Cryptographic Techniques for Securing Internet of Things (IoT) Devices

Hansala Jayawardana
dept.of computer science
NSBM Green university
Homagama, Sri Lanka
hansalajayawardana17@gmail.com

***Abstract*— Cryptographic Techniques for Securing Internet of Things (IoT) Devices focuses on how cryptography plays a crucial role in keeping IoT systems safe. This paper aims cryptographic methods customized for IoT security challenges. This study aims to create an IoT-specific security framework. It addresses IoT device security issues, offering techniques to safeguard data, reduce vulnerabilities, and ensure system integrity.**

The literature review section offers an examination of recent research on cryptographic solutions tailored for IoT security. The IoT security architecture is discussed, highlighting essential layers such as application, network, and physical security, each vital for ensuring integrity and safeguarding data. Key cryptographic techniques including symmetric and asymmetric encryption, hashing, and lightweight algorithms are explored for their significant roles in enhancing IoT security.

In the Future Directions section, potential advancements in the field are outlined. The evolution of the Internet of Things (IoT) towards increased device connectivity and automation, propelled by edge computing, is anticipated. Applications in smart cities are discussed, showcasing how IoT contributes to enhanced home and vehicle safety. The paper emphasizes the importance of prioritizing security and privacy to unlock the full potential of IoT. Furthermore, in the realm of the Internet of Medical Things (IoMT), the wireless monitoring of vital signs through devices like smartwatches is highlighted as an example of how cryptographic methods ensure security, thereby improving patient care through enhanced monitoring.

Keywords— Cryptography, Internet of Things (IoT), Security, Cryptographic Techniques, IoT Security Architecture, Symmetric Encryption, Asymmetric Encryption, Hashing, Lightweight Algorithms, Future Directions, Smart Cities, Internet of Medical Things (IoMT)

I. Introduction

The Internet of Things (IoT) connects everyday objects to the internet, allowing them to share data and be controlled remotely. It makes life easier, enhances safety, creates business efficiencies, and generates new services and products. [7] The Internet of Things (IoT) revolutionizes our interaction with everyday objects by enabling them to communicate over the Internet without human intervention. With interconnected devices ranging from air conditioners to wearable gadgets, IoT applications span various domains such as smart homes, healthcare, transportation, and more. [1] IoT devices lack sufficient security measures, prioritizing functionality over safeguarding user data. This exposes sensitive information to potential breaches. Essential security concepts like identification and authentication are often overlooked, allowing hackers to access devices easily. Encryption is crucial to protect data during transfer, achieved through cryptographic techniques like Elliptic Curve Cryptography (ECC), ensuring confidentiality, integrity, non-repudiation, and authentication.[3] As IoT devices collect and transmit sensitive data, ensuring their security against cyber-attacks is paramount. Authentication, encrypted communication, and maintaining data integrity are essential for safeguarding IoT systems. Moreover, the exponential growth of IoT contributes to the generation of big data, characterized by its volume, velocity, and variety (as depicted in Figure 1). [2]

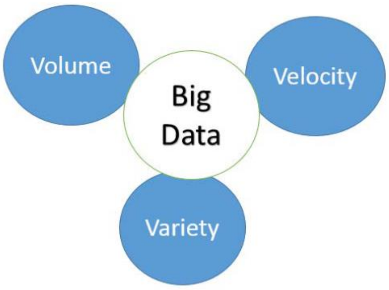

Figure 1: Three V's of Big Data [2]

This influx of data presents both opportunities and challenges, emphasizing the importance of robust security measures. In this context, understanding the concepts of cryptography becomes crucial for enhancing IoT security.[2]

