International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 04 | Apr 2023 www.irjet.net p-ISSN: 2395-0072

A Review of Cyber Security Challenges, Attacks and Solutions for Internet Based Home Automation System

Sudheer K. T[1]

[1]*Lecturer in Computer Engineering, IPT & Government Polytechnic College, Shoranur, Kerala, India*

Abstract - *Platforms for home automation make it simple for users to automate many different physical components of their houses. Customers are starting to grasp the potential of smart home appliances to enhance the standard of domestic life, which is causing them to become more popular. The core of IoT is the ability to remotely manage and observe physical objects (things) over the Internet. The Internet of Things (IoT) idea has recently been used to automate, improve, and secure the home environment. The major significant obstacles to establishing a smart home application, however, have been highlighted as regulating privacy and security in smart home environments. In this paper, reviews some recent articles about the most prevalent cyber security problems and cyber-attacks that take advantage of the weak points of smart home environments. In addition, significant findings on security, threats, and vulnerabilities related to smart homes will be covered in this paper. This study concludes by making some suggestions and recommendations for practical security measures that could be used to reduce cyber-attacks on internet-based smart homes.*

Key Words: **Cyber Security, Smart Home, Home Automation, IoT, *Vulnerability, Threat, Privacy***

1.INTRODUCTION

Since the late 1970s, the idea of home automation has been in existence. Yet, as technology and services have developed, so have people's expectations of what a home should be able to accomplish and how those services should be offered and accessed at home. This has also impacted how people see home automation systems. When comparing various home automation systems over time, we can see that each one has made an effort to give homeowners quick, easy, and secure access to their properties. The function of a home automation system has not changed, despite changes in user expectations, technological advancements, or the passage of time.

The work of John J. Greichen [1] covered some of the initial difficulties that home automation systems encountered. High manufacturing costs, high development costs, high installation costs, extra service and support costs, a lack of home automation standards, consumer technology illiteracy, and complicated user interfaces are a few of them. As time went on, technology and computing power advanced quickly, which significantly decreased the cost and size of devices. Because of all of these considerations, electronic devices are now quite popular, and people are no longer unsure or perplexed about how to use computers, smartphones, or tablets. In addition, other interface, communication, and home automation standards, including X10 [2], ZigBee [3], LonTalk [4], and CEBus [5], were developed throughout time. All of these elements helped early home automation systems address their problems and worries, which increased the appeal and acceptance of automated homes. The study done by A.J. Brush *et al*. [6] addresses the primary challenges faced by contemporary home automation systems, including their high total cost, lack of flexibility caused by the integration of many devices, lack of trustworthy home devices, confusing user interfaces, and dependency on knowledgeable consultants. Poor manageability and a lack of convincing security are the results of all these factors.

Internet of things (IoT) refers to various electronic devices and objects that are able to connect, and transfer data through the seamlessly Internet [7]. In order to satisfy user needs and add value and convenience to our everyday activities, the adoption of IoT devices in the home environment has significantly expanded over the past few years. [8][9]. IoT technologies are utilized to make homes smarter in order to increase security, effectiveness, and comfort. Today's smart homes have a wide range of devices, including several cameras, microphones, sensors, actuators, device controllers, and home databases that can be accessed remotely for the user's convenience. These devices and the home database contain a variety of personal data about the people who reside in a house, including health and financial information, videos, images, live feeds from the house, daily routines, favorite music, and even personal diaries. Various devices employed, bring distinct security vulnerabilities to the smart home. Hence, if or when these contemporary homes are penetrated, they pose a bigger threat to the privacy and physical wellness of the residents than ever before. Automation of the house [10] [11], its accessibility via the Internet [12] or mobile phones [13]

[14], energy conservation [15], technology-assisted senior citizen living [16], and security [17] have all been the subject of extensive research.

Hence, the smart home domain is considered as the main factor of the Internet future [18] [19]. However, privacy and security in IoT environments have been identified as the key barriers of the smart home and they require attention. [20][21][22]. In addition, there is no well-established practice from governments to enforce IoT-industries to design IoT devices with high security and privacy standards [23]. Additionally, the difficulties of integrating IoT devices in homes could be exacerbated by the complexity and heterogeneity of massively networked services and devices. [22][24][25].

