Analysis of Security and Vulnerabilities of Smart IoT Devices: A Review

Submitted by

Abidullah Afif

181-35-2472

Department of Software Engineering

Daffodil International University

Supervised by

Kaushik Sarker

Assistant Professor & Associate Head

Department of Software Engineering

Daffodil International University

This Project report has been submitted in fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering.

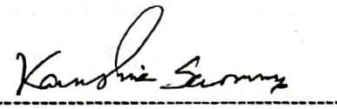
APPROVAL

This thesis titled on "Analysis of Security and Vulnerabilites in Smart IoT devices: A Review", submitted by Abidullah Afif, ID: 181-35-2472 to the
Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. Imran Mahmud
Associate Professor and Head
Department of Software Engineering
Daffodil International University



Internal Examiner 1

Kaushik Sarker
Assistant Professor
Department of Software Engineering
Daffodil International University

Internal Examiner 2

Md. Shohel Arman
Senior Lecturer
Department of Software Engineering
Daffodil International University

External Examiner

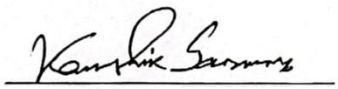
Md. Fazle Munim
Technology Expert
Access to Information (a2i) Programme

DECLARATION

It hereby declares that this thesis has been done by Abidullah Afif under the supervision of **Kaushik Sarkar, Assistant Professor & Associate Head,** Department of Software Engineering, Daffodil International University. It also declares that neither this thesis nor any part of this has been submitted elsewhere for award of any degree.

Student Name: Abidullah Afif
Student ID: 181-35-2472
Batch: 25th
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Certified by:



Kaushik Sarker
Assistant Professor & Associate Head
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

ACKNOWLEDGEMENT

This thesis is the consequence of an inspiring and exciting journey, where many passionate individuals have provided their heartiest support in many ways. I want to express my gratitude towards the Almighty for his divine blessings to let me complete my final year thesis successfully.

I would like to express my humble gratitude to our honorable **Kaushik Sarker** sir, **Associate Professor & Associate Head** for his constant support, guidance and advice. If it was not because of him, this thesis would never be completed. I am fortunate to have him as my supervisor. He not only played the role of our supervisor, but also played the role of a guardian.

Our heartfelt appreciation goes to **Mr. Maruf Hassan, Assistant Professor & Director of Cyber Security Center** for sharing his knowledge & wisdom about cyberthreats & cybersecurity and **Ms. Nusrat Jahan**, Assistant Professor, for sharing her knowledge & experience about research methodology & literature review. I also want to express my gratitude towards **Mr. Rony Shaha, Assistant Technical officer & Research Coordinator of Daffodil Robotics Lab** for his constant support and guidance on IoT based microcontrollers & smart devices.

We want to acknowledge our respectful gratitude & love to our **parents** and family members for their constant support & care they've always provided us.

Finally, I want to appreciate the entire department of **Software Engineering of Daffodil International University.**

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

As the term “Internet of Things” (IoT) was first introduced in 1999, our modern society is rapidly developing by these interconnected networks of smart devices. Cutting edge technologies and software engineering can make the smart devices connect with human to machine & machine to machine in a semi-automated or fully automated way so that IoT can be applied to the field of every aspect of a utopian society from remote medical surgery to automated home security. However, as the complexity grows in these networks & smart devices, the privacy and security risks are very significant to consider.

This paper will cover a review & analysis on cybersecurity threats and challenges of microcontroller based smart devices, software architectural security flaws & vulnerabilities to the node sensor module in IoT devices.

The growing demand of 5G and higher generation network systems will create a huge industrial revolution of IoT & Smart devices, however we, the cybersecurity researcher, should always find the best solutions for all the possible security threats & vulnerabilities.

Keywords: Internet of Things (IOT), microcontroller security, privacy & security issues, wireless sensor network security, smart devices, IoT security

CHAPTER 1

INTRODUCTION

1.1 Background

The rising usage of high-speed internet and automated computing has made our lives easier. We are now implementing internet of things in all possible sectors, weather forecast, industrial manufacturing robots, smart home sensors, automated vehicles, smart devices such as AC, Fridge, Interior Lights, all are now part of the IoT hub. As these smart devices can transmit data and communicate to each other, the data needs to be transmitted in a secure manner. As the triangle of Functionality, Usability & Security suggest, more features can lead to more cyberthreats.

1.2 Motivation of the Research

There are several reports on zero-day vulnerabilities about many new consumer based IoT devices. Hackers are now more aggressive and have better attacking frameworks to break through and compromise a vulnerable network and software systems. There have been recorded reports on hacking smart vehicles, controlling smart vehicles, bypassing smart locks, hacking medical IoT infrastructure all of these incidents are not very obsolete. We are still facing new challenges and trying to spread more awareness about these trending cyberthreats.

1.3 Problem Statement

The IoT industry is not a mature industry yet. Several researches have already shown there are so many security flaws in this sector and as the demands for IoT devices grows, the risk factor grows with the flow.

There is not enough contribution in this field, especially overall review of the IoT Node MCU

sensor enable device security systems.

1.4 Research Questions

Question 1: What are the common vulnerabilities according to the OWASP top 10 model?

Question 2: How can security systems be implemented in the OSI layers?

Question 3: How can we mitigate the privacy and data theft risks of IoT and Smart devices?

Question 4: How vulnerable is the Node MCU sensor network & How to secure them?

1.5 Research Objectives

- Finding the top 10 common vulnerabilities & attacks in IoT devices.
- Securing physical layer, network layer & application layer in IoT devices.
- Consumer based IoT products privacy protection policy & risk analysis.
- Node MCU home network security analysis & possible solutions.

1.6 Research Scope

This research will cover the summary of concurrent & relevant threat & vulnerability analysis of IoT networks and smart embedded systems. This research is completed within a period of eight month with limited access to academia lab instruments.

The scope of this thesis is to justify common security practices to prevent attack on smart IoT devices. This security field are covered within the analysis part of IoT Vulnerability assessments:

- Wireless sensor security.
- Network security
- Authentication & Authorization of the system administrator.
- Remote executable vulnerabilities.

- Privacy & Other risk factors.

1.7 Thesis Organization

This thesis has been conducted in the Daffodil International University Robotics lab. All the IoT related microcontroller & embedded systems are tested inside the lab.

As this thesis is a summary & review of other IoT security related thesis and research articles, I had to organize the thesis in a timeline to cover all basic fields related to IoT security analysis. These includes:

- Collecting, reading and understanding IoT related research papers and journals.
- Understanding & getting familiar with the IoT based smart device ecosystem.
- Exploring the vulnerabilities in a Node MCU home IoT network.
- Performing brutforce password dictionary attack to the network.
- Performing Wifi Deauther & Becon attack with ESP8266 arduino module.
- Analyzing the encryption method of data flow between smart devices.
- Finding other common risk factors & privacy issues related to IoT Based Smart Home.
- Finding common patterns of vulnerabilities from all relevant researchers in this field & giving a conclusion.

CHAPTER 2

LITERATURE REVIEW

In this paper [01], A review on IoT machine to machine (M2M) mythology, IoT Vision, RFID, Wireless Sensor Network (WSN), IoT security and the architecture of IoT devices are explained with easy to understand figures. The paper [02], reviewed the security of Smart farming technology & Precision Agriculture. Proposed article has in depth statistical report on different types of cyber attacks such as RF Jamming, DoS attack, Botnets, Side Channel Attack, MITM attack, Cloud computing attack, Data Leakage, False Data Injection, Misconfiguration, Software Update attacks, Malware Injection, Buffer overflow, SQL attacks, Data fabrication, Cyber-Terrorism, all classified with specified category (Availability, Confidentiality, Integrity, Non-Repudiation, Trust & Privacy). This paper also explains the 7 stages of cyber-attack according to CKC (Reconnaissance > Weaponization > Delivery > Exploitation > Installation > Command & Control > Action on Objectives.). The CKC-based OSI layer taxonomy on Cyber-threats to SF & PA is also present in this review paper.

In the paper [03], privacy & security requirements are analyzed for the emerging IoT devices. The term “Authentication & Key Management” is proposed in this paper. On the other hand Iqbal A. et al, reviewed a paper[04] on cybersecurity. Various types of malicious codes (Worms, Virus, Malware, Trojan Horse) and security threats & their impact is reviewed.

Another review paper [05] is about the future of emerging IoT technologies, IoT architecture, IoT challenges & IoT Applications. The potential applications of IoT are found such as Smart Traffic Management, Security & Surveillance, Agriculture Automation, Healthcare & Medicine, Smart Cities & Homes, Supply Chain and Energy consumption. The stability, reliability, law & regulatory rights for these smart ecosystems are also concluded.

Joel A. and Malekian R. proposed another review paper [06] of smart home automation security using access control, data security, intrusion detection & the physical infrastructure access control. This research concluded the Homeowners point of view, as well as a security Engineers point of view. The Context-aware home automation systems, Bluetooth based Home Automation System, Central Controller-based Home Automation System, GSM or

Mobile-based Home Automation System, GPRS-based Home Automation System, DTMF based Home Automation System & Internet-Based Home Automation System & Security issues of these system are addressed. Zhang W. et al, has in depth review about[07] the top 10 research topic in IoT field in 2019.

This paper [08], introduces with the 5G security & threat analysis. Security Challenges of Software defined networking (SDN) and Network Function Virtualization (NFV) n secure communication channels are introduced. Proposed model uses encrypted Host Identity Protocol in the Transport layer. For Radio Access Network (RAN), a cloud based secure solution C-RAN is introduced. The article [09] published by Rocha J. presents the ongoing vulnerability trends in sensor assisted security protection & IoT devices in 2018.

A case study [10] of a Smart Home for IoT device vulnerability studies and security postures. Different scenarios of abuse & misuse of the vulnerable smart home are overviewed from National Vulnerability Database (NVD) & the vulnerabilities are classified in a survey table. Another research [11] has proposed a large-scale report on vulnerability scanning of IoT devices in Jordan using Shodan using the Common Vulnerability Scoring system (CVSS). On the other hand Rehman A. [12] proposed a vulnerability model for Hybrid IT systems such as automated supply chain with CVSS framework.

This Paper [13] introduced the top vulnerability analysis in IoT devices for smart home Environment by PTES standard penetration testing approach. The industry standard penetration testing tools are used such as Kali Linux, Wireshark, Zenmap, Aircrack NG, Medusa, Ncrack, Hydra, OWASP Zap. The paper [16] is a comparative analysis on Smart Home systems to control, Monitor & Secure Home with wireless network microcontrollers like Zigbee, GSM, PIC, Bluetooth. On the other hand, another paper [17] is all about Arduino based smart homes with a mobile friendly user interface, WIFI based network & Bluetooth based controller which is suitable for smart cities.

