Challenges and Future Trends of Cryptography in Internet of Things

Varun Kumar, Ms Sonia,
Chandigarh Group of Colleges, Jhanjeri Mohali Chandigarh School of Business, Jhanjeri Mohali varunkumar87734@gmail.com

***Abstract*—**The incorporation of cryptographic techniques is crucial for guaranteeing data privacy and security processed additionally sent inside IOT ecosystems, particularly as the IOT keeps growing. Examining problems including resource limitations, scalability, and the dynamic nature of IOT environments, this research paper explores the complex obstacles that cryptographic solutions confront considering the IOT. Lightweight cryptography, post-quantum cryptography, and blockchain integration are some of the new trends and future prospects in cryptographic research that are examined in this study in an effort to address these issues. This work offers a useful viewpoint for scholars, practitioners, and legislators engaged in the constantly changing field of cryptographic protocols inside the IOT framework by clarifying current problems and projecting future advancements.

***Keywords*—** Cryptography, Internet of Things (IOT), Security,Challenges

1.INTRODUCTION

The security is critical element of the smart city, necessitating specific consideration for security of each IOT component involved in its creation. All parties involved in communication must agree to the system's collection of personal data for it to function properly. For example, data may be collected by various sensors on the street and by various gadgets, including mobile phones, at home [1].

IOT also raises new security issues, particularly regarding data integrity, confidentiality, and dependability. Since cryptography is a subject that is always changing, new protocols and techniques for encryption and data concealment are published in the pertinent research on a nearly daily basis. Simplicity of the protocols for communication used by intelligent gadgets is limited by the software and hardware capabilities of the Internet of Things devices. All of the necessary functional components must be taken into account when creating an IOT platform and the security component is one of the most crucial parts of any IOT system. This section covers data integrity and privacy protection in addition to authorization and authentication. IOT is quite useful [2].

Internet of Things applications, such as those for smartphones and embedded devices, assist in developing a digital world to promotes worldwide connectedness that enhances people's lives by being cognizant of, kind to, and receptive to human needs [3].

The term "Internet of Things" refers to a system of interconnected devices, articles, and equipment that can all communicate data autonomously over IOT networks and have individual IDs. Growing industrial IOT device integration across a range of industries, such as smart cities, healthcare, and the automotive sector, is transforming our way of life and work. New security threats and difficulties arise as the Internet of Things ecosystem grows, necessitating a thorough grasp of these consequences for efficient cyber security and the deployment of reliable IOT solutions within an IOT system. IOT devices are susceptible to a range of cyber risks as a result of design defects and developer errors since they are endpoints with internal elements. Malicious actors may take advantage of these vulnerabilities, compromising data and causing security lapses [4]

The IOT, has a variety of applications. These incorporate business segments that aren't typically connect to the Internet, like dams, food and agriculture, systems for water and wastewater, and sixteen crucial infrastructure sectors, three of which in the United States; they also include adversarial environments, like battlefields, where IOT is used in the Battlefield Internet and Military Internet of Things [23][24].

2. IOT Terminology

Internet of Things (IOT): For the complete security of the communication system, key management is crucial. Most attacks on infrastructure based on cryptology target the key management layer. Key generation is a necessary skill for participants in cryptographic systems. Others involved in the communication must be alerted right once if the key is misplaced or compromised in any other way. If not, the stolen key can be used by the adversary to decrypt messages. The primary justification for changing the keys on a regular basis is to guard against cryptanalysis because they have a finite lifespan. Since the inception of cryptography, the issue of secret key distribution has persisted. [8]. The IOT refers the system of equipment that control various processes. Although it is not new, it has been in its infancy for a long time as the Internet gradually made its way into the digital control of commonplace devices and equipment. For instance, a refrigerator used to only be a cooling device, but these days it has many features, is fully digital, and incorporates artificial intelligence, neural networks, and other technologies to allow refrigerators to think. A house a street or the whole city can be controlled by various mechanisms and systems such as street lighting traffic control, and drainage systems because of IOT. It has also entered into agriculture, medicine, other process industries, entertainment industry, etc. As the world rapidly moves in the direction of using IOT systems, in almost all areas, the demand for using IOT devices is geometrically increasing as per estimates that the number of IOT devices will exceed 200 million in 2020. The future is bright for the IOT industry; IOT security is still up for debate at the moment because there are so many devices and users managing security issues with these systems and devices, which are also in high demand. These issues include identity theft and hacking, sabotage, and other issues.. may be a matter of concern about IOT devices. High-level cryptographic software and hardware facilities are the only answer for IOT security attacks [19].