Many hardware design constraints, such as processing unit, energy, and storage limitations, are present in the heterogeneous smart home devices, making it more difficult to apply conventional security solutions. [26]. 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 [27]. Thus, the smart home environment needs superior security methods and daily monitoring, backup, and software updating [28] [29].

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 [19][30]. This is mostly because more countries are beginning to put stricter security rules on IoT companies. Therefore, security can no longer be looked as an additional feature, instead, it must be considered as a core built-in system [31].This paper mainly focuses on the security aspect of home automation.

2. SMART HOMES ARCHITECTURE

Internet based communication in home automation systems is a very popular choice. The Internet is a fairly common form of communication in the modern world because it is easily expandable, versatile in terms of access and easy to use. So the hardware and the network required for access is readily available, offers high bandwidth, very low communication cost, and devices can connect to and disconnect from the network easily. The features like these make the Internet such an attractive choice. Devices with user interfaces including laptops, cell phones, PCs, and tablets are widely available and are a part of many people's daily life. Hence, integrating home automation into these already-popular user devices appears to be a logical next step. Figure 1 shows the components of a typical home automation system using the Internet.

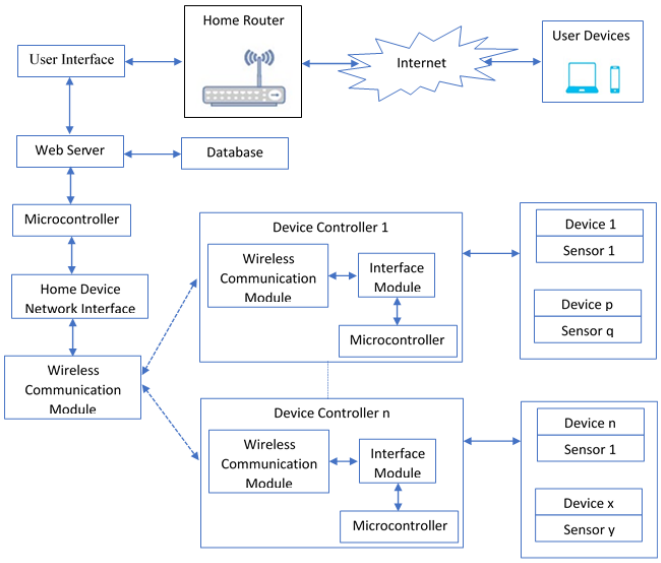

Fig – 1: Components of Internet-Based Home Automation System

The User Interface (UI): UIs are usually web pages or any Android/iOS/Windows applications developed. These applications or a web browser can be used by a user to connect to their house from a portable device over the Internet. A username and password are typically used by home automation systems to identify authorized users before giving access to the house.

Web Server, Database and the Microcontroller: A web server connects the user interface to the database. All of the home device's information and their present status are contained in the database. A user with remote access to their house can use the web server to query the database for the device's status information. A microcontroller manages all the operations and communications in the home network, as shown in Figure 1. As a PC can actually perform each of these activities, researchers have decided to replace the web server, database, and microcontroller with a Computer for simplicity.

Network Interface Module: It controls the communication between the controllers for home devices and the PC. With this interface, the device controllers receive commands from users to modify the status of the equipment in their homes. Following the execution of these operations, the interface transmits a device's status to the database.

Device Controller: A Device Controller has a microcontroller to manage its operations and interface,

wireless connectivity, and control modules. Many home sensors and devices are linked to a device controller. The device controller relays user instructions and requests for a device's status.

Communication Module: When deciding on the technology for the method of communication between the gadgets in the home, there are a few options. It is possible to use wired or wireless connections, depending on the resident's preferences. The most widely used communication protocol for wired communication is X10 because it can be deployed using existing wiring without requiring many significant changes. There are several options for wireless communication, including infrared, Bluetooth, Wi-Fi, and radio frequency (RF).

