Journal of Theoretical and Applied Information Technology
15th December 2020. Vol.98. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY CHALLENGES IN 6LOWPAN PROTOCOL FOR INTERNET OF THINGS: A REVIEW

MARINA MAZNI MAZLAN[1], NURUL AZMA ZAKARIA[2], ZAHEERA ZAINAL ABIDIN[3]

[1,2,3] Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat Dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka,Malaysia,

Email: [1]marinamazlan93@gmail.com, [2]azma@utem.edu.my, [3] zaheera@utem.edu.my

ABSTRACT

Internet of Things (IoT), is one of the Internet technology that has undergone rapid evolution over the past numerous years. The IoT connects various ranges of devices such as actuators, sensors and processes, which can assist in connecting several applications through the Internet. 6LowPAN plays an important role in the IoT world where the network type has its unique characteristics and applications. 6LoWPAN is an open standard protocol for IPv6 in wireless network.6LoWPAN is said to be the "mini" version of IPv6, which enables IP-based connection between smart objects and devices. However, the 6LoWPAN protocol is easily to be attacked due to its issues when trying to integrate into the Internet and the limitations shown by the LoWPAN itself. In order to overcome this issue, therefore a review study has been conducted to understand the 6LoWPAN packet formatting, methods to secure it, available tools or frameworks and challenges for IoT since it has been widely used in the wireless networks. It is expected from the review study that several approach or methods focusing on 6LoWPAN network security. Based on the review process conducted, we found out that main security challenges in 6LoWPAN network are still not yet to be tackled and have a better solution despite of its new achievement in researches.

Keywords; *Internet of Things, 6LoWPAN, Security, IoT Security, Systematic Literature Review*

1. INTRODUCTION

In the recent decades, Internet of Things (IoT) spaces have been studied extensively. This is primarily due to its capability in connecting several existing technologies in one ecosystem. The term "Internet of Things" is representing electrical or electronic devices of various sizes and capability, which are connected to the Internet [1]. IoT has developed and extended to different domains and applications, for example, healthcare, energy, smart cities, industry, environment and entertainment [2].

The primary objective behind the IoT is to have internet-enabled things, for instance, computers, mobile phones, RFID tags which are connected to the network dynamically, cooperate on shared center to accomplish different tasks [3]. Author in [4] highlights that around 25 billion uniquely identifiable objects are expected to be a part of this global computing network by the year 2030. This shows that such an enormous number; however, popularity of big network of interconnected devices will have higher chances of facing several kinds of issues including security and privacy threats.

The communication protocols for IoT can be classified into two categories: (1) Low Power Wide Area Network (LPWAN) and (2) Short Range Network [5]. The LPWAN is the new development of wireless sensor networks (WSN) and is used for long-range IoT applications. The examples of LWPAN are SigFox and Cellular. On the other hand, Short Range Network is used for short-range IoT applications that require low bandwidth power consumption and low latency. The examples of short-range networks are ZigBee, Bluetooth (BLE), RFID, NFC, Z-Wave and 6LoWPAN.

6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) [2] is one of the capable technology of IoT [6] which allows IP-based connection between smart objects and devices, accommodating independent Internet links without centralized architecture. 6LoWPAN is used to connect low power, IPv6 driven nodes and large mesh network to the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Internet thus making it suitable to be implemented for IoT applications.

However, despite of 6LoWPAN being the most commonly used standard in IoT, the issue highlighted by author in [7] is there are no security mechanism for the 6LoWPAN adaptation layer. This statement is supported by author in [8], which stated that 6LoWPAN depends on data link layer and the upper layers for security since 6LoWPAN does not provide any security by itself.

The main objective of this systematic review is to understand what are 6LoWPAN and its security challenges in IoT. This systematic review also aims to identify the current security challenges in 6LoWPAN protocol in IoT. In order to achieve these objectives, the systematic review will address these following research questions:
RQ 1 – What are 6LoWPAN protocol and its security challenges in IoT?
RQ 2 – What are the current security challenges in 6LoWPAN protocol in IoT?

The following section describes the methodology whereas Section 3 presents the analysis and results of the study. Section 4 and Section 5 discuss about the trends of security challenges in 6LoWPAN and the challenges and issues in 6LoWPAN for IoT. Finally, this paper ends with conclusion and future works.

