RESEARCH ON SECURITY AND

DATA PROTECTION RISK ANALYSIS AND MITIGATION IN IoT

**A PROJECT REPORT**

###### ***Submitted by***

##### Harsh Kumar (20BCY10015)

**Aayush Kumar** (20BCY10045)

**Shrishti Srivastava** (20BCY10133)

**Avina Jain** (20BCY10135)

*in partial fulfillment for the award of the degree*

*of*

**BACHELOR OF TECHNOLOGY**

*in*

# COMPUTER SCIENCE AND ENGINEERING

****

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRIKALAN, SEHORE**

**MADHYA PRADESH - 466114**

##### DECEMBER 2021

**VIT BHOPAL UNIVERSITY, KOTHRIKALAN, SEHORE**

**MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled “**RESEARCH ON SECURITY AND DATA PROTECTION RISK ANALYSIS AND MITIGATION IN IoT”** is the bonafide work of “**Harsh Kumar(20BCY10015), Aayush Kumar(20BCY10045), Shrishti Srivastava(20BCY10133), Avina Jain(20BCY10135)** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.



**PROGRAM CHAIR PROJECT GUIDE**

Dr. R. Rakesh Dr. Nitish Andola

School of Computer Science and School of Computer Science and

Engineering Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on 06/12/2021

**ACKNOWLEDGEMENT**

First and foremost We would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

We wish to express our heartfelt gratitude to, Head of the Department, School of Aeronautical Science for much of his valuable support encouragement in carrying out this work.

We would like to thank our internal guide Mr. Nitish Andola for continually guiding and actively participating in our project, giving valuable suggestions to complete the project work.

We would like to thank all the technical and teaching staff of the SCHOOL OF COMPUTING SCIENCE AND ENGINEERING who extended directly or indirectly all support.

Last, but not least, We are deeply indebted to our parents who have been the greatest support while we worked day and night for the project to make it a success.

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **Abbreviations** | **Meaning** |
| IoT | Internet of Things |
| EV | Electronic Vehicles |
| NIST | National Institute of Standards and Technology |
| MITM Attack | Man in the middle attack |
| DDOS | Distribute Denial of Service |
| NAS | Network Attached Storage |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| Nmap | Network Mapper |
| SSH | Secure Shell |
| IT | Information technology |
| OT | Operational technology |
| OS | Operating system |
| GDPR | General Data Protection Regulation |
| CDPA | Consumer Data Protection Act |
| IEC | Importer -Exporter Code |
| RJ 45 | Registered Jack-45 |
| CUPS | Common UNIX Printing System |
| SMB | System Server Message Block |
| CIFS | Common Internet File System |

**LIST OF FIGURES AND GRAPHS**

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | **TITLE** | **PAGE NO.** |
| 4.2 a. | Vulnerabilities in CUPS Server | 20 |
| 4.2 b. | Vulnerabilities in Open SSH | 21 |
| 4.2 c. | Vulnerabilities in SAMBA Server | 22 |
| 4.3 a. | Home-Based Router System | 22 |
| 4.3 b. | EV interconnection System | 23 |
| 4.4 a. | Subsystem Services running in Kali | 23 |
| 4.5 a. | CUPS Sever User Interface | 24 |
| 4.5 b. | SAMBA Server User Interface | 24 |
| 5.2 a. | Sample Configuration of SAMBA Server | 26 |
| 5.2 b. | Samba Server Configuration | 26 |
| 5.2 c. | Printer Configuration | 27 |
| 5.3 a. | Working Layout for Home-Based System | 27 |
| 5.3 b. | Working Layout for EV system | 28 |
| 5.4 a. | Printer Hosted on local network | 28 |
| 5.4 b. | Connecting to NAS Server | 29 |
| 5.5 a. | Performance Graph | 30 |
| 6.3.1 a. | Man-in-the-Middle Attack on EV | 33 |
| 6.3.1 b. | Packet Replay Attack on EV | 33 |
| 6.3.1 c. | Address Resolution Protocol Spoofing on EV | 33 |
| 6.3.1 d. | Denial-of-Service Attack on EV | 34 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | **TABLE NO.** | **PAGE NO.** |
| *5.5 1.* | *Computation of Performance* | 29 |

