Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

Analysis on Cryptographic Framework for IoE: Challenges and Issues

E. Baraneetharan

Associate Professor & Head, Department of EEE, Surya Engineering College, Erode, India

E-mail: hodeee@surya.ac.in

Abstract

The Internet of Things (IoT) has been supplanted by the Internet of Everything (IoE) since lately. Cities, states/provinces, and the federal government all face the same problem of how to fulfill rising public expectations while dealing with shrinking or static resources. A growing chasm exists between public expectations and what governments are able to offer as a result of this problem. In addition, a wide range of additional concerns must be dealt with, at the federal, city/state/local, healthcare, military, and education levels as well. Since the advent of the Internet, nothing has been held as much promising for public sector executives as the Internet of Everything, which has the ability to bridge the gap between citizens' expectations and what governments actually provide. The public sector has a unique chance to improve the quality of life for their citizens via the IoT. Type approval and cyber security methods, on the other hand, are critical for this new paradigm. Many traditional encryption algorithms fail in security and privacy in IoE which is not feasible for devices due to unawareness of the updated Trojan horse etc. The analysis of security and privacy issues for IoE domain is focused at various places such as home, city, government health center and more. In addition, it is at odds with the explanations offered by numerous IoE studies.

Keywords: IoE & IoT, machine to machine, privacy, security issues, communication network, big data

1. Introduction

Every day, millions of individuals across the world use technology to stay in touch with one another. The Internet connects a number of devices and allows them to communicate with one other. In every application, data is the most valuable resource for

DOI: https://doi.org/10.36548/jismac.2021.4.005
Received: 07.03.2022, received in revised form: 28.03.2022, accepted: 10.04.2022, published: 21.04.2022

making decisions. The goal of this procedure is to get the proper information to the right person or object. The IoE has four wings:

1. People,
2. Method,
3. Documents and
4. Device

Embedded technology and the Internet have opened the door to the interconnectedness of the items in our environment. It imagines a world in which Internet of Things IoT devices are ubiquitous and creates vast amounts of data without being noticed. To make this information intelligible and usable, this data must be kept and analyzed [1-5].

Mobile carriers, software developers, access technology suppliers, and others play a role in the Internet of Things paradigm. There are a wide range of uses for IoT, from industry and utility management to agricultural and health care. The Internet of Things is the next-generation paradigm for interconnecting objects and machines, making it possible for operations to be performed automatically without the need for human participation. In order to succeed in the IoT era, many communication infrastructures must be combined. Intelligent gateways have been developed to link IoT devices with the Internet. Cloud computing and the Internet of Things are now the focus of the most recent endeavors. Figure 1 shows the basic block diagram of IoE's privacy policy.

Governments may use big data and crowdsourcing to build new services that take advantage of machine-to-machine connections and provide them to citizens. Thus, the same innovative technologies that are altering supply chain management and logistics in the private sector may assist major businesses, government agencies, and cities. Mobile technology may be used to create "smart working" for workers, saving the company a lot of money in the process. These measures may also help to decrease expenses while making a good environmental effect. Researchers in academia and business must devote their whole focus to addressing the critical problem of privacy in the Internet of Everything. Protocols and frameworks for handling privacy in the IoE are urgently required. Remote health centres, power or energy consumption management, continuous monitoring places and novel measuring systems, all rely on the IoT. A user's personal information is critical in all of these apps, since it pertains to where they go and what they do [6-9].

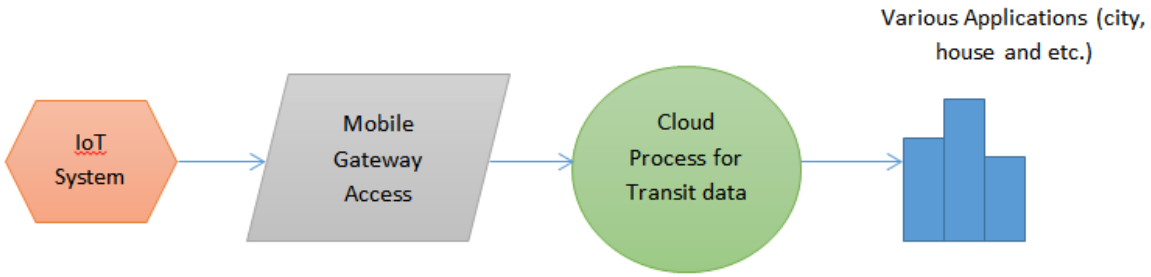

Figure 1. Basic block diagram of IoE's privacy policy

As a result of the Internet of Things in the public sector, services will be redesigned and repurposed in order to better serve residents. Near real-time data about citizen activities, such as where they are, what commodities they move across borders, how much they spend, and what would they buy in the future will be made available as a result of the IoE. As big data and the related analytics are applied to larger populations, predictive modeling and therefore improvements to public infrastructure will become more possible. Police departments are already using predictive modeling to assist them better deploy their resources in the battle against crime [10].