To ensure the security of connected devices and data, Internet of Things (IoT) security is crucial. Cryptographic algorithms provide strong encryption and authentication techniques, playing a vital role in this regard. By ensuring data privacy, integrity, and secure communication, they bolster the resilience of IoT ecosystems against cyberattacks and unauthorized access. Digital signatures, secure authentication, and data encryption and decryption are among the many uses of cryptographic algorithms, which are fundamental tools in information security. [6] Cryptographic technology is a trusted solution in IoT networks for privacy and security. It involves encryption/decryption techniques and keys to prevent unauthorized access. While there are various cryptographic algorithms available, none is a universal solution for IoT privacy concerns. [9]

II. Literature Review

Cryptography schemes create a basic security layer for data and applications. To address security issues in IoT environments, various security solutions using cryptography have been presented.[12] Privacy in IoT means that all the personal data, which the numerous devices gather, is stored appropriately and not used in an unauthorized way. Such data may include one's location, behavior, preferences, etc. Privacy is ensured by encryption, safe storage, and user-assistance in the decision of the extent one wants this or that data to be available. [10] To secure the IoT environment, cryptographic approaches are crucial. [6] The literature review section will delve into various cryptographic techniques employed to secure IoT devices. Cryptographic techniques are needed to protect IoT data whether it's stored or being sent. These techniques ensure that data is kept confidential, stays intact, verifies the identities of devices/people involved, confirms the authenticity of messages, manages keys securely, prevents denial of actions, ensures data platforms are reliable, and enables digital signatures.[4] Traditional security solutions have proven ineffective due to the unique nature of IoT devices, which often have limited resources and handle sensitive data.[5]

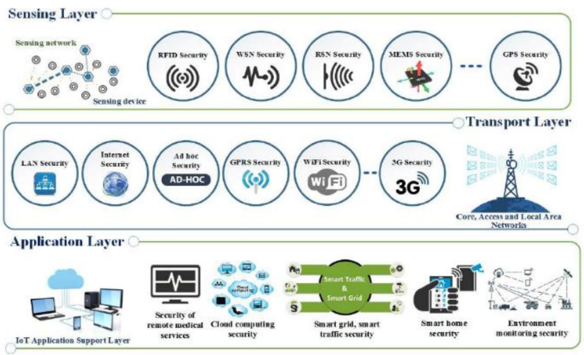

Figure 3: Layers Architecture of Internet of Things [2]

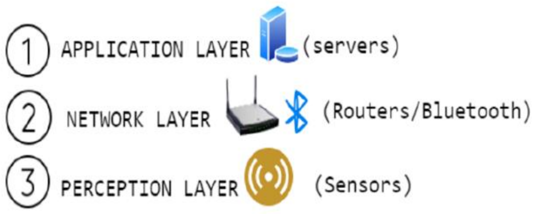
1 APPLICATION LAYER (servers)
2 NETWORK LAYER (Routers/Bluetooth)
3 PERCEPTION LAYER (Sensors)

Figure 4: Three-layered IoT Security Architecture [6]

The security architecture of the Internet of Things (IoT) encompasses multiple layers, each playing a crucial role in safeguarding the integrity, confidentiality, and accessibility of IoT systems. The application layer focuses on securing the applications and services running on top of the IoT infrastructure, employing measures such as access control, data validation, and input sanitization. Meanwhile, the network layer ensures secure data exchange between servers and IoT devices through encryption, authentication, and access control mechanisms. Finally, the physical layer, also known as the perception layer, protects the physical devices themselves using measures like secure boot, firmware updates, and device authentication.[6]
Cryptographic processing in IoT security involves encoding sensor data using complex algorithms.[13] Cryptographic techniques play a vital role in securing the Internet of Things (IoT) environment, ensuring the confidentiality, integrity, and authenticity (CIA) of exchanged information.[6] Cryptography is utilized in various ways, employing three main types of cryptographic algorithms [11]:

1. Symmetric cryptography
2. Asymmetric cryptography
3. Hash encryption

1. Symmetric Key Encryption: Symmetric key encryption involves using a single key for both data encryption and decryption. It employs mathematical algorithms to transform plaintext into ciphertext, which is then transmitted. Examples of symmetric key encryption algorithms include AES, DES, and TDEA.[6]