2. METHODOLOGY

In this study, a methodology called Systematic Literature Review (SLR) is applied for this research. The main guidelines for the systematic literature review are mainly adapted with necessary alteration to fit in this research.

2.1 Keywords and Search String

The keywords were selected suitably to search related to the subjects. Since this paper is focusing on two main domains that are 6LoWPAN and Security Issues in IoT, thus the search keywords include:

- Internet of Things
- IoT
- 6LoWPAN
- 6LoWPAN architecture
- Security
- IoT Security

The search strings were set as: (Internet of Things* OR IoT*) AND (6LoWPAN* OR "6LoWPAN architecture") AND (Security* OR "IoT Security").

2.2 Study Selection

Selection of journal articles and conference papers was completed based on the keywords and search strings. Since the research topic is mainly covering two main areas, it is reasonable to run the search strings and keywords through several databases that incorporate Proquest, ACM Digital Library and IEEE Xplorer. The languages for selected journals, articles and conference papers are restricted to only English and Malay languages. In order to accomplish the main purpose of this research, the date range for collection was set between years 2015 – 2020. The overall selection is shown in Table 1.

Table 1: Selection Criteria

Selection Criteria	
Languages	English, Malay
Publication Types	Journal Articles, Conference Papers
Database	Proquest, ACM Digital Library, IEEE Xplorer
Date Range	2015 – 2020

2.3 Inclusion and Exclusion Criteria

Table 2 lists the inclusion and exclusion criteria used in this study. The journal articles and papers that were selected after the inclusion and exclusion criteria were reordered in a reference management system, Mendeley for thorough data extraction and citation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Inclusion and Exclusion Criteria

Item	Inclusion Criteria	Exclusion Criteria	No of Papers
1	Titles that include the complete keywords in the search string Titles that include 'IoT', '6LoWPAN' and 'Security' in general settings	Titles that do not include 'IoT', '6LoWPAN' and 'Security' in general settings	99
2	Focusing on 6LoWPAN in IoT ecosystem	Where 6LoWPAN in IoT ecosystem is not compelling	45
3	Focusing on security in IoT ecosystem	Where security in IoT ecosystem is not compelling	31

2.4 Data Extraction

For the data extraction process, excel sheet template was prepared in order for the data extraction from each article to be done. The template includes columns to capture detailed information or description of each paper. Every chosen paper was read systematically for extracting the consistent information to the columns. The related information was then placed into the Excel sheet template.

3. ANALYSIS AND RESULTS

3.1 6LoWPAN

For IoT, there are two different types of networks, which are Non-IP or IP. 6LoWPAN, an adaptation layer that represent solution for IoT IPv6, runs on IEEE 802.15.4, a low-power radio for devices with limited space, power and memory. IPv6 has been selected as the IP IoT network fabric since IPv6 is more suitable for IoT systems compared to IPv4 [9].The 6LoWPAN architecture consists of three main parts: host node, router node and edge router.

The hosts are able to sense the physical environment and operate equipment. The routers are intermediate nodes, which forward data packets to the edge routers or to a destination within the 6LoWPAN network from the host.

Interconnection and traffic management between 6LoWPAN networks and other IP networks, for example, Neighbour Discovery (ND) and handling IPv4 interconnectivity, are provided by the edge routers [10]. Unique IPv6 address is use to identify each 6LoWPAN element when sending and receiving packets between 6LoWPAN and IP nodes in other networks occur in end-to-end structure.

3.1.1 6LoWPAN Protocol Stack

The adaptation layer is included in between the IPv6 network layer and the IEEE 802.15.4 link layer to suit the transmission of IPv6 packet inside the 802.15.4 framework. The 6LoWPAN protocol stack is shown in Figure 1.

