A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home

Talal A.A Abdullah[†], Waleed Ali[††], Sharaf Malebary[††] and Adel Ali Ahmed[††]

[†]Information Technology Department, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia
[††]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Jeddah 25729, Saudi Arabia

Summary
Internet of things (IoT) has been becoming an influential compound of the future since it provides a promising technology with great potential for addressing many societal challenges. Remotely controlling and monitoring real-world devices (things) via the Internet is the foundation that IoT bases on. Recently, IoT concept has been applied to home environment to make it safer, smarter, and automated. However, enforcing privacy and security in smart home environments have been identified as the main serious challenges required to settle in a smart home application. In this paper, we will review some recent articles regarding the most common issues of cybersecurity and cyberattack that exploit the vulnerabilities of smart home environments. Moreover, important observations on smart home threats, vulnerabilities, and security will be discussed in this study. Eventually, this paper provides some suggestions and recommendations on the effective security mechanism that can be used to mitigate the cyberattacks on IoT based smart home.

Key words:
Smart Home, IoT, Cybersecurity, Vulnerability, Threat, Privacy

1. Introduction

Internet of things (IoT) refers to various electronic devices and objects that are able to connect, and transfer data through the seamlessly Internet [1]. Gartner Press [2] expected more than 11.2 billion connected devices will be used worldwide and it will reach 20.4 billion by 2020. The adoption of IoT devices in the home environment has tremendously increased these years in order to fulfill the user needs and provide value and convenience to our daily activities [3][4].

As shown in Fig. 1, the multipurpose sensors are integrated into the appliance devices to produce the sensor network platform. Moreover, the sensory data cnamelyan be sent to the sink node and stored at the base station (gateway) of a local network or might be forwarded directly to IoT devices.

In a smart home, IoT technologies are used to make the homes smarter in order to improve security, efficiency, and comfort. Hence, the smart home domain is considered as the main factor of the Internet future [5][6]. Momentarily, more than 90 million people around the world will live in smart homes [5]. However, privacy and security in IoT environments have been identified as the key barriers of the smart home and they require attention. [7][8][9].

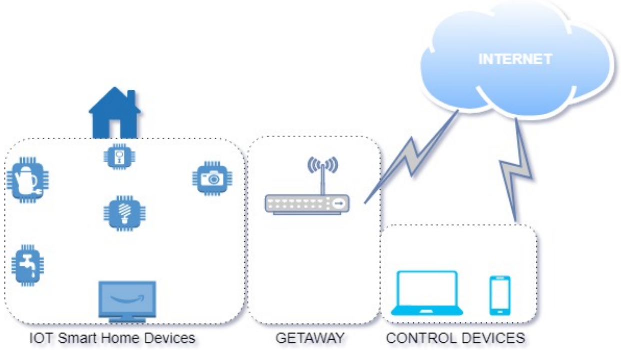

Fig. 1 An environment of IoT-based smart home

In the cyber era, the popularity of emerging technologies has led to more attention to the issues concerned with the privacy and security of services [10][4]. In addition, there is no well-established practice from governments to enforce IoT-industries to design IoT devices with high security and privacy standards [11]. Furthermore, the complexity and heterogeneity that massively interconnected services and devices may increase the challenges of embedding IoT devices at homes [9][12][13]. Trend Micro (2018) reported that some IoT-industry corporations still sell IoT devices that are not secure and have proven to be cumbersome and easy to be compromised. The recent IoT-device protocols lack the critical security features and the trust between devices is practically non-existent [14]. Therefore, many methods have been suggested to deal with critical system requirements, namely privacy and security [5][15][16][17][18].

The heterogeneous of smart home devices have many constraints in the hardware design, including the processing unit, energy, and storage limitations which will complicate the implementation of traditional security

Manuscript received September 5, 2019
Manuscript revised September 20, 2019

solutions on the constraint IoT devices [19]. Moreover, the home services and the sensitive information should be protected against any malicious attacks that exploit the vulnerabilities of traditional security and monitoring system [20]. Thus, the smart home environment needs superior security methods and daily monitoring, backup, and software updating [21][22].

Developing a lightweight IoT solution that satisfies the security requirement in terms of confidentiality and integrity becomes a hot topic in the recent research studies [18][6]. This is mainly due to the rising voice that imposes strengthen security regulations on IoT companies by some governments. Therefore, security can no longer be looked as an additional feature, instead, it must be considered as a core built-in system [23].