Many benefits come with Wi-Fi communication technology, including inexpensive installation costs, simplicity in deployment and installation, respectable communication range, scalable technology, high bandwidth, and little power consumption. AES encryption offers good security. Repeaters can also be employed to increase the transmission range. Without changing the current architecture, Wi-Fi is the best form of communication for automating an existing home. Also, since the transmission is wireless, the home's appearance is enhanced. Wi-Fi is the best option for wireless communication due to all these reasons. The work of A. El Shafee and K.A. Hamed [12] proposes an Internet-based system for home automation that makes use of Wi-Fi to allow communication between various gadgets and a server within the house. In their work, a PC with built-in Wi-Fi communication capabilities is used as a web server and a communication module that enables communication between the home devices and the server (PC). The home devices are connected to the PC via Wi-Fi by a hardware interface module.

Home Router: With a home's router, a home automation system is linked to the Internet. This allows the home's inhabitants to access their home from anywhere with the right credentials. .

Internet: If the home automation system is connected to the Internet, a resident can access and manage his or her house from any location in the globe. Although it offers benefits—as we've already discussed—connecting the home to the Internet makes it accessible to anyone with an Internet connection.

User Devices: People are now able to purchase and frequently use portable mobile devices for accessing the Internet because to improvements in electronics, processing power, and size and cost. In order to access their houses over the Internet, people utilize cell phones, laptops, and tablets. As a result, homeowners now have a flexible and practical option to access their house wherever they are. Users utilize the same device to perform daily duties like browsing, playing games, downloading apps, and viewing movies on the Internet in addition to accessing other applications. Due to this, there is a higher chance that the mobile device will have a security risk.

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 [31].

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.

3.1 Main Vulnerabilities

The research study in [32] estimated that 80% of IoT devices are vulnerable to a wide group of the hack. These weaknesses could be used by adversaries to affect environments in smart homes. IoT system has commonly three layers namely application layer, network layer, and perception Layer [33]. IoT devices are susceptible to attack and malicious behavior at every layer. Below is a description of some well-known vulnerabilities in smart homes.

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 [6]. 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 [34]. 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 [35]. 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 [6]. Security features in IoT protocols are limited and the trust between these devices is poorly embedded [19]. 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 [6]. Furthermore, some IoT device use a small encryption key which can make them vulnerable to hacked [36]. 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 [36].

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 pre-processing is done at either the sensor or some other proximate device [37]. The processing and storage capacities of IoT devices are, however, constrained by the resources available, which are relatively constrained due to the computational capability, available energy, and limited storage. Therefore, IoT-devices are vulnerable to Denial of Service attacks (DoS) [6].

E. Insecure Applications

There is a lack of systematic techniques for building privacy that has not been considered by IoT applications and middleware platforms [38]. Several IoT manufacturers create smart home products that can be managed using smartphone applications that are simple to hack.. A malicious code can be merged with applications software installed on the IoT system, which easily allow the attackers to perform harmful attacks [33].

F. Poor Authentication

Authentication is the method of having the credentials that validate your identity to a system or entity [19]. 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 [29]. The smart home gateway's poor access control setup poses the greatest risk to the processing of information. This risk is primarily because of weaknesses of authentication procedure and inadequate separation of privileges between user accounts [28, 38, 39].

G. Firmware Failure

Many IoT devices in the smart home setting encounter a significant issue since they cannot update their firmware. As the majority of Internet of Things (IoT) devices are inexpensive, manufacturers frequently overlook methods for verifying firmware integrity during installation, execution, or upgrading [40]. Also, the firmware of many IoT devices is similar, which increases the chance of successfully exploiting the device and makes it a significant vulnerability for IoT devices [41]. 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 [29].

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 major threats that can affect each layer and have an effect on the smart home environment are described in the following subsections.

A. Denial of Service (DoS)

Denial of service (DoS) is a kind of cyber-attack in which the attacker attempts to make a system or network unavailable to the user for a temporary or permanent period [40]. In order to overwhelm the targeted system or network and prevent it from responding to legitimate requests, DoS often involves sending a large number of unnecessary requests to the system or network [34].