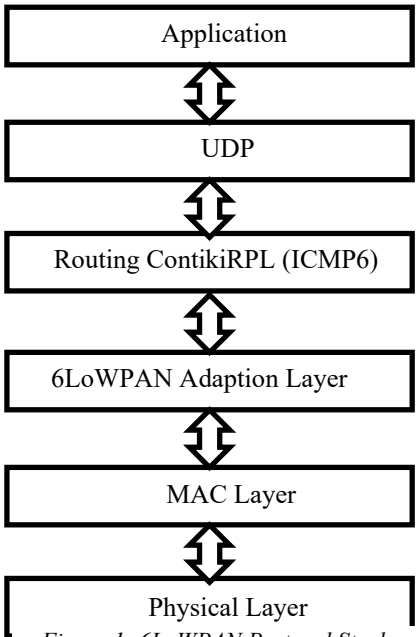

Figure 1: 6LoWPAN Protocol Stack

As described by IEEE 802.15.4 standard, the physical layer has the data rate of 250 Kbit/s,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

running in 2400 – 2483.5 MHz Industrial Scientific and Medical (ISM) frequency band [11]. The Medium Access Control (MAC) layer offers the mechanisms that enable the channel access for communication, for instance, handling the channel access through Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) device. 6LoWPAN provides the unassertive link layer condition; the fundamental benefit required by the interface layer is for one node to be able to send unicast packets to another node inside radio reach.

Header compression and decompression, fragmentation and reassembly, address auto-configuration and provides support for mesh-based routing are all done in the adaptation layer. The presence of this layer is actually to signify the main difference when compared to the conventional OSI layers. The 6LoWPAN outlines several types of encapsulation headers and these headers are incorporated into the payload of the IEEE 802.15.4 MAC protocol data unit (PDU) and the IPv6 packets are included as payload after these encapsulation headers.

In 6LoWPAN architecture, the network layer devices are implemented by IPv6 protocol and it is also responsible for routing. There are two types of routing that can be considered in 6LoWPAN network: routing inside the LoWPAN and routing between a LoWPAN and another IP network. For the transport layer, it is identified by two protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Internet Control Message Protocol v6 (ICMPv6) is used for control messaging, for instance, ICMP destination unreachable, ICMP echo and Neighbour Discovery messages. Due to its lightweight application, UDP is preferably to be used in 6LoWPAN architecture.

The application layer ensures reception and transmission of IPv6-compliant packets. The alteration of this layer is required due to several low power and lost network limitations. More broadly, 6LoWPAN architecture is mainly build up by several LoWPANs, which are connected to other IP networks through edge or border routers. These routers are a significant part and handles 6LoWPN compression, ND procedure, node address resolution, duplicate address detection, packets transmission from one 6LoWPAN to another or packets forwarding between backbone and 6LoWPAN networks.

3.2 Security

The topic of security issues is one of the most active areas in IoT research today. Yang et al. [12] indicated that security and privacy is still massive issues for IoT and these issues will lead to a whole new degree of online privacy concerns for consumers. The finding is consistent with the findings of previous studies by Tabrizi and Ibrahim [13] that states despite of the innovative technologies of IoT, the security issues is one of the challenges.

The security objective of IoT is to guarantee proper identity authentication devices and provides confidentiality regarding the data. The CIA triad, as shown in Figure 2,is a development model for security mechanisms. Any breaches in any of these three areas would cause serious security issues to the IoT ecosystem [4].

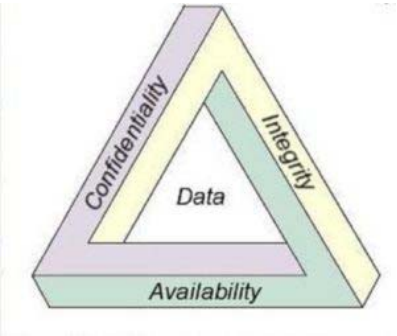

Figure 2: The CIA Triad [4]

3.2.1 IoT Security Issues

Figure 3 illustrates of the key security concern for IoT ecosystem by author [14]:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

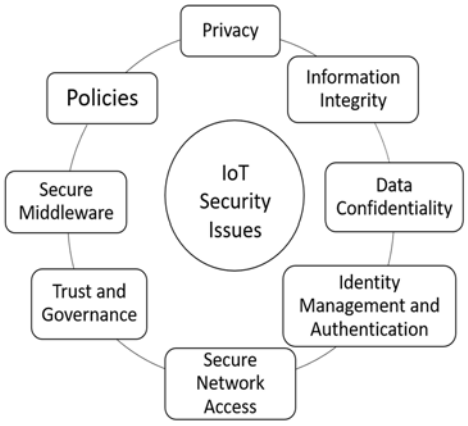

Figure 3: IoT Security Issues

3.2.1.1 Identity Management and Authentication

A major component of security is a solid and secures identity and authentication for an individual, which needs guidelines and instruments for the administration of the individuals' identity and objects. Communication between both parties can be control by using identity authentication and access control. This action will confirm true identity of an individual and prevent disguised attacks.