This paper is organized as follows. Section 2 reviews the recent related works to the smart home architecture, IoT threats and vulnerabilities, and smart home cybersecurity. The main observations on vulnerabilities and threats in smart home are then explained in Section 3. The suggested solutions and best practices are provided in Section 4. Finally, Section 5 concludes this paper

2. Related Work

IoT based Smart home architecture is highly insecure due to the IoT vulnerability to different types of cyberattacks such as replay attack, link spoofing attack, man-in-the-middle attack, dictionary attack, brute force attack, and session hijacking attack. Therefore, it is important to identify the possible security risks and then analyze these risks in order to develop a complete picture of the security situation of IoT based smart home system. The impact of cyberattacks and how to mitigate their effects have been discussed in several research studies. In this section, we will summarize the most interesting articles related to IoT based smart home architecture, cyber threats, and cybersecurity.

2.1 Smart Homes Architecture

Many existing smart home environments use either Zigbee or Bluetooth for wireless connections. However, the Wi-Fi based on IPv6 enables unlimited number of embedded devices to be connected through IoT system [16]. The approach in [16] proposed the IoT architecture system which was composed of a home gateway connected with several IoT devices through a Wi-Fi network. In this approach, the gateway was used to monitor and authenticate the communication between IoT-devices in the system. The home gateway could be accessed and controlled by the mobile device. The only way to communicate between IoT devices was through this gateway. This means the data travels from sender to the receiver through the gateway to respond to any appropriate action. Likewise, the research in [24] proposed a similar architecture that considered off-the-shelf components. The Hub was connected to the Router inside the smart home through either a wired or wireless connectivity, which was responsible for connecting IoT-devices with the Internet. Most commonly, the communication between the Hub and IoT devices uses wireless medium. In this approach, users can use different platforms to remotely control, monitor, and interact with IoT devices. Generally, IoT devices can communicate through either direct interaction with the services of the IoT Hub or using internet cloud services to reach the destination devices through the IoT Hub. The two scenarios can mostly work in parallel and even mixed together to support remote and local interactions with IoT objects.

2.2 Smart Home Threats and Vulnerabilities

An attacker might attempt to fabricate, intercept, manipulate, or interrupt the transmitted data. Some latest articles related to smart home threats will be described in this section. The research in [25] discussed the threats of cyberattacks from two categories targeted and non-targeted attack on industrial systems. Non-targeted attacks are infecting the victims randomly without any evidence of the selection of victims. The intruder aims to compromise systems as much as he can regarding monetary gains from the sale or exploit the extracted information. On the other hand, targeted attacks usually display a higher degree of sophistication. In the targeted attack, receivers of the attack are specifically selected since the attacker believes that the victim has some worthy information. The authors categorized the cyber-attacks into three common types named, malware short for malicious software, distributed denial-of-service (DDoS), and Stuxnet which is a complicated Internet worm exploiting industrial control systems (ICS). Furthermore, the research in [24] discussed two kinds of attacks which are internal and external entities attacks that can behave as malicious in a passive or active approach based on their aims. In both approaches, attackers target either the smart home’s infrastructure or the stored information in the cloud services. In a passive way, adversaries try to snoop available communications in order to gain significant information that can be used to observe users' behaviors or stored and exploited later to perform an active attack. On the other side, the active adversaries could influence not only users’ privacy, security and confidentiality, but also impact data integrity, gain unauthorized access and disrupt the smart home functions that provide services. After the authors have been done a test-bed architecture on commercial smart home products, they discussed in more details about the major threats affect smart homes such as eavesdropping, impersonation, deny of service, and software exploitation.