2. Organization of the Research

The entire research article consists of several sections as follows; section 3 gives recent works on security issues of Internet of Everything. Section 4 provides Cryptographic Framework for IoE. Section 5 discusses the elements of IoE in the public sectors. Finally, section 6 concludes with the future enhancement.

3. Recent Works on Internet of Everything

According to Buyya et al., the connectivity sensing part provides the maximum capacity to transfer digital data through standard framework that helps many types of application by IoT. Cloud computing of this research application is the main analysis for communication at both sides of data sharing [11].

When Tan and Wang described the Internet of Things, they do so from the perspective of communication, social and environmental contexts: IoE needs many authentication and profile based interfaces for communication at both ends such as transmission and reception field [12].

Paper [13] contains the latest current research on cloud based IoT security and privacy, which demonstrates the need of cloud computing for further process such as authentication through many nodes in the communication network domain for cloud security. For example, privacy advancements in the IoT may be found in numerous application areas, as outlined by the authors in [14]. The article also has a discussion of important future security needs for intelligent home systems. In addition, the authors proposed an appropriate secured communication at both ends for the IoE. Finally, for devices of limited resources and a need for high system availability, the gateway design is the best option suggested.

The security of mobile network challenges and issues are described in [15]. This architecture provided many resources through wireless domain with unstable topology of the security design issues. Despite these difficulties, it was feasible to create a multi-fence security system that provided comprehensive protection while achieving optimal network performance. Additional topics mentioned include packet delivery to many mobile nodes, as well as security.

The security of mobile sensing applications has been examined in [16]. Using these examples, the authors were able to highlight possible advantages that may be gained from their use. The data flow through the application architectures and the varied statistics of contemporary mobile sensing apps were examined by the authors.

In [17], the authors presented a low-power hardware-based IoT security strategy based on recognized standards and current Internet protocols. Due to its inability to avoid routing attacks and its weight, the suggested security solution does not work for low-power devices.

For Near Field Communication (NFC) based systems, Hameed et al., presented security issues in the IoE in [18]. NFC tags and dazzling posters were detected with little CPU and memory impact by the middleware in its early stages. Their middleware included additional lightweight primitives for use with any NFC applications requiring security and integrity.

3.1 Research statement

For safe communication and data transfer in an IoE environment, IoE devices employ the lightweight algorithm of the cryptographic scheme. Cryptography and steganography

methods are used to protect data sent over the Internet. An encryption key is used to encode information so that it can't be deciphered by an untrained eye. In steganography, information is disguised by hiding it in another medium, such as a picture or music.

4. Cryptographic Framework for IoE

The use of cryptography in the construction of security is widespread. Data may be protected via cryptography. A cryptographic hash function, for example, protects any devices in the public domain. This action is protected by encryption process using the SSL cryptography method.

Confidentiality: only the person to whom the material pertains has access to it;

Integrity: data cannot be changed or modified;

Authentication: the sender and recipient both validate their identities using cryptography.

To ensure that only the intended recipients and senders have access to or handle the data, cryptography encrypts it. That information is not accessible or understandable by intruders.

4.1 Cryptography using a Symmetric Key

It is possible to encrypt and decode a message using the same key. Using the same key, the sender and receiver decode the data that they've encrypted. To begin the discussion, the sender and recipient must first excise security issues from the channel. Some of the encryption done here is as follows:

1. The Caesar cypher,
2. Block cypher,
3. Stream cypher,
4. DES (Data Encryption Standard), and
5. AES (Advanced Encryption Standard) are all examples of symmetric-key cryptography.

4.2 Cryptography using Asymmetric Keys

This type of keys is also known as public key for the process of cryptography. There are many keys available for both encryption and decryption for this approach. A "public key" and a "private key" are the two types of keys. Public and private keys are used by both the sender and the recipient. In order to encrypt or decode a message, one key must be utilised. A private key is the one that is kept private. The secret key is never revealed to anybody. The public key has been released and made public. When sending data to a recipient, the sender encrypts it using the recipient's public key. The recipient will decrypt the incoming data in the decryption state of devices. Some of the example algorithms are as follows:

1. Diffie-Hellman,
2. RSA (Rivest-Shamir-Adleman), and
3. Elliptic Curve Cryptography

4.3 Identity management process in Privacy sector

4.3.1 User privacy and data protection in IoE

The protection of individual privacy is a top priority in the Internet of Everything. User privacy is a touchy subject in several studies. People, processes, data, and objects communicate and exchange data over the internet in IoE. The entire identity management, process in the privacy sector of IoE. The IoE network requires data privacy, exchange, administration, and security [19].