3.2.1.2 Data Confidentiality

Data confidentiality signifies an important issue in IoT ecosystem, demonstrating the assurance that only approved individual who can access and alter the information. Within the IoT context, only authorized objects or individuals may access to the data stored. For this issue, the requirement of two important aspects is crucial: the definition of an access control mechanism and the definition of an object authentication process.

3.2.1.3 Information Integrity

The information has to be the ones that we wait, and must not be modified in a prohibited way. So the considered elements must be accurate and complete[14]. Information integrity denotes the accuracy of the information to the primary subject and the suitability of the information for its intended use. Moreover, the information provided must a complete and not being tampered by any individual or by the organization bodies. Typical structure of information integrity consists of events or instances that have numerous attributes and characteristics, which may or not be included in the set of information. Some information requires a tiny attribute but some need large attributes depending on the intended use of the information. Thus, it is important to know the purpose of the information to be uses that called as meta-information. The parameter to measure information integrity is by using accuracy, relevance, precision, timelines and completeness [14].

3.2.1.4 Privacy

Internet of Things privacy is the special attentions needed to protect the information or data of an individual from disclosure in the IoT ecosystem. Any physical or logical individuals or objects are given special identifier and the ability to communicate independently over the Internet or other network. The privacy in Internet of Things plays an important subject to be considered and to be higher in changes of sensitive information leaking through unauthorized access due to devices interconnected 24 hours in 7 days with various hardware and software in the smart offices or smart manufacturing. Moreover, the privacy has category of level based on weightage, such as fair, legitimate and personal.

3.2.1.5 Secure Network Access

For any devices that are allowed, it gains access to the network or the servicing connection. All information providers must be capable to apply the access control on the information provided. One of the main functions in the network access system is the capability to inventory and tag every unknown piece of hardware inside the network. That way, you can categorize IoT devices into groups that have limited permission with what they can and cannot do. NAC tools will constantly monitor IoT activity to ensure outsiders have not hijacked the devices themselves. In order to monitor the IoT devices in the network, the available service to be used is the Software as a Service (SaaS) subscription, which typically a monthly service.

3.2.1.6 Trust and Governance

Trust is highly distributed and dependable on qualitative data, it is one of the important necessities in the IoT ecosystem. Trust

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

can be subdivided into three parts: device trust, entity trust and data trust.

3.2.1.7 Secure Middleware

In order to implement the integration and the security of IoT devices and the data in the same network, several types of middleware are installed. This is due to the very enormous numbers of various technologies place within the IoT ecosystem. When a middleware are used, any actions of exchanging data must be done respecting severe protection restrictions.

3.2.1.8 Policies

The policies permits keeping up order, security and information coherence. There must be policies and benchmarks to guarantee that information will be managed, protected and transmitted in an adequate way. Critically, all components must be enforced such policies in order to ensure every individuals or objects are applying the standards.

As what have been reviewed in the systematic review, the authors believe that the security challenges in 6LoWPAN protocol for IoT are still not yet to be tackled. This issue, thus, calls for more research focusing in the security challenges in 6LoWPAN protocol for IoT and how to overcome them. This review study will provide an important guidance to other researchers by documenting the available solutions in the field of 6LoWPAN security for IoT. Not only that, this review study will benefit them by accommodating on which area of security in 6LoWPAN that should be focused on for the future studies.

4. TRENDS OF SECURITY CHALLENGES IN 6LoWPAN

The papers extracted using the SLR method shows different types of data collection in accordance with the needs of the study. Muhammad and Kabir explain in [15] that data collection is the process to gather and to measure information factors of interests, in an established systematic manner that allows one to answer stated research question, test hypotheses and evaluate the results.

Table 3 displays a list of trends focusing in security in 6LoWPAN network. Ranging from 5 years (2015-2020) journal articles and conference papers which are extracted according to suitable trends.

