Internet of Things: Security, Issues, Threats, and Assessment of Different Cryptographic Technologies

Mostafa Raeisi-Varzaneh[1], Omar Dakkak[1,*], Hashem Alaidaros[2], and İsa Avci[1]

[1]Department of Computer Engineering, Karabük Universitesi, 78050 Karabük, Türkiye
[2]Cybersecurity Department, Dar Al-hekma University, Saudi Arabia
Email: mostafaraeisi1991@gmail.com (M.R-V.); omardakkak@karabuk.edu.tr (O.D.); haidarous@dah.edu.sa (H.A.); isaavci@karabuk.edu.tr (I.A.)
*Corresponding author

***Abstract*—As a network of objects, data, and the Internet, the Internet of Things can be characterized as a collection of interconnected devices. In the context of the Internet of Things, a thing refers to any object, such as a sensor, that forms a network and can transfer data with other devices. This interconnection of devices leads to the convergence of physical and digital domains, thereby enabling time optimization, cost reduction, and enhanced efficiency in human labor. The Internet of Things enables data exchange to monitor and control interconnected devices, manufacturers and operators. A discernible transition from non-IoT to IoT devices has been evident over the past decade. Projections indicate that by 2030, approximately 75% of all devices will be integrated into the IoT. Consequently, these devices generate a substantial influx of data, commonly called Big Data. Unlike traditional computing systems, IoT devices operate in diverse, often resource-constrained environments, making them susceptible to weak authentication, insecure communication, physical vulnerabilities, data privacy risks, DoS attacks, malware propagation, and interoperability issues. These concerns can lead to data breaches, unauthorized access, and system disruptions. Cryptography offers an efficacious means of bidirectional data transmission that can enhance the security of IoT devices and the data they transmit and store, employing authentication and key management, encryption, message integrity and authentication, and Post-Quantum cryptography. This manuscript comprehensively examines the security predicaments of the Internet of Things and illustrates the effectiveness of cryptographic methodologies in ameliorating these concerns. This research not only contributes to a comprehensive understanding of existing cryptographic techniques in IoT security but also offers a forward-looking perspective that can guide future research efforts and inform practical implementations.**

***Keywords*—IoT security, cryptography, systematic key algorithms**

I. Introduction

Agriculture, industry, and information technology are the initial triad of historical milestones in human development. The advent of these waves has brought about a substantial transformation in the overall standard of human life. Renowned experts in the global field of information technology concur that the Internet of Things (IoT) embodies the fourth wave of substantial economic and technological progress after the Internet. The IoT network comprises a set of information-sensing devices that engage in communication and information exchange via the Internet [1, 2]. With the remarkable progress achieved, all communication requirements can be met promptly, requiring minimal human intervention, facilitated seamlessly via the IoT. By integrating Artificial Intelligence (AI) and cloud computing, the IoT presents a diverse array of intelligent applications capable of substantially enhancing our overall standard of living [3]. Notably, the IoT facilitates the development of smart homes [4], healthcare systems [5], laboratories [6], industries [7, 8], and smart cities [9, 10].

In 1999, Kevin Ashton [11] introduced what is now known as the IoT as an idea, a concept that creates a network interconnected with real-world sensors, electronic devices, and systems.

The IoT is defined by the Institute of Electrical and Electronics Engineers (IEEE) [12] as a complex, self-configuring, adaptive network that connects various devices to the internet through standard communication protocols. There are interconnected things which are programmable and uniquely identifiable with physical or virtual representations, sensing, and actuation capabilities. In addition to its identity and status, an object's representation includes its location and any information relevant to its private, social, or business life. Things offer services to consumers with or without human involvement by capturing data, communicating, and actuating sensors. The provision of these services is facilitated by intelligent

Manuscript received January 9, 2023; revised March 1, 2023; accepted September 1, 2023; published February 10, 2024.

interfaces, ensuring accessibility from any location, at any time, and for any purpose, while ensuring security.

As smart devices such as sensors and actuators become more connected, the IoT is forming. In addition to their use in smart cities, smart homes, intelligent transportation systems, etc., these devices can also be used in environmental and public health monitoring. A visual representation of the IoT architecture is illustrated in Fig. 1.

The widespread presence of the IoT and its associated interactions, coupled with robust Quality of Service (QoS) implementations [13], will offer individuals convenience and invaluable services. Nevertheless, it will concurrently expose numerous vulnerabilities concerning security and privacy [14]. Without establishing trust and ensuring interoperability within an IoT ecosystem, the anticipated level of demand for emerging IoT applications may remain unattainable. Along with the challenges associated with Internet, wireless, cellular networks, as well as cloud and grid environments [15], the Internet of Things also faces significant security and privacy concerns [16–18].

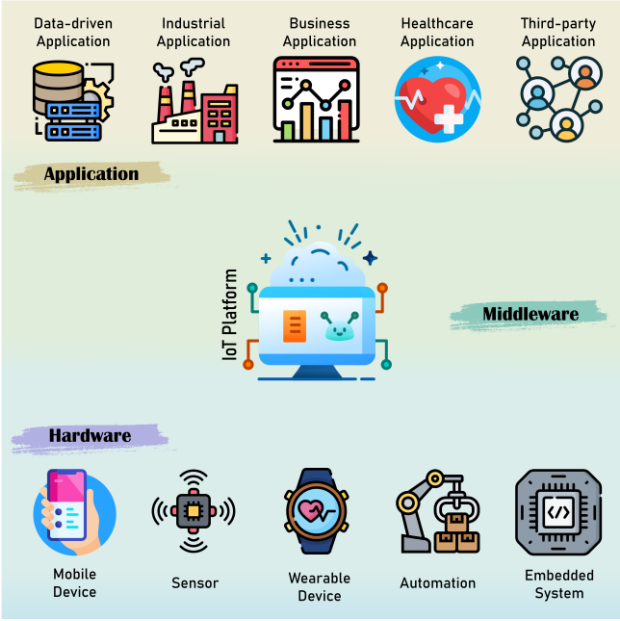

Fig. 1. Simple architecture for IoT platform.

Additionally, the IoT enables remote monitoring and control of objects worldwide [19]. Consequently, significant apprehensions persist regarding the security and privacy of IoT, giving rise to novel challenges concerning the online confidentiality of data sensed, gathered, and shared by IoT devices [20, 21]. That is because rather than merely collecting information such as names and phone numbers, these devices are also capable of monitoring their users' activities [18]. Due to its resource-constrained nature and the use of low-bandwidth channels, IoT is also susceptible to several security attacks, including DDoS [22], as explained by Doshi *et al.* [23], resulting in an insecure environment. Cyber threats and intrusions can be identified and interpreted using real-time analysis of High-Performance Computing systems (HPC) [24–26].

