96.

Ahakonye, L. a. C., Nwakanma, C. I. & Kim, D. S. 2024. Tides of Blockchain in IoT Cybersecurity. *Sensors,* 24.

Ahmed, A. A. & Barukab, O. M. 2022. Unforgeable Digital Signature Integrated into Lightweight Encryption Based on Effective ECDH for Cybersecurity Mechanism in Internet of Things. *Processes,* 10.

Aiyshwariya Devi, R. & Arunachalam, A. R. 2023. Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM. *High-Confidence Computing,* 3.

Al Shahrani, A. M., Rizwan, A., Sánchez-Chero, M., Rosas-Prado, C. E., Salazar, E. B. & Awad, N. A. 2022. An Internet of Things (IoT)-Based Optimization to Enhance Security in Healthcare Applications. *Mathematical Problems in Engineering,* 2022.

Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J. & Zakarya, M. 2022. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors,* 22.

Ali, A. S. & Hasan, D. S. 2023. An iot-based smart airport check-in system via three-factor authentication (3fa). *Zanco Journal of Pure and Applied Sciences,* 35**,** 1-13.

Alizadehsani, R., Roshanzamir, M., Izadi, N. H., Gravina, R., Kabir, H. M. D., Nahavandi, D., Alinejad-Rokny, H., Khosravi, A., Acharya, U. R., Nahavandi, S. & Fortino, G. 2023. Swarm Intelligence in Internet of Medical Things: A Review. *Sensors,* 23.

Alzubi, J. A., Alzubi, O. A., Beseiso, M., Budati, A. K. & Shankar, K. 2022. Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis. *Expert Systems,* 39.

Annamalai, C., Vijayakumaran, C., Ponnusamy, V. & Kim, H. 2023. Optimal ElGamal Encryption with Hybrid Deep-Learning-Based Classification on Secure Internet of Things Environment. *Sensors,* 23.

Arya, L., Sharma, Y. K., Kumar, R., Padmanaban, H., Devi, S. & Tyagi, L. K. Maximizing IoT Security: An Examination of Cryptographic Algorithms. 2023 International Conference on Power Energy, Environment and Intelligent Control, PEEIC 2023, 2023. Institute of Electrical and Electronics Engineers Inc., 1548-1552.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A. & Akin, E. 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland).* MDPI.

Azrour, M., Mabrouki, J., Guezzaz, A. & Kanwal, A. 2021. Internet of Things Security: Challenges and Key Issues. *Security and Communication Networks.* Hindawi Limited.

Babu, M. R. & K.N.Veena 2021. Implementing optimized classifier for distributed attack detection and BAIT-based attack correction in IoT. *International Journal of Systems Assurance Engineering and Management*.

Badr, A. M., Fourati, L. C., Ayed, S. & Mudheher Badr, A. 2023. An Improved GIFT Lightweight Encryption Algorithm to Protect Medical Data In IoT. 1-7.

Bakhsh, S. A., Khan, M. A., Ahmed, F., Alshehri, M. S., Ali, H. & Ahmad, J. 2023. Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet of Things (Netherlands),* 24.

Bedoui, M., Bouallegue, B., M. Ahmed, A., Hamdi, B., Machhout, M., Mahmoud & Khattab, M. 2023. A Secure Hardware Implementation for Elliptic Curve Digital Signature Algorithm. *Computer Systems Science and Engineering,* 44**,** 2177-2193.

Chanal, P. M. & Kakkasageri, M. S. 2020. Security and Privacy in IoT: A Survey. *Wireless Personal Communications.* Springer.

Cherbal, S., Zier, A., Hebal, S., Louail, L. & Annane, B. 2024. Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *Journal of Supercomputing,* 80**,** 3738-3816.

Corthis, P. B., Ramesh, G. P., García-Torres, M. & Ruíz, R. 2024. Effective Identification and Authentication of Healthcare IoT Using Fog Computing with Hybrid Cryptographic Algorithm. *Symmetry,* 16.

Duraisamy, A., Subramaniam, M. & Robin, C. R. R. 2021. An Optimized Deep Learning Based Security Enhancement and Attack Detection on IoT Using IDS and KH-AES for Smart Cities. *Studies in Informatics and Control,* 30**,** 121-131.

El-Sofany, H., El-Seoud, S. A., Karam, O. H. & Bouallegue, B. 2024. Using machine learning algorithms to enhance IoT system security. *Scientific Reports,* 14.

Gajendran, S., Muthusamy, R., Ravi, K., Chandraumakantham, O. & Marappan, S. 2024. Elliptic Crypt With Secured Blockchain Assisted Federated Q-Learning Framework for Smart Healthcare. *IEEE Access,* 12**,** 45923-45935.

Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K. & Nijdam, N. A. A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, 2020/11// 2020. Institute of Electrical and Electronics Engineers Inc., 490-495.

Guruprakash, J. & Koppu, S. 2020. EC-ElGamal and Genetic Algorithm-Based Enhancement for Lightweight Scalable Blockchain in IoT Domain. *IEEE Access,* 8**,** 141269-141281.

Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D. & Lloret, J. 2023. Cybersecurity Risk Analysis of Electric Vehicles Charging Stations. *Sensors.* Multidisciplinary Digital Publishing Institute (MDPI).

Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., Ciro Rodriguez, R. & Vargas, D. E. 2021. Lightweight Cryptographic

Algorithms for Guessing Attack Protection in Complex Internet of Things Applications. *Complexity,* 2021.

Jawed, M. S. & Sajid, M. A Swarm Intelligence-based Faster and Secure Algorithm for Improved Industrial IoT-Cloud Computing Communication. 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2024, 2024. Institute of Electrical and Electronics Engineers Inc., 1299-1303.

Kalyani, G. & Chaudhari, S. 2020. An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *International Journal of Computers and Applications,* 42**,** 306-314.

Kathamuthu, N. D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M. & Gandomi, A. H. 2022. Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application. *Electronics (Switzerland),* 11.

Khan, S., Singh, R., Khan, S. & Ngah, A. H. 2023. Unearthing the barriers of Internet of Things adoption in food supply chain: A developing country perspective. *Green Technologies and Sustainability,* 1**,** 100023-100023.

Kumari, S., Tulshyan, V. & Tewari, H. 2024. Cyber Security on the Edge: Efficient Enabling of Machine Learning on IoT Devices. *Information,* 15**,** 126-126.

Kureshi, R. R. & Mishra, B. K. 2022. A Comparative Study of Data Encryption Techniques for Data Security in the IoT Device. *Lecture Notes in Electrical Engineering.* Springer Science and Business Media Deutschland GmbH.

Lalem, F., Laouid, A., Kara, M., Al-Khalidi, M. & Eleyan, A. 2023. A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques.

Laturkar, K. & Laturkar, K. 2023. Internet of things: Architectures, applications, and challenges. *Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies.* IGI Global.

M, S. S. H., Akshaya, V., Mandala, V., Anilkumar, C., Vishnuraja, P. & Aarthi, R. 2023. Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things. *Measurement: Sensors,* 30.

Mahmood, M. S. & Al Dabagh, N. B. 2023. Blockchain technology and internet of things: review, challenge and security concern. *International Journal of Electrical and Computer Engineering,* 13**,** 718-735.

Makarenko, I., Semushin, S., Suhai, S., Ahsan Kazmi, S. M., Oracevic, A. & Hussain, R. A Comparative Analysis of Cryptographic Algorithms in the Internet of Things. 2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC), 2020/10// 2020. IEEE, 1-8.

Mehta, K., Singh, H., Kumar, Y. & Sidhu, H. S. 2020. Cryptographic Algorithms for Secure Internet of Things. *International Journal of Control and Automation,* 13**,** 1010-1018.

Mirani, A. A., Velasco-Hernandez, G., Awasthi, A. & Walsh, J. 2022. Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. *Sensors,* 22**,** 5836-5836.

Mohammed, M. A. & Wahab, H. B. A. 2024. Enhancing IoT Data Security with Lightweight Blockchain and Okamoto Uchiyama Homomorphic Encryption. *Computer Modeling in Engineering & Sciences,* 138**,** 1731-1748.

Mohan, M., Kavithadevi, M. K. & Jeevan Prakash, V. Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks. Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020, 2020/10// 2020. Institute of Electrical and Electronics Engineers Inc., 295-302.

Mousavi, S. K., Ghaffari, A., Besharat, S. & Afshari, H. 2021a. Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. *Journal of Ambient Intelligence and Humanized Computing,* 12**,** 2033-2051.

Mousavi, S. K., Ghaffari, A., Besharat, S. & Afshari, H. 2021b. Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks,* 27**,** 1515-1555.

Newroz, N. A. 2024. Generating of A Dynamic and Secure S-Box for AES Block Cipher System Based on Modified Hexadecimal Playfair Cipher. *Zanco Journal of Pure and Applied Sciences,* 36**,** 82-94.

Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A. & Biamba, C. 2021. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics (Switzerland),* 10.

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A. & Brown, J. 2020. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers,* 9**,** 44-44.

