978-1-7281-4452-8/20/$31.00 ©2020 IEEE

An Overview of Privacy Issues in IoT Environments

Suha Ibrahim Al-Sharekh
Computer Science Department
Qassim University
Saudi Arabia
soha.e.sh@gmail.com

Khalil H. A. Al-Shqeerat
Computer Science Department
Qassim University
Saudi Arabia
kh.alshqeerat@qu.edu.sa

***Abstract*—Many regions in the world have recently sought to integrate and apply advanced technologies in various aspects of life. IoT applications have become popular in different areas such as smart homes, e-health, smart cities, smart connected devices, and many more. However, the growth and spread of IoT technology increase the security and privacy risks that users may experience. Security and privacy problems cannot be eradicated but can be mitigated. Therefore, it is necessary to explore and update dedicated solutions to alleviate them. This paper aims to provide and identify a comprehensive overview of privacy issues and a set of enhanced solutions to protect user privacy in IoT environments. Moreover, it surveys the opinion of researchers and experts regarding challenges and solutions related to IoT privacy. Finally, a set of recommendations and guidelines are suggested to enhance privacy in IoT environments.**

Keywords—Internet of Things, Security, Privacy, Risks, Threats, Survey

I. INTRODUCTION

In the last decade, the Internet has high importance in various areas of life and spread throughout the entire world. The number of smart devices connected to Internet is increasing rapidly day by day, which led to the emergence of a new technology called Internet of Things (IoT). This technology connects physical components and devices to the Internet without the need for human intervention. Internet of Things is a new technology, but it is an old term. Kevin Ashton mentioned this term in 1999 while holding a presentation at Proctor & Gamble [1]. He used this term to link the idea of radio frequency identification (RFID) technology to the Internet.

In the early stage, the concept of the IoT is equivalent to the RFID technology plus the Internet. In the 1990s, sales points and logistics were considered the most significant and most promising applications of IoT. IoT technology was used to identify the goods automatically and share information via the Internet [2].

Nowadays, IoT contains many sensors that are used in daily life to exchange information. Most people do not know about them, such as sensors used in smartphones like the camera and Global Positioning System (GPS).

A. IoT Charactristics

IoT is a complex system that has a set of different fundamental characteristics. These characteristics vary from one domain to another. In this section, some of the general characteristics are identified as follows, [3, 4]:

- Heterogeneity: Features of IoT-devices are heterogeneous as they operate on different networks and platforms. Besides, there is a wide range of applications that connect with a wide range of devices under multiple various protocols.
- Intelligence: IoT is a smart technology that contains variety of algorithms, software, hardware, and smart devices. An intelligence feature is required to support and enhance the IoT environment to support multiple tasks and make it easy to respond.
- Connectivity: The connectivity helps things access the network at any time. Interactions between objects are essential because object-level interactions achieve intelligence in IoT. Through the communication process, things connect with smart applications and provide compatibility in data consumption and production.
- Enormous scale: The number of IoT devices that need to be managed and that communicate with each other is much higher than the current devices connected to the Internet. The IoT range is vast and wide because of the large number of connected devices.
- Security: Although the importance and usefulness of IoT, its components are vulnerable to various threats and security attacks. There is a high level of privacy and transparency issues in IoT are required. As a result, it is imperative to secure networks, devices, and data by developing a security model able to protect IoT-system against any potential attack.
- Dynamic changes and Nature: The primary activity of IoT is data collection from its diverse environments, where the status of devices such as connection, disconnect, temperature, location, must be changed dynamically.
- Sensing: IoT will not be possible without sensors; they are used to detect and measure changes and interactions in the environment.

B. IoT Benefits

IoT is one of the most critical technologies that can improve many aspects and used in many applications. This section discusses the critical benefits of IoT [4].

- Cost savings: costs can be reduced by improving the efficiency of many operations, such as remote patient monitoring in clinics.
- Processes and resource optimization: IoT provides analytics for extensive real-time data through sensors to improve operational efficiency, reduce power consumption, make more decisions and improve quality.
- Improved productivity: IoT has tremendous potential in improving productivity for companies and users by

978-1-7281-4452-8/19/$31.00 ©2019 IEEE

employing highly skilled people and reducing the mismatch of available skills.