Security and privacy-aware IoT technologies have significant practical implications across diverse sectors. Assuring data integrity, protecting sensitive patient data, and enabling remote monitoring are some of the benefits of these technologies in healthcare [27]. In smart homes, they enhance security through encrypted data transmission and user access control [28]. In smart cities [29], they ensure the security of critical infrastructure, maintain privacy in public spaces, and empower citizens by giving them control over data sharing [30]. Crop monitoring, resource management, and supply chain security are all made possible through these technologies [31]. Lastly, these technologies improve road safety in Vehicular Adhoc Networks (VANETs) by improving vehicle communication, preserving privacy in location information, and preventing unauthorized software updates [32, 33]. These implications underscore the importance of integrating security and privacy measures for responsible and effective IoT implementation across various domains.

Cryptography has played a pivotal role in enhancing network and internet security for numerous decades. Cryptography serves as a formidable safeguard for shielding and concealing sensitive data and information, effectively thwarting any unauthorized entities or collectives from gaining illicit access to it [34]. It makes data exchange and secure communications possible in typical networks.

This paper proceeds as follows: Section II introduces the essential domains of IoT security. Section III investigates the pragmatic implementations of cryptography within the IoT framework, encompassing exhaustive scrutiny and assessment of diverse cryptographic methodologies. A thorough review of 35 survey papers is presented in Section IV to gain insights into the challenges, future directions, open issues, and perspectives underlying IoT cryptographic research. Finally, a conclusive summary is presented in Section V.

II. IoT Security

IoT offers numerous advantages that profoundly reshape our lifestyles. By optimizing efficiency, conserving valuable time and resources, and fostering unprecedented prospects for advancement, it contributes significantly to societal progress. However, the expansive network of interconnected entities within the IoT also introduces new cyber threats, which pose significant risks to the security, privacy, and trust of all devices connected to this network [35]. IoT devices face unique security challenges, including limited resources affecting robust security implementation, inadequate authentication and authorization, and weak data privacy measures. They are also associated with a lack of regular updates and patches, potential for network-wide breaches due to interconnected networks, physical security vulnerabilities, user awareness gaps, ecosystem diversity hindering standardized security measures, susceptibility to Denial of Service (DoS) attacks, risks of firmware and supply chain compromise, and a rapidly evolving threat landscape. In the era of digital advancements, ensuring the security of the IoT platform and devices necessitates incorporating measures to counteract physical tampering and information-based attacks, encrypt data transmissions, and effectively address prevailing challenges. Hence, the

IoT is progressively acknowledged as an emerging vulnerability that could be subjected to intrusions. It is imperative to safeguard IoT components to guarantee the preservation of data, sensors, and interfaces in a confidential, secure, and authentic manner. The critical security objectives are represented in the context of Confidentiality, Integrity, and Availability (CIA) which necessitate comprehensive consideration in every security framework [36, 37].

A. Confidentiality

Data security is crucial, and data access should be restricted to unauthorized users. A high level of confidentiality allows the data to be available only to authorized users throughout the process and prevents nonauthorized parties from eavesdropping or interfering. Since many measurement devices are integrated into the IoT, confidentiality is a critical security principle. Therefore, guaranteeing that the measurement apparatuses maintain strict confidentiality of sensitive data from neighboring devices is imperative [38].

The management of data is another issue relating to confidentiality. It is imperative for users of the IoT to have comprehensive awareness regarding the mechanisms employed for data management, identification of accountable entities, and proactive measures they can adopt to guarantee the security and confidentiality of their data [39]. To attain elevated levels of confidentiality, it is critical to develop enhanced techniques, such as secure key management mechanisms [40].

B. Integrity

In the present age of big data, enterprises and individuals are amassing substantial volumes of information, particularly with the advent of the IoT [41]. Ensuring the accuracy of data and its credible origin, along with uninterrupted transmission devoid of intentional or unintentional tampering, is paramount. Data integrity encompasses the crucial aspects of upholding and guaranteeing the accuracy and consistency of data throughout its lifecycle [42]. Basically, it is the ability to establish the reliability of the data, i.e., ensuring that it has not been tampered with, altered, or modified [43]. Integrity compromises may result in serious adverse consequences. For example, medical devices, such as insulin pumps and pacemakers, may be the subject of integrity attacks that have potentially life-threatening consequences [44]. Ensuring end-to-end security can effectively uphold the integrity feature of IoT communication. However, the limited computational power of IoT nodes poses a challenge in providing adequate security measures, despite the implementation of firewalls and protocols for managing data traffic [45].

C. Authentication

Authentication is regarded as a critical requirement for the IoT [46]; A well-functioning IoT network relies on the trustworthiness of its participants. Compromises may result in a malicious node causing damage to the entire system or even catastrophic events [47]. Therefore, a network's authentication process is required to verify the identity of legitimate users and devices [48]. This process, however, may be challenging because of IoT's nature; there are many entities involved, and there are also times when objects must interact for the first time (with objects they are unfamiliar with) [49]. Consequently, every interaction in the IoT requires a mechanism for authenticating entities.

III. Cryptography

Letters are commonly transmitted within sealed enclosures. People often respond to why questions with comments like ‘I do not know, or ‘why not? The more reasonable response would be ‘to prevent the letter from falling out’ or ‘to prevent people from reading it’. The contents of our correspondence may not include sensitive or extremely confidential data. However, we believe that the envelope protects it from everyone but the recipient, even if the letters do not include sensitive or extremely confidential data. Letters sent in unsealed envelopes may be read by anyone who gets their hands on them. In addition, we would not be aware of the replacement of the letter in the envelope [50–53].

Assume two people communicate over the Internet but cannot see one another. The identities of the parties cannot be established immediately in that case. However, message recipients over a network may have to confirm that they know the sender's identity and that their message is the same as the one sent by the originator. Additionally, the recipient must ascertain that no subsequent messages can be falsely attributed to the sender. Addressing these critical concerns necessitates substantial efforts. Traditional non-automated business environments often rely on handwritten signatures to alleviate these apprehensions. The contemporary security landscape presents a pressing issue of identifying “digital counterparts” for social mechanisms that have been forsaken during the shift towards digital transactions, notably encompassing face-to-face authentication and handwritten endorsements. This predicament can be effectively addressed through the utilization of cryptography [34].