The research in [15] categorized types of cybercriminals into eight categories: hacker, crackers, cyber terrorists, salami attackers, pranksters, career criminals, cyber bulls, and industrial spy. In addition, [15] also described some hijacking techniques such as MEDJACK and spy agencies. The high economic countries such as USA, UK, and China are the most cyberattack suffering countries between 2015 and 2017. Moreover, [15] classified types of crimes along with their objectives. These categorizing, classification and reports provide a better understanding of kind of intruders and what their goals, what they would like to hack and how much damages they could make. The authors in research [6] deliberated the adversaries' motivations in IoT. One of these motivations is that IoT is a new area in computing, so for attackers, it seems like a very interesting subject because of the immaturity of the products and protocols used in current IoT-products. Implementing IoT in the smart home currently suffers from privacy and security vulnerabilities such as authentication and encryption [26]. The authors explained and discussed the following vulnerabilities of IoT-based smart home. Firstly, the communications can be intercepted, credentials can be extracted, authentication can be disrupted, and new firmware can be attacked with malware. Secondly, most of the malware takes advantages from the default authentications combinations that set a default password that can be used by anyone. Thirdly, malware can scan IP addresses for open ports for protocols like telnet and SSH to compromise IoT devices. Also, the authors in [27] adopted OCTAVE Allegro methodology to analyze how the users or devices use the information in the system. The authors used the OCTAVE Allegro methodology to collect all security threats found by conducting an assessment of the information security risk. The results of this research gave a better understanding and identified potential risks and the security threats in an IoT-based smart home environment. The authors summarized the found threats to (users' impersonation, theft (identities, credentials), malicious software, information modification and disclosure, Daniel of service, device and sensor compromising, function interruption, authentications, steal information).

2.3 Smart Home Cyber Security

The security issues should be considered as the highest priority in the IoT design and implementation. In IoT-based smart homes, a new level of security and privacy is required since smart home environments include private and sensitive information.

In order to protect the information assets and make the smart home more secure, possible countermeasures have been discussed in [27]. The key concepts of the proposed alleviation strategy in [27] is based on three measures: strong user authentication, correct technical configurations, and resident security awareness. Also, the suggested countermeasures are associated with security risks and threats. The research in [28] recommended methods based on cryptographic approaches to manipulate the main security services. With taking into account the traditional approaches, the authors focused on confidentiality, availability and privacy. They claimed that the traditional security solutions proposed in this article optimized the resources such as computation, memory and bandwidth. However, these solutions did not meet the heterogeneity, scalability and mobility challenges. Therefore, the authors discussed the new emerging security solutions for the Internet of Things. These emerging techniques were proposed as approaches to deal effectively with scalability issues and enhance security in IoT environments. Also, the authors in [29] discussed some security recommendation and practices in corporate and suggested several home network security practices. For corporate security, the article discussed two categories of corporate security named, security principles compartments, and security as a process. For home network security, the authors presented recommendations for the home network security. They considered the ITU-T X.1111 recommendation: framework of security technologies for home network, and US-CERT guidelines on home network security. US-CERT provided a range of recommendations for securing the home network, most of which are for endpoints. In addition, the authors in [18] designed a secure framework and implemented it on smart home to provide flexibility and secure smart home environment depending on CPS and IoT. They proposed a secure architecture to protect the system against external attackers that come through the Internet. In this approach, a Sicher firewall was utilized to detect and issue a warning about viruses and invoke its mitigation strategy against certain security breaches. In addition, this article discussed also internal security which provided encryption to prevent unethical activities such as communication from being hacked in the home automation system. Moreover, the authors in [17] presented a group of guidelines, as the core of a conceptual framework to combine the privacy-by-design principles to help software engineers to assess the privacy capabilities of Internet of Things applications and platforms. They explained how their framework can be utilized to assess two open-source IoT platforms namely, Eclipse Smart Home and OpenIoT. Furthermore, the authors in [30] developed a prototype of an alter system which sends alerts to the owner over voice calls using the Internet if any kind of human movement is sensed close to the house entrance. Another alarming option used in the system was sending alert messages to the owner in case of critical circumstance was happened.

On the other hand, if the person entering the house is an unexpected guest and not an intruder, the owner will make an arrangement instead of sending the security alarm.

We believe that prioritizing efforts on critical points in the home network infrastructure and developing appropriate tools to help home users with assessment, protection, monitoring, and incident response are viable to be considered.

3. Main Vulnerabilities and Threats in Smart Home

There is a trade-off between convenience, control, security and privacy in a smart home. The heterogeneous components of smart home that have different kinds of smart home applications such as securing homes, healthcare, energy, convenience as well as CPU and storage limitations make traditional security solutions for smart home not applicable.

There are few security concepts need to be in mind in order to provide the best notion for the smart home risk and mitigation [6].

- Assets: physical and virtual things that are valuable for users such as personal information, activities, money, and properties.
- Threats: any potential action that might cause damage, harm or loss.
- Vulnerabilities: weaknesses or gaps inside the system that potentially are exploited by attackers
- Risk: the potential loss or damage might impact the system by a threat advanced from the system vulnerabilities.