B. Eavesdropping

Owing to the heterogeneous IoT architecture of the smart home infrastructure, an attacker may employ a variety of tools and methods to record network data between the various IoT device components. These techniques are extremely based on the attacker's capabilities and location [40]. The adversary will be able to intercept all traffic between the smart hub and the users if he uses the flaws in smart home technology to compromise the network's security. The attacker might use well-known tools such as tcpdump3, wireshark4, etc., to gain access to the data [40]. 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 [40].

C. Impersonation

In some circumstances, the adversary seeks to mimic a trustworthy user and act on that user's behalf to harm or spy on the victim. 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 [33].

D. Theft (Identity, credentials, information)

Users of smart homes are significantly impacted by the loss of valuable assets. Theft is an activity through which a person's property is taken or used without his/her permission [42]. The adversary seeks to steal important information from users of smart homes, such as login passwords or credit card information, for authentication and authorization. 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 [40].

E. 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 [43]. Also, attacker can deploy his own node or even compromise one of the existing nodes [44]. Once a network is compromised, the eavesdropper can be secretly merged into network traffic, making detection extremely hard. The attacker then begins covertly employing its cyber tools to identify security holes within the critical network cables. A cyber-map of the network's topography will be created by the malicious software after it has scanned the smart home infrastructure and probing IoT devices to find any system vulnerabilities. This step can be easily done by using tools found on the Internet [43]. Real-time and autonomous interaction between devices make discovering and identifying the compromised nodes very difficult [24].

F. Malicious Software

Malicious software is a term used to describe the software code created by attackers to gain unauthorized access to private networks or systems, collect or erase sensitive data, disrupt business operations, or display unwelcome advertising. Examples of malicious software include worms, Trojan horses, rootkits, and spyware. Malicious software (malware) can be injected into IoT applications and then affects the IoT services and devices [33]. Since IoT devices have a lightweight autonomous version of the well-known operating system, the attackers can access to private information using over mentioned malicious software in order to look for vulnerabilities and exploit them [29].

4. RECOMMENDED SECURITY SOLUTIONS AND PRACTICES

IoT-based smart home environments have seen a lot of security practices and solutions presented since they can hold private, sensitive, and essential information. The following section discusses a number of security options for IoT-based smart homes that have been recommended in recent years.

4.1 Updating the Software

To ensure current security software, updating and upgrading device software, firmware, and firewall is crucial. A firewall acts as a filter between internet and interface and control the traffic between network and the Internet [46]. Moreover, the firewall protects the network from malicious codes and external threats [8]. Firewall can detect and issue warning to user and invoke its mitigation strategy against particular security breaches [30]. Furthermore, it is essential to update the firmware and device software to the latest version to avoid unpatched vulnerabilities [47]. 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 [30].

4.2 Utilizing Effective Encryption

Wherever possible, the diverse components in an IoT device should successfully secure the data connection. 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 [38].

4.3 Using Private Network

One of the most common techniques for preventing unauthorized access to IoT devices is the deployment of a secure communication channel. 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 [33].

4.4 Applying up-to-date Protocols

Using the most updated protocols in IoT devices is crucial for network security. One of the most crucial elements of IoT is the protocol [35].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 [19].

4.5 Changing Credentials Regularly

IoT manufacturers should require customers to update the default identity (username and password) into strong ones the first time they use an IoT device, otherwise the IoT device should not function [47]. Moreover, the password must be changed at least once every three months. Besides that, users should not use the same password for all IoT devices, but rather should use a distinct password for each type of IoT device. Furthermore, it is strongly advised against using the email as a username because attackers frequently use this method to attempt to phish email accounts and obtain the password [48].

4.6 Backup Significant Information

Some smart home devices, such as healthcare devices, include important information that can only be accessed by authorized individuals. The ideal strategy is to regularly backup such information to prevent falsification or theft. The research study in [33] 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

Monitoring an IoT device's connection during message transfer is one of the greatest ways to secure smart homes. There are many tools help to monitor the network and analyse the device messages such as Microsoft Message Analyzer. Furthermore, the monitoring software can search for vulnerabilities and then update IoT programs.