Cryptography: The English word "cryptography" comes from Greek word "cryptography," this implies "hidden writing." It is product of a fascinating history spanning hundreds of years. Ciphers and expertly coded differ greatly from one another. A cipher alters the message bit by bit or character by character

While A cipher alters the message bit by bit or character by character while disregarding the message's grammatical structure. A code, on the other hand, substitutes a different word or symbol for a single one. Despite having a long and illustrious history, coding is no longer used. A key-indicating method modifies the communications' plaintext that need to encrypted [5]. Following encryption process, the intended recipient receives the encrypted text via radio or messenger. When someone hears and precisely duplicates the encrypted text, they are considered an attacker or intrusive party. Because he lacks the decryption key, he is unable to access the encrypted content quickly. Before messages are recorded and replayed by the intruder, communication channels might be watched over. The field of cryptology includes the skill of interpreting as well as the ability to create fresh ciphers [6]. Data is transmitted and stored using cryptography so that only those who need it may read and understand it. Typically, the phrase refers to the process of converting plaintext messages into encrypted messages and vice versa [7].

Challenges of Cryptography: In the face of changing dangers and technical breakthroughs, modern cryptography faces several major obstacles in its quest to provide safe and dependable techniques for safeguarding data, communications, and systems. Among these difficulties are the following:

2.1 Dangers of Quantum Computing:

The emergence of quantum computing presents a considerable risk to classical cryptography methods, namely those that rely on discrete logarithms and factorization, like RSA and ECC. Post-quantum cryptography is required because these techniques could be broken by quantum computers with exponential speedups [18].

2.2 Quantum-Post Cryptography:

The computational cost of the cryptography techniques used for digital encryption and authentication may be prohibitive for resource-constrained IOT node devices, which were intended to be deployed in large quantities and occasionally in unreachable distant places, raising concerns about the security of IOT technology. For such low-end standards should be enforced if IOT technologies are to truly integrate with ordinary life, the military, industrial production, agriculture, and medical services. The current high computational cost of cryptography, which frequently increases with the key sizes of the methods used, is a major drawback when using it in the Internet of Things. Conversely, the most recent advancements in quantum computing will necessitate an upgrade to cryptographic standards because they may force the world to employ even more complicated cryptographic algorithms, aggravating the existing issue with IOT systems [17].

2.3 Channel-Side Attacks:

Side-channel attacks take the use of unintentional information leakage from systems, including power usage, electromagnetic radiation, and temporal information. To counter encryption these threats, secure software and hardware architectures are required.

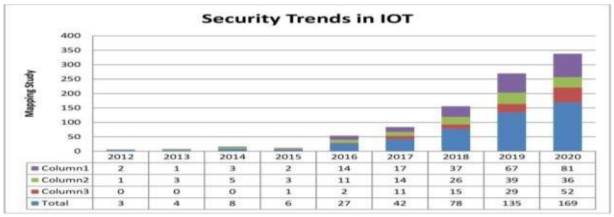
2.4 Problems with Practical Application:

Properly implementing cryptography systems in real-world scenarios can be challenging. Even with robust cryptography at its foundation, errors or misconfigurations may lead to vulnerabilities.

2.5 Moral Considerations to Make:

Cryptography is utilized in ethical discussions concerning surveillance, privacy, and individual rights. It could be challenging to find the right balance between security, privacy, and moral concerns.

