A SURVEY ON IOT SECURITY USING CRYPTOGRAPHIC ALGORITHMS

Bella Mohan Sai, Dr. Max Bhatia*

Department of Computer Science & Engineering, Lovely Professional University, Punjab, India

*Corresponding author: max.16870@lpu.co.in

Abstract. The Internet of Things (IoT) is a system of interconnected materials that have software, detectors, and network integration embedded that make it possible to gather information and communicate. But as the number of connected devices grows rapidly, privacy and security concerns raised by the IoT have been the primary concerns. IoT devices are vulnerable to a range of security hazards, including malware attacks, unauthorised access, and data breaches, which may jeopardise the confidentiality, integrity, and accessibility of the data they collect and process. This paper aims to provide a brief overview of IoT security, which helps identify the most significant issues with IoT ecosystem security and safety. The survey focuses on the cryptographic techniques that are used to provide security to IoT devices and summarises the proposed Internet of Things safeguarding algorithms.

Keywords- IoT, IoT security, Cryptographic algorithms, Lightweight cryptography.

1. Introduction

The Internet of Things (IoT) is a game-changing technology that links objects and devices to the Internet. This allows them to gather and share data, resulting in functionality and automation. However, the widespread use of devices has sparked worries about security. These interconnected systems are susceptible to cyberattacks that jeopardise data privacy, system integrity, and personal safety. It is crucial to implement security measures for the IoT to protect the reliability and trustworthiness of these interconnected ecosystems. The Internet of Things (IoT) includes a wide range of technologies, like sensors, home appliances, RFID tags, smartphones, and many more. Additionally, each Internet of Things device has a unique recognition that allows automatic interaction via the Internet and making choices without the need for human support [1]. The expression [2] "Internet of Things" combines a wide range of information-detecting devices and systems, including sensors, Radio Frequency Identification Devices (RFID), Global Positioning Systems (GPS), cardinal sensors, spotlight scanners, and vapour inductors, among others.

The IoT ecosystem comprises four essential components: devices, connections, data processing, and applications. The actual physical objects containing sensors, CPUs, and other electronics are commonly called devices. Connection relates to the network and protocols that let the devices communicate with each other and the cloud. Storage, analysis, and interpretation of the information produced by the devices are all parts of data processing computer applications known as apps that offer users access to and control over the Internet of Things. One of the issues with IOT is how to manage the enormous quantity of data that the devices create. This requires extremely complex machine learning algorithms, cloud computing platforms, and analytical tools. The IOT additionally presents substantial concerns regarding security and privacy due to the devices' capability to gather sensitive data and be vulnerable to attackers. For IoT applications, the data gathered by the sensors plays a crucial role, and edge computing delivers better resources [18].

To protect linked devices and data, Internet of Things (IoT) security is essential. Strong encryption and authentication techniques are provided by cryptographic algorithms, which play a crucial role. By guaranteeing data privacy, integrity, and secure communication, they strengthen the resistance of IoT ecosystems against cyberattacks and unwanted access. Digital signatures, secure authentication, and data encryption and decryption are only a few of the uses for cryptographic algorithms, which are fundamental instruments in information security. These algorithms transform plaintext data into ciphertext using intricate mathematical procedures, rendering it incomprehensible to unauthorised parties. They are essential in maintaining the confidentiality and integrity of sensitive data throughout digital transactions and transmissions.

2. IOT SECURITY LAYERED ARCHITECTURE
The increase in the use of IoT devices in various industries has led to the need for robust security measures to protect against cyber threats. The creation and execution of safeguarding protocols, methods, and processes designed to ensure the privacy, accuracy, and availability of information transferred between IoT devices is referred to as the IoT security architecture. The IoT security architecture also includes security policies and procedures that govern how devices are authorized, authenticated, and audited, as well as how data is stored, processed, and accessed. Effective IoT security architecture is crucial for ensuring the safety and privacy of individuals and organisations using IoT devices—risks associated with IoT devices and networks.