- Minimizing human efforts and errors: IoT technology reduces human interaction using intelligent and smart devices. Moreover, it reduces any additional effort resulting from fixing errors by including required mechanisms to correct and reduce errors.
- Increased safety and security: IoT is useful in improving and increasing safety and security within devices and in places using necessary sensors and cameras that help to secure environments.

IoT creates an excellent opportunity for economic and industrial growth as well as increases comfort in life. However, it is vulnerable to security risks and threats.

Recently, many kinds of researches have addressed IoT security issues and their requirements. Mirza Abdur Razzaq, Sajid Habib Gill et al. [5] focused on IoT security issues in particular and stated that many IoT devices lacked security and therefore discussed many security requirements such as confidentiality, authentication, etc. They surveyed and identified many types of IoT attacks and solutions. The authors in [6], have discussed the IoT components and their vulnerabilities. They studied various security issues related to IoT and mentioned some ways to develop the security of devices efficiently.

This paper conducts a comprehensive study on privacy issues and reviews the most appropriate techniques to enhance privacy in IoT environments. It focuses on answering the following two research questions:

1. What is the primary concern of privacy in IoT?

2. What are the best helpful techniques that might be used to enhance privacy in IoT environments?

The rest of the paper is organized as follows. Section II presents an overview of privacy issues in IoT. Section III reviews the appropriate techniques used to enhance the privacy of IoT. Section IV shows and discusses the results of the survey. Finally, a set of recommendations and guidelines are presented in section V.

II. OVERVIEW OF PRIVACY IN IOT

Privacy refers to access and manage personal information by an authorized user. It is one of the essential requirements required to achieve personal security and protecting sensitive and private user data such as passwords, credit card numbers. Any physical component can communicate privately and securely over IoT using a unique identifier.

IoT produces enormous amounts of sensitive personal data. These data must be sent, processed, and then stored in order to be secure. Due to the rapid spread of IoT technology, the protection and maintaining data privacy is very challenging in the IoT systems.

The International Telecommunication Union (ITU) has pointed out the user privacy as a significant challenge facing IoT [7].

A. Privacy Concept

Privacy assurance involves individuals who have the right to control and manage their information. Therefore, privacy is a prime requirement for people who deal with IoT. Figure 1 shows the essential five distinctive and prominent aspects of privacy [8]:

1) Unlinkability - the protection of information between elements related to the relationship, for example, topics, messages, and procedure.

2) Untraceability - inability to trace someone based on a set of actions that have been implemented.

3) Unobservability - intended to protect the identity and message exchanged between the sender and receiver.

4) Anonymity - intended to protect all information relating to the person who performed a particular action.

5) Pseudonymity - intended to use aliases instead of real names or identifiers.

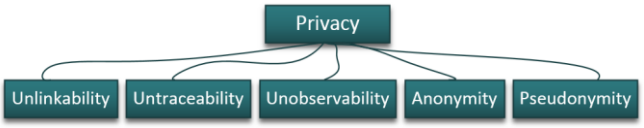

Fig. 1. Privacy Services

B. IoT Privacy Requirements

Privacy ensures that personal information is hidden from intruders. There are essential requirements for privacy that aim to achieve high reliability in IoT [9]. These requirements are illustrated as follows:

- Access control: Data providers must have access control mechanisms to protect IoT personal data from damage or abuse by other people. Data must be available only to authorized persons.
- Client privacy: Data providers must follow a set of steps to refrain from observing the use of the user's search system. The promotion of privacy in the IoT has become a prerequisite, and privacy management has been suggested to tag data to maintain data and to use a privacy model called the Anonymity model.
- Trust: Providing trust for data exchanged between users and service providers is one of the privacy requirements in IoT. Its presence helps enable reliable data flow through the IoT system using identity authentication, signature, and more. IoT devices must serve their identity and data to make other devices and users trust them.
- Identity management: It is not limited to identifying users and determining their access to different types of data. However, Identity Management can identify devices, sensors, and manage their access to sensitive data. It must be able to do some procedures such as identifying who can access data, adding authentication instructions in IoT devices, establishing safeguards to protect privacy of personal information.

C. Privacy Concerns in IoT

The nature of IoT is different from the conventional Internet in that it contains enormous information collected around the user. Data is collected globally in IoT, and it is used to build a user profile [10]. The privacy of users and the

protection of their data is one of the most critical challenges in IoT. There are many privacy concerns that must be considered [11,12].