Over the past three decades, cryptography has undergone considerable evolution. A broader range of applications has been possible thanks to technological advancements. The pervasive influence of this technology extends to every individual, whether directly or indirectly. Thus, a comprehensive understanding of its functionality and operational principles becomes imperative.

Data is exchanged between two devices during communication, potentially encompassing personal and confidential information. [54]. To ensure secure transmission, it is imperative to employ encryption for safeguarding such sensitive data as it traverses from one device to another [55]. Enhanced data security is achieved by implementing encryption, which employs cryptographic techniques to transform plain text into unintelligible form, bolstering safeguards against intruders [56]. Cryptography aims to achieve four fundamental objectives: authentication, confidentiality, integrity, and nonrepudiation [57, 58].

The technique of cryptography is a well-established, secure method for transmitting information and

communicating data, which relies on mathematical concepts and a set of algorithm-based calculations. The message (cipher) is transformed in several ways so that it is not easily decipherable [59].

The foundations of contemporary cryptography lie in the fundamental disciplines of mathematics and computer science. Cryptographic algorithms built upon the foundation of hardness computation assumption possess an impervious nature, rendering them impregnable to any potential adversary. Despite the theoretical possibility of breaching their security, the system's robust design has effectively thwarted any attempts to compromise. The term computationally secure is therefore used to describe these schemes [60].

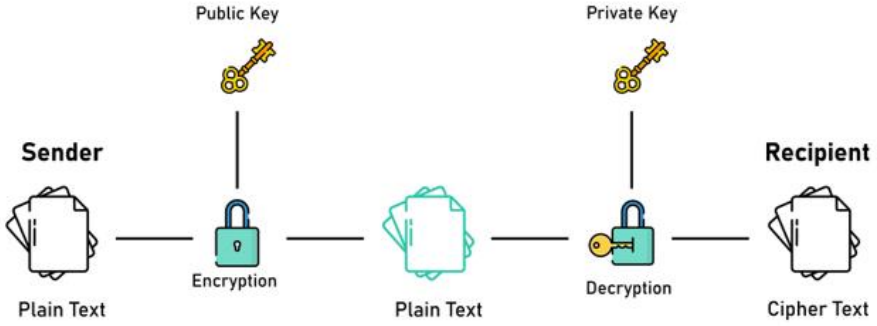

Fig. 2. Public key cryptographic system.

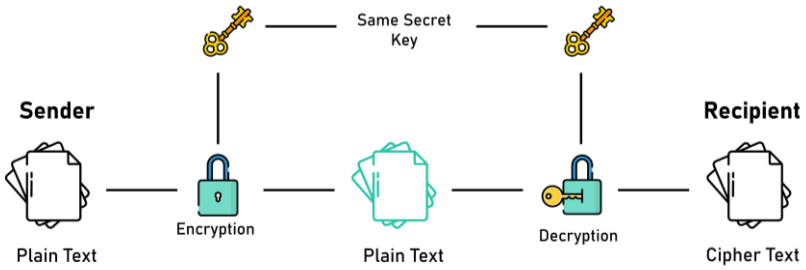

Fig. 3. Symmetric cryptographic system.

In this section, we provide a comprehensive overview of several prominent cryptosystems. Notably, these cryptosystems have undergone significant refinements since their initial conception. Regrettably, this manuscript cannot encompass the latest advancements in this domain due to its intricate and specialized nature.

A. Public Key

Introducing public key cryptography was a seminal contribution made by Diffie and Hellman [61]. Since its inception, pursuing an efficient and feasible public key system has remained a persistent endeavour, driving the research community to explore novel solutions and advancements. In public-key cryptography, it is a prevailing practice to employ a dual set of cryptographic keys: the public key, which divulges the confidentialities of a cryptographic framework, and the private key, which remains exclusively accessible to its rightful owner [62]. The public key cryptographic system is illustrated in Fig. 2.

There is a computational challenge involved in retrieving private keys from public keys [63]. Authentication and encryption can be achieved with this mechanism [64]. Public Key systems that are most known are listed here:

- RSA: Presently recognized as one of the most extensively employed cryptographic systems for ensuring secure data transmission [65], Rivest *et al.* [66] developed one of the first public key cryptosystems. RSA, a prevalent form of asymmetric encryption, is widely employed to safeguard sensitive information, particularly during transmission over unreliable networks, such as the Internet [67]. In this cryptosystem, two prime numbers are factorized to increase the factorization's difficulty. According to Peter [68], a quantum computer can break RSA in polynomial time. The RSA cryptographic protocol facilitates the safeguarding, integrity, authenticity, and non-repudiation of entities such as digital transactions and data aggregation.
- ELGAMAL: The ElGamal encryption scheme, formulated by Taher Elgamal in 1985, emerged from the principles of Diffie-Hellman key exchange [69] [62]. The process of encryption and decryption involves the utilization of distinct cryptographic keys. By disseminating the receiver's publicly available encryption key, any individual possessing it can securely transmit confidential messages to the intended recipient. This encryption key is openly accessible through a public directory. To decrypt the ciphertext, the recipient employs their private deciphering key. ElGamal encryption is employed by contemporary versions of PGP or GNU Privacy Guard.
- Elliptic Curve Cryptography (ECC): Using elliptic curves over finite fields in the ECC technique is an encryption method for public keys [70]. Independently proposed in 1985 by Neal Koblitz and Victor Miller

[71], ECC cryptography employs smaller keys than non-ECC cryptography while maintaining an equivalent level of security. This approach offers numerous advantages, including diminished key sizes, reduced bandwidth requirements, and accelerated implementations. These benefits make ECC particularly appealing for security applications in small devices, such as those encountered in the IoT realm [72]. Furthermore, ECC is founded upon the NP-Hard problem of Elliptic Curve Discrete Logarithm [73].