2.1 Application Layer

In the security system, the application layer refers to the layer responsible for securing the applications and services that run on top of the IoT infrastructure. This layer is critical to protecting the general privacy and security of the IoT ecosystem. The application layer includes a radius of security initiatives like access control, information validation, and input sanitization. Access control is used to limit access to applications and services to only authorized users, while data validation and input sanitization are used to ensure that only valid and safe data is processed by the applications and services. Ultimately, protecting the IoT ecosystem's overall security and privacy using a secure application layer is essential. By securing the applications and services that run on top of the IoT infrastructure, groups may assist in defending their IoT deployments outside of potential DDoS attacks and mitigate the risk of data breaches. Right now, the development of the IoT application layer has no global standards. Among all, some companies perform in M2M (Machine to Machine) mode. Antonio et al. [6] developed a design scheme for smart home security on this layer.

2.2 Network Layer

The network layer in IoT security architecture refers to the layer responsible for encrypting the data exchange between servers and IoT devices. The security, reliability, and accessibility of data transported across the network must all be guaranteed by this layer. The network layer includes a range of security measures, such as encryption, authentication, and access control. Encryption is used to protect data in transit by encoding it so that only authorized parties can read it. With a range of different devices and protocols communicating over the network, it can be difficult to make sure every tool is tightly fastened and that data is transmitted securely. To address these challenges, IoT security experts have developed a range of best practices for securing the network layer. These include implementing secure communication techniques and using firewalls and intrusion detection systems to monitor network traffic and detect potential threats. Ultimately, a secure network layer is critical for ensuring the overall security of the web. The layer must guard against broad assaults that compromise device coordination and information sharing [5].

2.3 Physical Layer/Perception Layer

The perception layer in IoT security architecture refers to the first layer of security, which is responsible for securing the physical devices that make up the IoT ecosystem. This layer is also known as the device layer and includes measures such as secure boot, firmware updates, and device authentication. The perception layer is vital for protecting the safety of IoT devices because it is the first line of defence against potential cyber threats. This layer is responsible for securing the physical devices themselves and their software components from unauthorised access, malware, and other threats. The devices in the device layer include detectors, buttons, gateways, and other gadgets that communicate with the real world [3]. Secure layer protection includes using hardware-based security measures, such as secure boot and trusted execution environments, and implementing secure software development practices, such as regular firmware updates and vulnerability management. Ultimately, a secure perception layer is critical for ensuring the overall security of the IoT ecosystem. By securing the physical devices themselves, organisations can help mitigate the risk of cyber threats and protect their IoT deployments from potential security breaches. The main technologies in this section are radio frequency identification and wireless sensor networks [4].
Figure 1 represents the three layers of the IoT security architecture. Ensuring data privacy and integrity and tackling the various security concerns associated with the Internet of Things need a well-thought-out, three-layered security architecture.

3. CRYPTOGRAPHIC ALGORITHMS IN IOT SECURITY

To secure the IoT environment, cryptographic approaches are crucial. They are employed to guarantee the CIA the information exchanged via networks. In Internet security, cryptographic algorithms are used to encrypt data and prevent unauthorised access, ensure data integrity by detecting any modifications during transmission, and provide authentication so that only individuals with permission can get information. By using techniques for encryption of the data, cryptography is the art and science of keeping the information safe while it is being carried across a network. To safeguard networks, many encryption methods are used. The three main forms are the following: symmetrical algorithms, asymmetrical algorithms, and protocols for cryptography. Asymmetric algorithms, which use both private and public keys, and symmetric algorithms, which encrypt and decode data using separate keys, are differentiated by the number of keys they use. Private keys are used for decryption, whereas public keys are used for encryption. Considering the reality that these approaches are essential for information system protection, they use a lot of memory, Central Processing Unit time, and battery life. The amount of key that is used indicates how secure the symmetric key encryption is. For example, RC2 uses a 64-bit key, whereas DES is also a 64-bit key; 3DES (Triple DES) utilises two 64-bit keys; AES and RC6 may utilise keys of any bit count between 128, 192, and 256 bits; and blowfish can use keys that are any size between 32448 bits (the default is 128 bits) [7]. For data and safe services, cryptography offers a basic security layer. Thus, the cryptography algorithm's structural design and associated technological functions are crucial factors to take into account [19].