Security: Many times, people look to cryptographic strategies to secure IIOT (and other technologies). For instance, the inability to do arithmetic operations on encrypted information, like that drawn from IIOT gadgets when outsourcing the data to the cloud or a centralized server presents numerous issues. Therefore, there has been interest in creating solutions related to fully homomorphic encryption (FHE) [9]. An authentication technique is one possible way to ensure a safe line of communication between IOT gadgets and other systems. Li and others [10]. Additionally, there are situations in which anonymous authentication is necessary. In these cases, techniques like the attribute-based signature with revocation technique supported by the server suggested in [11] as well as the key agreement protocols and privacy-preserving authentication for group dialogue within [12]. In most applications, it is important to closely adhere to the access policy; nonetheless, there may be situations where encrypted data must be accessed by previously unauthorized individuals. For instance, Deng, Yang, and Liu [13] suggested a thin-film glass-break access control mechanism that can handle both the more atypical break-glass access and the standard attribute-based access. To be more precise in the latter case, a break-glass entry system enables someone, such as a doctor working in an emergency room abroad, to get around the patient's data and the policy for access that is kept in the healthcare system of their home nation in order to create an urgent treatment plan. Another popular research area is blockchain, and attempts have been made to use or integrate blockchains to guarantee IOT or IIOT security within the parameters of this unique topic [14] [15]. Outlined the use of a consortium blockchain for safe energy trade considering the IOT. Specifically, they suggest an optimal pricing technique based on the Stackelberg game.



	2012	2013	2014	2015	2016	2017	2018	2019	2020
🟪 Column1	2	1	3	2	14	17	37	67	81
🟩 Column2	1	3	5	3	11	14	26	39	36
🟥 Column3	0	0	0	1	2	11	15	29	52
🟦 Total	3	4	8	6	27	42	78	135	169

Figure 1

Security issue related to IOT: In today's linked society, security concerns pertaining to IOT devices are a serious worry. Notwithstanding technological breakthroughs, no hardware- or software-based system can truly be immune to all threats and attacks. There's an old proverb that states that 50% of security is broken the moment a password is created. This also applies to Internet of Things (IOT) devices, which are vulnerable to many kinds of attacks.

IOT systems' nature, which frequently requires them to handle rapidly changing real-time data, raises concerns about their capacity for performance. These gadgets are essential for commercial data collection, machine-to-machine connectivity, and remote monitoring. Therefore, it is crucial to guarantee that IOT systems operate consistently and dependably. Preventing downtime and maintaining continuous performance are essential

demands, particularly in industries such as industrial, defense, aerospace and widely used in home security and healthcare.
It's also critical to understand how much IOT devices depend on networks and computers to function. As such, they take on the security risks related to these systems. IOT devices are subject to a wide range of security risks, from virus assaults to data breaches.

Since IOT is being adopted widely across many different sectors, it is necessary to solve these security risks. The sectors of essential infrastructure, defense, and industry are particularly vulnerable to cyberattacks on Internet of Things devices. Thus, in order to protect against these risks and guarantee the integrity and dependability of IOT systems, strong security mechanisms and protocols must be put in place.[19].

IOT security and privacy have been shown to be among the most difficult topics to tackle, as seen by the numerous studies that have been published in recent years. However, there is still much to learn about IOT cryptography and security. Both the industrial and scientific sectors have put forth alternative and distinct concepts.

The two key characteristics of IOT technology are heterogeneity and scale. For algorithmic methods and protocols to be implemented effectively across a wide range of devices and applications, security is necessary. In other cases, widespread adoption of IOT services is not feasible. IOT technologies need to be as user-friendly as feasible. Applied approaches must be created in this direction to facilitate scalability and heterogeneity, maintain user anonymity, and handle the security of personal information.
In addition to the services and applications that the Internet of Things facilitates being user-friendly, the security issue is also a fantastic foundation for confidence. Since having a lot of trust is crucial to users, they prioritize it while using speech, text, e-commerce, and other forms of communication in their daily "online lives." Despite the fact that other gadgets are more connected than before, security and privacy flaws have grown significantly. Nearly every day, cyberattacks are reported, mostly as a result of devices, services, and apps that are not properly secured[25].