This paper [18] proposed Smart Home Automation System & Security systems using Arduino microcontroller & Sensor modules such as Flex Sensor, Flame Sensor, Fire Sensor, Relay Driver, LDR & DC Motors. Another paper [19] finds the requirements on Secure & Privacy focused IoT Architecture with compared IoT Protocols such as Azure-IoT, CoAP, DDS, DPWS. This also includes the security of WSN, NFC & RFID technologies as well. Similarly another paper [20] concludes the security and privacy issues for an IoT based Smart Home with Zigbee module in the European Union. Another paper [21] introduces the IoT

ecosystem architecture of Smart city applications such as Smart energy grid & power supply, Intelligent healthcare network, Smart Industry, Intelligent Navigation & Traffic control, the challenges of these interconnected ecosystems & the solution to the challenges.

In this paper [22], an In-Hub Security Manager is proposed for securing vulnerable home IoT devices from different kinds of DOS & DDOS attacks. In the forensic part, the paper [23], a Forensic Investigation Framework is proposed for Zigbee & Z-wave based IoT Smart Home Environment. Another paper [24] has proposed RSA & AES encryption systems for the secure integration of IoT Cloud Computing. In the network segment, Ahmed I. et al [25] introduces the challenges & solutions for 5G technology, 5G-PPP, SDN, NFV & Mobile Edge Computing (MEC).

The journal paper [26], laser-based Audio-Injection attacks are performed on consumer-based voice-controllable systems such as "Google Home mini", targeted to the MEMS microphones. The sound wavelength is compared with the light wavelength to exploit the target. With a range of 100m, the cyber weaponized laser light 60mW High-Power laser & 5mW Low Power Lasers are used in the attack vector to manipulate user authentication from a voice record.

Benjamin K. et al, has published a review paper[27] on the public knowledge about energy sustainability, and vulnerability in the demographics of smart home technology diffusion. On the other hand Xiao L. [28] has proposed Machine Learning techniques on the security of IoT based smart devices such as WSN, RFID, Zigbee to prevent DoS attacks and Network Jamming. On the other hand, Ishan A. et al, published a review paper[29] on Arduino & Raspberry Pi based IoT and Smart Home security analysis. On the other hand Weber R. proposed a paper [30] about the Privacy enhancing policy & Rule making process for the regulations on IoT Smart devices. Another paper [31] designed Arduino & Wireless NodeMCU based Intelligent Smart Home Automation & Security System with extended sensor modules.

Jose A. et al published a paper [32] which represents an automated Smart Home Security & Door locking system using logical sensors and predefined algorithms. Relatively, the paper [33] by the same authors proposed the integration of Fingerprint Sensors to improve Smart Home Automation Security. In the vulnerability segment, another paper [34] proposed penetration testing methodology to find vulnerabilities in WIFI Network using WNS WIFI Deauther, USB Rubber Ducky & Backdoor APK. Similarly another paper [35] Concludes the

cyber threats and vulnerabilities of Smart Autonomous Vehicular Technologies. Another paper [38] has proposed the Security Vulnerability Qualification for Social IoT Devices based on "Game Theory" mathematical model. Jiang X. [43] performs different types of cyber attacks for an Experimental Analysis on Industrial IoT device vulnerabilities. On the other hand [47] a risk analysis methodology is proposed for threat analysis on Smart Home Automation System

A Journal [36] on Home IoT resistance by Lee H. has specified some common vulnerabilities & privacy issues in the IoT environment & Smart devices. In this paper, Lova K. et al proposed [37] a Smart Home ecosystem has been developed for IoT Automation using Arduino based NodeMCU and Other sensors. The smart home system can be remotely controlled by using an Open Source remote control App "Blynk".

In the cloud computing sector, [39] has reviewed the security and privacy issues on Fog Computing for the IoT devices. Sontowski et al, [40] has performed a vulnerability analysis and penetration testing on IoT based Smart Farming Technologies & Sensors. Ali B. [41] has evaluated the Cyber & Physical Security Vulnerabilities for IoT based Smart Homes using OCTAVE Risk analysis methodology specified with the OSI layers. Similarly, this paper [42] focuses on the Consumer based IoT Vulnerabilities case studies and their solutions.

A survey on security loophole and privacy analysis of IoT Smart systems such as WSN and RFID has been analysed by Borgohain T. [14]. The paper published by Hassan R. [15] is an analogy of future smart cities and a smart ecosystem within the smart cities, opportunities and challenges, architecture, environment and sustainable lifestyle in that IoT based futuristic environment. Another Survey on Improving Home Automation Security for Fingerprint enabled Smart Home Security Systems [44] has conducted on 2017, by Sankar A. et al. The paper [45] is a survey on Security & Privacy issues in Internet of Things on 2017. Another survey-based paper [46] on Architectures, Enabling technologies, Security &Privacy & Applications of Internet of Things.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction to the Secure System Model Related to this Research

Technology is getting more complex and smarter every day. A few decades ago, it was just a hypothetical concept about autonomous smart vehicles & automated smart homes. The rapid development of the high speed internet network and super-efficient semi-conductors has made it possible to merge cutting edge technologies from various fields.

As a result of 5G high speed internet, the world will see a rapid growth in the IoT field, most importantly the automatic vehicles such as Tesla Electric cars. These smart embedded systems will make our life more convenient, but there's a catch. As the benefit grows, the risk factor also grows with it.

This industry is very new both for the manufacturer & for the consumers. The ideal security standards are not enough for handling next generation cyber threats. More academic and industry-based research is a necessity for the sustainable development of IoT ecosystems. The lack of compliance on IoT makes it a more vulnerable target to the black hat hackers. There are already reported botnet attacks & DDoS attacks on several IP cameras and Smart vehicles which are a very critical part of the IoT ecosystem. Nowadays, hackers are placing crypto-mining malicious codes in vulnerable IoT devices which have a moderate CPU or GPU unit.

Another biggest challenge is the lack of knowledge about smart device security and vulnerability & easily accessible hacking tools. Consumers and the end user cannot know the security & privacy related issues with their owned devices. On the other hand, hackers can easily find the common vulnerabilities from open sources like SHODAN.

The consequences of a compromised device can be economically significant & can also be life threatening! It is the duty for cyber security analysts to ensure the highest level of security standards in IoT and Smart devices as well as any connected devices to make a better society. There are new techniques and terms being introduced every year in the cyber world. High level programming languages are easier to maintain and easier to control. As it is a good step for the programming community, the risk factors are higher than previous generations. Many powerful cyber warfare tools are being developed by the high end programming community. Some of the community members have the black hat motive, they choose to hack into other devices and government server systems. We need an active team of white hat hackers and cybersecurity experts to protect cyber infractures against any kind of threats.

3.2 OSI Layers:

The Open System Interconnection or OSI-Model represents 7 architectures of a digital device. All these 7 layers work to communicate and transmit data in a collaborative way in all IoT Devices.

The layers are expressed in a sequence in figure no.1

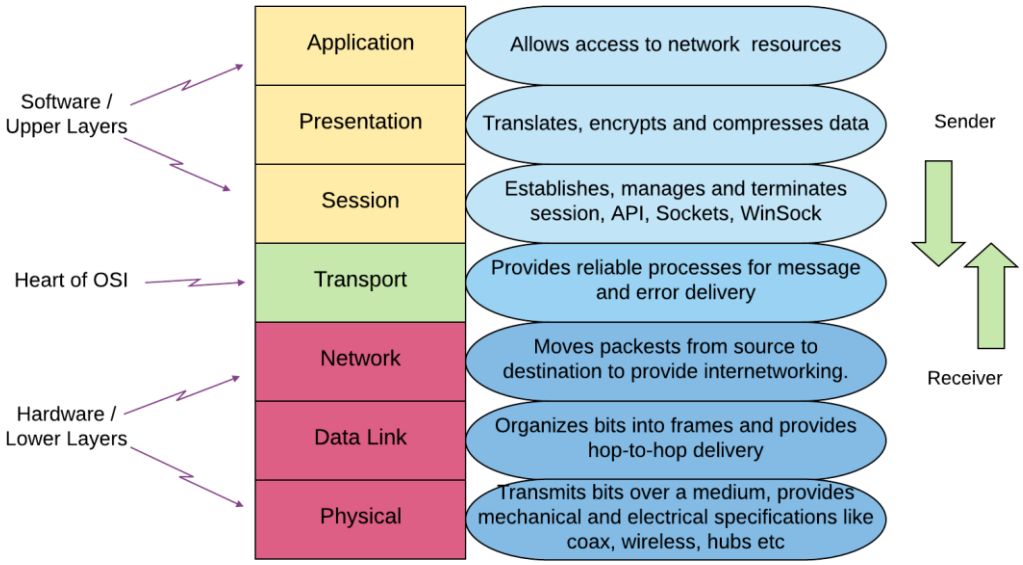


Figure 3.1: OSI Layers

Layer 1 – Physical Layer

The physical layer concerns the part of the model used for transmitting raw data bits (0s and 1s) across the network between sending and receiving devices. This can be through a physical cable or even a wireless connection between physical nodes. The physical layer can also represent voltages, frequencies, pin layouts, and other things. Any other physical devices part of this transmission, like hubs and modems, are also included.

Ethernet, USB, Bluetooth, IEEE 802.11 etc. protocols work on Physical Layer.

Layer 2 – Data Link Layer

The data link layer is in charge of establishing or eliminating a connection between physical nodes that may be connected through a cable or wirelessly. In addition, it also takes care of any data correction for errors that might be made in the physical layer. The data link layer is made up of two sub layers of its own which are:

– The media access control (MAC) is responsible for the data transmission and the provision of data flow by defining permissions across the network.

– The Logical Link Control (LLC) is responsible for controlling the data flow and identifying errors that occur from flow from physical media. In addition, it also identifies network protocols.

PPP, ATM etc. protocols work on Data Link Layer.

Layer 3 – Network Layer

The network layer's primary responsibility is receiving packets of data from the data link layer and then moving them ahead. It fulfills this duty by finding the best route of forwarding these packets using the address that has been given to them by the data link layer. In essence, it routes the packets to the destination, and this is where router devices tend to come in handy as the 'routing' of information is taking place.

IP, ARP, ICMP, IPsec etc. protocols work on Network Layer.

Layer 4 – Transport Layer

The transport layer is responsible for data transmission between the transmitting and receiving ends. It does this by initially breaking up the data at the transmission end and then constructing it back at the receiving end. The transport layer also deals with error control and checks if there is any incorrect data sending. If an error has occurred during transmission, it is responsible for requesting it again from the transmission end.

An excellent example of the transport layer is the Transmission Control Protocol (TCP). UDP also works on Transport Layers.

Layer 5 – Session Layer

The session layer is responsible for creating sessions between computers, i.e., communication channels to transfer data between them. In addition, it is responsible for keeping these channels open during data transmission and ending them when this transfer has been completed. It can also create checkpoints in data transfer to resume the transfer from the last checkpoint in case the session has been interrupted.

Examples of Session Layer protocols are NetBIOS, PPTP etc.

Layer 6 – Presentation Layer

The presentation layer is responsible for the encryption of data between two devices. It informs the devices how it has coded and compressed the data to be decrypted at the receiving end. In this way, it is essentially responsible for preparing the data for the application layer and transmits any data from it back to the session layer if needed.