**ABSTRACT**

Based on interoperable communication technologies, IoT technologies are currently enabling advanced services that interconnect physical and virtual things. Most importantly, IoT applications are no longer restricted to small-scale laboratory environments, but are now part of large-scale enterprise deployments. IoT applications are already improving people's lives and making the world a better place to live, according to consumers. The IoT ecosystem is primarily concerned with addressing specific and practical challenges in order to deliver applications that can be integrated into society. When it comes to addressing practical challenges, the cybersecurity aspects of IoT take center stage. When it comes to deploying real-life IoT applications that are ethical, trustworthy, and protect citizens' rights, security, privacy, and data protection cannot be compromised. It does, however, introduce new cybersecurity challenges, such as new methods for conducting large-scale attacks and a plethora of vulnerabilities and risks at various parts of an IoT system, such as smart objects, IoT networks, edge gateways, and cloud elements. Through our work we try to find out the breaches associated with IoT devices and thereby finding solutions to mitigate them. We also analyze the latest emerging technology in India that is Electric Vehicle and its components. We also try to do a project at home using Raspberry Pi, Samba Server, Cups Server to connect a printer to it.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | List of Abbreviations  List of Figures and Graphs  List of Tables  Abstract | iv  v  vi  vii |
| 1 | **CHAPTER-1:**  **PROJECT DESCRIPTION AND OUTLINE** Introduction 1.2 Motivation for the work  1.3 About Introduction to the project  1.4 Problem Statement  1.5 Objective of the work  1.6 Summary | 10  10  11  12  12  12 |
| 2 | **CHAPTER-2:**  **RELATED WORK INVESTIGATION**  2.1 Introduction  2.2 Core area of the project  2.3 Existing Approaches/Methods  2.3.1 NIST Consideration  2.3.2 OCTAVE  2.3.3 TARA  2.3.4 ISO/IEC 27001  2.4 Issues/observations from investigation  2.5 Summary | 13  14  14  14  14  14  14  15  15  15 |
| 3 | **CHAPTER-3:**  **REQUIREMENT ARTIFACTS**  3.1 Introduction  3.2 Hardware and Software requirements  3.3 Specific Project requirements  3.3.1 Data requirement  3.3.2 Performance and security requirement  3.4 Summary | 16  16  16  16  16  17 |
| 4 | **CHAPTER-4:**  **DESIGN METHODOLOGY AND ITS NOVELTY**  4.1 Methodology and goal  4.2 Functional modules design and analysis  4.3 Hardware Architectural designs  4.4 Subsystem services  4.5 User Interface (photos of cups n samba interface) | 17  19  21  21  22 |
| 5 | **CHAPTER-5:**  **TECHNICAL IMPLEMENTATION & ANALYSIS**  5.1Outline  5.2 Technical coding and code solutions  5.3 Working Layout of Forms  5.4 Test and validation  5.5 Performance Analysis (Graphs/Charts)  5.6 Summary | 24  24  26  27  28  29 |
| 6 | **CHAPTER-6:**  **PROJECT OUTCOME AND APPLICABILITY**  6.1Outline  6.2 Key implementations outline of the System  6.3 Significant project outcomes  6.3.1 EV project outcome  6.3.2 Home-Based Router System outcome  6.4 Project applicability on Real-world applications  6.4 Inference | 29  30  30  30  33  35  35 |
| 7 | **CHAPTER-7:**  **CONCLUSIONS AND RECOMMENDATION**  7.1Outline  7.2 Limitation/Constraints of the System  7.3 Future Enhancements  7.4 Inference | 36  36  36  37 |
|  | Appendix A  Appendix B  References |  |

**1. PROJECT DESCRIPTION AND OUTLINE**

**1.1 INTRODUCTION**

The Internet of Things (IoT) is a network of physical objects—"things"—embedded with sensors, software, and other technologies for connecting and exchanging data with other devices and systems via the internet. It's a term that refers to a collection of devices that communicate utilising a variety of technologies and protocols. It is a promising technology that offers major advantages to different sectors such as health, commerce, construction, building management, energy, and transportation by connecting devices of all types over the Internet, whether wired or wirelessly. IoT technologies are currently enabling advanced services that interconnect physical and virtual things based on interoperable communication technologies. IoT devices include wireless sensors, software, actuators, computer devices and more. They are attached to a particular object that operates through the internet, enabling the transfer of data among objects or people automatically without human intervention.

But with these emerging technologies, there is threat to IoT devices. IoT systems have become more vulnerable to security vulnerabilities in the recent decade, including unwanted access to services and network attacks. The secrecy, integrity, and availability of the information were harmed and damaged. It does, however, introduce new cybersecurity challenges, such as new methods for carrying out large-scale attacks, vulnerabilities, and threats in many aspects of an IoT system, such as smart products, IoT networks, edge gateways, and cloud elements.

**1.2 MOTIVATION FOR THE WORK**

In recent years, we have seen the rise of the Internet of Things (IoT) paradigm, which is enabled and propelled by an increasing number of internet-connected devices. One distinguishing feature of these applications is their ability to make intelligent decisions based on large amounts of data collected and processed from the physical world. In some cases, these decisions involve actuation and control activities that affect the physical world and the surrounding environment of IoT systems. However, as new requirements emerge, IoT systems are becoming more vulnerable to various security issues, such as malicious access to services and network attacks. These issues have caused significant harm and have questioned the secrecy, integrity, and availability of information. To overcome the breaches and vulnerabilities associated with IoT, risk assessment is done to understand the flaws which gives rise to the attacks and breaches.

These increasing challenges makes us curious to move deeper with the topic. So we are trying to analyze various challenges associated with IoT devices, how risk assessment is done when any of the attack occurs and some of the mitigation strategies that IoT associated companies should follow to overcome these risks of attacks.

**1.3 INTRODUCTION TO THE PROJECT**

Our project is basically research on **SECURITY AND DATA PROTECTION RISK ANALYSIS AND MITIGATION IN IoT.** In our project or research work, we try to find out various challenges that IoT devices faces, risk assessment methodology, some of the mitigation approaches to overcome the challenges. We also try to analyze latest case studies where IoT devices are compromised which leads to data loss, privacy issues, security issues etc. Electronic Vehicle which is gaining popularity now in India, have many issues with its charging technology. As it is very latest in India, we thereby try to find out challenges with EV charger. Smart home appliances are in demand since long go. In our research we used a home-based router system along with Cups Server, Samba Server, Open SSH to use printer as a home device and to find vulnerabilities and providing more security use NMAP and Hydra Tool.

**1.4 PROBLEM STATEMENT**

The Internet of Things (IoT) is gaining importance and is hailed as the key to widespread connectivity. In this environment, developing and implementing effective techniques to manage IoT security risks is critical to a secure IoT deployment. Cyberattacks on the Internet of Things (IoT) can be the source of great economic damage.

Security and Data Protection are significant challenges in IoT domain. To overcome these challenges, we are trying to analyze various risk assessment methods and their mitigation approaches. Our basic motive is to do risk assessment of threats that took place in IoT devices and thereby implementing our knowledge in home-based router system as well.

**1.5 OBJECTIVE**

The objective or motive of our work is to get in depth knowledge about challenges that IoT devices faces. How risk assessment is done to minimize the outcome of the threats that occurred due to IoT devices. We also researched on many mitigation approaches that should be followed to minimize the risk due to IoT devices. Our objective is to make people aware that the smart appliances they are using today has many in built defects that could lead to data loss, privacy issues and many more. By doing the research we want people to be aware about what they are using and hoe it can benefit or harm their lives.