Table 3: Security Challenges for 6LoWPAN

Secure Middleware	[4],[8],[16],[17], [18]
Data Confidentiality	[4],[8],[12],[14],[18], [21]
Identity Management and Authentication	[4],[8],[12],[13],[14], [20],[22],[24],[25], [26]
Privacy	[4], [14], [19], [20]
Secure Access Network	[8], [20], [22],[24]
Information Integrity	[4], [7], [14], [19], [21]
Trust and Governance	[24]

As illustrated in Figure 4, the identity management and authentication has been identified as the most popular trend for security challenges for 6LoWPAN, whereas the least favorable trends is trust topic. For each trend shown in Figure 4, it will be further discussed in the Section 5.

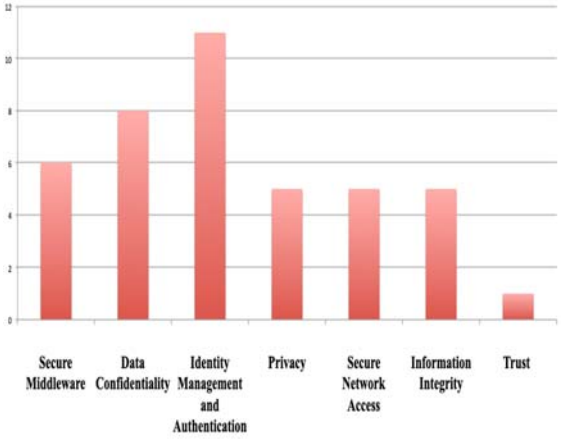

Figure 4: Security Challenges Trends

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CHALLENGES AND ISSUES IN 6LOWPAN FOR INTERNET OF THINGS (IoT)

This section further explains the trends of 6LoWPAN challenges and issues as depicted in Figure 4 such as secure middleware, data confidentiality, identity management and authentication, privacy, and information integrity

5.1 Secure Middleware

The first issue that needs to be highlighted is the middleware issue in 6LoWPAN networks. The security challenges for this middleware can be described as follows:

5.1.1 Unauthorized Access

Middleware layer provides different interfaces for the application and data storage capabilities for example, cloud computing. If the middleware is not secured, the attacker can easily damage the system by deleting the existing data in the network. In fact, lack of standard protocols in the middleware layer gives an opportunity for cracker to penetrate the existing network.

5.1.2 Malicious Insider

Anyone that has the right to access to the 6LoWPAN network might be malicious to tamper with the data, for both personal and third party benefits. On the other hand, the unintended acts of the malicious insider also contribute to network vulnerability.

5.1.3 Deny-of-Service (DoS) Attack

DoS attack is done to cause resource exhaustion in which will cause the system or network to be unavailable. The challenges described above not only can happened to the middleware layer but also in the other layers available in the generic architecture of IoT network which are the perception layer, network layer and application layer as depicted in Figure 5.

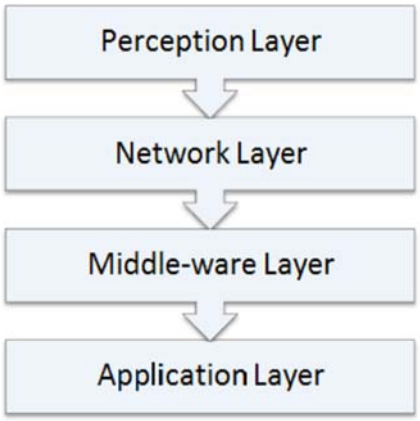

Figure 5: Generic IoT Architecture [4]

5.2 Data Confidentiality

Next issue is the data confidentiality. The explanation by [28] states that confidentiality are defined as the safeguarding of data privacy from uninvited and prohibited users. The followings are the security challenges for data confidentiality.

5.2.1 Snooping

Snooping is an attack, which attackers try to access confidential data such as login credentials or passwords. This attack triggers a host or application to imitate legal actions.

5.2.3 Traffic Analysis

The pattern of network traffic is useful to attackers. As mentioned by Butun et al. in [24], attacker will attempt to track the direction of contact between the sender and the recipient. Using this method, the attacker will discover the amount of data travelling between the sender and the receiver path.