TABLE I. COMPARISON OF SYMMETRIC-KEY ALGORITHMS

	Block Size	Key Length	Round(s)	Year	Security Level	Vulnerabilities
DES	64 bits	56 bits	16	1975	Not secure enough	Brute force, Man-in-the-middle attacks
3DES	64 bits	112 or 168 bits	48	1978	Adequate security	Theorical attacks
AES	128 bits	128/192/256 bits	10/12/14	2001	Excellent security	Side channel attacks
PRESENT	64	80/128	31	2007	Adequate security	Differential power analysis attacks

B. Symmetric

Symmetric-key algorithms enable the encryption and decryption of messages using identical keys [74]. To ensure the safeguarding of confidential data, the encryption keys are exchanged covertly between the involved parties [75]. Fig. 3 illustrates the fundamental configuration employed in symmetric encryption. Symmetric techniques follow a self-certification methodology, in which the key is certified by itself [76]. It is imperative to share the key secretly. An attacker can easily decrypt an encrypted message if it has been compromised. In addition to providing faster service, this type of cryptographic technique requires few resources to implement. In the following list, we will discuss popular symmetric cryptosystems:

- Advanced Encryption Standard (AES): In January 1997, the National Institute of Standards and Technology (NIST) initiated the AES project, brought into being through the collaboration of Vincent Rijmen and Joan Daemen [77]. AES is a subset of the Rijndael cipher. Encryption and decryption operations can be carried out using a minimum block size of 128 bits, demonstrating superior resilience compared to the DES algorithm. The process commences with byte substitution, followed by row shifting, column mixing, and the final addition of the round key. This cryptographic system can safeguard information of varying sensitivities, encompassing classified and unclassified data.
- Data Encryption Standard (DES): In the 1970s, IBM pioneered the development of a cutting-edge algorithm that operates efficiently on 64-bit blocks [78]. A total of 16 stages are involved in the encryption process, consisting of eight S-Boxes [79]. Initially, a bit shuffling procedure is executed as the primary stage, which is subsequently succeeded by nonlinear substitutions. A pivotal XOR operation is then performed to yield the desired outcome, combining a subkey with the result of a particular round. Notably, the reversal of subkeys occurs in the decryption process.
- Triple Data Encryption Standard (3DES): In essence, this algorithm represents an upgraded iteration of the DES algorithm, boasting a considerably robust key length of 192 bits, thereby ensuring exceptional reliability [80]. The initial step involves partitioning a key into three different subkeys comprising 64 bits. Apart from the occurrence of this partitioning process, the subsequent procedure follows an indistinguishable methodology from that of the DES algorithm [81]. Data is subjected to encryption and decryption procedures utilizing the first and second keys correspondingly. Subsequently, after the data has been decrypted, it is again encrypted using a third key. However, there is not much potential for long-term data protection.
- PRESENT: PRESENT [82] stands out as the most compact option, renowned as an extensively favoured 64-bit block cipher of the lightweight category [83]. Its exceptional popularity among IoE systems is a testament to its widespread adoption and utilization [84]. It makes use of a 64-bit block size and an 80-bit or 128-bit key size in the PRESENT algorithm [85]. PRESENT was developed to attain the utmost power efficiency and chip effectiveness. Nevertheless, this lightweight cryptographic algorithm fails to offer sufficient security measures for devices possessing constrained computational capabilities [86].

Table I presents a comprehensive theoretical analysis of the block size, key length, and number of rounds for the DES [87], 3DES [88], AES [89], and PRESENT [90] encryption algorithms.

C. Squantum and Post-quantum

Applying quantum mechanics in cryptographic protocols offers a promising solution for achieving secure communication. Unlike traditional public-key algorithms, it is believed to resist quantum computer attacks. To gain a comprehensive understanding of the vulnerability of current classical cryptosystems, it is crucial to recognize that their fragility poses a more significant and realistic threat in the future rather than merely a potential threat. Presently, eavesdroppers can intercept encrypted messages that cannot be deciphered. However, these intercepted

communications can be stored and decrypted later when a sufficiently powerful quantum computer becomes available. Consequently, the confidentiality of messages can only be maintained for a brief period [91]. Different approaches are now being used in post-quantum cryptography research:

- Hash-based cryptography: Hash functions that deliver security, such as SHS (Secure Hash Standard), are constructed as cryptographic primitives [92].
- Multivariate cryptography: The use of polynomials over finite fields as a basis for cryptographic systems.
- Lattice-based cryptography: The computational challenge known as the Shortest Vector Problem involved post-quantum algorithms, which is difficult to solve even with quantum computers [93].
- Code-based cryptography: Various cryptographic schemes incorporate diverse error-correcting codes, including but not limited to McEliece's encryption algorithm, Niederreiter's encryption algorithm, and the Courtois, Finiasz, and Sendrier signature schemes. McEliece's public key encryption system presents a viable approach for safeguarding data against quantum computer attacks [94].
- Super singular elliptic curve isogeny cryptography: Super singular elliptic curves are used in this cryptographic system to replace Diffie-Hellman encryption [95]. To the best of our knowledge, no patent has been identified for this cryptographic system.

D. Attribute-Based

Attribute-Based Encryption (ABE) is a contemporary form of public-key encryption that leverages attributes to establish the user's secret key and ciphertext. As an illustration, geographical factors such as the individual's city or country of residence can be employed to encode information. The decryption process necessitates matching attributes between the user key and the ciphertext [96]. ABE presents a potent approach for facilitating versatile, precise, and nuanced data access control policies by integrating conditional statements or regulations grounded on attributes such as features, descriptors, or metadata [97].

E. Broadcast

The utilization of broadcast encryption enables the transmission of encrypted data through a broadcast medium, such as a Television Series. Consequently, the decryption process is restricted to authorized users or subscribers [98–100]. One of the challenges lies in altering the designated recipients for every transmitted emission. It is imperative to develop a broadcast transmission system that enables the revocation of individual users' access without disrupting the activities of those still actively engaged.

F. Secret Sharing

Participants distribute secrets among themselves in secret sharing, each receiving a share [72]. Combining enough shares will allow the secret to being reconstructed [101]. Highly sensitive and important information can be stored using secret sharing schemes. Bank accounts numbers, encryption keys, and launch codes are a few examples.

An overview of the threats facing IoT devices and the cryptography techniques that can help solve them is provided in Table II.