4.3.2 Privacy through identity

An authentication process (privacy) and identity management in the Internet of Things rely on a variety of technologies and procedures. With this, data and resources are better managed and protected. Authentication happens when two parties communicate across a network and exchange a set of credentials [20].

4.3.3 IoE secure communication

Things communicate in the IoE scenario. Secure communication between objects is impossible without trust. In order to build user confidence in the IoE system, a reliable mechanism must be in place [21].

4.3.4 Authorization and access control:

When a person or item is recognized, an authorization may be used to determine if they are allowed to access the resource. Access to resources is provided or restricted based on a variety of factors. Authorization is handled via the use of access controls [22].

4.3.5 End-to-End security:

IoE devices and Internet hosts must be protected using End-to-End Encryption (E2EE). A safe implementation of session keys and algorithms is required in order to guarantee total security end-to-end [23].

4.3.6 Attack resistant security solution:

The internet of things is interconnected with a wide range of gadgets. There are a variety of assaults that may take place on these devices, including as Denial-of-Service (DoS) and flood attacks [24].

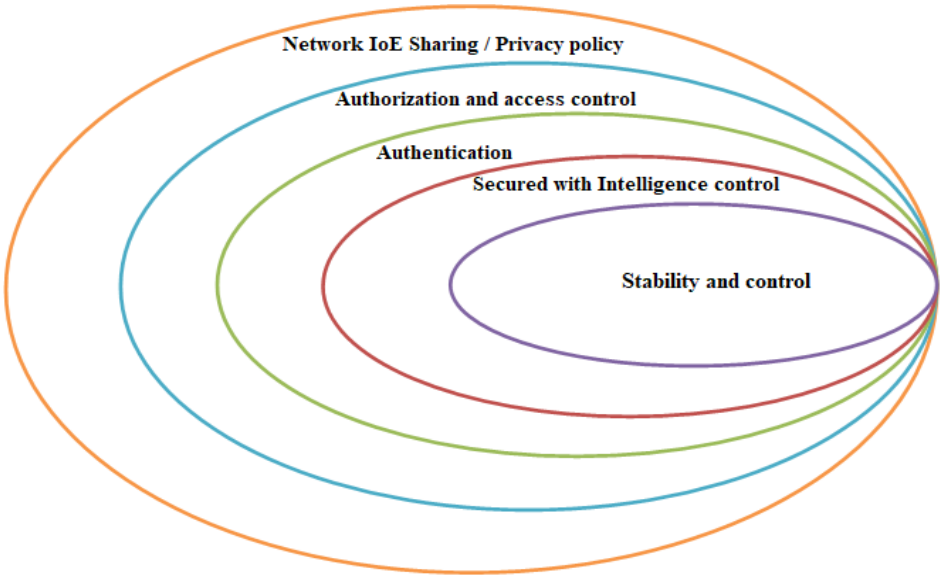

Figure 2. Identity management process in Privacy sector of IoE

4.4 IoE Security parameters

4.4.1 Confidentiality

Protecting data against unauthorized access ensures that it is only accessible to those with a legitimate need for it.

4.4.2 Integrity

Data integrity may be maintained by utilizing digital signatures to guarantee the integrity of IoE communications.

4.4.3 Availability

Every time a user wants to access data, devices, or services, they should be able to.

4.4.4 Authentication

There are a wide range of participants in the IoE, including individuals, services, service providers, and processing units. Therefore, every object must identify and authenticate other objects in order to function properly.

4.4.5 Nonrepudiation

A prerequisite for cyber-security in IoE networks is that no one can deny their actions.

5. Various Applications of IoE

5.1 Smart Home

The Internet of Everything's most popular use is the smart home. As an extension of building automation, a smart home is controlled and automated in a domestic setting. The term "smart home" refers to a house equipped with a variety of high-tech features, such as interconnected appliances, lighting, heating, cooling, televisions, computers, and other entertainment systems, as well as security and camera systems that can be operated remotely via plan schedule, communication devices and IoE.

5.2 Smart Supply Chain

For a few years now, supply networks have been growing smarter. Some of the more popular services include helping suppliers communicate inventory information and finding solutions to challenges like monitoring items while they're being transported. Various sensors carry data (information) of sensing devices such as IoE devices. The proposed IoE system is also capable of analyzing workflow and adjusting equipment settings to improve performance. For most farmers, distant agricultural operations and a huge herd of cattle are common, and the Internet of Everything may transform day-to-day operations.

5.3 Smart City

Data are collected and analyzed by IoE devices such as sensors, lighting, and meters in smart cities. After this, cities utilize the information for communication in public sector, private services etc. Using IoE in the smart city domain solves a variety of issues, including traffic congestion and air and noise pollution.