5.2.4 Eavesdropping

According to [28], eavesdropping is the easiest type of attack, which the host is configured to tapped and capture data not belonging to it. Since 6LoWPANs are short-range networks, it is most likely to be susceptible to eavesdrop attack. Interference of the messages conveyed through

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the network can reveal useful information such as cluster heads, gateways, key distributions, etc.

5.2.5 DNS Poisoning

DNS poisoning is an attack that the attackers will modify archives in DNS databases. This action will cause users to be directed to a deceitful website by clicking on a genuine web URLs.

5.3 Identity Management and Authentication

The next issue is identity management and authentication. Jurcut et al. [29] presented a brief review of authentication in IoT. Authentication is the first stage of any process for access control. In order to maintain the trust of system, any decision to allow the authorized individual to accessing the network or system is ensured. Figure 6 shows the taxonomy of the IoT authentication. Authentication factor and use of tokens are key elements that need to be considered in IoT authentication.

i. Authentication Factor

Identity: Information given to authenticate itself. One or a combination of hash, symmetric or asymmetric cryptographic algorithms can be used for identity-based authentication schemes.

Physical and behavioral context: Physical context is biometric information based on physical characteristics such as fingerprints and retina scans. On the other hand, behavioral context is biometric information based on behavioral characteristics such as voice ID.

ii. Use of Tokens

Token-Based Authentication: Authentication of an individual or a device is based on an identification token created by server, for example, OAuth2 and openID. [30].

Non-Token Based Authentication: Authentication of an individual or a device is based on the usage of credentials, which are username and password every time there is the need to exchange data.

For the identity management, Carnley and Kettani [31] stated that the terms identity management is where the system that handles the creation of a digital identification or account assigned to an individual. The system manages the user's digital identity as well as their passwords, tokens and other authentication method. It is crucial for the access to be removed once the individual is no longer working for the company.

Examples of security challenges for identity management and authentication are as fabrication and spoofing. In [32], Razzaq et al. classified fabrication as one of the extremely high threat level to any 6LoWPAN in IoT systems. Attacker can inject counterfeited data, which leads to destroying the authenticity of information. Moreover, by using a fake identity, for example Media Access Control (MAC) or Internet Protocol (IP) address of the legitimate user, spoofing attacks are easy to be spread in any IoT networks. [33].

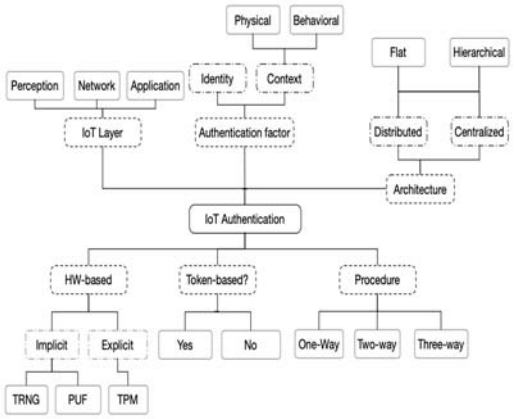

Figure 6: Taxonomy of IoT Authentication Scheme [30]

5.4 Privacy

The idea for both privacy and security are not fully outlined and having numerous definitions in many literatures. Tank et al. [19] described that security issues such as integrity and availability are the complimentary requirements for any IoT network and due to the vulnerabilities in the traditional networks, different attacks in 6LoWPAN network will affect the functionalities and degrades the 6LoWPAN network.

As for the next issue, authors in [29] raised concerns regarding secure network access, which both authentication and access control mechanisms are very important in IoT. Since IoT

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

devices are dependent on the trustfulness of the other devices connected to them, the authors also suggested that without an appropriate access control, the whole IoT system could be jeopardized. The access control mechanisms are shown in Figure 7 below.

One of the famous security challenges for access control system is brute force attack. By using this attack, the attacker tries to break a password, passphrase or PIN with any possible combination of letters, number and characters.