In this section, we will describe and categorize the main vulnerabilities in the smart home environment. Furthermore, the main threats in smart home will be presented and discussed in this section.

3.1 Main Vulnerabilities

The research study in [31] estimated that 80% of IoT devices are vulnerable to a wide group of the hack. Adversaries might exploit these vulnerabilities to influence smart home environments. IoT system has commonly three layers namely application layer, network layer, and perception Layer [27]. At each layer, IoT devices are vulnerable to attack and malicious actions. The popular smart home vulnerabilities will be described below.

A. Heterogeneous Architecture

To build a smart home system, we need a collection of a variety of smart home devices that work effectively using different systems. A dynamic heterogeneous architecture in a smart home needs to be built through the perception layer, the network layer, and the application layer. One of the most common challenges in IoT network is to identify the nodes that may have access to users' privacy information related to the heterogeneous architecture of IoT [1]. Smart home system is a platform that consists of heterogeneous data, technologies, devices, and protocols. The heterogeneous architecture of smart devices and the dynamic environment of the Internet of things enforce IoT companies to figure out new security strategies to come up with the new challenges that should be considered [28]. Therefore, in order to get better IoT-devices homogeneous, the awareness of using IoT applications and systems is very important.

B. Outdated Protocols

Since the Internet was established, there are some protocols are outdated without any upgrade which can be compromised by attackers [32]. In addition, the alarming development of IoT devices makes the current security protocols and techniques are not enough because the existing devices have limitations in their levels of integrity, scalability, and interoperability [1]. Security features in IoT protocols are limited and the trust between these devices is poorly embedded [6]. Therefore, new techniques must be implemented to meet the privacy, security, and reliability requirements of IoT.

C. Weak Encryption

Encryption is the process of cipher information in such a way that only authorized people can access it in order to prevent attackers from eavesdropping and tampering with data during transmission. If one piece of data is not encrypted or isolated, the data will be transparent and easy to be exploited by attackers [1]. Furthermore, some IoT device use a small encryption key which can make them vulnerable to hacked [32]. Most of IoT devices use different control platforms and protocols, so the cryptography solutions to protect all IoT systems differ based on the constraints of IoT devices. Smart home devices contain sensitive information about user’s daily life. Thus, encryption should be at the core of IoT industries as it is an easy and beneficial security method [33].

D. Limited Storage and CPU

Smart home devices collect a great amount of data that needs to be computed, analyzed, stored and processed. Mostly, data preprocessing is done at either the sensor or some other proximate device [34]. However, the processing and storage capabilities of IoT devices are limited by the resources available, which are very restricted due to the computing capability, available energy, and limited storage [35]. Therefore, IoT-devices are vulnerable to Denial of Service attacks (DoS) [1].

E. Insecure Applications

There is a lack of systematic techniques for building privacy that has not been considered by IoT applications and middleware platforms [17]. Some IoT companies produce smart home devices that can be controlled using smartphone applications which are easy to compromise. A malicious code can be merged with applications software installed on the IoT system, which easily allow the attackers to perform harmful attacks [27].

F. Poor Authentication

Authentication is the method of having the credentials that validate your identity to a system or entity [6]. In network communication, the main risks come from poor confidential settings and poor authentication. Default credentials should change before using IoT devices because once guessed, they can be exploited to hack many devices [22]. The highest risk of information processed is from inadequate access control of the configuration in the smart home gateway. This risk is primarily because of weaknesses of authentication procedure and inadequate separation of privileges between user accounts [21, 36, 42].

G. Firmware Failure

In the smart home environment, many IoT devices face a big problem due to no way to update the firmware. Since most of IoT devices are low-cost, manufacturers do not usually consider techniques for validating firmware integrity during installation, execution or upgrade [24]. Furthermore, many IoT devices have similar firmware which can increase the possibility of successfully exploiting the device which can make the firmware a big vulnerability of IoT devices [37]. Since the firmware on a device is fixed and never modified, attackers can exploit this problem to launch attacks with confidence that the virus will work on similar devices [22].

3.2 Main Threats

In order to secure any system, it is necessary to analyze the type of threats that will be faced, and how the threats will affect system security. The following subsections explain the main threats that can influence each layer and impact on the smart home environment.

A. Denial of Service (DoS)

Denial of service (DoS) is a kind of cyberattack in which the attacker attempts to make a system or network unavailable to the user for a temporary or permanent period [24]. DoS is typically done by flooding the targeted system or network with unnecessary requests in order to overload the systems and make it unable to respond to the legitimate requests [28].