- Privacy in Devices: Sensitive information might be leaked from IoT devices by unauthorized manipulation or hackers. For example, the intruder may re-configure the smart surveillance camera and send data to other people. Devices also have a role in the security of data privacy. If security is poor, this will address several issues affecting data privacy — for example, identifying and damaging the user ID. In order to provide privacy in the devices used, there are many issues and concerns that need to be addressed, such as user privacy that must be protected in case of theft of the device.
- Privacy during Communication: Users are always concerned about the privacy of their data. Data may be lost or modified during the transmission due to the use of an unsecured wireless medium, especially in the case of sheer scale and large amount of distributed data among IoT systems.
- Privacy in Storage: Privacy of information storage is a privacy concern in IoT because of the large amount of data, making data storage process is very difficult. Two steps are considered to protect the privacy of information storage; storing information that a user needs and maintaining the security of personal information.
- Privacy in Processing: Personal data must be handled consistently with the intended purpose. It should not be disclosed without the permission of owners. The user must define data privacy policies as they are processed, using secure and efficient devices.
- Privacy in Ownership: Ownership is also a concern for IoT privacy, especially if more than one person share system resources. Data ownership privacy issues can create many differences and conflicts between participants.

III. PRIVACY ENHANCING TECHNOLOGIES (PETS)

The privacy of user data is a major concern in IoT. Privacy requirements are difficult to meet because of the difficulty in controlling the amount of data resulting from misuse of devices. As a result, protecting and enhancing privacy becomes vital in IoT. There are several techniques used to enhance the privacy of personal data as follow:

- Domain Name System Security Extensions (DNSSEC) provide access to public key encryption for signing records to ensure data integrity and validity [13]. However, DNSSEC can only include the validity of information in one case if the Internet community adopts it.
- Private Information Retrieval (PIR) Systems are intended to hide client information. However, there are problems in the critical management of the system, for example, registration that makes this method not practical.
- Onion routing is one of the techniques used to enhance privacy in IoT. It works to encrypt and integrate Internet traffic from a different number of sources. So, it encapsulates and distortion data in multiple encryption layers using public keys for the onion routers in the transmission path [14]. This process helps in blocking the matching of a specific packet of IP with a particular source. However, it increases waiting time and thus may lead to many performance problems.
- Encryption mechanisms are used to protect sensitive information from being stolen or modified during transmission [15]. IoT devices need to be built with strong encryption standards to safeguard transmitted data through an encrypted and anonymous tunnel.
- Virtual Private Networks (VPN) are extranets have established by a group of close partners. Only partners can access them. These networks have a common goal of making data confidential and secure in addition to maintaining their integrity. However, the virtual network does not provide a solution for the dynamic global exchange of information. It cannot share its information outside the extranet, which makes privacy enhancement technology ineffective because the information is binding within a limited framework between partners only without third parties.
- Transport Layer Security (TLS) improves the confidentiality and provides data integrity. However, it faces the problem that every object needs and requires a new connection with the TLS. As a result, the search for information will be negatively affected by many of these layers.
- Personal information management systems (PIMS) help individuals to control their private data in secure local storage systems over the Internet.
- Identity management (IdM) controls user information in the IoT-system. It includes information for authenticating the user identity and manages personal private information.
- Privacy Enforcement Point (PEP) allows the user to protect the access to his data and control privacy even in a case if the network is not protected. It provides adequate security for privacy. The PEP has two main tasks; data protection as a basis for privacy mechanisms which requires a secure infrastructure [16]. Therefore, it provides main functions for data protection by encrypting data with the public key, placing it in the cloud, and then decrypts only when need to access data. Moreover, it controls flexible access by allowing only those who are authorized to access their data.
- Identity-Based Encryption (IBE): It is an encryption scheme on IoT devices. It is a secure exchange of data because it helps devices by using a personal ID such as a user name or a serial number such as a public key. It uses simple and confidential keys, through which data is controlled and encrypted from unauthorized persons [17].

- Privacy Verification Chains (PVC) is one of the solutions used to protect privacy in IoT. It is a framework that allows data exchange between participating entities such as applications and users based on digital contracts. All contracts are made available to the participating entities, and each entity has a privacy book, so that the user can verify which entities are using his data. IoT applications can prove that this information is their own through contracts, and this solution ensures the confidentiality and privacy of data in the IoT. Therefore, it helps to improve and enhance the level of privacy in the IoT systems.