**1.6 SUMMARY**

Internet of Things (IoT) is a global network of physical and virtual ‘things’ connected to the internet. Authentication, Identification and device heterogeneity are the major security and privacy concerns in IoT. Our study aims to support IoT adopters from any sector to formulate or reframe their IoT security risk management strategies to achieve robust strategies that effectively address IoT security issues. Since by each passing day IoT is gaining importance and had a become a important part of human life it is very important for people to know their drawbacks with their risk assessment strategies.

**2. RELATED WORK INVESTIGATION**

**2.1 INTRODUCTION**

In recent years, the rapid proliferation of internet-connected devices has led to the growth of Internet of Things (IoT) systems and applications. The later are evolving both in terms of the functionalities that they provide to end users and in terms of the technologies that they comprise. Moreover, IoT systems are deployed in scalable edge/cloud computing infrastructures, which include broadband networks, edge gateways, and devices, as well as cloud data centers. The growing sophistication of IoT systems provides the means for developing and deploying new IoT applications, which in turn brings with it significant cybersecurity challenges. There have been a number of recent cybersecurity attacks against Internet of Things (IoT) infrastructures and services. These challenges include-

* The emergence of new large-scale security attacks against IoT systems, such as large-scale distributed denial of service (DDoS) attacks exploit vulnerabilities in specific IoT devices.
* Cyber-physical systems are vulnerable because they are associated with cyber resilience challenges.
* Security threats related to the ways that IT and OT assets interact and the different security requirements of each.
* Compliance with complex regulatory requirements is demanding and volatile in a demanding and volatile landscape, such as the need for compliance to the General Data Protection Regulation (GDPR) in Europe and the Consumer Data Protection Act (CDPA) in California, in the U.S.

IoT’s becoming a necessity in all fields as it becomes more popular over time. People depend on it every day. Through various research papers and articles on the Internet, we researched various mitigation methods, what their approaches are, what previous risks were, and how they could be overcome. What are the strengths of existing mitigation methods and the weaknesses that can be modified to better manage the risks and challenges of the IoT? Then what was the observation of various mitigation techniques and the issues in them.

**2.2 CORE AREA OF THE PROJECT**

Our project basically is a research work where we try to find out the challenges in IoT devices which is very important for the companies as well as for the end users to know what are the challenges faced. It not only helped them to find out solution for these challenges as well as makes them aware about these devices so that their information is not compromised.

In our research we also added about IoT risk, various types of IoT risk, about risk assessment strategies, various frameworks that were already existing for IoT risk assessment. We thereby find out various mitigation approaches to mitigate the IoT risks.

After getting knowledge about all the mentioned topics, we study latest case studies where IoT devices are compromised. These include latest emerging technology i.e. EV charger where its charging technology is not that much secure.

**2.3 EXISTING APPROACHES AND METHODS**

There are various existing approaches for risk assessment of IoT devices that are given by various governmental bodies as well as private companies. Some of these approaches are-

**2.3.1. NIST considerations for IoT**

NIST's Cybersecurity for IoT program has developed and linked norms, rules, and related tools to improve the security of connected devices and the environments in which they operate. NIST suggests several ways to assess IoT compatibility, including: (a) different assessments can be generated based on device type and function, (b) industry can lead to best practices for creating requirements and assessment methods, and (c) assessments can be designed to enable the necessary flexibility To meet market demand, and (d) valuations can be designed to allow flexibility to meet market demand, and the environment. The National Institute of Standards and Technology (NIST) has three aims for Internet of Things risk management: device security, data security, and individual privacy.

**2.3.2. OCTAVE for IoT**

OCTAVE is ideal for assessing the risk of smart homes because it includes an asset container that covers both cyber and physical security. OCTAVE assists in identifying numerous security vulnerabilities in IoT-based smart homes, presenting the dangers to residents, and suggesting mitigation strategies. It consists of 4 steps:

1) Develop risk measurement criteria: It establishes the foundation for risk assessment by developing risk measurement criteria.

2) Profile Asset phase: The asset profile phase creates asset limitations and specifies security requirements.

3) Danger phase: This phase identifies security threats.

4) Risk mitigation phase: A risk mitigation strategy for the identified assets is developed and implemented.

**2.3.3. TARA for IOT**

TARA is a software program that predicts the most important exposures. Tara has three specific advantages. It reduces the chances of attacks. It increases the quality of risk and control evaluations and informs the organization about risks and suggestions. It can improve outcomes, reduce risk analysis work, and assist in making better decisions.

**2.3.4. ISO/IEC 27001**

The international standard 27001 defines and maintains information security risk criteria, assesses risks connected to information security and availability, identifies risk owners, and analyses information security risks based on particular criteria. ISO/IEC 30141 specifies the reference architecture that minimizes risks and maximizes advantages in IoT applications. In addition, ISO/IEC 27030 establishes security and privacy rules for IoT systems for the purpose of ensuring the protection of personal data.

**2.3 ISSUES AND OBSERVATION FROM IVESTIGATION**

When we researched about IoT and its emerging needs the main issue which we observe is that with the growing demand for IoT humans are getting more and more dependent on IoT devices. They are depending on smart devices for their day-to-day work. Smart Robots are the one that is replacing humans and doing their work. These dependence on smart devices is not a good move. By these humans were getting lazy day by day.

With growing the demand of IoT devices, companies are not looking at the security provision of devices which leads to various attacks on IoT devices.

**3. REQUIREMENT ARTIFACTS**

**3.1 INTRODUCTION**

For any project or research work, there is need of various tools, software, and other devices to complete the work. We also require various components to complete our research work. For our home-based router system, we need various components to get the work done.