SSL and TLS are the best examples of Presentation Layers.

Layer 7 – Application Layer

The Application is the layer at the top of the OSI Model and is what users mostly see when they are using end-user software, like their web browser or Microsoft Office. It provides protocols to the software to allow it to send and receive information directly from users and display it to them. Some of these protocols include HTTP, FTP, and DNS. It is important to note that the applications themselves are not present in this layer, but instead, it allows them to communicate to the lower layers for communication with applications on the other side.

3.3 Case Study and Literature Review:

There have been several IoT related research papers published in recent years. This thesis is mainly based on reviewing these relevant research papers related to IoT, IoT Hub, Smart Home, Smart City, IoT security & Vulnerability issues, NodeMCU based sensor network & 5G technology network challenges and solutions. The top influential papers & Journals related to IoT security are highlighted in Table 3.1.

Table 3.1: Literature Reviews

Title	Authors	Result Discussion
IoT Security Techniques Based on Machine Learning. Digital Object Identifier	Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu	Machine Learning techniques on the security of IoT based smart devices such as WSN, RFID, Zigbee to prevent DoS attacks and Network Jamming.
Security and Privacy in Smart City Applications: Challenges and Solutions.	Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen	IoT ecosystem architecture of Smart city applications such as Smart energy grid & power supply, Intelligent healthcare network, Smart Industry, Intelligent Navigation & Traffic control, the challenges of these interconnected ecosystems & the solution to the challenges.
Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems.	Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu.	Audio-Injection attacks are performed on consumer-based voice-controllable systems such as “Google Home mini”, targeted to the MEMS microphones.

Security and Privacy in Smart City Applications: Challenges and Solutions.	Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen.	IoT ecosystem architecture of Smart city applications such as Smart energy grid & power supply, Intelligent healthcare network, Smart Industry, Intelligent Navigation & Traffic control, the challenges of these interconnected ecosystems & the solution to the challenges.
A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures.	Abbas Yazdinejad 1 , Behrouz Zolfaghari 1 , Amin Azmoodeh 1 , Ali Dehghantanha 1,*, Hadis Karimipour 2 , Evan Fraser 3 , Arthur G. Green 3 , Conor Russell 3 and Emily Duncan	Reviewed the security of Smart farming technology & Precision Agriculture. Proposed article has in depth statistical report on different types of cyber attacks such as RF Jamming, DoS attack, Botnets, Side Channel Attack, MITM attack, Cloud computing attack, Data Leakage, False Data Injection, Misconfiguration, Software Update attacks, Malware Injection, Buffer overflow, SQL attacks, Data fabrication, Cyber-Terrorism, all classified with specified category (Availability, Confidentiality, Integrity, Non-Repudiation, Trust & Privacy).
Security and Privacy Issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS).	Aqeel-ur-Rehman1 , Sadiq Ur Rehman2 , Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan.	Requirement Analysis for Secure & Privacy focused IoT Architecture with compared IoT Protocols such as Azure-IoT, CoAP, DDS, DPWS. This also includes the security of WSN, NFC & RFID technologies as well.

3.4 Significance of vulnerabilities

The significance of IoT vulnerability can be huge in terms of scale. As IoT devices will be crowded in the medical industry, autonomous vehicle industry, Home Security industry, Drone & Air transport industry, Power hubs, Supply chain & manufacturing industry, a hacker group can take control of critical infrastructure.

This can be economically significant as well as life threatening if it comes to the vehicle & medical industry. All the IoT components generate and transmit massive collections of data to the cloud server, so we have to consider the risk of private data leakage also in order to use these devices in our daily life.

.

3.4.1 OWASP Top 10 - Vulnerability Types & Impact

Open Web Application security project or OWASP top 10 is an open community to identify the top 10 vulnerabilities in web app technologies. These top 10 vulnerabilities are collected from the official website of OWASP.ORG in 2021.

A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.

A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was a broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.

A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.

A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.

A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.

A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.

A09:2021-Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

3.4.2 Lab Experiments

A Smart Home automation system based on Arduino & ESP Node MCU has been developed as the following architecture:

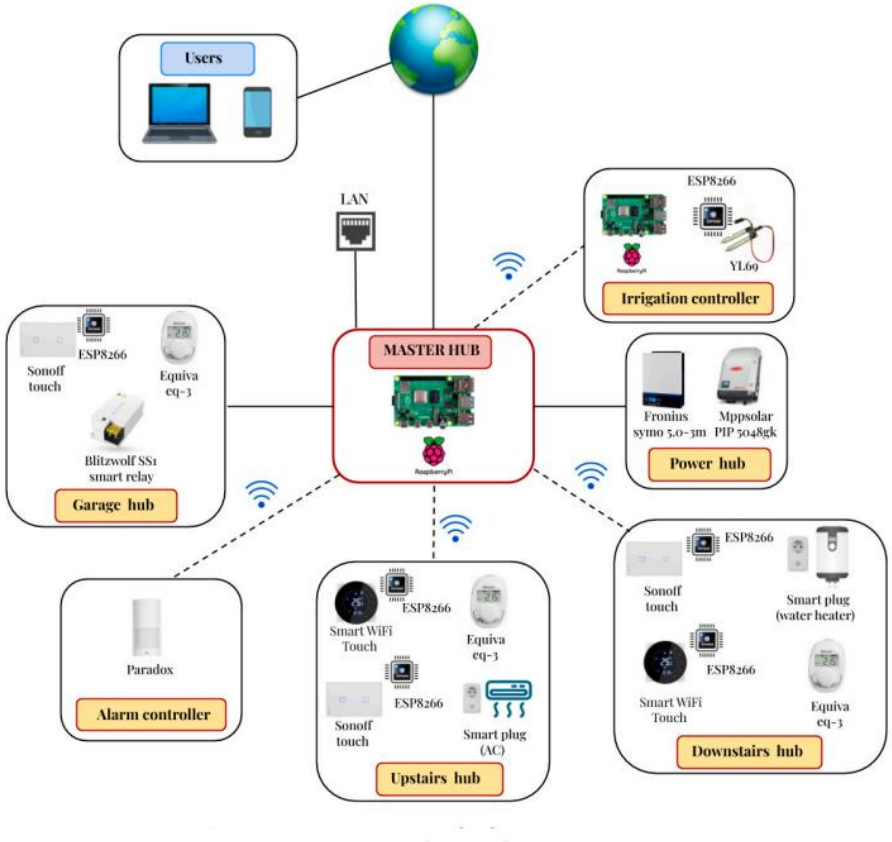


Figure 3.2: Smart Home Architecture

The raspberry pi acted as the central hub or Cloud server for the smart home environment. The sensors are connected with the ESP 8266 NodeMCU.

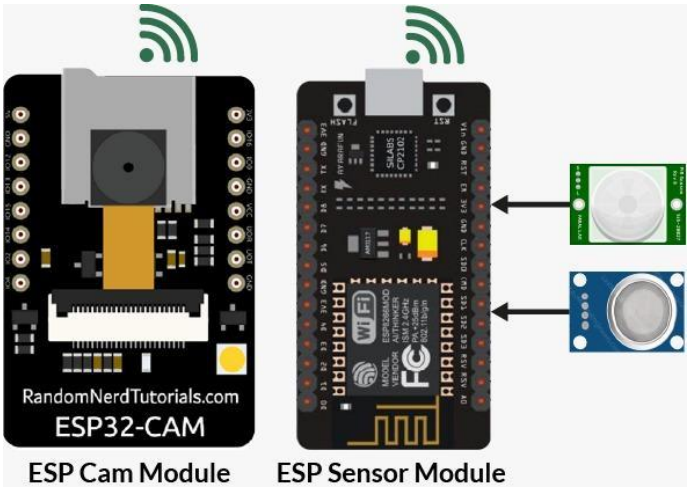


Figure 3.3: ESP Camera Module

There have been several sensor and relay actuators for automatic smart home doors. The ESP 8266 Module has been flashed with a custom BIOS for targeting the Smart home IoT network. Wi-Fi Deauther works with 100% accuracy within the range of the network.

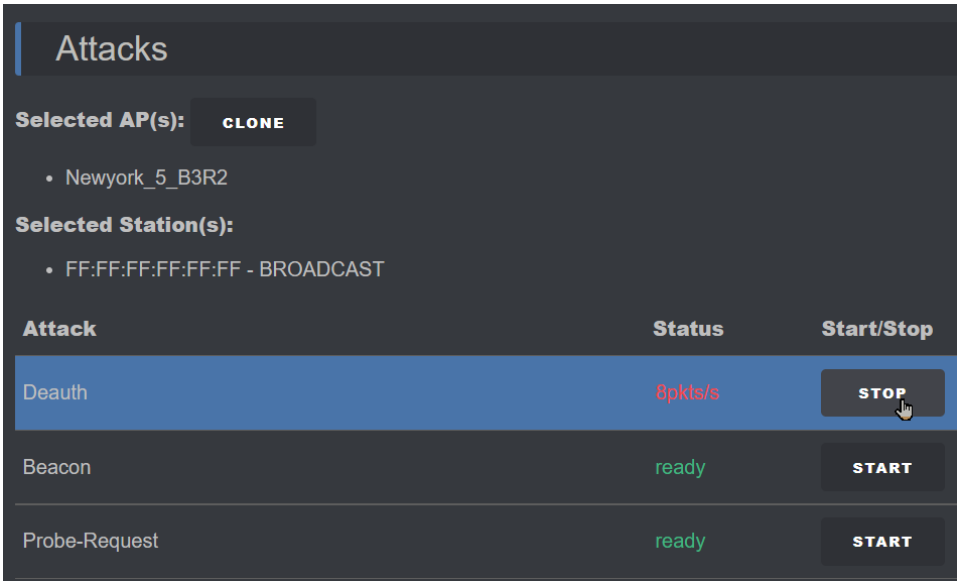


Figure 3.4: Interface of ESP8266

3.4.3 Risk Assessment

The risk assessment of the IoT environment is performed on the analogy of all the literatures relevant to this IoT Security segment.

Table 3.2: Risk Assessment

Risk ID	Risk Name	Risk Impact	Risk Type	Likelihood	Security Attribute Compromised
01	Weak Password	Critical	Vulnerability	High	Authentication
02	Weak Encryption	Critical	Vulnerability	low	Integrity, Privacy, Authentication
03	Misconfiguration	High	Vulnerability	Very High	Authorization, Access control
04	Network Jamming	High	Physical Security	High	Availability & Reliability
05	Network Spoofing	High	Vulnerability	High	Access control, Spyware
06	Malicious Code Injection	Critical	Vulnerability	High	Integrity, Non-Reputation, Access Control
07	Improper session management	High	Vulnerability	Low	Access control, Privacy
08	Backdoors	Critical	Vulnerability	Low	Access Control, Authentication
09	DoS Attack	Medium	Vulnerability	Moderate	Availability
10	Remote Access	Critical	Vulnerability	Moderate	Authorization, Access Control

3.4.4 Privacy Impact

As the data is transmitted through the secure communication from the Sensor elements to the central hub, there are some risk factors of Man in the Middle Attack.