3. Literature Review

3.1 Network Security Model:

The management of specific Internet features will be used to spread a message from one group to the next. It is conceivable that some outsider obtained the odd data and disclosed it to the sender and recipient while keeping the following factors into account when creating aother companies in the dark [7]. It is important to take the dependable and safe system.

3.1.1 Preserving Confidentiality: means that the person who isn't authenticated has to stop looking at the information.

3.1.2 Integrity: This feature guarantees that no changes have been made to the data collected by the collectors since it was provided by the sender. When creating a security system, there are always two things to take into account

3.1.3 Availability: Guarantees that systems operate

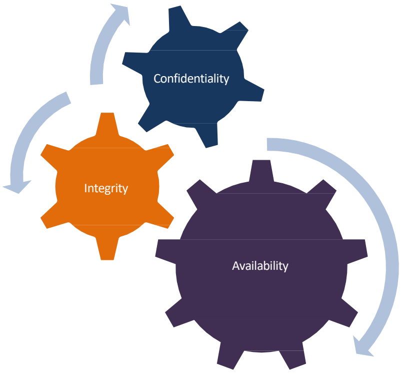


Figure 2 Network Security Model

A modification made to the security-related data being delivered. The communication must first be jumbled using a key in order to confuse the opponent. The message is jumbled prior to being delivered and is only decoded once it has arrived at its destination. When it becomes necessary or enticing to stop data flow from a competitor who could compromise integrity, classification, or other factors, security issues become crucial [16].

3.2 Key Management:

For the entire communication system to be secure, key management is crucial. Most attacks on cryptology-based infrastructure target the key management layer. In cryptographic systems, key generation is a necessary skill for participants. Others in the communication must be alerted right away if key is misplaced or in any other manner jeopardized by any party. If not, the adversary will be able to use stolen key to decrypt messages. Since the keys have a finite lifespan, defense against cryptanalysis is the primary justification for replacing them on a regular basis. Secret key distribution has been an ongoing issue since the inception of cryptography.

3.2.1 Secure key storage: Leading retailers must keep potentially dangerous customers out of their doors. A malevolent client that gains access to the keys will be able to decode any data that is connected to them. This means that the important data must be protected during both its transportation and backup medium storage.

3.2.2 Access to key stores: The important stores should only be open to patrons who have authority to view sensitive material. It is advised to use component partitioning in order to better manage access. Separating the material that stores a key from the substance that uses one is crucial.

3.2.3 Backup and recovery of important data: Reliable recovery methods and secure reinforcement of keys are required. Even if it is possible to remove access to data, losing credentials can have serious consequences for a business. Therefore, cloud service providers must make sure that backup and recovery procedures don't lose the secret key.

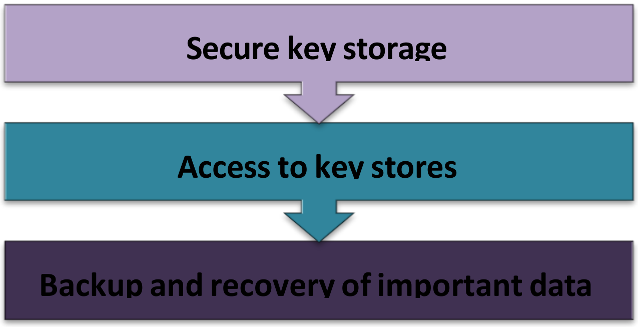


Figure 3 key management

4. Future Works

Although the research included within this particular edition helped to address a number concerning privacy, security, and performance-related IIOT-related issues, There exist still many unanswered questions and areas for further investigation. This is partly because the technologies supporting IIOT and the nature of cyber threats are always changing. Possible study topics consist of:

- A simple encryption method for IOT devices.
- Simple cryptographic primitives for Internet of Things devices
- Realistic assaults against IIOT infrastructure
- Software management and system IIOT architectures
- IOT protocol and architecture designs
- For the IOT, data integrity and access control

One finding we found for this special issue is that most of the suggested schemes that were submitted and accepted for publication used simulations to assess how well they worked. We emphasize the significance of linking research and application, for example, by developing cryptographic and security solutions that are both secure and practical. As a result, in order to jointly develop and assess potential solutions, researchers must work with the pertinent industry players.