**3.2 HARDWARE AND SOFTWARE REQUIREMENTS**

For research work, we used various resources for studying about IoT. For our home-based router system, we used various components-

1. a couple of raspberry pi.  
2. External hard disk (for NAS using samba server)  
3. Ubuntu server OS for Raspberry pi.  
4. A four port-based switch for ethernet connection.  
5. RJ-45 cable for connecting the switch with the raspberry pi.  
6. 2 microSD cards for booting up raspberry pi.  
7. An old printer for network-based printing.  
8. Cups server for printing using arm-based devices.  
9. A relay system for controlling light and fan of the room from raspberry pi.  
10. Laptop for controlling.  
11. Android smartphone with Termux.

**3.3 SPECIFIC PROJECT REQUIREMENTS**

**3.3.1. DATA REQUIREMENT**

In our research work, for data we took help of-

1.Google Scholar 2. Previous research papers

3.YouTube 4. Books

5. Metasploit 6. Exploit-DB

**3.3.2. PERFORMANCE AND SECURITY REQUIREMENT**

For providing security to home-based router system, we use 2 tools-

1. NMAP
2. Hydra Tool
3. Nessus

**3.4 SUMMARY**

For work or research to be successfully done, there are various requirements which needs to be fulfilled. It includes data requirements, hardware requirements, software requirements and various tools to carry out various functions. All these components play a very important role in completing various functions.

**4. DESIGN METHODOLOGY AND ITS NOVELTY**

**4.1 METHODOLOY AND GOAL**

Our methodology is first to give a basic idea about what IoT is. After basic understanding of IoT and IoT devices, we then look into various challenges that IoT devices faces including DDoS attacks, MitM attack, ransomware attacks, threats due to third party software, and many more. After throwing a light towards challenges we move towards risk assessment strategies, basic steps of risk assessment process. IoT risk is something which is very important to understand so we then discussed about IoT risks, types of IoT risk. There are many approaches or framework designed to mitigate these IoT risk, some of well - known frameworks were discussed.

After all these topics were discussed, we try to add some of the latest case studies in our paper.

The first case study we go through is EV and its charging technologies. One of the biggest trends in vehicles today are EV, fueled by government regulation and the ‘Green Movement’. The complexity of the interaction between electric vehicles, electric vehicle chargers, charge management, the Internet, phone apps, and the power infrastructure makes developing cyberattacks difficult. A successful attack will almost certainly necessitate a highly sophisticated attack path that exploits many vulnerabilities across multiple components in the charging path. We try to find out various attacks and their mitigation approaches.

The second case study is something different. Here we try to find vulnerabilities by setting up a home-based router system using Raspberry Pi, Cups Server and Samba Server. How they work and what are the various vulnerabilities in the system and finally how we can mitigate these vulnerabilities.

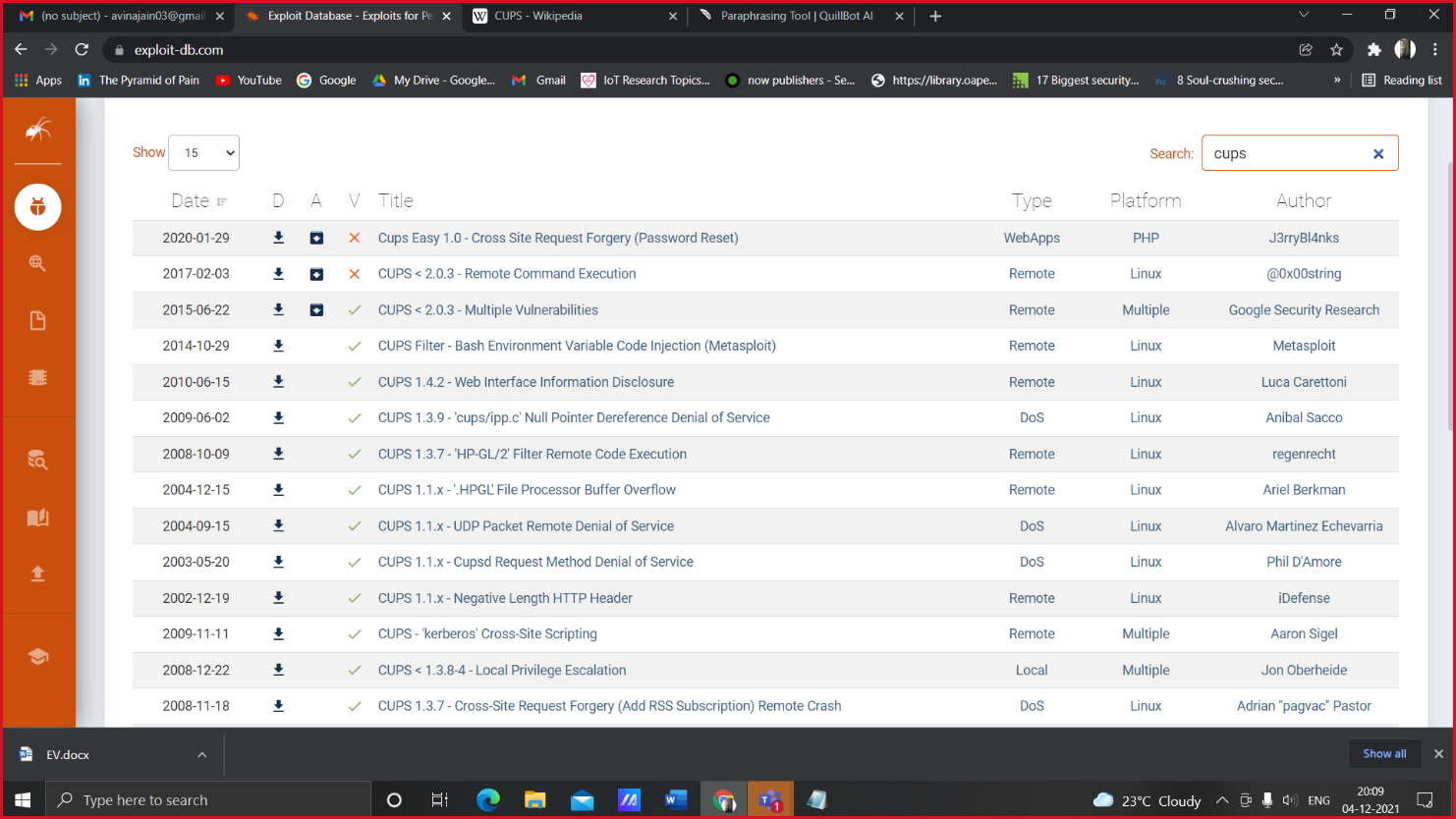
**4.2 FUNCTIONAL MODULE DESIGN AND ANALYSIS**