There are possibilities of password and other sensitive information leakage when communicating with the IoT network.

There are some consumer based IoT devices which collect the user data without the concern of the end user. The European Union has taken steps in the law and regulations of the IoT Device policies.

The end user must get a clear message about what kind of data will be collected and stored from an IoT device.

CHAPTER 4

RESULTS AND DISCUSSION

This thesis is a review paper on IoT and Smart Device Security and Privacy Analysis, based on collected resources and Research papers. The objective of the lab performance was to develop and build a Smart Home environment with IoT based Node Microcontroller Units. A scenario is created where a black hat hacker deauthorizes the IoT network and works as a jammer. The result has been discovered to verify other sources of security assessment and risk analysis from the IoT network. The central hub is easily vulnerable without any secure architecture of the entire ecosystem of the IoT Network.

The lab performance has been conducted with the Raspberry Pi 4 model as the central hub with ESP8266 as the WiFi Node module. All IoT devices have the OSI 7 layers, which are individual targets of a pre-planned cyber-attack. The OWASP top 10 web app vulnerability is partially related to the segment of IoT & Embedded systems.

Thus, IoT Smart Home devices aren't at a mature stage, the risk factors are yet to consider. More real-life scenarios and case studies are needed to support the IoT security community. Proper infrastructure & lab facilities are an essential part of the VAPT tests.

The test report may vary from device to device and attacking method. Due to a strict schedule for the publication of this thesis, several penetration testing methods were proposed but couldn't get to a result conclusion. Common vulnerabilities such as Dictionary attack brutforce, WIFI Deauther, Network spoofing have been conducted with a successful attempt. A firewall and & Wifi jammer detector can help to prevent such incidents.

There are different kinds of scenarios for a cyber attack including pre-attack phase and post attack phase. The pre attack phase includes the planning, vulnerability findings, target setting, exploit delivering and access gaining. Lack of cybersecurity knowledge is one of the most common issues in the cybersecurity issue. Even the IoT smart devices are connected with the internet through a protocol, the security threats are more similar to a vulnerable website or a vulnerable server system. Common vulnerabilities are Misconfiguration, Low level Encryption, Open ports and command shells, Authentication loopholes, Weak password, Lack of cybersecurity risk assessment, Lack of Vulnerability Analysis and Penetration Testing, Programming bugs, Open Wifi ports, Insecure design and programming. The way to mitigate these challenges is to allow white hat ethical hackers and penetration testers to check security issues and apply patch updates on a regular basis. Spreading awareness will always create an impact in the cyberworld.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings and Contributions

IoT devices are still not saturated in our daily life but soon it will transform our life. With the famous saying of "With big power comes big responsibility", we have to focus on both the good and bad side. IoT smart devices can lead to exposure of our private data and cyber criminals might get more control over our life with vulnerable IoT devices. Most of the IoT Ecosystems are connected through Wireless Sensor Network (WSN), Zigbee, Bluetooth & NODE MCU like Arduino & Raspberry Pi. These are open source community products which have not been properly tested for real life hazardous & emergency scenarios. Cyber Intruders might take advantage of these electronic devices as these all will be connected through an internet network.

There should be strong regulation and privacy enhanced policy to all IoT related manufacturing in the term of collecting user data. End to end encryption shouldn't be tested and verified before mass production of these smart devices. Spreading awareness about cyber risk and privacy issues will play the most significant part in order to ensure secure usages of IoT & Smart Devices.

5.2 Recommendations for Future Works

There are lots of micro fields in the IoT macro field. From the OSI 7 layers, we can implement more secure communication architecture in all 7 layers of a Smart IoT device. An Arduino based small IoT smart city ecosystem can be developed for the vulnerability analysis & penetration testing of these user end IoT Devices.

REFERENCES

[01] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal. A Review on the Internet of Things (IoT). International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015

[02] Abbas Yazdinejad 1 , Behrouz Zolfaghari 1 , Amin Azmoodeh 1 , Ali Dehghantanha 1,*, Hadis Karimipour 2 , Evan Fraser 3 , Arthur G. Green 3 , Conor Russell 3 and Emily Duncan(2021). A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures.

[03] Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi University of Louisiana at Lafayette (2016). A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches.

[04] Saloni Khurana Department of Electronics & Communication Vivekananda Institute of Technology. A Review Paper on Cyber Security. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org VIMPACT - 2017 Conference Proceedings.

[05] Sachin Kumar1* , Prayag Tiwari2 and Mikhail Zymbler. Internet of Things is a revolutionary approach for future technology enhancement: a review. Kumar et al. J Big Data (2019) 6:111 https://doi.org/10.1186/s40537-019-0268-2

[06] Arun Cyril Jose1 and Reza Malekian2. Smart Home Automation Security: A Literature Review. Smart Computing Review, vol. 5, no. 4, August 2015.

[07] Wei Emma Zhang1 , Quan Z. Sheng2 , Adnan Mahmood2 , Dai Hoang Tran2 , Munazza Zaib2 , Salma Abdalla Hamad2 , Abdulwahab Aljubairy2 , Ahoud Abdulrahmn F. Alhazmi2 , Subhash Sagar2 , and Congbo Ma1. The 10 Research Topics in the Internet of Things. arXiv:2012.01594v1 [cs.DC] 2 Dec 2020.

[08] Ijaz Ahmad∗ , Tanesh Kumar† , Madhusanka Liyanage‡ , Jude Okwuibe§ , Mika Ylianttila¶ , Andrei Gurtovk. 5G Security: Analysis of Threats and Solutions. 2017 IEEE Conference on Standards for Communications and Networking (CSCN).

[09] Junia da Rocha Valente, PhD The University of Texas at Dallas, 2018. VULNERABILITY TRENDS IN IOT DEVICES AND NEW SENSOR-ASSISTED SECURITY PROTECTIONS.

[10] Brittany D. Davis, Janelle C. Mason, and Mohd Anwar. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. Citation information: DOI 10.1109/JIOT.2020.2983983, IEEE Internet of Things Journal IoT-8794-2019

[11] Haneen Al-Alami, Ali Hadi, Hussein Al-Bahadili. Vulnerability Scanning of IoT Devices in Jordan Using Shodan. Conference Paper · December 2017 DOI: 10.1109/IT-DREPS.2017.8277814

[12] Attiq Ur-Rehman, Iqbal Gondal, Joarder Kamruzzuman, Alireza Jolfaei. Vulnerability Modelling for Hybrid IT Systems. 2019 IEEE International Conference on Industrial Technology, ICIT 2019; Melbourne, Australia; 13th-15th February 2019 Vol. 2019-February, p. 1135-1142.

[13] Lu´ıs Costa1 Joao Paulo Barros ˜ 1,2 and Miguel Tavares1,2,3. Vulnerabilities in IoT Devices for Smart Home Environment (2020). DOI: 10.5220/0007583306150622 In Proceedings of the 5th International Conference on Information Systems Security and Privacy.

[14] Tuhin Borgohain, Department of Instrumentation Engineering, Assam Engineering College, Uday Kumar Delivery Manager, Tech Mahindra Limited, Sugata Sanyal Corporate Technology Office, Tata Consultancy Services, Mumbai, India. Survey of Security and Privacy Issues of Internet of Things.

[15] Rondik J. Hassan1* , Subhi R. M. Zeebaree1 , Siddeeq Y. Ameen1 , Shakir Fattah Kak1 , Mohammed A. M. Sadeeq1 , Zainab Salih Ageed2 , Adel AL-Zebari1 and Azar Abid Salih1 (2021). State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions. Asian Journal of Research in Computer Science 8(3): 32-48, 2021; Article no.AJRCOS.68484 ISSN: 2581-8260

[16] Vishakha D. Vaidya, Pinki 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.

[17] Tanweer Alam. Abdulrahman A. Salem. Ahmad O. Alsharif. Abdulaziz M. Alhujaili. " Smart Home Automation Towards the Development of Smart Cities.", Computer Science and Information Technologies. Vol 1(1). 2020. DOI: 10.11591/csit.v1i1.p17-25.

[18] Smart Home Automation and Security System using Arduino and IOT Siddharth Wadhwani1, Uday Singh2, Prakarsh Singh3, Shraddha Dwivedi4 1234 Student, Dept. o EC, IMS Engineering College, Ghaziabad, UP, INDIA.

[19] Aqeel-ur-Rehman1 , Sadiq Ur Rehman2 , Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan. Security and Privacy Issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS) Vol. x, No. x, November 2016.

[20] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino. Security and Privacy Issues for an IoT based Smart Home. MIPRO 2017, May 22- 26, 2017, Opatija, Croatia.

[21] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen. Security and Privacy in Smart City Applications: Challenges and Solutions. 0163-6804/17/$25.00 © 2017 IEEE IEEE Communications Magazine, January 2017. Digital Object Identifier: 10.1109/MCOM.2017.1600267CM.

[22] Anna Kornfeld Simpson, Shwetak N. Patel, Franziska Roesner, Tadayoshi Kohno. Securing Vulnerable Home IoT Devices with an In-Hub Security Manager. IEEE PerCom 2017.

[23] Arnoud Goudbeek, Kim-Kwang Raymond Choo, Nhien-An Le-Khac. A Forensic Investigation Framework for Smart Home Environment. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference On Big Data Science And Engineering.

[24] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and Cloud Computing, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.031.

[25] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, March 2018.

[26] Takeshi Sugawara, The University of Electro-Communications; Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu, University of Michigan. Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems. August 12–14, 2020 978-1-939133-17-5 Open access to the Proceedings of the 29th USENIX Security Symposium is sponsored by USENIX.

[27] Benjamin K. Sovacool, Mari Martiskainen , Knowledge, energy sustainability, and vulnerability in the demographics of smart home technology diffusion. Dylan D. Furszyfer Del Rio. https://doi.org/10.1016/j.enpol.2021.112196 Received 4 April 2020; Received in revised form 2 February 2021; Accepted 4 February 2021.

[28] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. IoT Security Techniques Based on Machine Learning. Digital Object Identifier 10.1109/MSP.2018.2825478 Date of publication: 28 August 2018.

[29] Abdulrahman Ihsan Abdulla1 , Ahmad Sinali Abdulraheem2 , Azar Abid Salih3 , Mohammed A. M. Sadeeq4 , Abdulraheem Jamel Ahmed5 , Barwar M. Ferzor, Sardar6 , Omar Salih7 , Sarkaft Ibrahim Mohammed. Internet of Things and Smart Home Security. ISSN: 04532198 Volume 62, Issue 05, June, 2020.

[30] Rolf H. Weber. Computer law & security review 31 (2015). Internet of things: Privacy issues revisited. http://dx.doi.org/10.1016/j.clsr.2015.07.002 0267-3649/© 2015.