B. Eavesdropping

Due to IoT heterogeneous architecture in the smart home infrastructure, an attacker might use numerous programs and techniques to capture the traffic in the network among the different components of IoT devices. These techniques are extremely based on the attacker's capabilities and location [24]. If the adversary takes advantage of the vulnerabilities of smart home devices to compromise the network components, he will be able to capture all the traffic between the smart hub and the users. The attacker might use well-known tools such as tcpdump3, wireshark4, etc., to gain access to the data [24]. Also, the adversary might use several types of hardware equipment like the Wi-Fi Pineapple5, which can spoof the access points and intercept the underlying communication [24].

C. Impersonation

In some cases, the adversary aims to impersonate a legitimate user and act on behalf of that user to harm or eavesdrop the user. Obtaining the user credentials (user ID and password) can be achieved through social engineering or by intercepting the network traffic in order to provide access to the IoT devices [27].

Theft (Identity, credentials, information)

The loss of important assets has significant effects on smart home users. Theft is an activity through which a person's property is taken or used without his/her permission [38]. The adversary tries to thieve useful information or data of authentication and authorization from the smart-home users such as login credentials or credit card information. There are well-known types of equipment and hardware that might be used by the attackers to hack the smart home and obtain information about the user [24].

D. Compromising

The attacker tries to hack several devices and systems regardless of the identity of these systems to achieve monetary gains from exploiting the information extracted [25]. Also, attacker can deploy his own node or even compromise one of the existing nodes [39]. Once a network is compromised, the eavesdropper can be secretly merged into network traffic, making detection extremely hard. The adversary then starts secretly deploying its cyber tools to figure out security flaws within the vital links in the network. The malicious software will then scan the smart home infrastructure and probing IoT devices to identify the system vulnerabilities and create a cyber map for the topography of the network. This step can be easily done by using tools found on the Internet [25]. Real-time and autonomous interaction between devices make discovering and identifying the compromised nodes very difficult [12].

Malicious Software

Malicious software is a malware software code designed by attackers to get unauthorized access to private network or systems, gather or delete sensitive data, damage the operations, or display unsolicited advertising. The worms, trojan horses, rootkit, and spyware are examples of malicious software. Malicious software (malware) can be injected into IoT applications and then affects the IoT services and devices [27]. Since IoT devices have a lightweight autonomous version of the well-known operating system, the attackers can access to private information using overmentioned malicious software in order to look for vulnerabilities and exploit them [29].

4. Recommended Security Solutions and Practices

As smart home environments can contain sensitive, important, and private information, many security solutions and practices have been proposed in IoT based smart home environments. In the recent years, numerous security solution for IoT based smart home suggested in the literature which are discussed below.

4.1 Updating the Software

Updating and upgrading device software, firmware, and firewall are a very important part to ensure up-to-date security software. A firewall acts as a filter between internet and interface and control the traffic between network and the Internet [40]. Moreover, the firewall protects the network from malicious codes and external threats [3]. Firewall can detect and issue warning to user and invoke its mitigation strategy against particular security breaches [18]. Furthermore, it is essential to update the firmware and device software to the latest version to avoid unpatched vulnerabilities [14]. Out of date software still has the same flaws and exploitable vulnerabilities in the code that allow cybercriminals and hackers to exploit them. The security issues in home automation can be mitigated by updating the firewall and device software systems [18].

4.2 Utilizing Effective Encryption

The heterogeneous components in an IoT device should effectively encrypt the data communication wherever possible. Encrypted data communication would reduce the potential privacy risks and prevent unauthorized access getting benefits from the data transferred between components. Encrypted data reduces any privacy violation due to malicious attacks and unauthorized access [17].

4.3 Using Private Network

A secure communication channel is one of the most popular methods used to protect IoT devices from unauthorized access. The secure communication channel can utilize a secure virtual private network (VPN) and limit network traffic such that it is accessible only to authorized users [27].

4.4 Applying up-to-date Protocols

It is essential to apply up-to-date protocols in IoT devices in order to protect the network. The protocol is one of the most important components in IoT [32]. It provides regulations for communications between devices to be established in a uniform way. Therefore, embedded computing services require a group of rules to control, communicate and exchange data [6].