In our research work, we are trying to find vulnerabilities in home-based router system. For these, we use various modules. They include-

1. CUPS Server - CUPS (previously Common UNIX Printing System) is a Unix-like computer operating system's modular printing system. A CUPS-enabled computer acts as a host, accepting print jobs from clients, processing them, and sending them to the appropriate printer. It also supports the System V and Berkeley print systems' traditional command line interfaces.

**CUPS Sever works on a default port number that is 631**

The possible vulnerabilities are-



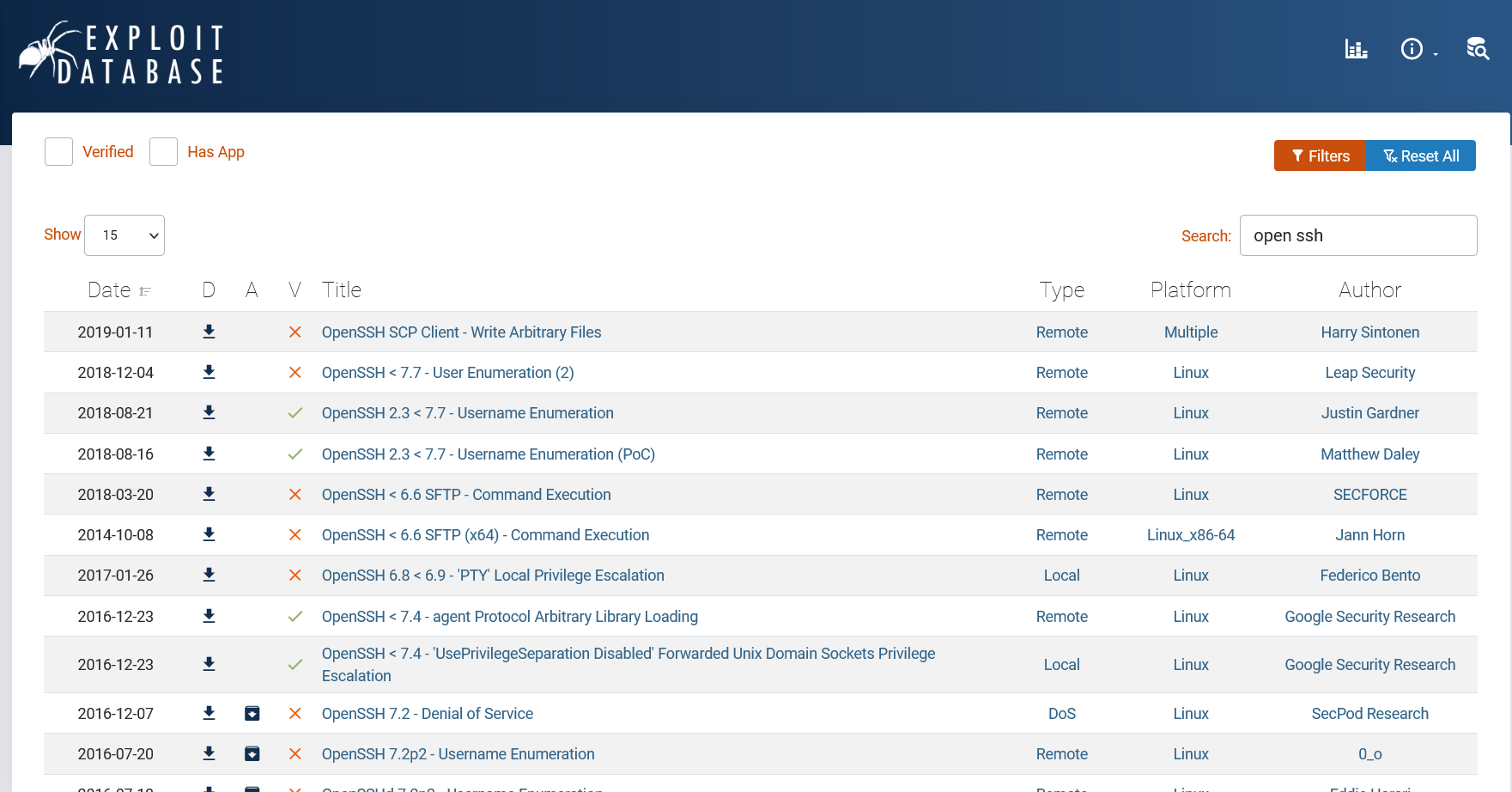
*Fig. 4.2 a. Vulnerabilities in CUPS Server*

Without purchasing a new printer, we are utilizing Cups server to convert our existing printer to a network-based printer. It's used to convert any standard printer to a network printer.

2. Open SSH – OpenSSH is the premier connectivity tool for remote login with the SSH protocol. It prevents unauthorized spying on your computer. In addition, OpenSSH provides a large suite of secure tunneling capabilities, diverse authentication methods, and advanced configuration options. SSH can be used to provide services that provide encrypted access to a variety of operating systems (Windows XP-10, Mac OS X, and Linux). This is not possible if you provide a Windows network drive (using the SMB / CIFS communication protocol). SSH is reliable and secure, and is often used in the high-performance computing community for this reason.