4.1 Future trends in IOT:

Protecting, managing, and defending the sensitive data in the IOT environment are a challenging task as the software and hardware of IOT devices are susceptible to severe attacks from outside communication channels or through the Internet. As we know IOT communication is also done with mobiles and, in most instances, IOT devices are handled, monitored, and controlled by mobile devices, mobiles are easily hacked and, demonstrating unequivocally how susceptible IOT devices are. In a few instances, the selection of IOT devices and gadgets is purely based on an economic factor that means cheap cost [19].

4.1.1 Due to resource constraints on the majority of IOT devices, security-enhancing solutions need to be computationally efficient. Regretfully, several cutting-edge methods and technologies—like blockchain, searchable encryption, homomorphic encryption, and machine learning algorithms—demand a lot of processing and storage power. As a result, with the Internet of Things infrastructure, balancing security and performance is difficult.

4.1.2 Many IOT applications operate better and are more secure when edge computing and IOT technologies are combined. Nevertheless, adversaries can quickly compromise the edge layer because of its great susceptibility to attacks. Since edge devices are usually resource-constrained, common edge computing vulnerabilities include location-based attacks and battery- draining attacks. Furthermore, recovery procedures become difficult when edge nodes are deployed locally, at the network's edge.

4.1.3 Fog computing is used by the Internet of Things to meet various security concerns. Fog nodes work together to give the Internet of Things users latency-sensitive, real- time services. However since a fog node doesn't know anything about other nodes, it can be difficult to establish mutual trust across all joining fog nodes. In actuality, consumers can collaborate with several fog nodes to ensure IOT services. It is therefore essential to choose reliable fog nodes.

4.1.4 IOT adoption is accelerating across several industries. As a result, when everyday devices become more and more integrated into different surroundings, system scalability must be guaranteed. Nevertheless, a huge number of IOT devices is beyond the capabilities of centralized SDN architecture. Additionally, in highly dynamic IOT contexts like vehicle networks, SDN-based solutions are ineffective. Therefore, in SDN networks, the scalability property must be enforced.

4.1.5 Sensitive data is among the vast amounts of data generated and transferred over the Internet by the rapidly growing number of Internet of Things devices. Blockchain technology's distributed architecture effectively addresses the problem of scalability. However, it is vulnerable to data leaks and does not guarantee the privacy of transactions. Fog nodes in an fog computing- based architecture are in charge of transferring information to the cloud. Fog nodes have potential to reveal personal information if they are unreliable or compromised by an enemy. Additionally, during the training phase of machine learning algorithms, a variety of threats may be launched against them, revealing sensitive data that the classifiers rely on.

4.1.6 Encryption techniques are a means to achieve data transfer security. Transmitted data is encrypted to keep message contents secret from hackers. When the parties involved in the communicatio exchange encryption/decryption keys, this strategy can be used. Symmetric encryption methods, such as block ciphers, stream ciphers, and hash functions, require the key to be securely communicated or disseminated beforehand. Key management, which includes distribution, agreement, updating, and revocation, is still a significant issue in scalable IOT setups.

5 Conclusions

Companies employing private systems with internet access need to secure their data and systems because of the Internet's explosive growth. Security of data is important. Security of cloud data is essential. As scientific tools are created, cryptographic systems adjust and employ multiple keys. Cryptography for network security was demonstrated in the study. Encryption using a private key must be used for cloud security.