[31] J.Chandramohan1 , R.Nagarajan2 , K.Satheeshkumar3 , N.Ajithkumar4 , P.A.Gopinath5 , S.Ranjithkumar6. Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi J. International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 3 March 2017, Page No. 20694-20698 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.53

[32] Improving Smart Home Security; Integrating Logical Sensing into Smart Home. Arun Cyril Jose, Reza Malekian, Senior Member, IEEE.

[33] ARUN CYRIL JOSE1 , REZA MALEKIAN1 , (MEMBER, IEEE), AND NING YE2,3 . Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home. Digital Object Identifier 10.1109/ACCESS.2016.2606478.

[34] Nandani Tambi1 , Milan Soni2 , Meemansa Tailor3 , Jai Jethanandani4 , Mr. Yadvendra Bedi. Identifying the Vulnerabilities in WIFI Network, Computer and Mobile Devices using WIFI Deauther, USB Rubber Ducky, Backdoor APK. International Journal of Global Research in Science & Technology ISSN: 2455-3832, Volume No.-7, Issue No-1, Jan-Dec 2021.

[35] Anil Lamba1 , Satinderjeet Singh2 , Natasha Dutta3 , Sivakumar Sai Rela Muni4 Department of Computer Science, Charisma University, Turks and Caicos Islands. IDENTIFYING & MITIGATING CYBER SECURITY THREATS IN VEHICULAR TECHNOLOGIES. International Journal for Technological Research In Engineering Volume 3, Issue 7, March-2016.

[36] Lee, H., Home IoT resistance: Extended privacy and vulnerability perspective, Telematics and Informatics (2020), doi: https://doi.org/10.1016/j.tele.2020.101377

[37] K. Lova Raju1*, Member, IEEE, V. Chandrani1 , SK. Shahina Begum1 , M. Pravallika Devi1 , 1 Vignan's Foundation for Science, Technology & Research, Guntur, Andhra Pradesh, India. Home Automation and Security System with Node MCU using Internet of Things. 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN).

[38] S. Lee, S. Kim, K. Choi, T. Shon, Game theory-based Security Vulnerability Quantification for Social Internet of Things, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.09.032.

[39] Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing · March 2017.

[40] Sina Sontowski∗ , Maanak Gupta† , Sai Sree Laya Chukkapalli‡ , Mahmoud Abdelsalam§ , Sudip Mittal¶ , Anupam Joshik , Ravi Sandhu. Cyber Attacks on Smart Farming Infrastructure.

[41] Bako Ali 1 ID and Ali Ismail Awad. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes (2018).

[42] Tejasvi Alladi, Vinay Chamola, Biplab Sikdar and Kim-Kwang Raymond Choo. Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine · October 2019 DOI: 10.1109/MCE.2019.2953740.

[43] Xingbin Jiang, Michele Lora, and Sudipta Chattopadhyay. 2020. An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. ACM Trans. Internet Technol. 20, 2, Article 16 (May 2020), 24 pages. https://doi.org/10.1145/3379542.

[44] Athira Sankar1 Lakshmi S. A Survey On Improving Home Automation Security by Integrating Device Fingerprinting Into Smart Home. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 04 | Apr -2017.

[45] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li∗ , and Hongbin Zhao. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal · April 2017.

[46] Jie Lin∗ , Wei Yu† , Nan Zhang‡ , Xinyu Yang∗ , Hanlin Zhang§ , and Wei Zhao. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications.

[47] A. Jacobsson, M. Boldt, B. Carlsson, A risk analysis of a smart home automation system, Future Generation Computer Systems (2015), http://dx.doi.org/10.1016/j.future.2015.09.003

PLAGIARISM REPORT

Turnitin Originality Report

Processed on: 25-Jan-2022 10:21 +06
ID: 1747613106
Word Count: 6950
Submitted: 1

181-35-2472 By Abidullah Afif

Similarity Index	Similarity by Source	
17%	Internet Sources:	17%
	Publications:	3%
	Student Papers:	9%

8% match (Internet from 09-Jan-2022)
https://systemzone.net/what-are-the-7-layers-of-osi-model-and-how-do-they-work/

5% match (Internet from 15-Jan-2022)
https://github.com/OWASP/www-project-top-ten/blob/master/index.md

1% match (student papers from 07-Apr-2018)
Class: Article 2018
Assignment: Journal Article
Paper ID: 942529588

1% match (Internet from 23-Jul-2021)
https://www.ijert.org/different-security-issues-of-internet-of-things-iot

1% match (student papers from 15-May-2018)
Submitted to Victoria University on 2018-05-15

< 1% match (Internet from 12-Aug-2021)
https://mdubravski.medium.com/

< 1% match (student papers from 28-Nov-2021)
Submitted to University of Hertfordshire on 2021-11-28

< 1% match (student papers from 13-May-2021)
Submitted to University of Teesside on 2021-05-13

< 1% match (publications)
Antonio Mangino, Morteza Safaei Pour, Elias Bou-Harb. "Internet-scale Insecurity of Consumer Internet of Things", ACM Transactions on Management Information Systems, 2020

< 1% match (publications)
Haneen Al-Alami, Ali Hadi, Hussein Al-Bahadili. "Vulnerability scanning of IoT devices in Jordan using Shodan", 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS), 2017

< 1% match (Internet from 03-Jan-2022)
https://ideas.repec.org/a/eee/enepol/v144y2020ics0301421520303669.html

< 1% match (Internet from 04-Jan-2022)
https://muras.eu/assets/img/OWASP_top_10_2021.pdf

< 1% match (Internet from 02-Sep-2021)
https://repositorio.uniandes.edu.co/bitstream/handle/1992/41225/u830940.pdf

< 1% match (Internet from 14-Nov-2021)
https://www.huntress.com/defenders-handbook/persistence-in-cybersecurity?utm_=

< 1% match (Internet from 09-Sep-2021)
https://www.ijrte.org/wp-content/uploads/Souvenir_Volume-8%20Issue-3_September_2019.pdf

< 1% match (Internet from 10-Sep-2021)
https://www.researchgate.net/publication/318223878_5G_Security_Analysis_of_Threats_and_Solutions

< 1% match (Internet from 05-Jan-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5693/171-35-1870%20%2824_%29.pdf?isAllowed=y&sequence=1

CHAPTER 1 INTRODUCTION 1.1 Background The rising usage of high-speed internet and automated computing has made our lives easier. We are now implementing internet of things in all possible sectors, weather forecast, industrial manufacturing robots, smart home sensors, automated vehicles, smart devices such as AC, Fridge, Interior Lights, all are now part of the IoT hub. As these smart devices can transmit data and communicate to each other, the data needs to be transmitted in a secure manner. As the triangle of Functionality, Usability & Security suggest, more features can lead to more cyberthreats. 1.2 Motivation of the Research There are several reports on zero-day vulnerabilities about many new consumer based IoT devices. Hackers are now more aggressive and have better attacking frameworks to break through and compromise a vulnerable network and software systems. There have been recorded reports on hacking smart vehicles, controlling smart vehicles, bypassing smart locks, hacking medical IoT infrastructure all of these incidents are not very obsolete. We are still facing new challenges and trying to spread more awareness about these trending cyberthreats. 1.3 Problem Statement The IoT industry is not a mature industry yet. Several researches have already shown there are so many security flaws in this sector and as the demands for IoT devices grows, the risk factor grows with the flow. There is not enough contribution in this field, especially overall review of the IoT Node MCU sensor enable device security systems. ©Daffodil International University 1.4 Research Questions Question 1: What are the common vulnerabilities according to the OWASP top 10 model? Question 2: How can security systems be implemented in the OSI layers? Question 3: How can we mitigate the privacy and data theft risks of IoT and Smart devices? Question 4: How vulnerable is the Node MCU sensor network & How to secure them? 1.5 Research Objectives ● Finding the top 10 common vulnerabilities & attacks in IoT devices. ● Securing physical layer, network layer & application layer in IoT devices. ● Consumer based IoT products privacy protection policy & risk analysis. ● Node MCU home network security analysis & possible solutions. 1.6 Research Scope This research will cover the summary of concurrent & relevant threat & vulnerability analysis of IoT networks and smart embedded systems. This research is completed within a period of eight month with limited access to academia lab instruments. The scope of this thesis is to justify common security practices to prevent attack on smart IoT devices. This security field are covered within the analysis part of IoT Vulnerability assessments: ● Wireless sensor security. ● Network security ● Authentication & Authorization of the system administrator. ● Remote executable vulnerabilities. ● Privacy & Other risk factors. 1.7 Thesis Organization This thesis has been conducted in the Daffodil International University Robotics lab. All the IoT related microcontroller & embedded systems are tested inside the lab. As this thesis is a summary & review of other IoT security related thesis and research articles, I had to organize the thesis in a timeline to cover all basic fields related to IoT security analysis. These includes: ● Collecting, reading and understanding IoT related research papers and journals. ● Understanding & getting familiar with the IoT based smart device ecosystem. ● Exploring the vulnerabilities in a Node MCU home IoT network. ● Performing brutforce password dictionary attack to the network. ● Performing Wifi Deauther & Becon attack with ESP8266 arduino module. ● Analyzing the encryption method of data flow between smart devices. Home. ● Finding other