**Open SSH works on a default port number that is 22**

The possible vulnerabilities are-

****

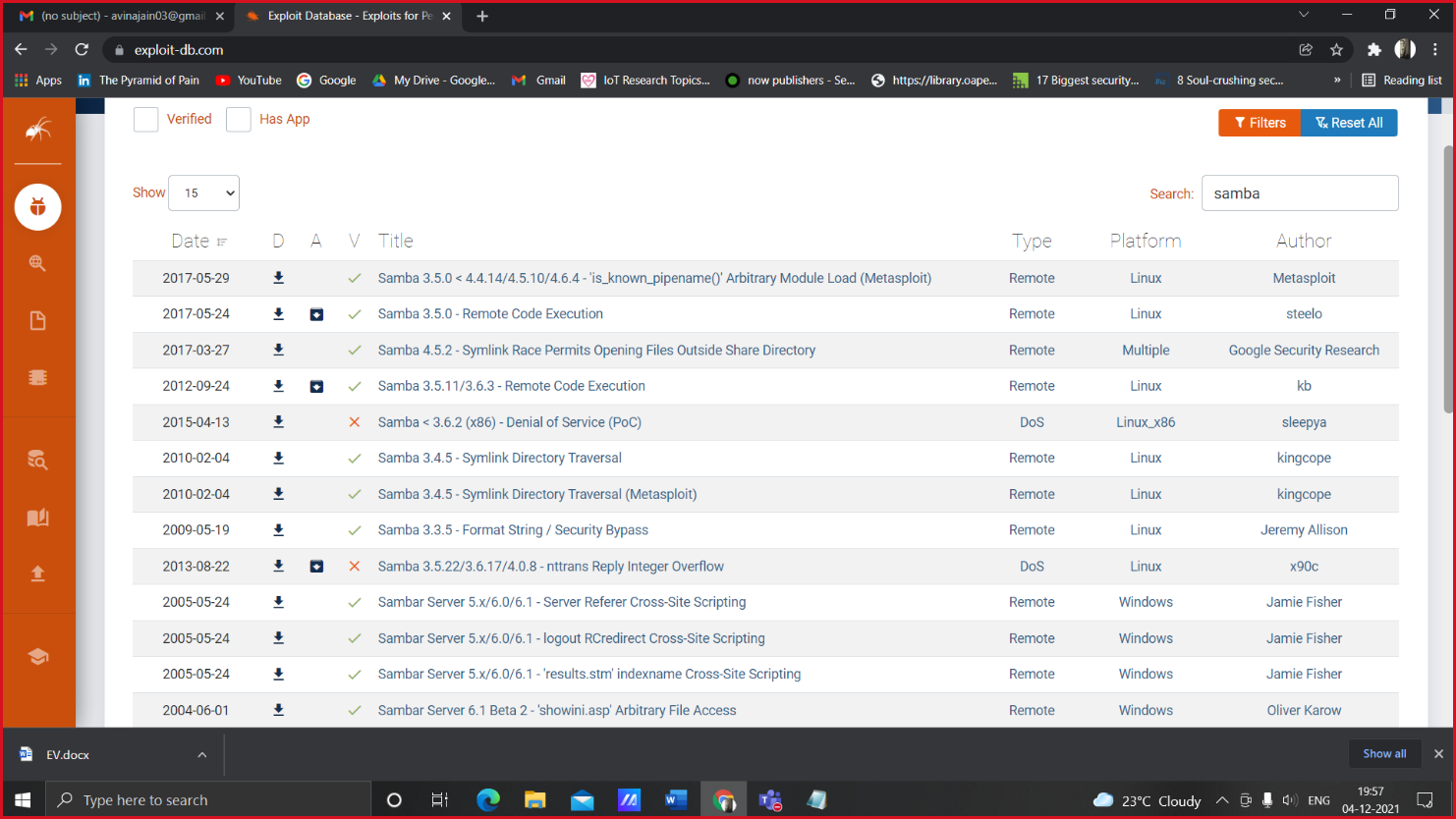
*Fig. 4.2 b. Vulnerabilities in Open SSH*

First and foremost, it supports almost all operating systems available, right from the legacy open based project to the most recent Linux or Windows distribution. This is achieved by various levels of encryption as well as few built-in facilities which block security holes especially in the areas of routing and DNS spoofing. While there are many features available in OpenSSH, let's discuss those which are important from security and operations point of view.

3. SAMBA Server - Samba also offers better performance under heavy loads, outperforming Windows 2000 Server by a factor of 2 to 1 on identical PC hardware, according to published third-party benchmarks. Samba is reliable software that runs on reliable Unix operating systems, resulting in fewer problems and a low cost of maintenance. Samba is an extremely useful networking tool for anyone who has both Windows and Unix systems on his network.