Ozkan-Okay, M., Akin, E., Aslan, O., Kosunalp, S., Iliev, T., Stoyanov, I. & Beloev, I. 2024. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access,* 12**,** 12229-12256.

Pereira, G. C. C. F., Alves, R. C. A., Da Silva, F. L., Azevedo, R. M., Albertini, B. C. & Margi, C. B. 2017. Performance evaluation of cryptographic algorithms over IoT platforms and operating systems. *Security and Communication Networks,* 2017.

Prabhakaran, V. & Kulandasamy, A. 2021. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection.

Neural Computing and Applications, 33**,** 14459-14479.

Radhakrishnan, I., Jadon, S. & Honnavalli, P. B. 2024. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors,* 24.

Rahman, Z., Yi, X., Billah, M., Sumi, M. & Anwar, A. 2022. Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *Electronics (Switzerland),* 11.

Ranjan, A. K. & Kumar, P. 2024. Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. *Multimedia Tools and Applications*.

Reshi, I. A. & Sholla, S. 2022. Challenges for Security in IoT, Emerging Solutions, and Research Directions. *International Journal of Computing and Digital Systems,* 12**,** 1231-1241.

Sadhu, P. K., Yanambaka, V. P. & Abdelgawad, A. 2022. Internet of Things: Security and Solutions Survey. *Sensors,* 22**,** 7433-7433.

Saini, A. & Sehrawat, R. 2024. Enhancing Data Security through Machine Learning-based Key Generation and Encryption. *Engineering, Technology and Applied Science Research,* 14**,** 14148-14154.

Saleh, M., Jhanjhi, N., Abdullah, A. & Saher, R. IoTES (A Machine learning model) Design dependent encryption selection for IoT devices. International Conference on Advanced Communication Technology, ICACT, 2022. Institute of Electrical and Electronics Engineers Inc., 239-246.

Sarker, V. K., Gia, T. N., Tenhunen, H. & Westerlund, T. Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes. IEEE International Conference on Communications, 2020/6// 2020. Institute of Electrical and Electronics Engineers Inc.

Satyanarayana, P., Sriramdas, N., Madhavi, B., Arun, M., Phani Sai Kumar, N. V. & Gokula Krishnan, V. Enhancement of Security in IoT Using Modified AES Algorithm for IoT Applications. International Conference on Sustainable Communication Networks and Application, ICSCNA 2023 - Proceedings, 2023. Institute of Electrical and Electronics Engineers Inc., 380-386.

Silva, C., Cunha, V. A., Barraca, J. P. & Aguiar, R. L. 2024. Analysis of the Cryptographic Algorithms in IoT Communications. *Information Systems Frontiers,* 26**,** 1243-1260.

Singh, S., Sharma, P. K., Moon, S. Y. & Park, J. H. 2024. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing,* 15**,** 1625-1642.

Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H. & Alkhzaimi, H. A. 2023. Cryptography Algorithms for Enhancing IoT Security. *Internet of Things,* 22**,** 100759-100759.

Thakor, V. A., Razzaque, M. A. & Khandaker, M. R. A. 2021. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access,* 9**,** 28177-28193.

Tidrea, A., Korodi, A. & Silea, I. 2023. Elliptic Curve Cryptography Considerations for Securing Automation and SCADA Systems. *Sensors,* 23.

Tsantikidou, K. & Sklavos, N. 2022. Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare. *Cryptography,* 6**,** 45-45.

Velliangiri, S., Manoharn, R., Ramachandran, S., Venkatesan, K., Rajasekar, V., Karthikeyan, P., Kumar, P., Kumar, A. & Dhanabalan, S. S. 2022. An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography. *IEEE Transactions on Industrial Informatics,* 18**,** 6494-6502.

Velmurugadass, P., Dhanasekaran, S., Shasi Anand, S. & Vasudevan, V. Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Materials Today: Proceedings, 2020. Elsevier Ltd, 2653-2659.

Williams, P., Dutta, I. K., Daoud, H. & Bayoumi, M. 2022. A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things,* 19**,** 100564-100564.

Zhang, L. & Wang, L. 2024. A hybrid encryption approach for efficient and secure data transmission in IoT devices. *Journal of Engineering and Applied Science,* 71.

Zhou, W., Jia, Y., Peng, A., Zhang, Y. & Liu, P. 2019. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal,* 6**,** 1606-1616.

Zhou, X., Xu, K., Wang, N., Jiao, J., Dong, N., Han, M. & Xu, H. 2021. A Secure and Privacy-Preserving Machine Learning Model Sharing Scheme for Edge-Enabled IoT. *IEEE Access,* 9**,** 17256-17265.