common risk factors & privacy issues related to IoT Based Smart ● Finding common patterns of vulnerabilities from all relevant researchers in this field & giving a conclusion. CHAPTER 2 LITERATURE REVIEW In this paper [01], A review on IoT machine to machine (M2M) mythology, IoT Vision, RFID, Wireless Sensor Network (WSN), IoT security and the architecture of IoT devices are explained with easy to understand figures. The paper [02], reviewed the security of Smart farming technology & Precision Agriculture. Proposed article has in depth statistical report on different types of cyber attacks such as RF Jamming, DoS attack, Botnets, Side Channel Attack, MITM attack, Cloud computing attack, Data Leakage, False Data Injection, Misconfiguration, Software Update attacks, Malware Injection, Buffer overflow, SQL attacks, Data fabrication, Cyber-Terrorism, all classified with specified category (Availability, Confidentiality, Integrity, Non-Repudiation, Trust & Privacy). This paper also explains the 7 stages of cyber-attack according to CKC (Reconnaissance > Weaponization > Delivery > Exploitation > Installation > Command & Control > Action on Objectives.). The CKC-based OSI layer taxonomy on Cyber-threats to SF & PA is also present in this review paper. In the paper [03], privacy & security requirements are analyzed for the emerging IoT devices. The term "Authentication & Key Management" is proposed in this paper. On the other hand Iqbal A. et al, reviewed a paper[04] on cybersecurity. Various types of malicious codes (Worms, Virus, Malware, Trojan Horse) and security threats & their impact is reviewed. Another review paper [05] is about the future of emerging IoT technologies, IoT architecture, IoT challenges & IoT Applications. The potential applications of IoT are found such as Smart Traffic Management, Security & Surveillance, Agriculture Automation, Healthcare & Medicine, Smart Cities & Homes, Supply Chain and Energy consumption. The stability, reliability, law & regulatory rights for these smart ecosystems are also concluded. Joel A. and Malekian R. proposed another review paper [06] of smart home automation security using access control, data security, intrusion detection & the physical infrastructure access control. This research concluded the Homeowners point of view, as well as a security Engineers point of view. The Context-aware home automation systems, Bluetooth based Home Automation System, Central Controller-based Home Automation System , GSM or Mobile-based Home Automation System, GPRS-based Home Automation System, DTMF based Home Automation System & Internet-Based Home Automation System& Security issues of these system are addressed. Zhang W. et al, has in depth review about[07] the top 10 research topic in IoT field in 2019. This paper [08], introduces with the 5G security & threat analysis. Security Challenges of Software defined networking (SDN) and Network Function Virtualization (NFV) n secure communication channels are introduced. Proposed model uses encrypted Host Identity Protocol in the Transport layer. For Radio Access Network (RAN), a cloud based secure solution C-RAN is introduced. The article [09] published by Rocha J. presents the ongoing vulnerability trends in sensor assisted security protection & IoT devices in 2018. A case study [10] of a Smart Home for IoT device vulnerability studies and security postures. Different scenarios of abuse & misuse of the vulnerable smart home are overviewed from National Vulnerability Database (NVD) & the vulnerabilities are classified in a survey table. Another research [11] has proposed a large-scale report on vulnerability scanning of IoT devices in Jordan using Shodan using the Common Vulnerability Scoring system (CVSS). On the other hand Rehman A. [12] proposed a vulnerability model for Hybrid IT systems such as automated supply chain with CVSS framework. This Paper [13] introduced the top vulnerability analysis in IoT devices for smart home Environment by PTES standard penetration testing approach. The industry standard penetration testing tools are used such as Kali Linux, Wireshark, Zenmap, Aircrack NG, Medusa, Ncrack, Hydra, OWASP Zap. The paper [16] is a comparative analysis on Smart Home systems to control, Monitor & Secure Home with wireless network microcontrollers like Zigbee, GSM, PIC, Bluetooth. On the other hand, another paper [17] is all about Arduino based smart homes with a mobile friendly user interface, WIFI based network & Bluetooth based controller which is suitable for smart cities. This paper [18] proposed Smart Home Automation System & Security systems using Arduino microcontroller & Sensor modules such as Flex Sensor, Flame Sensor, Fire Sensor, Relay Driver, LDR & DC Motors. Another paper [19] finds the requirements on Secure & Privacy focused IoT Architecture with compared IoT Protocols such as Azure-IoT, CoAP, DDS, DPWS. This also includes the security of WSN, NFC & RFID technologies as well. Similarly another

paper [20] concludes the security and privacy issues for an IoT based Smart Home with Zigbee module in the European Union. Another paper [21] introduces the IoT ecosystem architecture of Smart city applications such as Smart energy grid & power supply, Intelligent healthcare network, Smart Industry, Intelligent Navigation & Traffic control, the challenges of these interconnected ecosystems & the solution to the challenges. In this paper [22], an In-Hub Security Manager is proposed for securing vulnerable home IoT devices from different kinds of DOS & DDOS attacks. In the forensic part, the paper [23], a Forensic Investigation Framework is proposed for Zigbee & Z-wave based IoT Smart Home Environment. Another paper [24] has proposed RSA & AES encryption systems for the secure integration of IoT Cloud Computing. In the network segment, Ahmed I. et al [25] introduces the challenges & solutions for 5G technology, 5G-PPP, SDN, NFV & Mobile Edge Computing (MEC). The journal paper [26], laser-based Audio-Injection attacks are performed on consumer-based voice-controllable systems such as "Google Home mini", targeted to the MEMS microphones. The sound wavelength is compared with the light wavelength to exploit the target. With a range of 100m, the cyber weaponized laser light 60mW High-Power laser & 5mW Low Power Lasers are used in the attack vector to manipulate user authentication from a voice record. Benjamin K. et al, has published a review paper[27] on the public knowledge about energy sustainability, and vulnerability in the demographics of smart home technology diffusion. On the other hand Xiao L. [28] has proposed Machine Learning techniques on the security of IoT based smart devices such as WSN, RFID, Zigbee to prevent DoS attacks and Network Jamming. On the other hand, Ishan A. et al, published a review paper[29] on Arduino & Raspberry Pi based IoT and Smart Home security analysis. On the other hand Weber R. proposed a paper [30] about the Privacy enhancing policy & Rule making process for the regulations on IoT Smart devices. Another paper [31] designed Arduino & Wireless NodeMCU based Intelligent Smart Home Automation & Security System with extended sensor modules. Jose A. et al published a paper [32] which represents an automated Smart Home Security & Door locking system using logical sensors and predefined algorithms. Relatively, the paper [33] by the same authors proposed the integration of Fingerprint Sensors to improve Smart Home Automation Security. In the vulnerability segment, another paper [34] proposed penetration testing methodology to find vulnerabilities in WIFI Network using WNS WIFI Deauther, USB Rubber Ducky & Backdoor APK. Similarly another paper [35] Concludes the cyber threats and vulnerabilities of Smart Autonomous Vehicular Technologies. Another paper [38] has proposed the Security Vulnerability Qualification for Social IoT Devices based on "Game Theory" mathematical model. Jiang X. [43] performs different types of cyber attacks for an Experimental Analysis on Industrial IoT device vulnerabilities. On the other hand [47] a risk analysis methodology is proposed for threat analysis on Smart Home Automation System A Journal [36] on Home IoT resistance by Lee H. has specified some common vulnerabilities & privacy issues in the IoT environment & Smart devices. In this paper, Lova K. et al proposed [37] a Smart Home ecosystem has been developed for IoT Automation using Arduino based NodeMCU and Other sensors. The smart home system can be remotely controlled by using an Open Source remote control App "Blynk". In the cloud computing sector, [39] has reviewed the security and privacy issues on Fog Computing for the IoT devices. Sontowski et al, [40] has performed a vulnerability analysis and penetration testing on IoT based Smart Farming Technologies & Sensors. Ali B. [41] has evaluated the Cyber & Physical Security Vulnerabilities for IoT based Smart Homes using OCTAVE Risk analysis methodology specified with the OSI layers. Similarly, this paper [42] focuses on the Consumer based IoT Vulnerabilities case studies and their solutions. A survey on security loophole and privacy analysis of IoT Smart systems such as WSN and RFID has been analysed by Borgohain T. [14]. The paper published by Hassan R. [15] is an analogy of future smart cities and a smart ecosystem within the smart cities, opportunities and challenges, architecture, environment and sustainable lifestyle in that IoT based futuristic environment. Another Survey on Improving Home Automation Security for Fingerprint enabled Smart Home Security Systems [44] has conducted on 2017, by Sankar A. et al. The paper [45] is a survey on Security & Privacy issues in Internet of Things on 2017. Another survey-based paper [46] on Architectures, Enabling technologies, Security &Privacy & Applications of Internet of Things. CHAPTER 3 RESEARCH METHODOLOGY 3.1 Introduction to the Secure System Model Related to this Research Technology is getting more complex and

smarter every day. A few decades ago, it was just a hypothetical concept about autonomous smart vehicles & automated smart homes. The rapid development of the high speed internet network and super-efficient semi-conductors has made it possible to merge cutting edge technologies from various fields. As a result of 5G high speed internet, the world will see a rapid growth in the IoT field, most importantly the automatic vehicles such as Tesla Electric cars. These smart embedded systems will make our life more convenient, but there“s a catch. As the benefit grows, the risk factor also grows with it. This industry is very new both for the manufacturer & for the consumers. The ideal security standards are not enough for handling next generation cyber threats. More academic and industry-based research is a necessity for the sustainable development of IoT ecosystems. The lack of compliance on IoT makes it a more vulnerable target to the black hat hackers. There are already reported botnet attacks & DDoS attacks on several IP cameras and Smart vehicles which are a very critical part of the IoT ecosystem. Nowadays, hackers are placing crypto-mining malicious codes in vulnerable IoT devices which have a moderate CPU or GPU unit. Another biggest challenge is the lack of knowledge about smart device security and vulnerability & easily accessible hacking tools. Consumers and the end user cannot know the security & privacy related issues with their owned devices. On the other hand, hackers can easily find the common vulnerabilities from open sources like SHODAN. The consequences of a compromised device can be economically significant & can also be life threatening! It is the duty for cyber security analysts to ensure the highest level of security standards in IoT and Smart devices as well as any connected devices to make a better society. There are new techniques and terms being introduced every year in the cyber world. High level programming languages are easier to maintain and easier to control. As it is a good step for the programming community, the risk factors are higher than previous generations. Many powerful cyber warfare tools are being developed by the high end programming community. Some of the community members have the black hat motive, they choose to hack into other devices and government server systems. We need an active team of white hat hackers and cybersecurity experts to protect cyber infractures against any kind of threats. 3.2 OSI Layers: The Open System Interconnection or OSI-Model represents 7 architectures of a digital device. All these 7 layers work to communicate and transmit data in a collaborative way in all IoT Devices. The layers are expressed in a sequence in figure no.1 Figure 3.1: OSI Layers Layer 1 – Physical Layer The physical layer concerns the part of the model used for transmitting raw data bits (0s and 1s) across the network between sending and receiving devices. This can be through a physical cable or even a wireless connection between physical nodes. The physical layer can also represent voltages, frequencies, pin layouts, and other things. Any other physical devices part of this transmission, like hubs and modems, are also included. Ethernet, USB, Bluetooth, IEEE 802.11 etc. protocols work on Physical Layer. Layer 2 – Data Link Layer The data link layer is in charge of establishing or eliminating a connection between physical nodes that may be connected through a cable or wirelessly. In addition, it also takes care of any data correction for errors that might be made in the physical layer. The data link layer is made up of two sub layers of its own which are: – The media access control (MAC) is responsible for the data transmission and the provision of data flow by defining permissions across the network. – The Logical Link Control (LLC) is responsible for controlling the data flow and identifying errors that occur from flow from physical media. In addition, it also identifies network protocols. PPP, ATM etc. protocols work on Data Link Layer. Layer 3 – Network Layer The network layer“s primary responsibility is receiving packets of data from the data link layer and then moving them ahead. It fulfills this duty by finding the best route of forwarding these packets using the address that has been given to them by the data link layer. In essence, it routes the packets to the destination, and this is where router devices tend to come in handy as the „routing“ of information is taking place. IP, ARP, ICMP, IPsec etc. protocols work on Network Layer. Layer 4 – Transport Layer The transport layer is responsible for data transmission between the transmitting and receiving ends. It does this by initially breaking up the data at the transmission end and then constructing it back at the receiving end. The transport layer also deals with error control and checks if there is any incorrect data sending. If an error has occurred during transmission, it is responsible for requesting it again from the transmission end. An excellent example of the transport layer is the Transmission Control Protocol (TCP). UDP also works on