**SAMBA Server works on a default port number that is 445**

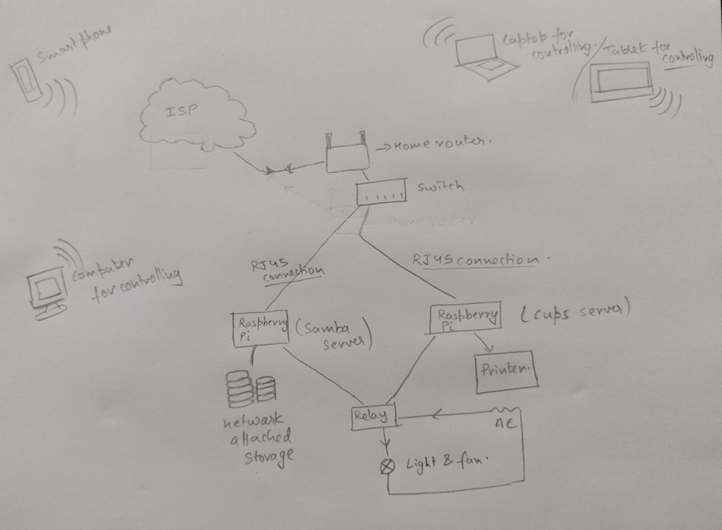
The possible vulnerabilities are-



*Fig. 4.2 c. Vulnerabilities in SAMBA Server*

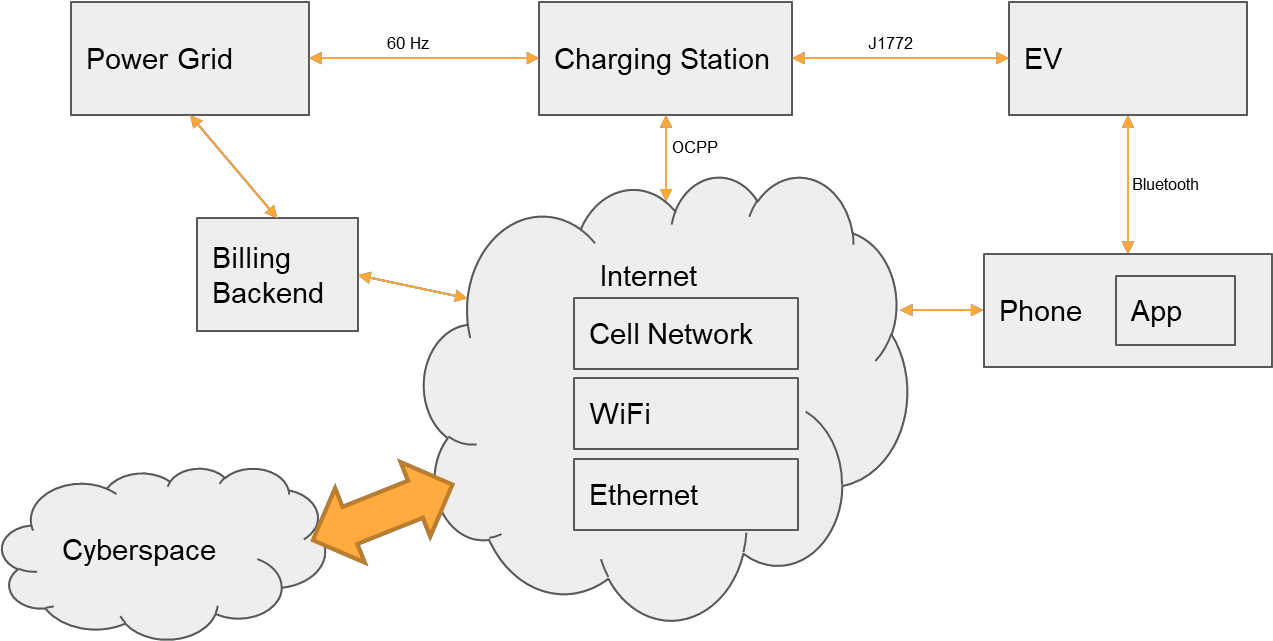
**4.3 HARDWARE ARCHITECTURAL DESIGN**

* For our home-based router system, the overall design for our system is-



*Fig. 4.3 a. Home-Based Router System*

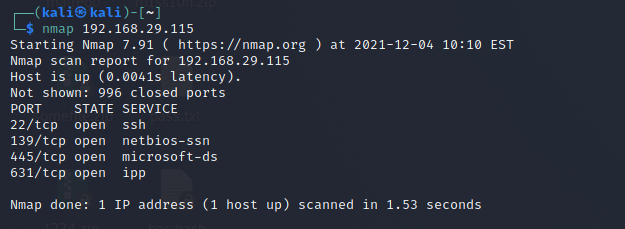
* For EV based system, the overall design for the system is-



*Fig. 4.3 b. EV interconnection System*

**4.4 SUBSYSTEM SERVICES**

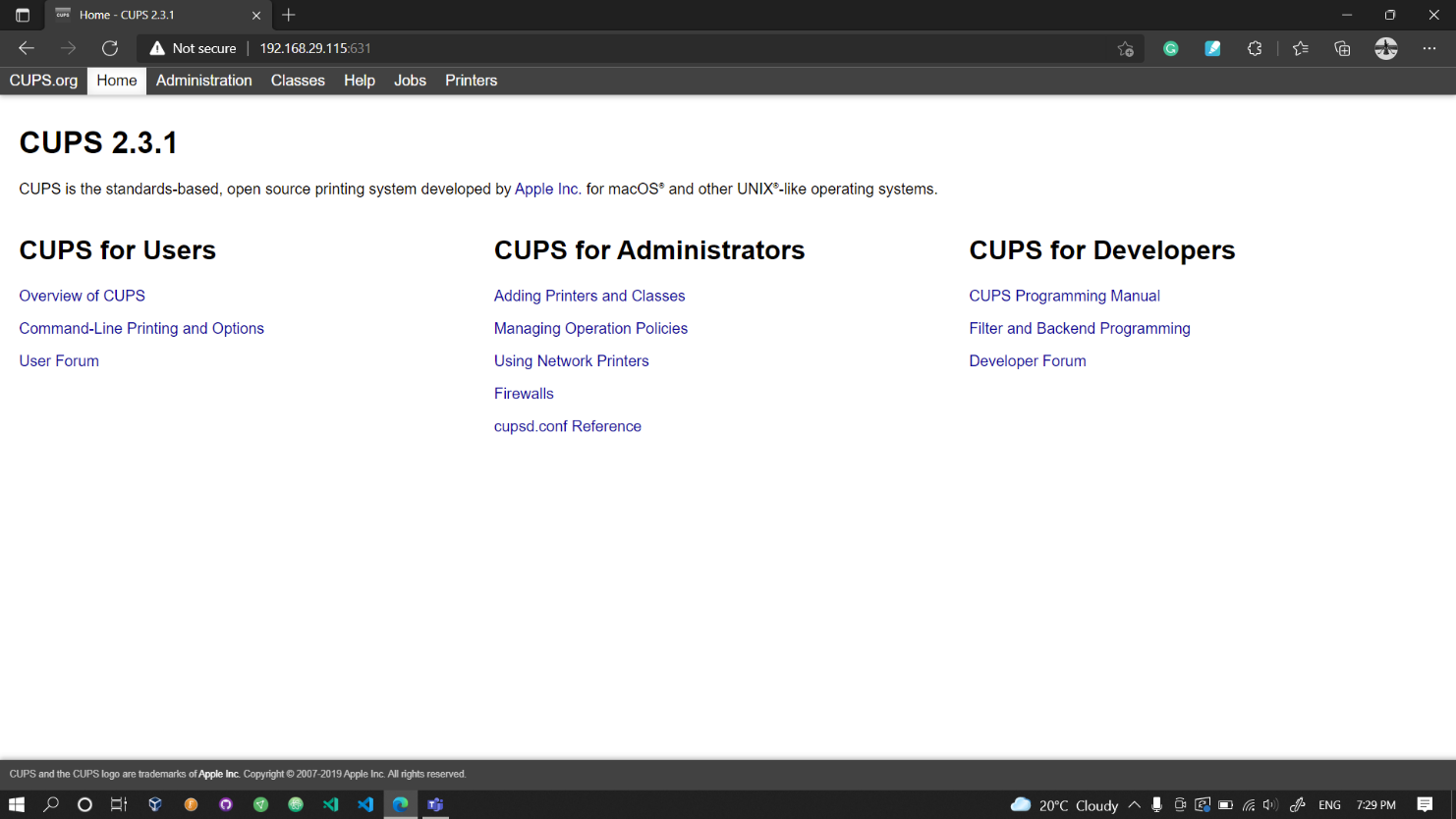
The services which are running in home-based router system-