4.5 Changing Credentials Regularly

At the first time of using IoT device, IoT manufactories should enforce users to change the default identity (username and password) into strong ones, unless the IoT device should not be worked [14]. In addition, the password should be regularly changed every three months maximum. Furthermore, users should use a different password for various IoT devices and not use the same password for all IoT devices. Moreover, it is highly recommended to not use the email as a username since it is a common technique for attackers to try to phish email account and catch the password [41].

4.6 Backup Significant Information

Some smart home devices such as healthcare devices include significant information that must be accessed just by authorized people. Regularly backup such information is the best practice to keep them away from fabrication or stealing. The research study in [27] gives guidelines of how-to backup sensitive information such as media information and store them off-site either digitally or physically.

4.7 Monitoring the Network

One of the best practices to secure smart homes is monitoring the connection of IoT device during message transfer. There are many tools help to monitor the network and analyze the device messages such as Microsoft Message Analyzer. Furthermore, the monitoring software can search for vulnerabilities and then update IoT programs.

5. Conclusion

In recent years, the integration of IoT devices in the home environment has tremendously increased these years in order to enhance the quality of our lives at home by making it easier, more comfortable and convenient. However, privacy and security in IoT environments have been identified as the key barriers of the smart home. This paper reviewed some articles related to the architecture, threats, and security of smart homes environments. Some common existing architecture suggested in smart home environment were presented in this paper. More significantly, the most common threats and vulnerabilities of smart homes were described and discussed. Finally, the best users practice and solutions suggested for smart home environments were provided in this paper.

References

[1] Y. Lu and L. Da Xu, “Internet of things (IoT) cybersecurity research: A review of current research topics,” IEEE Internet Things J., vol. 6, no. 2, pp. 2103–2115, 2019.

[2] Egham, “Gartner,” 2017. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Accessed: 22-Aug-2019].

[3] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic,” 2017.

[4] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, “User Perceptions of Smart Home IoT Privacy,” Proc. ACM Human-Computer Interact., vol. 2, no. CSCW, pp. 1–20, 2018.

[5] A. Jacobsson and P. Davidsson, “Towards a model of privacy and security for smart homes,” IEEE World Forum Internet Things, WF-IoT 2015 - Proc., pp. 727–732, 2015.

[6] D. Bastos, M. Shackleton, and F. El-Moussa, “Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments,” In IET Conference: Living in the Internet of Things: Cybersecurity of the IoT – 2018, pp. 30 (7 pp.), 2018.

[7] A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smart home automation system,” Futur. Gener. Comput. Syst., vol. 56, pp. 719–733, 2016.

[8] “Privacy in iot threats and challenges2014.pdf.” .

[9] R. Heartfield et al., “A taxonomy of cyber-physical threats and impact in the smart home,” Comput. Secur., vol. 78, pp. 398–428, 2018.

[10] S. Safavi, A. M. Meer, E. Keneth Joel Melanie, and Z. Shukur, “Cyber Vulnerabilities on Smart Healthcare, Review and Solutions,” Proc. 2018 Cyber Resil. Conf. CRC 2018, pp. 1–5, 2019.

[11] D. Marikyan, S. Papagiannidis, and E. Alamanos, “A systematic review of the smart home literature: A user perspective,” Technol. Forecast. Soc. Change, vol. 138, no. September 2018, pp. 139–154, 2019.

[12] A. Dehghantanha, K. Franke, and S. Journal, “Internet of Things Security and Forensics: Challenges and Opportunities,” Future Generation Computer Systems, pp. 2–8, 2018.

[13] A. R. Devidas, M. V. Ramesh, and V. P. Rangan, “High performance communication architecture for smart distribution power grid in developing nations,” Wirel. Networks, vol. 24, no. 5, pp. 1621–1638, 2018.

[14] T. M. Secur, “PA R A D I G M.”

[15] J. H. Awan, S. Memon, S. Memon, K. T. Pathan, and N. H. Arijo, “Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities,” Mehran Univ. Res. J. Eng. Technol., vol. 37, no. 2, pp. 359–366, 2018.

[16] Freddy K.Santoso and V. Nicholas C.H., “Securing IoT for smart home system,” Proc. Int. Symp. Consum. Electron. ISCE, pp. 5–6, 2015.

[17] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, “Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms,” pp. 83–92, 2016.

[18] S. Ur Rehman and V. Gruhn, “An approach to secure smart homes in cyber-physical systems/Internet-of-Things,” 2018 5th Int. Conf. Softw. Defin. Syst. SDS 2018, pp. 126–129, 2018.