IV. SURVEY RESULTS ANALYSIS AND DISCUSSION

The conducted questionnaire is based on the research questions in this study. It was distributed to a sample of people who have an interest in IoT, such as IT experts, faculty members, and graduate students from various universities in Saudi Arabia and other countries. The number of participants was 223 participants.

It was noticed that approximately 8.5% of respondents are not aware of the concerns facing privacy, and 26.5% are unaware of the most critical technologies that promote privacy. These percentages indicate that users need to be more aware of the security and privacy issues in IoT environments.

A. Major Privacy Concern in IoT

The responses to the first question are represented graphically in Figure 2. Data privacy is always concerned for users. 33.2% of respondents have concerns about privacy during communication. It is the primary concern of privacy in IoT because sensitive and private data may be lost during the connection process because of the nature of unsecured wireless networks.

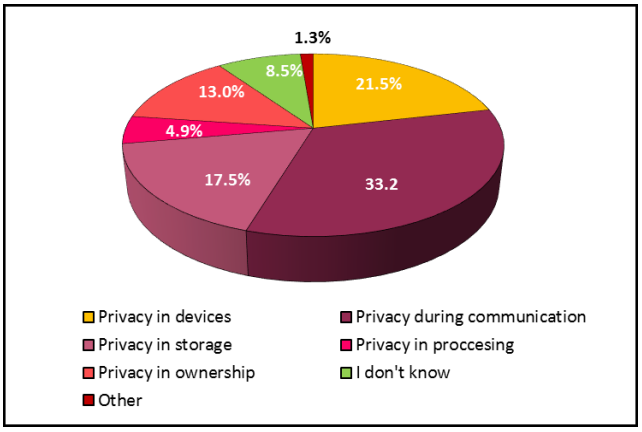

Fig. 2. Response chart for privacy concern in IoT

21.5% of the respondents agree the privacy in devices is are a significant concern of privacy in IoT. From their point of view, there may be leakage of private information through the devices using unauthorized access by hackers and intruders. If the security of devices is weak, lead to losing privacy within them.

There are 17.5%of the participants selected privacy in storage. We want to give our view to respondents who did not choose this choice. The extensive data stored in IoT leads the storage too tricky, and some data may lose their privacy.

The privacy in ownership got 13.0% votes from the respondents. We notice the respondents have concerns about ownership. They have a view that if there are a group of developers within the IoT system may attribute some people's private data to themselves and therefore, cause concern in privacy concerned about who owns the data.

Some respondents have selected privacy in processing (4.9%). Interestingly, only 8.5 % of respondents do not know about the concern of privacy in IoT.

Finally, 1.3% of the respondents think that there are other concerns may affect privacy.

B. Technologies to Enhance the Privacy in IoT

The responses to this question are represented graphically in Figure 3. Although privacy is very important for the user, however, disappointing that 26.5% of those included in the questionnaire did not have any background about the technologies used to enhance privacy in IoT.

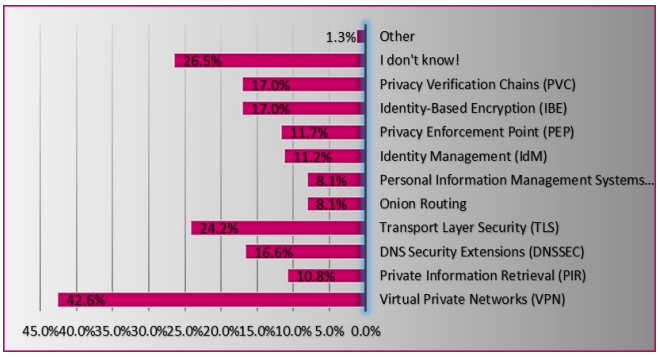

Fig. 3. Response chart for privacy technologies used in IoT

From Figure 3, the most technique that got the highest vote rate (42.6%) by a large ratio of respondents is virtual private networks (VPN). This virtual network maintains privacy so that no one except owners can access it, but it does not provide a solution to share information outside the framework of its network, where information is required and limited to the partners only. We think about the reason they choose this technique because it is a well-known technique for privacy, but they may not know about the existence of Blockchain technology to enhance privacy.