2. Asymmetric Key Encryption: Asymmetric key encryption, also known as public-key encryption, utilizes two different keys for encryption and decryption. These keys, mathematically related but not identical, consist of a public key for encryption and a private key for decryption. Algorithms such as Rivest-Shamir-Adleman (RSA), elliptic curve cryptography (ECC), and Diffie-Hellman key exchange are employed in asymmetric key encryption. While it eliminates the need for secure key distribution, it tends to be slower and computationally intensive compared to symmetric key encryption.[6]

3. Hash encryption: Hashing is a process that converts any type of data into a unique string of characters. This means that regardless of the size or type of data, it can be transformed into a fixed-size string of characters using hashing.[11]

In IoT security, both symmetric and asymmetric key encryption techniques are commonly employed, often in combination with other secure methods, to provide layered security and ensure the confidentiality, integrity, and authenticity of transmitted data. [6]

Various implementation environments for IoT and their unique security needs were identified. A blockchain-based cryptographic method was suggested to validate devices and maintain data integrity. Every IoT security plan should have an architecture supporting cryptographic protocols for data verification, ensuring the integrity and secure management of all connected devices.[8] Several researchers have proposed lightweight encryption algorithms to boost the security of data from IoT devices. Muhammad Tausif et al. studied 13 lightweight ciphers designed for IoT, focusing on factors like RAM use and execution time. They emphasized the need to minimize resource consumption for IoT's limited capabilities. Another study by Muhammad Usman et al. introduced "Secure IoT," a 64-bit key encryption with 5 rounds, aiming for efficiency and security. Manish Kumar et al. suggested a dynamic key method using 128-bit key encryption, effective against known attacks. Jagdish Patil et al. developed "LiCi," a power-efficient 128-bit key block cipher for IoT data. Ria Das et al. proposed a hybrid method combining cryptography and steganography for data privacy. These innovative solutions, by optimizing resources and enhancing resilience, advance IoT security effectively.[2]

SECoS secures IoT communications effectively via cryptographic techniques, secure routing protocols, and efficient key management mechanisms. SHIELD secures heterogeneous IoT securely and safely by managing trust, device integration, and data serialization. SIFA assesses IoT device security and functionality via risk-based testing and vulnerability analysis. Further, iCoreSec provides all-around IoT security using device authentication, secure communication, access management, and intrusion detection and prevention mechanism. MAMID puts much emphasis on secure device authentication via machine-to-machine protocol for trust establishment leading to secure communication with verified devices. Moreover, PRoSPECT enables secured development of resource constrained IoT devices selection rather than the last option by integrating threat modeling, secure coding, and vulnerability assessment into the software development life cycle. These frameworks deploy various cryptographic algorithms, including RC4, AES, RSA, and ECC, among others, to prevent buffer overflows, unauthorized access, and data leak risks. Additionally, techniques like microcontroller-friendly differential power analysis and cloud-based encryption contribute to safe and energy-efficient IoT device connectivity. As the digital ecosystem evolves, lightweight timing-based cryptography becomes crucial for improving the performance of resource-constrained devices. It is essential for modern security frameworks to incorporate lightweight cryptographic solutions to ensure data privacy, protection, and resilience against timing-based attacks.[5]

Table 1: Framework Analysis [5]

Framework	Description	Cryptographic Techniques
SECoS	Protecting IoT communications involves using codes to keep messages safe, making sure data travels through secure paths, and managing keys securely.	RC4, AES, RSA, ECC
SHIELD	Managing security issues in diverse IoT setups by establishing trust among devices and ensuring safe transmission of data.	AES, RSA, ECC
iCoreSec	A complete IoT security plan involves making sure devices are genuine, communication is safe, access is controlled, and unusual activity is detected.	RC4, AES, RSA, ECC
MAMID	Making sure that IoT devices can securely connect and communicate with each other without any unauthorized devices getting in.	RC4
PRoSPECT	Managing security issues in IoT devices with limited resources throughout their development process.	AES, RSA, ECC

III. Future Directions

The Internet of Things (IoT) encompasses a network of interconnected devices capable of communicating and sharing data over the internet. Ranging from everyday objects to industrial machinery, these devices facilitate automation, remote monitoring, and data-driven decision-making. While IoT presents numerous opportunities for innovation across various domains, it also raises concerns regarding security, privacy, and interoperability.