Transport Layers. Layer 5 – Session Layer The session layer is responsible for creating sessions between computers, i.e., communication channels to transfer data between them. In addition, it is responsible for keeping these channels open during data transmission and ending them when this transfer has been completed. It can also create checkpoints in data transfer to resume the transfer from the last checkpoint in case the session has been interrupted. Examples of Session Layer protocols are NetBIOS, PPTP etc. Layer 6 – Presentation Layer The presentation layer is responsible for the encryption of data between two devices. It informs the devices how it has coded and compressed the data to be decrypted at the receiving end. In this way, it is essentially responsible for preparing the data for the application layer and transmits any data from it back to the session layer if needed. SSL and TLS are the best examples of Presentation Layers. Layer 7 – Application Layer The Application is the layer at the top of the OSI Model and is what users mostly see when they are using end-user software, like their web browser or Microsoft Office. It provides protocols to the software to allow it to send and receive information directly from users and display it to them. Some of these protocols include HTTP, FTP, and DNS. It is important to note that the applications themselves are not present in this layer, but instead, it allows them to communicate to the lower layers for communication with applications on the other side. 3.3 Case Study and Literature Review: There have been several IoT related research papers published in recent years. This thesis is mainly based on reviewing these relevant research papers related to IoT, IoT Hub, Smart Home, Smart City, IoT security & Vulnerability issues, NodeMCU based sensor network & 5G technology network challenges and solutions. The top influential papers & Journals related to IoT security are highlighted in Table 3.1. Table 3.1: Literature Reviews Title Authors Liang Xiao, Xiaoyue IoT Security Techniques Wan, Xiaozhen Lu, Based on Machine Learning. Yanyong Zhang, and Digital Object Identifier Di Wu Result Discussion Machine Learning techniques on the security of IoT based smart devices such as WSN, RFID, Zigbee to prevent DoS attacks and Network Jamming. Security and Privacy in Kuan Zhang, Jianbing IoT ecosystem architecture Smart City Applications: Ni, Kan Yang, of Smart city applications Challenges and Solutions. Xiaohui Liang, Ju such as Smart energy grid & Ren, and Xuemin power supply, Intelligent (Sherman) Shen healthcare network, Smart Industry, Intelligent Navigation & Traffic control, the challenges of these interconnected ecosystems & the solution to the challenges. Light Commands: Laser- Takeshi Sugawara, Audio-Injection attacks are Based Audio Injection Benjamin Cyr, Sara performed on consumer- Attacks on Voice- Rampazzi, Daniel based voice-controllable Controllable Systems. Genkin, and Kevin Fu. systems such as "Google Home mini", targeted to the MEMS microphones. Security and Privacy in Kuan Zhang, Jianbing IoT ecosystem architecture Smart City Applications: Ni, Kan Yang, of Smart city applications Challenges and Solutions. Xiaohui Liang, Ju such as Smart energy grid & Ren, and Xuemin power supply, Intelligent (Sherman) Shen. healthcare network, Smart Industry, Intelligent Navigation & Traffic control, the challenges of these interconnected ecosystems & the solution to the challenges. A Review on Security of Abbas Yazdinejad 1 , Reviewed the security of Smart Farming and Precision Behrouz Zolfaghari 1 , Smart farming technology Agriculture: Security Amin Azmoodeh 1 , & Precision Agriculture. Aspects, Attacks, Threats Ali Dehghantanha 1,*, Proposed article has in and Countermeasures. Hadis Karimipour 2 , depth statistical report on Evan Fraser 3 , Arthur different types of cyber G. Green 3 , Conor attacks such as RF Russell 3 and Emily Jamming, DoS attack, Duncan Botnets, Side Channel Attack, MITM attack, Cloud computing attack, Data Leakage, False Data Injection, Misconfiguration, Software Update attacks, Malware Injection, Buffer overflow, SQL attacks, Data fabrication, Cyber- Terrorism, all classified with specified category (Availability, Confidentiality, Integrity, Non-Repudiation, Trust & Privacy). Security and Privacy Issues Aqeel-ur-Rehman1 , Requirement Analysis for in IoT. International Journal Sadiq Ur Rehman2 , Secure & Privacy focused of Communication Networks Iqbal Uddin Khan, IoT Architecture with and Information Security Muzaffar Moiz and compared IoT Protocols (IJCNIS). Sarmad Hasan. such as Azure-IoT, CoAP, DDS, DPWS. This also includes the security of WSN, NFC & RFID technologies as well. 3.4 Significance of vulnerabilities The significance of IoT vulnerability can be huge in terms of scale. As IoT devices will be crowded in the medical industry, autonomous vehicle industry, Home Security industry, Drone & Air transport industry, Power hubs, Supply chain & manufacturing industry, a hacker

group can take control of critical infrastructure. This can be economically significant as well as life threatening if it comes to the vehicle & medical industry. All the IoT components generate and transmit massive collections of data to the cloud server, so we have to consider the risk of private data leakage also in order to use these devices in our daily life. . 3.4.1 OWASP Top 10 - Vulnerability Types & Impact Open Web Application security project or OWASP top 10 is an open community to identify the top 10 vulnerabilities in web app technologies. These top 10 vulnerabilities are collected from the official website of OWASP.ORG in 2021. A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category. A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was a broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise. A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition. A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures. A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it"s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category. A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores. A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping. A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category. A09:2021-Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn"t well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics. A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it"s not illustrated in the data at this time. 3.4.2 Lab Experiments A Smart Home automation system based on Arduino & ESP Node MCU has been developed as the following architecture: Figure 3.2: Smart Home Architecture The raspberry pi acted as the central hub or Cloud server for the smart home environment. The sensors are connected with the ESP 8266 NodeMCU. Figure 3.3: ESP Camera Module There have been several sensor and relay actuators for automatic smart home doors. The ESP 8266 Module has been flashed with a custom BIOS for targeting the Smart home IoT network. Wi-Fi Deauther works with 100% accuracy within the range of the network. Figure 3.4: Interface of ESP8266 3.4.3 Risk Assessment The risk assessment of the IoT environment is performed on the analogy of all the literatures relevant to this IoT Security segment. Table 3.2: Risk Assessment Risk Risk Name ID Risk Impact Risk Type Likelihoo d Security Attribute

Compromise d 01 Weak Password Critical Vulnerabilit y High Authentication 02 Weak Encryption Critical Vulnerabilit y low Integrity, Privacy, Authentication 03 Misconfiguration High Vulnerabilit y Very High Authorization, Access control 04 Network Jamming High Physical Security High Availability & Reliability 05 Network Spoofing High Vulnerabilit y High Access control, Spyware 06 Malicious Code Critical Injection Vulnerabilit y High Integrity, Non- Reputation, Access Control 07 Improper session High management Vulnerabilit y Low Access control, Privacy 08 Backdoors Critical Vulnerabilit y Low Access Control, Authentication 09 DoS Attack Medium 10 Remote Access Critical Vulnerabilit y Vulnerabilit y Moderate Availability Moderate Authorization, Access Control 3.4.4 Privacy Impact As the data is transmitted through the secure communication from the Sensor elements to the central hub, there are some risk factors of Man in the Middle Attack. There are possibilities of password and other sensitive information leakage when communicating with the IoT network. There are some consumer based IoT devices which collect the user data without the concern of the end user. The European Union has taken steps in the law and regulations of the IoT Device policies. The end user must get a clear message about what kind of data will be collected and stored from an IoT device. CHAPTER 4 RESULTS AND DISCUSSION This thesis is a review paper on IoT and Smart Device Security and Privacy Analysis, based on collected resources and Research papers. The objective of the lab performance was to develop and build a Smart Home environment with IoT based Node Microcontroller Units. A scenario is created where a black hat hacker deauthorizes the IoT network and works as a jammer. The result has been discovered to verify other sources of security assessment and risk analysis from the IoT network. The central hub is easily vulnerable without any secure architecture of the entire ecosystem of the IoT Network. The lab performance has been conducted with the Raspberry Pi 4 model as the central hub with ESP8266 as the WiFi Node module. All IoT devices have the OSI 7 layers, which are individual targets of a pre-planned cyber-attack. The OWASP top 10 web app vulnerability is partially related to the segment of IoT & Embedded systems. Thus, IoT Smart Home devices aren“t at a mature stage, the risk factors are yet to consider. More real-life scenarios and case studies are needed to support the IoT security community. Proper infrastructure & lab facilities are an essential part of the VAPT tests. The test report may vary from device to device and attacking method. Due to a strict schedule for the publication of this thesis, several penetration testing methods were proposed but couldn“t get to a result conclusion. Common vulnerabilities such as Dictionary attack brutforce, WIFI Deauther, Network spoofing have been conducted with a successful attempt. A firewall and & Wifi jammer detector can help to prevent such incidents. There are different kinds of scenarios for a cyber attack including pre-attack phase and post attack phase. The pre attack phase includes the planning, vulnerability findings, target setting, exploit delivering and access gaining. Lack of cybersecurity knowledge is one of the most common issues in the cybersecurity issue. Even the IoT smart devices are connected with the internet through a protocol, the security threats are more similar to a vulnerable website or a vulnerable server system. Common vulnerabilities are Misconfiguration, Low level Encryption, Open ports and command shells, Authentication loopholes, Weak password, Lack of cybersecurity risk assessment, Lack of Vulnerability Analysis and Penetration Testing, Programming bugs, Open Wifi ports, Insecure design and programming. The way to mitigate these challenges is to allow white hat ethical hackers and penetration testers to check security issues and apply patch updates on a regular basis. Spreading awareness will always create an impact in the cyberworld. CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 5.1 Findings and Contributions IoT devices are still not saturated in our daily life but soon it will transform our life. With the famous saying of “With big power comes big responsibility”, we have to focus on both the good and bad side. IoT smart devices can lead to exposure of our private data and cyber criminals might get more control over our life with vulnerable IoT devices. Most of the IoT Ecosystems are connected through Wireless Sensor Network (WSN), Zigbee, Bluetooth & NODE MCU like Arduino & Raspberry Pi. These are open source community products which have not been properly tested for real life hazardous & emergency scenarios. Cyber Intruders might take advantage of these electronic devices as these all will be connected through an internet network. There should be strong regulation and privacy enhanced policy to all IoT related manufacturing in the term of collecting user data. End to end encryption shouldn“t be tested and verified