24.2% of respondents selected transport layer security (TLS), It is useful to increase data confidentiality, but the problem is that the object requires a new connection each time with the transport layer security.

We notice the respondents have a similar vision about the techniques to improve privacy in IoT. Therefore, identity-based encryption (IBE) and privacy verification chains (PVC) occupy the same rank (17.0% of the respondents). Distinguishes between these two technologies, the privacy verification chains (PVC) is one of the best techniques based on Blockchain to enhance privacy in IoT because it ensures the confidentiality and privacy of data through smart contracts compared to the identity-based encryption which uses simple secret keys that may be controlled by unauthorized users.

DNS security extensions (DNSSEC) with 16.6% votes from responding. It provides access to public-key encryption in IoT to ensure the integrity of information, but it is not considered an ideal technology from our point of view because it contains information in one case only if adopted by the Internet community.

11.7% of respondents selected the privacy enforcement point (PEP), and 11.2%, of them, were selected identity management (IdM). We notice from the close voting ratios (11.7% and 11.2%) the respondents say that these two technologies have similar mechanisms to maintain privacy in IoT and enhance it by protecting user data by encryption, control the information, and access method.

Although the private information retrieval (PIR) allows user information to be hidden well, it may encounter problems in the system management, only 10.8% of the sample use it to enhance privacy in IoT.

The findings show the technique based on personal information management systems (PIMS), and the technique of onion routing occupy the same rank (8.1%) of respondents.

1.3% of the respondents added suggestions to enhance privacy in IoT such as using Blockchain techniques encryption for enhancing privacy in IoT.

V. RECOMMENDATIONS AND GUIDELINES

This section presents a set of baselines recommendations and guidelines for developers and users to use when adapting IoT technology in their systems.

Recommendations and guidelines are distributed into two categories. First, protection devices and networks in IoT environments, while another to ensure privacy in IoT systems.

A. Protect IoT Devices and Networks

- Set strong passwords: IoT users must set new and strong passwords to prevent their devices from being hacked by using uppercase and lowercase letters, numbers, and symbols. Besides, do not use common default passwords and names.
- Create a separate network: Creating a separate VLAN to keep their smartphones and devices connected to their network. This method prevents others from unauthorized access, which also helps to keep important information and files.
- Update firmware: Updating the IoT firmware regularly to protect and secure devices from any potential cyber-attacks.
- Use a firewall: The firewall must be used in smart devices to monitor traffic between devices to detect threats. The firewall has the advantage of preventing the attacker from accessing the device.
- Research before buying: The user should search for high-security devices and verify other users' opinions before buying the device to see if the device has problems. For example, it might include some known vulnerabilities.
- Use binary (two-factor) authentication mechanisms: This type of authentication provides high security and prevents attackers from accessing the device, by using an additional security layer with the password, for example, send code to email or SMS before entering to any programs.
- Secured connections: IoT devices are connected to the Internet. Therefore a secure network such as a virtual private network (VPN) must be used.
- Limit the connections: Reducing the number of ports through which the device can be accessed, making it more secure and connecting the device to the Internet if necessary.
- Testing the devices regularly: One of the best ways to identify the security of the device is to test it through some programs that identify malware.
- Provide an appropriate environment: This is done by putting the device in safe places, for example, placing the smart device in a package containing an alarm device to alert in case of tampering or case of bad weather.

B. Protect IoT Devices and Networks

Protect data privacy in IoT such as personal data, passwords, encryption keys, according to the following recommendations:

- Companies are must respect a user's IoT usage by not tracking, monitoring or publishing their information.
- Companies should also find and adopt privacy enhancing techniques and mechanisms.
- Encrypt the stored data in IoT environments to minimize the risks and attacks that result from if the device connected to another device or network. If the encryption key is lost, the data will also be lost.
- Protect privacy in IoT by solutions related to Blockchain technology which maintains the confidently of data and encryption to enhance privacy in IoT.
- Back-up data in a safe place to provide backup in case of data breach or loss.
- Protection of personal ownership data by establishing their rights. Therefore, no one else can attribute this data to them as it does in some companies.
- Enhancing privacy by using some techniques that protect personal user data.
- Applying end-to-end encryption is essential in ensuring that sensitive information captured by IoT devices is protected.
- Minimize the number of data sources due to collecting data from different sources helps malicious parties to identify personal and sensitive information for IoT users.
- Encrypt data communications by encrypting communications from one device to another using

encryption devices and securing the connection to the cloud by securing Transport Layer Security (TLS).