Looking ahead, the future of IoT promises even greater connectivity and integration, with billions of devices expected to be interconnected, fundamentally reshaping our interaction with technology and the physical world. Advancements in IoT technologies, such as edge computing, 5G networks, artificial intelligence, and blockchain, will enable more efficient data processing, real-time analytics, and automation. However, addressing challenges such as security vulnerabilities, data privacy concerns, interoperability standards, and ethical considerations will be crucial in realizing the full potential of IoT while ensuring trust, reliability, and societal benefit.

Smart city is one of the trendy application areas of IoT and Smart city is one of the important application areas for IoT developers. A smart city integrates IoT technology into everyday life, including smart homes. In a smart home, IoT-enabled appliances like AC/heating, TVs, and security systems communicate for comfort, security, and energy efficiency. This communication is managed by a central control unit via the internet, allowing seamless interaction between devices. Ultimately, smart homes enhance convenience and safety while reducing energy usage.[14]
Smart vehicles are a part of smart cities, with cars now having advanced tech like sensors and smart devices controlling everything from lights to engines. The Internet of Things (IoT) is working on making cars even smarter, with wireless communication between cars and drivers for predictive maintenance. This means cars can talk to each other (car-to-car) and to the driver (car-to-driver), ensuring a safer and more comfortable driving experience. The image given below shows some IoT applications related to the smart city concept. [14]

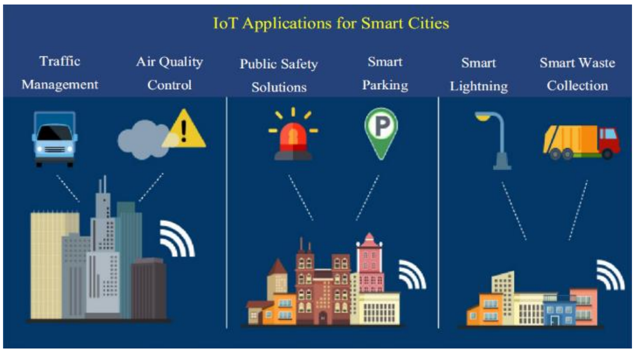

Figure 5: Potential IoT application areas for smart cities [14]

The integration of health features into IoT devices creates an IoMT environment. IoMT, or the Internet of Medical Things, connects people with medical devices wirelessly. These devices use technologies like Bluetooth, WiFi, 3G, 4G, 5G, ZigBee, etc., to share health data with medical facilities such as doctors and hospitals. With advancements in microelectronics, medical devices have become smart, able to monitor vital signs like blood pressure, heart rate, and oxygen levels. These devices can take the form of watches, belts, shoes, clothes, necklaces, and more. IoMT is a significant advancement in healthcare, providing continuous monitoring and treatment for people of all ages, especially those with medical conditions.[15]

All these IoT things are the future of IoT. It is essential to pay more attention to security while producing them. Because all these things are related to our life. Cryptographic techniques are crucial for securing IoT devices and systems in smart cities, including smart homes and smart vehicles. Using cryptographic techniques is like giving smart city devices a secret code to keep them safe. For smart homes, it means ensuring devices are real, keeping data private, and controlling who can use them. In smart vehicles, it's about secure communication between cars, safe updates, and protecting driver and vehicle data. Meanwhile, IoMT connects smart medical devices wirelessly, aiding doctors in monitoring vital signs and enhancing healthcare for patients, particularly those with medical conditions, representing a significant advancement in medical technology.