IV. Challenges and Future Directions

IoT applications are found across a broad range of areas, such as industries, healthcare, and everyday household use. Automated objects can be easily integrated with this technology, making them desirable to a broad audience. Due to the substantial reliance on data in many of these applications, the risk of potential attacks is elevated. Therefore, scholars are actively exploring emerging trends in IoT security and potential future directions for cryptographic technologies. A comprehensive analysis of 35 survey papers has been conducted to understand the challenges, future directions, open issues, and perspectives they hold on the present landscape of cryptographic research in the IoT. Compiling relevant survey articles is accomplished by utilizing digital libraries such as IEEE Xplore, ScienceDirect, Springer, MDPI, Taylor & Francis, Hindawi, and Wiley online library. To gather sufficient literature for this review, specific criteria for inclusion and exclusion were developed. Dismissals were detected after the initial screening, and any discrepancies among authors were resolved. Subsequently, the publications collected were scrutinized to improve overall study quality. Detailed information about the selection review process, search criteria, databases, and inclusion and exclusion criteria is presented in Table II.

TABLE II. Review Methodology, Databases, Inclusion and Exclusion Criterion

Publications	**Journal articles** **Transaction papers**
Year	2020 – 2023
Keywords	Internet of Things (IoT) Security Cryptography Cybersecurity Cryptographic Algorithms Encryption
Digital libraries	https://www.sciencedirect.com/ https://ieeexplore.ieee.org/Xplore/home.jsp https://www.springer.com/ https://onlinelibrary.wiley.com/ https://www.mdpi.com/ https://www.tandfonline.com/ https://www.hindawi.com/
Inclusion Criterion	English papers Systematic literature reviews published after 2020 Informal literature surveys Conference, symposium, and workshop papers
Exclusion Criterion	Articles not clearly specifying the use of cryptographic algorithms in IoT Publications in low impact factor journals Short review articles

Based on an extensive review of the collected papers, 11 key areas were identified that represent open issues and potential directions for further investigation and development in the field of IoT cryptographic systems:

Lightweight Cryptography: Small and limited resources are common characteristics of many IoT devices, such as sensors and RFIDs. For instance, insufficient memory for application storage and execution, constrained

battery power, and limited computing capabilities for data processing. Moreover, since most IoT applications are real-time in nature, it is challenging to maintain robust security while providing prompt and accurate responses. Conventional cryptographic algorithms, initially designed for standard computing devices like personal computers, cannot be directly implemented in IoT systems. Specifically tailored for the resource-constrained environment of the IoT, lightweight cryptography has emerged as a promising alternative to traditional cryptography [102]. A security mechanism can be made lighter by simplifying the key generation algorithm, offloading some computations to the edge layer, or reducing the complexity of the round function. To achieve optimal performance, lightweight cryptography (LWC) algorithms must strike a balance between cost, implementation complexity, and security level. While it is feasible to manage a trade-off between any two of these factors, achieving equilibrium among all three poses a significant challenge. Consequently, various open research issues in LWC algorithm development await effective solutions.

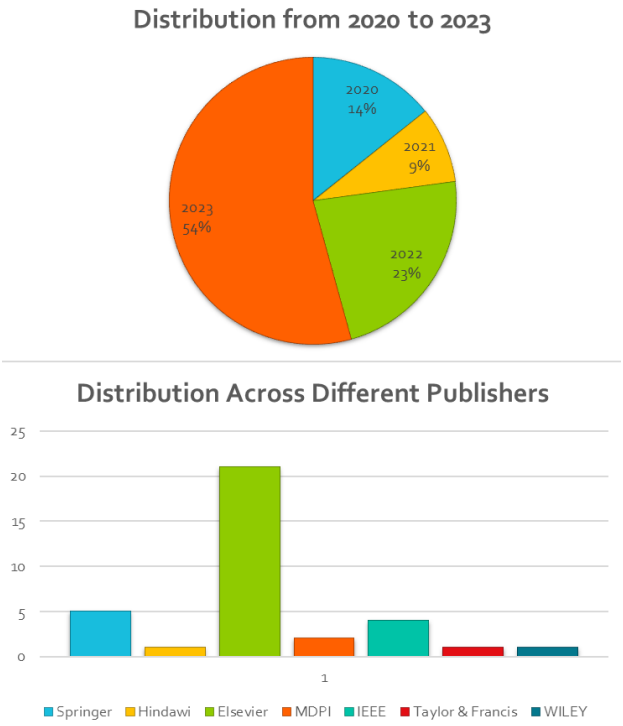

Fig. 4. Survey articles distribution.

Post-Quantum Cryptography: Research and development are currently underway in the field of post-quantum cryptography [103, 104]. Cryptographic algorithms based on classical algorithms are at risk of being insecure because of the arrival of quantum computers, which perform complex calculations in polynomial time. The Shor algorithm, for instance, is a quantum computer algorithm that finds prime factors in polynomial time for a given number. Therefore, asymmetric cryptography can be broken since it is based on integer factorization. In the era of quantum computing, traditional cryptographic tools are susceptible to attack, requiring the creation of post-quantum cryptographic tools [105]. A post-quantum solution will be required to combat quantum computing's approaching threats. Researchers should identify and address potential security vulnerabilities in quantum cryptography systems and develop countermeasures that can handle evolving threats.

Integrating IoT, cloud, and edge: Cloud computing is gaining popularity because it offers advantages such as lower costs, impressive scalability, and 24/7 availability [106]. IoT utilizes both cloud and edge computing to meet diverse security requirements [107]. IoT users can access real-time and time-sensitive services via collaborative edge nodes. While edge computing addresses a variety of limitations, including bandwidth consumption, resource constraints, and latency issues, it can also lead to malicious activity on edge nodes and IoT devices if data privacy and intrusion detection measures are not adequate. In recent years, research has focused on the integration of cloud, edge, and IoT to establish secure device identity, ensure data provenance, and implement decentralized access control. Nevertheless, this area needs to be improved in terms of scalability and energy efficiency.

Heterogeneity of IoT Environment: IoT can connect various entities, spanning from low-power RFID tags to robust servers. With billions of interconnected smart devices operating across different platforms, users face unprecedented challenges, including security [108]. Using static cryptographic mechanisms across all types of users and entities proves ineffective, requiring device-specific parameters to be incorporated when implementing security measures. An attestation protocol must accommodate the vast array of IoT devices, which encompass varying hardware and software configurations.

Scalability: Millions of IoT devices are expected to be interconnected by 2025. The cryptographic infrastructure needs to demonstrate its ability to handle an expanding amount of data and transactions securely and efficiently as the IoT network continues to grow. Cryptographic protocols must be scalable to meet the requirements of a rapidly growing network without compromising performance or security. In existing literature, various cryptographic schemes are often described as scalable [109]; however, practical observations reveal that these claims are only sometimes valid in reality.