5.4 Smart Grids

Integrated into an IoE framework, the Smart Grid is capable of monitoring and managing everything from lights of traffic signals to the standing place of any vehicle through early prediction process, also during power activity such as seismic activity or other severe weather.

5.5 Public / Private Health center

The most recent IoE developments are put to good use in the healthcare industry. The cloud computing services is used to exchange the information (data) through communication networks carrying the storage devices by collecting and analyzing patient information.

5.6 Smart Retail

The IoE makes it possible for retail establishments to become more customer-centric by collecting real-time data on their patrons' preferences, requirements, and behaviors. By doing so, businesses are able to determine what their consumers want and need, and then provide it to them.

6. Conclusion

The Internet of Everything will eventually take the place of the IoT. Today, IoE network security and privacy is a critical factor in the cloud storage and process. IoE has tremendous hurdles when it comes to security and privacy. There are a variety of IoE security standards that may be used in a wide range of industries to make systems more automated. The network's intrinsic security will be used by devices connected to the network, ensuring IoE security using network-powered technologies rather than trying to ensure security at the device level. On the other hand, in order to maintain privacy, businesses will need to use technological solutions with sound procedures and regulations. For the IoT to be a success,

enterprises must establish new privacy models that fulfill the needs of both the corporation and the consumer.

References

[1] S. Hameed and U. Ali, "HADEC: hadoop-based live DDoS detection framework," EURASIP Journal on Information Security, vol. 2018, no. 1, p. 11, 2018.

[2] S. Hameed and H. A. Khan, "SDN based collaborative scheme for mitigation of DDoS attacks," Future Internet, vol. 10, no. 3, p. 23, 2018.

[3] Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. IEEE Access 2018, 6, 6900–6919.

[4] Conti, M.; Dehghantanha, A.; Franke, K.;Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 78, 544 – 546.

[5] Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mob. Netw. Appl. 2019, 24, 796–809.

[6] Li, Y.; Gao, M.; Yang, L.; Zhang, C.; Zhang, B.; Zhao, X. Design of and research on industrial measuring devices based on Internet of Things technology. Ad. Hoc. Netw. 2020, 102, 102072.

[7] Radanliev, P.; De Roure, D.; Page, K.; Nurse, J.R.; Mantilla Montalvo, R.; Santos, O.; Maddox, L.; Burnap, P. Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity 2020, 3, 1–21.

[8] Sharma, V.; Kim, J.; Kwon, S.; You, I.; Lee, K.; Yim, K. A framework for mitigating zero-day attacks in IoT. arXiv 2018, arXiv:1804.05549 .

[9] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.

[10] N. Aleisa and K. Renaud, "Privacy of the internet of things: a systematic literature review," in Proceedings of 50th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 2017.

[11] Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.

[12] Tan, L.; Wang, N. Future internet: The Internet of Things. In Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Karachi, Pakistan, 5–7 April 2010; pp. 376–380.

[13] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.

[14] H. Lin and N. Bergmann, "IoTprivacy and security challenges for smart home environments," Information, vol. 7, no. 3, p. 44, 2016.

[15] H. Yang, H. Luo, Y. Fan, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38–47, 2004.

[16] S. Gutwirth, R. Leenes, P. De Hert, and Y. Poullet, European Data Protection: Coming of age, Springer Science & Business Media, Berlin, Germany, 2012.

[17] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of ,ings with two-way authentication," in Proceedings of Local Computer Networks, LCN (2012), pp. 956–963, Clearwater Beach, FL, USA, October 2012.

[18] S. Hameed, B. Hameed, S. A. Hussain, and W. Khalid, "Lightweight security middleware to detect malicious content in NFC tags or smart posters," in Proceedings of 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 900–905, Beijing, China, September 2014.

[19] Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Commun. Surv. Tutor. 2020, 22, 616–644.

[20] Yu, M.; Zhuge, J.; Cao, M.; Shi, Z.; Jiang, L. A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. Future Internet 2020, 12, 27.

[21] Bansal, S.; Kumar, D. IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication. Int. J. Wirel. Inf. Netw. 2020, 27, 1–25.

[22] Granjal, J.; Monteiro, E.; Silva, J.S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Commun. Surv. Tutor. 2015, 17, 1294–1312.

[23] Deep, S.; Zheng, X.; Hamey, L. A survey of security and privacy issues in the Internet of Things from the layered context. arXiv 2019, arXiv:1903.00846.

[24] Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet Things J. 2017, 4, 1125–1142.

Author's biography

E. Baraneetharan is an Associate Professor and Head in the Department of EEE at Surya Engineering College, Erode, India. His area of research includes power electronics, electromagnetics, electric drives, IoT and data mining.