3.1 SYMMETRIC KEY ENCRYPTION

One key is used for both data encryption and decryption in an encryption process known as symmetric key encryption. This means that the same key is used by both the sender and the recipient to secure the data being transmitted. In symmetric key encryption, the plaintext is encrypted by applying a mathematical algorithm to it using a secret key. The encrypted data, called ciphertext, is then transmitted to the recipient. The recipient decrypts the ciphertext into the original plaintext using the same secret key. If the wrong person obtains the key, it can be used to decrypt the ciphertext and access the plaintext data. Symmetric key encryption is widely used in IoT security, particularly for securing data transmissions between devices in a network. It is commonly combined with other cryptographic methods to provide layered security and guarantee the privacy, reliability, and validity of transferred data, such as electronic signatures or hash functions. Examples of symmetric key encryption algorithms include AES (Advances Encryption Standard), DES (Data Encryption Standard), and TDEA (Triple Data Encryption Algorithm). These algorithms use different key lengths and mathematical operations for Data encryption and decryption.
3.2 ASYMMETRIC KEY ENCRYPTION

Public-key encryption, frequently referred to as asymmetric key encryption, is a kind of security technique that encodes and decodes data with two different keys. These keys are mathematically related but are not identical, unlike in symmetric key encryption. A user produces a set of keys made up of a private key and a public key. Anyone may use the public key to encrypt data provided to the user and distribute it for free. However, the secret key is only available to the user and is employed to gain access to protected data using the public key. Asymmetric key encryption's fundamental benefit is that it does away with the necessity for safe key distribution. Asymmetric key encryption's fundamental benefit is that it does away with the necessity for safe key distribution, which is a key challenge in symmetric key encryption. However, asymmetric key encryption is typically slower and more computationally intensive than symmetric key encryption. It is also more complex and requires a greater level of computational power to be implemented effectively. It is frequently used combined with other secure methods to offer layered security and secure the confidentiality, probity, and authenticity of transmitted data, including symmetric key encryption, hash functions, and digital signatures. A sample of these involves the Rivest-Shamir Adleman, elliptic curve cryptography, and the Diffie-Hellman key exchange algorithms. These algorithms use different mathematical operations and key lengths to encrypt and decrypt data.

4. Related Work

This paper presents a brief overview of the related work conducted in the domain of IoT security, with a particular focus on the utilization of cryptographic algorithms for security purposes in IoT devices.

Roy et al. [8] proposed a lightweight cryptographic algorithm, which is a cipher based on cellular automata (CA). Information is protected using this method at the perception layer, which is more effective than some of the ciphers already in use, such as DES and 3DES. The National Institute of Standards and Technology (NIST) has determined that this approach satisfies the randomness tests. Furthermore, it passes every diehard test, demonstrating LCC's excellent security features.

Jassim et al. [9] put forward a scheme related to lightweight stream cipher schemes to provide a high level of encryption. The dynamic key-dependent approach provides a framework for this level of security. Only a few basic cost-saving activities are included in this system. It makes use of cryptographic fundamentals that change dynamically and efficiently for every input block. The proposed encryption delivers a high level of efficiency and robustness, making it appropriate for IoT devices with limited resources. It employs a nonce and secret key of 128, 192, and 256 bits. This approach, which has 12 to 14 rounds, combines CR4, a pseudo-random number generator (PRNG), and a linear feedback shift register (LFSR). High periodicity, low energy consumption, and resistance to statistical, algebraic, and brute-force assaults are all characteristics of this method. For disclosure and desynchronization assaults, this method is insufficient.

M.A. Khan et al. [10] proposed Improved Elliptical Curve Cryptography as an effective framework for the encryption and authentication of information from IoT-based medical sensors. The Improved Elliptical Curve Cryptography is a curve-related system with one particular bottom point generated from prime number functions. The framework combines user credentials with biometric criteria. Yet another creation of a secret key enhances network security in comparison to ECC in ordinary circumstances. A common key is used to safeguard the data, while a private key is used to decode it. The elliptic curve, the public key, and the private key combine to form the elusive key. The system has minimal security requirements. slow encryption and decryption speeds and minimal communication overheads. The typical encrypting and decrypting times for IECC are 1.032 and 1.004 seconds, respectively. This value is lower than the ECC and RSA values. The effectiveness of this approach is further demonstrated by statistical analysis.

Ghaffari et al. [11] proposed new hybrid cryptographic algorithms, SHA-256, RC4, and ECC, which have been used for security in Internet of Things-related irrigation systems. The algorithm known as SHA-256 mostly makes cipher data. They proved the security-related issues of the IoT-based irrigation system with the algorithms that were proposed. Finally, it was mentioned that the suggested approach will be evaluated and improved in subsequent work to make it appropriate for actual irrigation systems.
Cao et al. [12] came up with a safe, compact, multi-sensor D2D communication system. The foundation of their proposed communication system is LW-created keys. This dissemination scheme utilises the use of a motion sensor to secure near-field identification that uses a device's microphone and talker as detectors and for the exchange of data, along with audio and RF encryption and decryption processes.