[19] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, “On security challenges and open issues in Internet of Things,” Futur. Gener. Comput. Syst., vol. 83, pp. 326–337, 2018.

[20] V. D. Vaidya and P. Vishwakarma, “A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation,” 2018 Int. Conf. Smart City Emerg. Technol. ICSCET 2018, pp. 1–4, 2018.

[21] Cisco, “Cisco Annual Cybersecurity Report 2017,” Bioinforma. Biomed. Eng. 2008. ICBBE 2008. 2nd Int. Conf., pp. 7–58, 2017.

[22] G. Corser et al., “IEEE Internet Technology Policy Community White Paper INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES,” Ieee, no. February, 2017.

[23] S. on Security, “New IoT Security Regulations.” [Online]. Available: https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html?fbclid=IwAR3LlVY7hsuXOpFxNwlURp2MjOVifqqYssgJCbh7MLg_qFsIyNmecNiFKUo. [Accessed: 27-Jul-2019].

[24] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, “Security and privacy issues for an IoT based smart home,” 2017 40th Int. Conv. Inf. Commun.

Technol. Electron. Microelectron. MIPRO 2017 - Proc., pp. 1292–1297, 2017.

[25] I. G. Seissa, J. Ibrahim, and N. Yahaya, “Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review,” Int. J. Sci. Res., vol. 6, no. 1, pp. 180–186, 2017.

[26] “Top 10 Challenges,” IBM Developer. [Online]. Available: https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/. [Accessed: 27-Jul-2019].

[27] B. Ali and A. I. Awad, “Cyber and physical security vulnerability assessment for IoT-based smart homes,” Sensors (Switzerland), vol. 18, no. 3, pp. 1–17, 2018.

[28] D. E. Kouicem, A. Bouabdallah, H. Lakhlef, D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security : A top-down survey To cite this version : HAL Id : hal-01780365 Internet of Things Security : a top-down survey,” 2018.

[29] N. Nthala and I. Flechais, “Rethinking Home Network Security,” no. April, 2018.

[30] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, “IoT based smart security and home automation system,” Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016, no. October 2017, pp. 1286–1289, 2017.

[31] Rambus, “Smart Home: Threats and Countermeasures - Rambus.” [Online]. Available: https://www.rambus.com/iot/smart-home/. [Accessed: 23-Aug-2019].

[32] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, “Security vulnerabilities in bluetooth technology as used in IoT,” J. Sens. Actuator Networks, vol. 7, no. 3, pp. 1–26, 2018.

[33] iot for all, “How Encryption is Powering the Future of IoT | IoT For All,” 2018. [Online]. Available: https://www.iotforall.com/future-iot-encryption/. [Accessed: 01-Aug-2019].

[34] P. Sethi and S. R. Sarangi, “Internet Of Things: Architecture,Issues and Applications,” Int. J. Eng. Res. Appl., vol. 07, no. 06, pp. 85–88, 2017.

[35] W. Z. Khan, M. Zahid, M. Y. Aalsalem, H. M. Zangoti, and Q. Arshad, “Ethical aspects of internet of things from islamic perspective,” 2017 9th IEEE-GCC Conf. Exhib. GCCCE 2017, 2018.

[36] A. Jacobsson, M. Boldt, and B. Carlsson, “A risk analysis of a smart home automation system,” Futur. Gener. Comput. Syst., vol. 56, pp. 719–733, 2016.

[37] W. Paper, “Cyber Security in the Era of Smart Homes,” pp. 1–114.

[38] J. M. Hatfield, “Social engineering in cybersecurity: The evolution of a concept,” Comput. Secur., vol. 73, pp. 102–113, 2018.

[39] H. Rahmani, N. Sahli, and F. Kamoun, “Distributed denial-of-service attack detection,” no. May 2010, pp. 839–859, 2011.

[40] F. Steps, S. Strategy, M. Risks, O. Security, and F. Steps, “How to Develop an IT Security Strategy,” pp. 1–5, 2018.

[41] NetFormation, “8 Best Practices for Security Within the Internet of Things.” [Online]. Available: https://www.netformation.com/featured/8-best-practices-for-security-within-the-internet-of-things/. [Accessed: 23-Aug-2019].

[42] Ahmed, A.A. and Ahmed, W.A. An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. Sensors, 19(17), 2019, p.3663.