Standardization: Through accurate encryption and decryption mechanisms, cryptographic technology continues to evolve, ensuring precise privacy and data protection. It is nevertheless challenging to integrate security protocols seamlessly across diverse IoT sectors due to an absence of standardized practices. Various IoT devices utilize unstructured data stored in a variety of database formats (such as NoSQL (Non-relational Structured Query Language)) using different querying methods, leading to contradictions across different systems [110]. Government agencies, including Homeland Security, NIST, and ENISA (European Union Agency for Cybersecurity), actively develop regulations and guidelines for safeguarding the public [111]. IoT's evolving landscape however, remains in conflict with existing regulations like GDPR (General Data Protection Regulation).

Fig. 5. Future research horizons: A sunburst map of hot topics.

Performance and security balance: Cryptographic algorithms must strike a proper balance between cost, performance, and security. Therefore, planning fast, straightforward, yet robust diffusion and confusion properties is crucial [112]. A smaller number of S-boxes need to be used to reduce memory consumption and computing power while providing adequate protection. Nevertheless, it remains an exciting research question how to create a robust S-box using different confusion techniques while maintaining acceptable security and minimizing overhead.

Ai-based cryptography: The continuous advancement of artificial intelligence, machine learning, and blockchain technology is also creating promising solutions for securing the IoT. The robustness, adaptability, and flexibility of AI methods may improve the performance of security solutions. Their drawbacks, however, include high computing costs, complexity, and the need for frequent updates. It is vital to investigate how AI techniques, such as machine learning and neural networks, can be integrated into IoT cryptography. Integration of these technologies could facilitate the development of adaptive, self-learning security mechanisms that can identify and neutralize threats in real-time [113].

Randomness: Random Number Generator (RNG)s have a significant impact on cryptographic techniques for IoT devices [114], directly affecting their security. IoT networks depend heavily on RNGs to generate cryptographic keys, initialization vectors, and nonces, which ensure confidentiality, integrity, and authenticity of data. Flawed or predictable random number generation processes can compromise IoT devices. The resource constrained IoT devices make implementing robust RNGs more challenging.

Energy Efficiency: IoT devices generally operate on small batteries or they are even battery-less. Therefore, using cryptography or learning-based security solutions is nearly impossible [115]. Protecting those devices is a challenging task, and many researchers focus on the energy efficiency of such devices to improve the harvesting efficiency, thus having more energy for their security or application needs. There is still a need to explore energy-harvesting techniques and energy-efficient protocols that enable cryptographic operations while not significantly depleting the device's limited energy resources. Cryptographic computations can be optimized by integrating renewable energy sources or increasing energy efficiency.

Software Defined Networking: Software-defined networking (SDN) is an emerging computing concept that separates routing decisions made by network elements (e.g., routers, switches, and gateways) from the forwarding process [116]. SDN exposes a powerful tool for adaptive and intelligent security policies, enabling programs to control forwarding devices and collect data from connected devices. Researchers have primarily focused on software-based solutions for IoT security. However, in recent years, hardware-based solutions have started to gain popularity in the world of IoT security.

As depicted in Fig. 5, the sunburst map represents 11 critical areas of future research directions based on a Comprehensive analysis of 35 survey papers. To depict the urgency or 'hotness' of each topic, a color spectrum from dark red to dark green is used. There is an interesting

correlation between the varying hues and how frequently each topic was discussed in the surveyed papers, with the deepest red hues highlighting the most pressing and widely debated research areas and the darkest green hues indicating directions for future investigation that have been relatively less discussed. This visualization provides a comprehensive overview of the landscape of unresolved issues and guides the focus for upcoming research endeavors.

V. Conclusion

In distributed systems such as the IoT, data preservation, communication confidentiality, and integrity have conventionally been prioritized. However, the vast diversity of IoT applications, ranging from LED bulbs to complex industrial supply chains, significantly amplifies the potential risk landscape associated with this technology. This realm encompasses integrity, commitment, availability, privacy, suitability, non-repudiation, and trust, all of which are reinforced by security technologies, such as cryptography. This paper has provided a comprehensive analysis of cryptographic systems in the context of IoT security. Most widely used mentioned cryptographic algorithms were not initially conceived to accommodate devices with specific limitations, such as restricted storage capacity, limited computational capabilities, or small battery. Cryptography algorithms in IoT devices pose challenges due to the extensive computational requirements, demanding the storage of large amounts of data or keys. Developing new cryptographic protocols that balance security and computational overhead is essential. A further consideration will be the exploration of post-quantum cryptographic algorithms and techniques to ensure long-term security as quantum computing technologies become more prevalent. Moreover, integrating blockchain technology with cryptographic systems can enhance transparency and tamper resistance for IoT deployments.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Analyzing, reviewing, and writing the original draft, Mostafa Raeisi-Varzaneh; Supervising, reviewing, editing, and coordinating, Omar DAKKAK; Funding and reviewing, Hashem Alaidaros; Research idea, İsa AVCI. All authors have read and agreed to the published version of the manuscript.

References

[1] J. Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, *Towards the Internet of Things*, Springer, 2020.

[2] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[3] W. K. Lee, K. Jang, G. Song, H. Kim, S. O. Hwang, and H. Seo, "Efficient implementation of lightweight hash functions on gpu and quantum computers for iot applications," *IEEE Access*, vol. 10, pp. 59661–59674, 2022.

[4] A. H. Sodhro *et al.*, "Toward convergence of AI and IoT for energy-efficient communication in smart homes," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9664–9671, 2020.

[5] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE access*, vol. 3, pp. 678–708, 2015.

[6] M. Chen *et al.*, "Wireless AI-powered IoT sensors for laboratory mice behavior recognition," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 1899–1912, 2021.

[7] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on* industrial *informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[8] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE transactions on industrial informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[9] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[10] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE* Internet *of Things journal*, vol. 1, no. 1, pp. 22–32, 2014.

[11] K. Ashton, "That 'internet of things' thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[12] B. Russell and D. V. Duren, *Practical Internet of Things Security*. Packt Publishing Ltd, 2016.

[13] O. Dakkak, S. A. Nor, S. Arif, and Y. Fazea, "Improving QoS for non-trivial applications in grid computing," *Emerging Trends in Intelligent Computing and Informatics: Data Science, Intelligent Information Systems and Smart Computing*, Springer, pp. 557–568, 2020.

[14] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, 2014.