Nao et al. [13] studied three IoT security algorithms: symmetric, asymmetric, and hybrid encryption. All the algorithms are compared according to security factors. Based on the study's findings, ECC (Elliptic Curve Cryptography) operates most accurately of all methods. The authors left open the possibility of mitigating intrusion into IoT devices by using asymmetrical techniques to support the complicated growth of cryptography.

Memon et al. [14] proposed a quick and simple authentication method based on the public key elliptic curve discrete logarithm problem, which is based on ElGamal encryption. The work done in the paper provides a public key infrastructure-related authorization system that encrypts the private key using ElGamal and includes ECC to provide key pair selection.

Meshram et al. [15] proposed an effective and strong authentication protocol for IoT-based smart cities that supports safe resource management and communication. Wide chaotic maps are used in the proposed protocol to increase security and mitigate different types of assaults. Its dependability and potency for smart card-based password authentication are established using BAN logic verification.

Runa et al. [16] proposed a method for a lightweight cryptographic algorithm called Present, which has been altered. The recommended method farther borrows just a small amount of information from the TEA lightweight cipher. It was successfully designed for the Delphi C++ platform. The viability of the modified PRESENT encryption in comparison to the original PRESENT cipher has been proven using software parameter analysis using Cryptool. For all input file types, the suggested method's non-homogeneity test yields the ideal chi-square value. The N-gram test, which analyses the periodicity of characters in cipher text, consistently produces far lower results than the present cipher. An efficient graph for the modified present is also produced by the floating frequency test and histogram. Different tests' outcomes suggested that the modified present approach is more effective than the original present method.

Taloba et al. [17] have proposed a blockchain-based framework for safe healthcare. Blockchain has been used to ensure the availability of documents, the protection of medical data, and the transparency of the shipping process between suppliers and clients.

Rahul Saha et al. [20] proposed a bilinear map scheme solution for IoT security. In this, aggregate signing is used to improve network performance, and time stamps are used in the key generation process. The proposed solution is intended to be used in the fog layer of the IoT infrastructure. The results of the scheme are compared with the existing schemes, and the comparison stated that the proposed scheme is efficient for IoT applications.

Tarandeep Singh et al. [21] proposed a novel cryptography and steganography model that uses low-complexity elliptic Galois cryptography (EGCrypto) in IoT security. Matrix XOR steganography is employed in combination with EGCrypto. The extensive experiments show that EGCrypto outperforms competitive models in terms of various metrics. The future work on this is to focus on optimising EGCrypto's efficiency and security against advanced attacks in IoT security.

Reji Thomas et al. [22] proposed an authentication protocol for IoT security that is based on LiSP signcryption. They used two cryptographic modules that are lightweight and have efficient properties. The outcome of the experiment is that LiSP-XK is 35% better in efficiency compared to other encryption approaches. The remaining work by the authors is related to a distributed key generation mechanism.
Table 1. Comparative analysis of IoT security models [8-17,20,21,22].