IV. Conclusion

The Internet of Things (IoT) brings significant benefits in convenience and efficiency, from smart homes to smart cities. However, with the increasing use of IoT devices, concerns about data security become more pressing. Cryptographic techniques, such as employing special codes and virtual locks, are crucial for securing IoT. These methods, such as encryption and hashing, make sure data is private, unaltered, and genuine. They create secure paths for devices to talk to each other, prevent unauthorized access, and make updates safe. As IoT grows with new tech like edge computing and 5G, strong cryptographic tools will be vital. Prioritizing these security measures is key to building a safe and reliable IoT world, where we can enjoy the benefits without risking our privacy and safety.

V. References

[1] M. S. Henriques and N. K. Vernekar, “Using symmetric and asymmetric cryptography to secure communication between devices in IoT,” *IEEE Xplore*, 2017. https://ieeexplore.ieee.org/abstract/document/8073643

[2] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad, “A review of data security and cryptographic techniques in IoT based devices,” *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems - ICFNDS ’18*, 2018, doi: https://doi.org/10.1145/3231053.3231100.

[3] 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, Jan. 2020, doi: https://doi.org/10.1109/tsmc.2019.2903785.

[4] S. Zeadally, A. K. Das, and N. Sklavos, “Cryptographic technologies and protocol standards for Internet of Things,” *Internet of Things*, p. 100075, Jun. 2019, doi: https://doi.org/10.1016/j.iot.2019.100075.

[5] A. S. Dandotiya and S. K. Gupta, “Analysis and Development of Security Framework for IOT Device,” *Tuijin Jishu/Journal of Propulsion Technology*, vol. 44, no. 4, pp. 995–1008, Oct. 2023, doi: https://doi.org/10.52783/tjjpt.v44.i4.955.

[6] B. M. Sai and M. Bhatia, “A Survey on IoT Security Using Cryptographic Algorithms,” *E3S Web of Conferences*, vol. 453, p. 01048, 2023, doi: https://doi.org/10.1051/e3sconf/202345301048.

[7] A. Kurniawan, R. Mayasari, and M. Murti, “IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHM ON IOT DEVICE’S ID.” Accessed: Apr. 22, 2024. [Online]. Available: https://apic.id/jurnal/index.php/jsc/article/download/10/10

[8] B. T. Asare, K. Quist-Aphetsi, and L. Nana, “A Cryptographic Technique for Communication among IoT Devices using Tiger192 and Whirlpool,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, 2021, doi: https://doi.org/10.14569/ijacsa.2021.0120853.

[9] A. J. Akinboboye, A. S. Oluwole, O. Akinsanmi, and A. E. Amoran, “Cryptographic Algorithms for IoT Privacy: A Technical Review,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 185–193, Aug. 2022, doi: https://doi.org/10.14445/22315381/ijett-v70i8p219.

[10] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011, doi: https://doi.org/10.1109/mc.2011.291.

[11] M. K. Hasan *et al.*, “Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications,” *Complexity*, vol. 2021, pp. 1–13, Apr. 2021, doi: https://doi.org/10.1155/2021/5540296.

[12] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, “Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2033–2051, Jul. 2020, doi: https://doi.org/10.1007/s12652-020-02303-5.

[13] E. Leloglu, “A Review of Security Concerns in Internet of Things,” *Journal of Computer and Communications*, vol. 05, no. 01, pp. 121–136, 2017, doi: https://doi.org/10.4236/jcc.2017.51010.

[14] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” *Journal of Big Data*, vol. 6, no. 1, Dec. 2019, doi: https://doi.org/10.1186/s40537-019-0268-2.

[15] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, “Internet of Things: Security and Solutions Survey,” *Sensors*, vol. 22, no. 19, p. 7433, Sep. 2022, doi: https://doi.org/10.3390/s22197433.