[15] O. Dakkak, A. S. C. Mohamed Arif, and S. A. Nor, "A critical analysis of simulators in grid," *Jurnal Teknologi*, vol. 77, no. 4, pp. 111–117, 2015.

[16] O. Dakkak, S. Arif, and S. A. Nor, "Resource allocation mechanisms in computational grid: A survey," *Asian Research Publishing Network (ARPN)*, vol. 10, 2015.

[17] M. N. Hindia, A. W. Reza, O. Dakkak, S. Awang Nor, and K. A. Noordin, "Cloud computing applications and platforms: A Survey," 2014.

[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[19] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad, "A review of data security and cryptographic techniques in IoT based devices," in *Proc. 2nd International Conference on Future Networks and Distributed Systems*, 2018, pp. 1–9.

[20] J. M. Carracedo *et al.*, "Cryptography for security in IoT," in *Proc. 2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pp. 23–30, 2018.

[21] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE *Internet of things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[22] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[23] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *Proc. 2018 IEEE Security and Privacy Workshops (SPW)*, pp. 29–35, 2018.

[24] O. Dakkak, Y. Fazea, S. A. Nor, and S. Arif, "Towards accommodating deadline driven jobs on high performance computing platforms in grid computing environment," *Journal of Computational Science*, vol. 54, p. 101439, 2021.

[25] O. Dakkak, S. A. Nor, and S. Arif, "Proposed algorithm for scheduling in computational grid using backfilling and optimization techniques," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 8, no. 10, pp. 133–138, 2016.

[26] O. Dakkak, S. A. Nor, and S. Arif, "Scheduling through backfilling technique for HPC applications in grid computing environment," in

Proc. 2016 IEEE Conference on Open Systems (ICOS), 2016: IEEE, pp. 30–35.

[27] S. P. Amaraweera and M. N. Halgamuge, "Internet of things in the healthcare sector: overview of security and privacy issues," *Security, Privacy and Trust in the IoT Environment*, pp. 153–179, 2019.

[28] A. Yang, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu, "Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2521–2530, 2019.

[29] M. Alsamman, Y. Fazea, F. Mohammed, and M. A. Kehail, "Fog Computing in Smart Cities: A Systematic Review," in 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2023: IEEE, pp. 1-8.

[30] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," *Journal of advanced research*, vol. 5, no. 4, pp. 491–497, 2014.

[31] G. Witjaksono, A. A. Saeed Rabih, N. b. Yahya, and S. Alva, "IOT for agriculture: food quality and safety," in *Proc. IOP Conference Series: Materials Science and Engineering*, vol. 343, 2018.

[32] O. Dakkak, S. A. Nor, M. S. Sajat, Y. Fazea, and S. Arif, "From grids to clouds: Recap on challenges and solutions," in *Proc. AIP Conference Proceedings*, no. 1, 2018.

[33] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "Vppcs: Vanet-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.

[34] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," in *Proc. 2017* international *Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 887–890, 2017.

[35] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. 2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180–187, 2015.

[36] H. Damghani, H. Hosseinian, and L. Damghani, "Cryptography review in IoT," in *Proc. 2019 4th* Conference *on Technology In Electrical and Computer Engineering (ETECH2019)*, 2019.

[37] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, 2017.

[38] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1–7, 2015.

[39] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[40] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.

[41] M. M. Rathore, A. Paul, A. Ahmad, and G. Jeon, "IoT-based big data: From smart city towards next generation super city planning," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 13, no. 1, pp. 28–47, 2017.

[42] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. 2017 IEEE International Conference on Web Services (ICWS)*, pp. 468–475, 2017.

[43] M. N. Aman, B. Sikdar, K. C. Chua, and A. Ali, "Low power data integrity in IoT systems," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3102–3113, 2018.

[44] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[45] T. N. Minh, "Confidentiality and integrity for IoT/mobile networks," *Recent Trends in Communication Networks*, p. 25, 2019.

[46] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[47] M. E. Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, 2019.

[48] T. Nandy *et al.*, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054-151089, 2019.

[49] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[50] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Proc. 2012 International Conference on Computer Science and Electronics Engineering*, vol. 3, pp. 648–651, 2012.

[51] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the internet of things," *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.

[52] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: A security framework for the internet of things," *Security and communication networks*, vol. 9, no. 16, pp. 3083–3094, 2016.

[53] F. Piper and S. Murphy, *Cryptography: A very Short Introduction*, Oxford Paperbacks, 2002.

[54] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73–80, 2019.

[55] I. Lino and J. Cecílio, "A comparative analysis of the impact of cryptography in IoT lora applications," in *Proc. 2022 IEEE 20th International Conference on Industrial Informatics (INDIN)*, 2022, IEEE, pp. 220–225.

[56] R. Vishalchandar and P. Madhavan, "Securing IoT medical data using cryptography and steganography," in *Proc. 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 2022, vol. 1, pp. 1–6.

[57] M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of cryptographic algorithms on iot hardware platforms," in *Proc. 2018 2nd Cyber Security in Networking Conference (CSNet)*, 2018, IEEE, pp. 1–5.

[58] S. Bathula and K. S. Rao, "Efficient cryptography integrated IoT model for data security management," in *Proc. 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 1481–1488.

[59] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next generation lightweight cryptography for smart IoT devices:: Implementation, challenges and applications," in *Proc. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 707–710.

[60] N. Sklavos and I. D. Zaharakis, "Cryptography and security in internet of things (iots): Models, schemes, and implementations," in *Proc. 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2016, pp. 1–2.

[61] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, no. 6, 1976.

[62] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[63] R. S. Vignesh, S. Sudharssun, and K. J. Kumar, "Limitations of quantum and the versatility of classical cryptography: A comparative study," in *Proc. 2009 Second International Conference on Environmental and Computer Science*, 2009, pp. 333–337.

[64] W. Stallings, *Cryptography and Network Security, 4/E*, Pearson Education India, 2006.

[65] S. Kwon, J. S. Kang, and Y. Yeom, "Analysis of public-key cryptography using a 3-regular graph with a perfect dominating set," in *Proc. 2021 IEEE Region 10 Symposium (TENSYMP)*, 2021, IEEE, pp. 1–6.

[66] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[67] K. Pavani and P. Sriramya, "Enhancing public key cryptography using RSA, RSA-CRT and N-prime RSA with multiple keys," in *Proc. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021, pp. 1–6.