<table>
<thead>
<tr>
<th>Ref</th>
<th>Objectives</th>
<th>Technique used</th>
<th>Type of data</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roy et al. [8]</td>
<td>Find an effective cipher at the perception layer.</td>
<td>Lightweight cryptography</td>
<td>Chi-square values from input files</td>
<td>A cellular automata-based cryptographic algorithm has been proven to provide enhanced security and has received positive evaluations from NIST and rigorous tests.</td>
</tr>
<tr>
<td>Jassim et al. [9]</td>
<td>To provide security using Lightweight stream cipher</td>
<td>Stream Cipher</td>
<td>Sensor data</td>
<td>The proposed lightweight IoT stream cipher, while efficient and robust, is vulnerable to disclosure and desynchronization attacks.</td>
</tr>
<tr>
<td>M.A Khan et al. [10]</td>
<td>To get an improved Elliptical curve cryptography framework from sensors.</td>
<td>Elliptic Curve Cryptography</td>
<td>Medical Data</td>
<td>Elliptical Curve Cryptography (IECC) improves IoT medical sensor data security through biometrics and faster encryption, outperforming ECC and RSA with minimal security requirements and communication overhead.</td>
</tr>
<tr>
<td>Ghaffari et al. [11]</td>
<td>Cryptographic algorithms for irrigation system purposes.</td>
<td>SHA-256</td>
<td>Sensor data</td>
<td>The IoT irrigation system security is enhanced with the introduction of a hybrid cryptographic algorithm that combines SHA-256, RC4, and ECC.</td>
</tr>
<tr>
<td>Cao et al. [12]</td>
<td>Communication system based on Lightweight key.</td>
<td>D2D</td>
<td>Sensor data</td>
<td>The proposed D2D communication system utilizes LW-generated keys, motion and audio sensors, and encryption processes for secure and compact data exchange.</td>
</tr>
<tr>
<td>Nao et al. [13]</td>
<td>Study on Three IoT Security Algorithms.</td>
<td>Encryption</td>
<td>Test data of the 3 layers</td>
<td>The study suggests the use of ECC for IoT security and suggests the potential for asymmetric techniques to enhance cryptography against device intrusions.</td>
</tr>
<tr>
<td>Memon et al. [14]</td>
<td>Authentication Method based on public key.</td>
<td>PKI</td>
<td>Authentication data in public key</td>
<td>The proposed authentication method integrates ElGamal encryption and ECC to establish a secure and efficient public key infrastructure-based authorization system.</td>
</tr>
<tr>
<td>Meshram et al. [15]</td>
<td>Chaotic based Authentication</td>
<td>Chaotic map</td>
<td>Smart city</td>
<td>The new authentication protocol enhances security in IoT-based smart cities by utilizing wide chaotic maps and establishing reliability through BAN logic verification for robust smart card-based password authentication.</td>
</tr>
<tr>
<td>Runa et al. [16]</td>
<td>Evaluate and demonstrate the effectiveness of the modified PRESENT cryptographic algorithm.</td>
<td>Cryptool</td>
<td>Cryptographic key data</td>
<td>The modified cryptographic algorithm, combining Present and TEA, proves more efficient than the original Present cipher in various tests and software parameter analysis.</td>
</tr>
<tr>
<td>Taloba et al. [17]</td>
<td>Framework for security and accessibility.</td>
<td>Blockchain</td>
<td>Medical data</td>
<td>proposed blockchain-based healthcare framework</td>
</tr>
<tr>
<td>Rahul Saha et al [20]</td>
<td>Proposed bilinear map scheme</td>
<td>Aggregate Signcryption</td>
<td>Sensor data</td>
<td>Bilinear map-based IoT security solution with aggregate signing and timestamp-assisted key generation.</td>
</tr>
<tr>
<td>Reji et al [22]</td>
<td>Authentication protocol</td>
<td>LiSP signcryption</td>
<td>Sensor data</td>
<td>A novel IoT security model integrating low-complexity EG Crypto and matrix XOR steganography proves effective.</td>
</tr>
</tbody>
</table>

Table 1 gives a brief overview of the related work. It explains the objectives and techniques used and the type of data used by the authors in IoT security.
5. Conclusion

IoT devices have an important effect on the way we live, but they also create safety risks that need consideration. By allowing safe interaction, authentication, and data protection, cryptographic methods may significantly enhance IoT security. Implementing cryptographic techniques is essential for securing IoT devices and networks. Cryptography provides a means of securing sensitive data and communication channels in IoT systems. The use of cryptography can help prevent unauthorised access, tampering, and theft of data. Moreover, it can enable secure communication between IoT devices, enabling the sharing of sensitive information without exposing it to attackers. Although not all cryptographic systems are created equal, some could be better suited for Internet of Things (IoT) devices than others. To ensure that IoT security solutions are appropriate for resource-constrained IoT devices, it is crucial to thoroughly evaluate the cryptographic algorithms and protocols implemented in such solutions. The security and privacy of IoT systems must be ensured using cryptographic advances in technology. However, careful consideration and evaluation of the cryptographic techniques used are necessary to ensure that they are effective and suitable for specific IoT applications. AI and cryptographic algorithms will help IoT security provide a dynamic and proactive defense against ever-evolving threats in IoT ecosystems. Threat detection powered by AI, adaptive security, analysis of user behavior, automated reaction, predictive security, improved data encryption, sophisticated authentication, autonomous security, and privacy protection is some of the features that will be available. Finally, our review paper gives a brief overview of existing cryptographic algorithms that are used for the IoT device's security.

6. References