5. CONCLUSIONS

The internet based 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 the main obstacles to the smart home have been identified as privacy and security in IoT environments. This paper reviewed some articles related to the architecture, threats, and security of smart homes environments. Some common existing architecture 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 user practices and solutions suggested for smart home environments were provided in this paper.

REFERENCES

[1] Greichen, J.J., “Value based home automation or today's market,” *IEEE Transactions on Consumer Electronics*, vol. 38, no. 3, pp.34-38, Aug. 1992.

[2] “The X10 Specification,” *X-10 (USA) Inc.*, 1990.

[3] “ZigBee Specifications,” *ZigBee Alliance*, version 1.0 r13, Dec. 2006.

[4] “LonTalk Protocol Specification Version 3.0,” *Echelon Co*, 1994.

[5] “EIA-600 CEBus Standard Specification,” *EIA*, 1992.

[6] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, “Home automation in the Wild: Challenges and Opportunities,” in *CHI ’11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2115-2124, 2011.

[7] 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.

[8] 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.

[9] 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.

[10] K. Madhuri, B. L. Sai, B. S. Sirisha, "A Home Automation System Design Using Hardware Descriptive Tools," *International Journal of Engineering Research & Technology*, vol. 2, no. 7, Jul. 2013

[11] E.M.C Wong, "A Phone-Based Remote Controller for Home and Office Automation," *IEEE Transactions on Consumer Electronics*, vol. 40, no. 1, pp.28-34, Feb. 1994.

[12] A. ElShafee, K. A. Hamed, "Design and Implementation of a WiFi Based home automation System," *World Academy of Science, Engineering and Technology*, vol. 6, 2012.

[13] M. Danaher, D. Nguyen, "Mobile Home Security with GPRS," in p*roceedings of the 8 th International Symposium for Information Science,* Oct. 2002.

[14] A. Alheraish, "Design and Implementation of Home Automation System," *IEEE Transactions on Consumer Electronics*, vol. 50 , no. 4, pp.1087-1092, Nov. 2004.

[15] V. Singhvi, A. Krause, C. Guestrin, James H. Garrett Jr., H. Scott Matthews, "Intelligent Light Control using Sensor Networks," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*, SenSys '05, pp. 218-229, 2005.

[16] A. Gaddam, "Development of a Bed Sensor for an Integrated Digital Home Monitoring System," *IEEE International Workshop on Medical Measurements and Applications*, pp. 33-38, May 2008.

[17] U. Saeed, S. Syed, S.Z. Qazi, N.Khan, A.Khan, M.Babar, "Multi-advantage and security based home automation system," *2010 Fourth UKSim European Symposium on Computer Modeling and Simulation (EMS)*, pp.7-11, Nov. 2010.

[18] 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.

[19] 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.

[20] 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.

[21] "Privacy in iot threats and challenges2014.pdf."

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

[23] 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.

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

[25] 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.

[26] 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.

[27] 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.

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

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

[30] 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

[31] S. on Security, "New IoT Security Regulations." [Online]. Available: https://www.schneier.com/blog/

archives/2018/11/new_iot_securit.html?fbclid=IwAR3LlVY7hsuXOpFxNwlURp2MjOVifqqYssgJCbh7MLg_qFsIyNmecNiFKUo

[32] Rambus, "Smart Home: Threats and Countermeasures - Rambus." [Online]. Available: https://www.rambus.com/iot/smart-home/

[33] 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.

[34] 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

[35] 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.

[36] iot for all, "How Encryption is Powering the Future of IoT | IoT For All," 2018. [Online]. Available: https://www.iotforall.com/future-iot-encryption/.

[37] 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.

[38] 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.

[38] 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.

[39] 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.

[40] 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.

[41] W. Paper, "Cyber Security in the Era of Smart Homes," pp. 1–114.

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

[43] 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.

[44] H. Rahmani, N. Sahli, and F. Kamoun, "Distributed denialof-service attack detection," no. May 2010, pp. 839–859, 2011.

[45] N. Nthala and I. Flechais, "Rethinking Home Network Security," no. April, 2018.

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

[47] T. M. Secur, "PA R A D I G M."

[48] 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/.