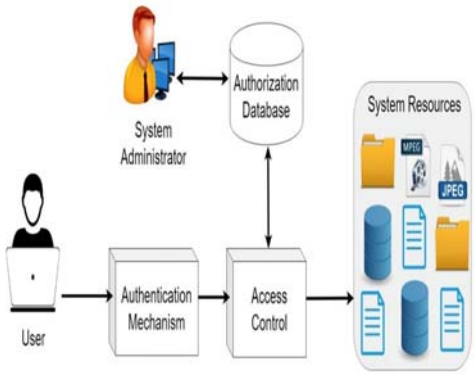

Figure 7: Access Control System [29]

5.5 Information Integrity

The next issue is information integrity. Integrity is said to be define easily but far less easy to ensure it. Musonda presented in [34] that any individual or organization that stores information needs it to have integrity. There are several critical factors that influences data or information integrity. The first critical factor is that protection against sabotage and the use of forged units or components.

The next critical factor is the robustness and fault tolerance capabilities of the IoT system. The other critical factor is the sensor itself. For example, RFID has limited capabilities to overcome integrity issues since the components of sensors spend most of the time without being attended.

Resources in common IoT related systems do not support traditional cryptographic solutions. This is due to the limited resources that are available to be used. Not only that, password-based is one of the solutions to guarantee data integrity. Thus, bringing into justifications the limitations of password protection, for example, weaknesses related to password length and randomness.

5.6 Trust and Governance

Trust is also one of the challenges in 6LoWPAN network. According to [35], the concept of trust is used in various contexts with different meanings. The fundamental issue with numerous approaches towards the definition of trust is they do not lend themselves to the foundation of measurements and evaluation techniques. In addition, the fulfillment of trust necessities are carefully related to the identity management and access control issues.

IoT ecosystem enables a continuous transfer and sharing of data among things and users in order to achieve specific objectives. In such environment, authentication and confidentiality are very crucial. Many worth efforts have been conducted in the Wireless Sensor Network (WSN) fields, however, it still lacks of a well-defined solution to guarantee confidentiality and authentication in 6LoWPAN for IoT ecosystem [35].

6. CONCLUSION

This review study presents a brief explanation on the general review of the 6LoWPAN protocol and the security issues in IoT. It details on the 6LoWPAN protocol stack, which each layer is explained. As for the security issues in IoT, each element is stated and also being described and explained. Next, the trends for security challenges in 6LoWPAN protocol, ranging from year 2015 to 2020 is also illustrated. At the end of the paper, several challenges and issues in 6LoWPAN for IoT are studied to highlight what can be addressed in the future work.

7. FUTURE SCOPE

As a future work, an in-depth review of the 6LoWPAN network architecture should be done. This future work involves the security issues in IoT and a proposed solution for each issue to focus on. As recommendation, a better keyword or search string and addition of databases can be used in order to retrieve much more papers on the related subjects.

There are various new research achievements focusing in securing a 6LoWPAN

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for IoT ecosystem. However, it is recommended for the future work for new researches to be further expanded, focusing more on the least favorable research trends. The best work area motivates researchers to having various types of results from different trends. This is to ensure varieties of results that is useful for future references and for further expand the new achievements in IoT fields instead of focusing the attention towards seeking a new possible security solution.

ACKNOWLEDGMENTS

A high appreciation to Ministry of Higher Education, Malaysia for sponsoring this research under the fundamental research grant (**A New Rebroadcast Algorithm of 6LoWPAN Network for IoT Ecosystem Routing Protocol Standard** and research grant number**: FRGS/2018/FTMK-CACT/F00392**). Utmost gratitude also goes to the Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat Dan Komunikasi (FTMK) and Universiti Teknikal Malaysia Melaka (UTeM).

REFERENCES

[1] S. Engineering, S. Arabia, and D. Campus, "A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," pp. 219–224.

[2] M. Seliem and K. Elgazzar, "IoTeWay : A Secure Framework Architecture for 6LoWPAN based IoT Applications," *2018 IEEE Glob. Conf. Internet Things*, pp. 1–5, 2018.

[3] A. Giri, "Internet of Things (IoT): A Survey on Architecture , Enabling Technologies , Applications and Challenges," 2017.

[4] M. U. Farooq and M. Waseem, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," vol. 111, no. 7, pp. 1–6, 2020.

[5] S. Al-sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Review," pp. 685–690, 2017.

[6] G. Glissa, "6LoWPAN multi-layered security protocol based on," pp. 264–269, 2017.