Key exchanges must be secure between the transmitter and receiver. Classifies information on customers. It could confirm the accuracy of the message. Cryptography is used in security applications and standards. PC security is discussed in this article along with related issues. It should be feasible to do mist cryptography computations, critical circulation, and administration. Secrecy, non-repudiation, integrity, and authentication are all provided by cryptography. These objectives call for cryptography. Networks are protected by cryptography. The research and algorithms related to cryptography are covered in this publication. Digital signatures will encrypt personal, financial, e-commerce, and health data. Data transfer across networks is secured by cryptography. It is the foundation for non- repudiation, authentication, etc. Networks are secured via cryptography. Algorithm studies, network security, and cryptography were validated by this review.

Reference

[1] Saračević M., et al. “Cryptographic Keys Exchange Model for Smart City Applications”. IET Intelligent Transport Systems 14.11 (2020): 1456-1464.

[2] Saračević M., et al. “Data Encryption for IOT Applications Based on Catalan Objects and Two Combinatorial Structures”. IEEE Transactions on Reliability 70.2 (2021): 819-830.

[3] N. Mishra et al. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review. IEEE Access(2021).

[4] Louise José. “internet-of-things-and-cybersecurity-emerging-trends-challenges-and-solutions”.

[5] A. Mittelbach, and M. Fischlin, The Theory of Hash Functions and Random Oracles. An Approach to Modern Cryptography, Cham: Springer Nature, (2021).

[6] S. Bhattacharya, Cryptology and information security-past, present, and future role in society. International Journal on Cryptography and Information Security (IJCIS), 9(1/2), (2019).

[7] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3, (2019).

[8] Saračević M., et al. “Source and Channel Models for Secret-key Agreement Based on Catalan Numbers and the Lattice Path Combinatorial Approach”. Journal of Information Science and Engineering 37.2 (2021): 469-482.

[9] Keke Gai, Meikang Qiu. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. IEEE Transactions on Industrial Informatics (2018).

[10] Xiong Li, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah, Saru Kumari. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. IEEE Transactions on Industrial Informatics (2018).

[11] Hui Cui, Robert H. Deng, Joseph K. Liu, Xun Yi, Yingjiu Li. Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices. IEEE Transactions on Industrial Informatics (2018)

[12] Mingjun Wang, Zheng Yan. Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications. IEEE Transactions on Industrial Informatics (2018)

[13] Yang Yang, Ximeng Liu, Robert H. Deng. Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things. IEEE Transactions on Industrial Informatics (2018)

[14] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo. A blockchain future to Internet of Things security: A position paper. Digital Communications and Networks (2018)

[15] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, Kim-Kwang Raymond Choo. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Computing 5(1): 31-37 (2018)

[16] M. Warner, J. Childress, The Use of Force for State Power: History and Future. Springer Nature, (2020).

[17] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in Proceedings 35th annual symposium on foundations of computer science, pp. 124–134, Ieee, 1994.

[18] Dr.Shubhamangala Sunila Cryptography Challenges Award-winning Cyber security Expert.

[19] K. S. KAVITHA Department of CSE, Global Academy of Technology, Bangalore, India.

[20] Willliam Stallings,” Network System Essentials “-4th Edition Copyright © 2011 Pearson education, Inc., publishing as Prentice Hall

[21] Atul Khahate, “Cryptography and network security”,3rd Edition, Copyright © 2013 TMH Publishing

[22] Kuldeep Singh Kohar, “Network Security”, revised reprint 2011.Vayu Education of India, New Delhi.

[23] Aniello Castiglione, Kim-Kwang Raymond Choo, Michele Nappi, Stefano Ricciardi. Context Aware Ubiquitous Biometrics in Edge of Military Things. IEEE Cloud Computing 4(6): 16-20 (2018)

[24] Amin Azmoodeh, Ali Dehghantanha, Kim-Kwang Raymond Choo. Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. IEEE Transactions on Sustainable Computing (2018)

[25] M. Katsaiti, A. Rigas, I. Tzemos, N. Sklavos, “Real-World Attacks Toward Circuits & Systems Design, Targeting Safety Invasion”, proceedings of the International Conference on Modern Circuits and Systems Technologies (MOCAST’15), Thessaloniki, Greece, May 14-15, 201