- Get IoT apps certified to increase confidence in their applications.
- Do not share sensitive data between users.
- Enhance awareness of data risks and benefits.

VI. CONCLUSION

Nowadays, IoT technology has great importance in many areas and aspects of lives. However, it faces many security and privacy challenges. This paper has presented a comprehensive study on privacy issues and concerns. Also, it reviewed a set of solutions and mechanisms to enhance user privacy in IoT environments. Furthermore, a survey has been conducted among IT experts, researchers, faculty members, and graduate students from many universities in Saudi Arabia and other countries. It surveyed the opinion of 223 participants on main privacy concern and the best techniques used to enhance IoT privacy. Finally, a set of recommendations and guidelines have been suggested to enhance privacy in IoT environments. Recommendations and guidelines were distributed into two categories; protection of IoT components and privacy assurance in IoT-systems.

REFERENCES

[1] Peña-López, "the internet of things, "ITU. Internet report, Geneva, Switzerland, 2005.

[2] F.A. Alaba, M. Othman, I.A.T. Hashem and F. Alotaibi, Internet of Things security: A survey," JNCA. Journal of Network and Computer Applications, vol. 88, pp .10-28, Jun, 2017.

[3] O. Vermesan and P. Friess, "Internet of things-from research and innovation to market deployment,". Aalborg: River publishers, 2014, Vol. 29.

[4] K.K. Patel and S.M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," IJSER. vol. 6, May, 2016, DOI. 10.4010/2016.1482.

[5] Razzaq, M.A., Gill, S.H., Qureshi, M.A. and Ullah, S., 2017. Security issues in the Internet of Things (IoT): A comprehensive study. International Journal of Advanced Computer Science and Applications, 8(6), p.383.

[6] Youm, H.Y., 2017. An Overview of Security and Privacy Issues for Internet of Things. IEICE TRANSACTIONS on Information and Systems, 100(8), pp.1649-1662.

[7] X. Lu, Z. Qu, Q. Li and P. Hui, "Privacy information security classification for internet of things based on internet data, IJDSN, vol. 8, Aug, 2015, DOI. ID 932941.

[8] K. Thinakaran, J.S. Dhillon, S.S. Gunasekaran and L.F. "A CONCEPTUAL PRIVACY FRAMEWORK for privacy-aware IoT health applications," ICOCI, vol. 138, no. 6th, pp. 175-183, Apr, 2017.

[9] R.H. Weber, Internet of things: "Privacy issues revisited," ScienceDirect. vol. 31, no. 5th, pp. 618- 627, Oct, 2015.

[10] C. Lu, "Overview of security and privacy issues in the internet of things, Washington University," pp. 1-11, May, 2014.

[11] B.D. Weinberg, G.R. Milne, Y.G. Andonova, Y.G. and F.M. Hajjat, Internet of Things: Convenience vs. privacy and secrecy," ScienceDirect, vol. 58, no. 6, pp.615-624, Dec, 2015.

[12] J.S. Kumar and D.R. Patel, "A survey on internet of things: Security and privacy issues," IJCA, vol. 90, no. 11, Mar, 2014.

[13] S.C. Cha, T.Y. Hsu, Y. Xiang and K.H. Yeh, "Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges," IEEE Internet of Things Journal, Oct, 2018.

[14] R.H. Weber, "Internet of Things–New security and privacy challenges," IEEE, vol. 26, no, 1, pp. 23-30, Jan, 2010.

[15] S.U. Rehman, I.U. Khan, M. Moiz and S. Hasan, "Security and privacy issues in IoT, IJCNIS. International Journal of Communication Networks and Information Security," vol. 8, no. 3, p. 147-157, Dec, 2016.

[16] Henze, L. Hermerschmid., D. Kerpen, R. Häußling, B. Rumpe and K. Wehrle, "User-driven privacy enforcement for cloud-based services in the internet of things," IEEE, pp. 191-196, August, 2014.

[17] T. Güneysu and T. Oder, "Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things," IEEE, pp. 319-324, Mar, 2017.