[68] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[69] R. C. Merkle, "Secure communications over insecure channels," *Communications of the ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[70] G.-J. Lay and H. G. Zimmer, "Constructing elliptic curves with given group order over large finite fields," in *Proc. Algorithmic Number Theory: First* International *Symposium*, 1994, pp. 250–263.

[71] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conference on the Theory and Application of Cryptographic Techniques*, 1985. Springer, pp. 417–426.

[72] A. H. Koblitz, N. Koblitz, and A. Menezes, "Elliptic curve cryptography: The serpentine course of a paradigm shift," *Journal of Number theory*, vol. 131, no. 5, pp. 781–814, 2011.

[73] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic curve cryptography," *Ubiquity*, vol. 2008, no. May, pp. 1–8, 2008.

[74] S. Chandra, S. Bhattacharyya, S. Paira, and S. S. Alam, "A study and analysis on symmetric cryptography," in *Proc. 2014 International Conference on* Science *Engineering and Management Research (ICSEMR)*, 2014, pp. 1–8.

[75] H. Delfs, H. Knebl, H. Delfs, and H. Knebl, "Symmetric-key cryptography," *Introduction to Cryptography: Principles and Applications*, pp. 11–48, 2015.

[76] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *Proc. 2014 international conference on electronics, communication and computational engineering (ICECCE)*, 2014, pp. 83–93.

[77] K. Muttaqin and J. Rahmadoni, "Analysis and design of file security system AES (advanced encryption standard) cryptography based," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 1, no. 2, pp. 113–123, 2020.

[78] P. K. Tiwari, V. Choudhary, and S. R. Aman, "Analysis and comparison of DES, AES, RSA encryption algorithms," in *Proc. 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2022, pp. 1913–1918.

[79] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM journal of research and development*, vol. 38, no. 3, pp. 243–250, 1994.

[80] S. Sanap and V. More, "Analysis of encryption techniques for secure communication," in *Proc. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2021, pp. 290–294.

[81] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *Proc. 2017 international conference on engineering and technology (ICET)*, 2017, pp. 1–7.

[82] M. Bellare and P. Rogaway, "Introduction to modern cryptography," ed: mihir@ cs. ucsd. edu, 2005.

[83] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," *Sony Corporation*, vol. 2008, pp. 7–10, 2008.

[84] E. J. Gomez, F. M. Sarmiento, and H. M. Ariza, "Functional comparison of the present algorithm on hardware and software embedded platforms," *HIKARI CES*, vol. 10, no. 27, pp. 1297–1307, 2017.

[85] Z. M. J. Kubba and H. K. Hoomod, "A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system," in *Proc. 2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019: IEEE, pp. 199–203.

[86] H. D. Azari and P. V. Joshi, "An efficient implementation of present cipher model with 80 bit and 128 bit key over FPGA based hardware architecture," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 14, pp. 1825–1832, 2018.

[87] D. E. Standard, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, 1999.

[88] S. Bruce, "Applied cryptography: Protocols, algorithms, and Source code in C.-2nd," ed: John Wiley & Sons, 1996.

[89] D. Joan and R. Vincent, "The design of Rijndael: AES-the advanced encryption standard," *Information Security and Cryptography*, 2002.

[90] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Proc. Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13*, 2007, Springer, pp. 450–466.

[91] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in Optics* and Photonics, vol. 12, no. 4, pp. 1012–1236, 2020.

[92] Q. H. Dang, "Secure hash standard," Fips Pub, 2015.

[93] S. Khot, "Hardness of approximating the shortest vector problem in lattices," *Journal of the ACM (JACM)*, vol. 52, no. 5, pp. 789–808, 2005.

[94] R. Overbeck and N. Sendrier, "Code-based cryptography," in *Post-Quantum Cryptography*, Springer, 2009, pp. 95–145.

[95] C. Costello, D. Jao, P. Longa, M. Naehrig, J. Renes, and D. Urbanik, "Efficient compression of SIDH public keys," in *Porc. Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 679–706, 2017.

[96] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Porc. 2007 IEEE symposium on security and privacy (SP'07)*, 2007, pp. 321–334.

[97] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT," in *Proc. 2014 IEEE International Conference on Communications (ICC)*, pp. 725–730, 2014.

[98] A. Fiat and M. Naor, "Broadcast encryption," in *Proc. Advances in Cryptology—CRYPTO'93: 13th Annual* International *Cryptology Conference Santa Barbara, California*, pp. 480–491, 1994.

[99] N. Kogan, Y. Shavitt, and A. Wool, "A practical revocation scheme for broadcast encryption using smartcards," *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 3, pp. 325–351, 2006.

[100] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Managing Requirements Knowledge, International Workshop on*, pp. 313–313, 1979.

[101] A. Shamir, "How to share a secret," Communications *of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[102] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, 2020.

[103] Y. Fazea, F. Mohammed, and M. Alsamman, "Side-Channel Vulnerabilities in Discrete Ziggurat Sampler in Post-Quantum Cryptography," in 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2023: IEEE, pp. 01-08.

[104] Y. Fazea, F. Mohammed, M. Alsamman, and O. Dakkak, "Finite Field Multiplication for Supersingular Isogeny Diffie–Hellman in Post-Quantum Cryptosystems," in 2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2022: IEEE, pp. 1-6.

[105] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, p. 100174, 2020

[106] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," *Computer Science Review*, vol. 44, p. 100467, 2022.

[107] M. Raeisi-Varzaneh, O. Dakkak, A. Habbal, and B.-S. Kim, "Resource Scheduling in Edge Computing: Architecture, Taxonomy, Open Issues and Future Research Directions," IEEE Access, vol. 11, pp. 25329-25350, 2023.

[108] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[109] V. Rao and K. Prema, "A review on lightweight cryptography for Internet-of-Things based applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 8835–8857, 2021.

[110] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, 2023.

[111] N. A. Gunathilake, A. A. Dubai, and W. J. Buchana, "Recent advances and trends in lightweight cryptography for IoT security," in *2020 16th International Conference on Network and Service Management (CNSM)*, pp. 1-5, 2020.

[112] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer* Systems, vol. 129, pp. 77–89, 2022.

[113] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges,"

IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020.
[114] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, 2022.
[115] M. Mahamat, G. Jaber, and A. Bouabdallah, "Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges," *Wireless Networks*, vol. 29, no. 2, pp. 787–808, 2023.
[116] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in internet of things: A comprehensive survey," *IEEE Access*, vol. 9, pp. 113292–113314, 2021.