before mass production of these smart devices. Spreading awareness about cyber risk and privacy issues will play the most significant part in order to ensure secure usages of IoT & Smart Devices. 5.2 Recommendations for Future Works There are lots of micro fields in the IoT macro field. From the OSI 7 layers, we can implement more secure communication architecture in all 7 layers of a Smart IoT device. An Arduino based small IoT smart city ecosystem can be developed for the vulnerability analysis & penetration testing of these user end IoT Devices. REFERENCES [01] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal. A Review on the Internet of Things (IoT). International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015 [02] Abbas Yazdinejad 1 , Behrouz Zolfaghari 1 , Amin Azmoodeh 1 , Ali Dehghantanha 1,*, Hadis Karimipour 2 , Evan Fraser 3 , Arthur G. Green 3 , Conor Russell 3 and Emily Duncan(2021). A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. [03] Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi University of Louisiana at Lafayette (2016). A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches. [04] Saloni Khurana Department of Electronics & Communication Vivekananda Institute of Technology. A Review Paper on Cyber Security. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org VIMPACT - 2017 Conference Proceedings. [05] Sachin Kumar1* , Prayag Tiwari2 and Mikhail Zymbler. Internet of Things is a revolutionary approach for future technology enhancement: a review. Kumar et al. J Big Data (2019) 6:111 https://doi.org/10.1186/s40537-019-0268-2 [06] Arun Cyril Jose1 and Reza Malekian2. Smart Home Automation Security: A Literature Review. Smart Computing Review, vol. 5, no. 4, August 2015. [07] Wei Emma Zhang1 , Quan Z. Sheng2 , Adnan Mahmood2 , Dai Hoang Tran2 , Munazza Zaib2 , Salma Abdalla Hamad2 , Abdulwahab Aljubairy2 , Ahoud Abdulrahmn F. Alhazmi2 , Subhash Sagar2 , and Congbo Ma1. The 10 Research Topics in the Internet of Things. arXiv:2012.01594v1 [cs.DC] 2 Dec 2020. [08] Ijaz Ahmad∗ , Tanesh Kumar† , Madhusanka Liyanage‡ , Jude Okwuibe§ , Mika Ylianttila¶ , Andrei Gurtovk. 5G Security: Analysis of Threats and Solutions. 2017 IEEE Conference on Standards for Communications and Networking (CSCN). [09] Junia da Rocha Valente, PhD The University of Texas at Dallas, 2018. VULNERABILITY TRENDS IN IOT DEVICES AND NEW SENSOR-ASSISTED SECURITY PROTECTIONS. [10] Brittany D. Davis, Janelle C. Mason, and Mohd Anwar. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. Citation information: DOI 10.1109/JIOT.2020.2983983, IEEE Internet of Things Journal IoT-8794-2019 [11] Haneen Al-Alami, Ali Hadi, Hussein Al-Bahadili. Vulnerability Scanning of IoT Devices in Jordan Using Shodan. Conference Paper · December 2017 DOI: 10.1109/IT-DREPS.2017.8277814 [12] Attiq Ur-Rehman, Iqbal Gondal, Joarder Kamruzzuman, Alireza Jolfaei. Vulnerability Modelling for Hybrid IT Systems. 2019 IEEE International Conference on Industrial Technology, ICIT 2019; Melbourne, Australia; 13th-15th February 2019 Vol. 2019-February, p. 1135-1142. [13] Lu´ıs Costa1 Joao Paulo Barros ˜ 1,2 and Miguel Tavares1,2,3. Vulnerabilities in IoT Devices for Smart Home Environment (2020). DOI: 10.5220/0007583306150622 In Proceedings of the 5th International Conference on Information Systems Security and Privacy. [14] Tuhin Borgohain, Department of Instrumentation Engineering, Assam Engineering College, Uday Kumar Delivery Manager, Tech Mahindra Limited, Sugata Sanyal Corporate Technology Office, Tata Consultancy Services, Mumbai, India. Survey of Security and Privacy Issues of Internet of Things. [15] Rondik J. Hassan1* , Subhi R. M. Zeebaree1 , Siddeeq Y. Ameen1 , Shakir Fattah Kak1 , Mohammed A. M. Sadeeq1 , Zainab Salih Ageed2 , Adel AL-Zebari1 and Azar Abid Salih1 (2021). State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions. Asian Journal of Research in Computer Science 8(3): 32-48, 2021; Article no.AJRCOS.68484 ISSN: 2581-8260 [16] Vishakha D. Vaidya, Pinki 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. [17] Tanweer Alam. Abdulrahman A. Salem. Ahmad O. Alsharif. Abdulaziz M. Alhujaili. " Smart Home Automation Towards the Development of Smart Cities.", Computer Science and Information Technologies. Vol 1(1). 2020. DOI: 10.11591/csit.v1i1.p17-25. [18] Smart Home Automation and Security System using Arduino and IOT Siddharth Wadhwani1, Uday Singh2, Prakarsh Singh3, Shraddha Dwivedi4 1234 Student, Dept. o EC, IMS Engineering College, Ghaziabad, UP, INDIA.

[19] Aqeel-ur-Rehman1 , Sadiq Ur Rehman2 , Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan. Security and Privacy Issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS) Vol. x, No. x, November 2016. [20] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino. Security and Privacy Issues for an IoT based Smart Home. MIPRO 2017, May 22- 26, 2017, Opatija, Croatia. [21] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen. Security and Privacy in Smart City Applications: Challenges and Solutions. 0163- 6804/17/$25.00 © 2017 IEEE IEEE Communications Magazine, January 2017. Digital Object Identifier: 10.1109/MCOM.2017.1600267CM. [22] Anna Kornfeld Simpson, Shwetak N. Patel, Franziska Roesner, Tadayoshi Kohno. Securing Vulnerable Home IoT Devices with an In-Hub Security Manager. IEEE PerCom 2017. [23] Arnoud Goudbeek, Kim-Kwang Raymond Choo, Nhien-An Le-Khac. A Forensic Investigation Framework for Smart Home Environment. 2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering. [24] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and Cloud Computing, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.11.031. [25] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, March 2018. [26] Takeshi Sugawara, The University of Electro-Communications; Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu, University of Michigan. Light Commands: Laser- Based Audio Injection Attacks on Voice-Controllable Systems. August 12–14, 2020 978-1- 939133-17-5 Open access to the Proceedings of the 29th USENIX Security Symposium is sponsored by USENIX. [27] Benjamin K. Sovacool, Mari Martiskainen , Knowledge, energy sustainability, and vulnerability in the demographics of smart home technology diffusion. Dylan D. Furszyfer Del Rio. https://doi.org/10.1016/j.enpol.2021.112196 Received 4 April 2020; Received in revised form 2 February 2021; Accepted 4 February 2021. [28] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. IoT Security Techniques Based on Machine Learning. Digital Object Identifier 10.1109/MSP.2018.2825478 Date of publication: 28 August 2018. [29] Abdulrahman Ihsan Abdulla1 , Ahmad Sinali Abdulraheem2 , Azar Abid Salih3 , Mohammed A. M. Sadeeq4 , Abdulraheem Jamel Ahmed5 , Barwar M. Ferzor, Sardar6 , Omar Salih7 , Sarkaft Ibrahim Mohammed. Internet of Things and Smart Home Security. ISSN: 04532198 Volume 62, Issue 05, June, 2020. [30] Rolf H. Weber. Computer law & security review 31 (2015). Internet of things: Privacy issues revisited. http://dx.doi.org/10.1016/j.clsr.2015.07.002 0267-3649/© 2015. [31] J.Chandramohan1 , R.Nagarajan2 , K.Satheeshkumar3 , N.Ajithkumar4 , P.A.Gopinath5 , S.Ranjithkumar6. Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi J. International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 3 March 2017, Page No. 20694-20698 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.53 [32] Improving Smart Home Security; Integrating Logical Sensing into Smart Home. Arun Cyril Jose, Reza Malekian, Senior Member, IEEE. [33] ARUN CYRIL JOSE1 , REZA MALEKIAN1 , (MEMBER, IEEE), AND NING YE2,3 . Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home. Digital Object Identifier 10.1109/ACCESS.2016.2606478. [34] Nandani Tambi1 , Milan Soni2 , Meemansa Tailor3 , Jai Jethanandani4 , Mr. Yadvendra Bedi. Identifying the Vulnerabilities in WIFI Network, Computer and Mobile Devices using WIFI Deauther, USB Rubber Ducky, Backdoor APK. International Journal of Global Research in Science & Technology ISSN: 2455-3832, Volume No.-7, Issue No-1, Jan-Dec 2021. [35] Anil Lamba1 , Satinderjeet Singh2 , Natasha Dutta3 , Sivakumar Sai Rela Muni4 Department of Computer Science, Charisma University, Turks and Caicos Islands. IDENTIFYING & MITIGATING CYBER SECURITY THREATS IN VEHICULAR TECHNOLOGIES. International Journal for Technological Research In Engineering Volume 3, Issue 7, March-2016. [36] Lee, H., Home IoT resistance: Extended privacy and vulnerability perspective, Telematics and Informatics (2020), doi: https://doi.org/10.1016/j.tele.2020.101377 [37] K. Lova Raju1*, Member, IEEE, V. Chandrani1 , SK. Shahina Begum1 , M. Pravallika Devi1 , 1 Vignan“s Foundation for Science, Technology & Research, Guntur, Andhra Pradesh, India. Home Automation and Security System with Node MCU using Internet of Things. 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking

(ViTECoN). [38] S. Lee, S. Kim, K. Choi, T. Shon, Game theory-based Security Vulnerability Quantification for Social Internet of Things, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.09.032. [39] Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing · March 2017. [40] Sina Sontowski∗ , Maanak Gupta† , Sai Sree Laya Chukkapalli‡ , Mahmoud Abdelsalam§ , Sudip Mittal¶ , Anupam Joshik , Ravi Sandhu. Cyber Attacks on Smart Farming Infrastructure. [41] Bako Ali 1 ID and Ali Ismail Awad. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes (2018). [42] Tejasvi Alladi, Vinay Chamola, Biplab Sikdar and Kim-Kwang Raymond Choo. Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine · October 2019 DOI: 10.1109/MCE.2019.2953740. [43] Xingbin Jiang, Michele Lora, and Sudipta Chattopadhyay. 2020. An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. ACM Trans. Internet Technol. 20, 2, Article 16 (May 2020), 24 pages. https://doi.org/10.1145/3379542. [44] Athira Sankar1 Lakshmi S. A Survey On Improving Home Automation Security by Integrating Device Fingerprinting Into Smart Home. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 04 | Apr -2017. [45] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li∗ , and Hongbin Zhao. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal · April 2017. [46] Jie Lin∗ , Wei Yu† , Nan Zhang‡ , Xinyu Yang∗ , Hanlin Zhang§ , and Wei Zhao. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. [47] A. Jacobsson, M. Boldt, B. Carlsson, A risk analysis of a smart home automation system, Future Generation Computer Systems (2015), http://dx.doi.org/10.1016/j.future.2015.09.003 1 2 ©Daffodil International University 3 ©Daffodil International University 4 ©Daffodil International University 5 ©Daffodil International University 6 ©Daffodil International University 7 ©Daffodil International University 8 ©Daffodil International University 9 ©Daffodil International University 10 ©Daffodil International University 11 ©Daffodil International University 12 ©Daffodil International University 13 ©Daffodil International University 14 ©Daffodil International University 15 ©Daffodil International University 16 ©Daffodil International University 17 ©Daffodil International University 18 ©Daffodil International University 19 ©Daffodil International University 20 ©Daffodil International University 21 ©Daffodil International University 22 ©Daffodil International University 23 ©Daffodil International University 24 ©Daffodil International University 25 ©Daffodil International University