[7] R. A. Rahman, "Security analysis of IoT protocols : A focus in CoAP," 2016.

[8] H. Sardeshmukh, "Internet of Things : Existing Protocols and Technological Challenges in Security," 2017.

[9] Z. Yang, "A 6LoWPAN IoT Platform on the Global Internet," pp. 351–356, 2019.

[10] A. H. Kemp, "Comparison of 6LoWPAN and LPWAN for the Internet of Things," *Aust. J. Electr. Electron. Eng.*, no. December, pp. 1–7, 2017.

[11] G. Gardasevic, S. Mijovic, A. Stajkic, and C. Buratti, "On the Performance of 6LoWPAN Through Experimentation," pp. 696–701, 2015.

[12] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," vol. 4662, no. c, pp. 1–10, 2017.

[13] S. S. Tabrizi and D. Ibrahim, "Security of the Internet of Things : An Overview," pp. 146–150, 2016.

[14] A. Harit, "Internet of Things Security : Challenges and Perspectives," 2017.

[15] S. Muhammad and S. Kabir, "Methods of data collection," no. July 2016, 2018.

[16] E. Bertino, "Internet of Things (IoT): Smart and Secure Service Delivery," vol. 16, no. 4, pp. 1–7, 2016.

[17] "Internet of Things- Security in the Keys.pdf." .

[18] M. Waseem, "A Review on Internet of Things (IoT) A Review on Internet of Things (IoT)," no. March, 2015.

[19] B. Tank, H. Upadhyay, and H. Patel, "A Survey on IoT Privacy Issues and Mitigation Techniques," pp. 9–12, 2016.

[20] C. Hennebert and J. Dos Santos, "Security Protocols and Privacy Issues into 6LoWPAN Stack : A Synthesis," vol. 4662, no. c, pp. 1–16, 2014.

[21] C. Matthias, S. Kris, and B. An, "Study on impact of adding security in a 6LoWPAN based network," no. SPiCy, pp. 577–584, 2015.

[22] S. Choudhary, "Detection and Prevention of Routing Attacks in Internet of Things," *2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng.*, pp. 1537–1540, 2018.

[23] M. Surendar and A. Umamakeswari, "InDReS : An Intrusion Detection and Response System for Internet of Things with 6Lo WP AN," pp. 1903–1908, 2016.

[24] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things : Vulnerabilities , Attacks and Countermeasures," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[25] I. Halcu, G. Stamatescu, and V. Sgârciu,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"Enabling Security on 6LoWPAN / IPv6 Wireless Sensor Networks," pp. 1–4, 2015.

[26] A. Kamble and S. Bhutad, "SURVEY ON INTERNET OF THINGS (IOT)," *2018 2nd Int. Conf. Inven. Syst. Control*, no. Icisc, pp. 307–312, 2018.

[27] A. Verma, S. Member, and V. Ranga, "Security of RPL based 6LoWPAN Networks in the Internet of Things : A Review," vol. 1748, no. c, 2020.

[28] G. Kumar, A. Kaur, and S. Sethi, "Computer Network Attacks - A Study," no. January 2014, 2019.

[29] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT Security," in *IoT Security : Advances in Authentication*, 2019.

[30] A. Schemes, "Authentication Schemes," pp. 1–43, 2019.

[31] P. R. Carnley and H. Kettani, "Identity and Access Management for the Internet of Things," vol. 8, no. 4, pp. 129–133, 2019.

[32] M. A. Razzaq, M. A. Qureshi, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," vol. 8, no. 6, 2017.

[33] N. Wang, L. Jiao, P. Wang, M. Dabaghchian, and K. Zeng, "Efficient Identity Spoofing Attack Detection for IoT in MmWave and Massive MIMO 5G Communication," *IEEE Glob. Commun. Conf. (GLOBECOM), Abu Dhabi, United Arab Emirates*, pp. 1–6, 2018.

[34] C. Musonda, "Security , Privacy and Integrity in Internet of Things – A Review," in *Security , Privacy and Integrity in Internet of Things – A Review*, 2019, no. April.

[35] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-porisini, "Security , privacy and trust in Internet of Things : The road ahead," *Comput. NETWORKS*, vol. 76, pp. 146–164, 2015.