*Fig. 4.4 a. Subsystem Services running in Kali*

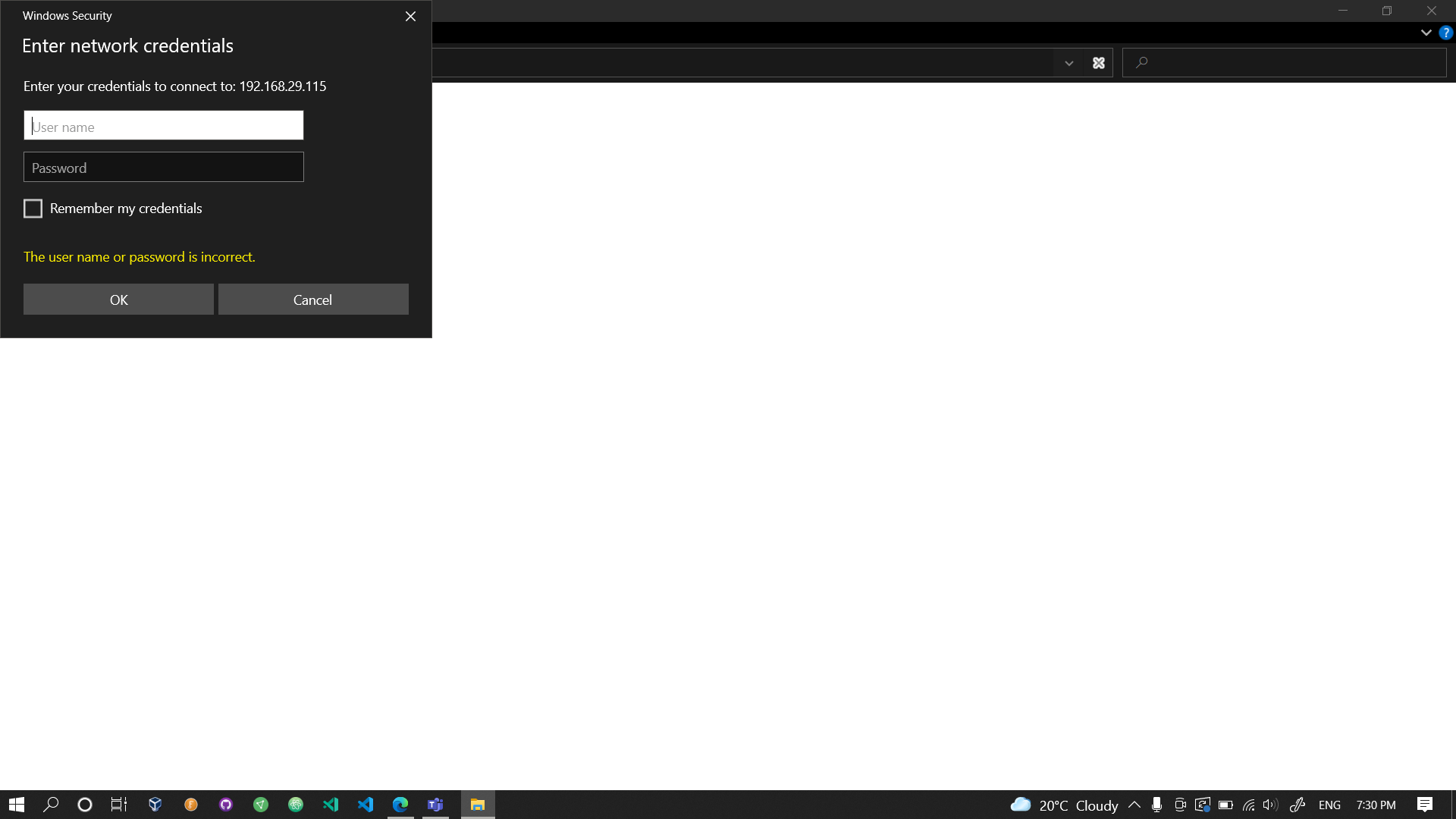
**4.5 USER INTERFACE**

* The user interface for CUPS Server is



*Fig 4.5 a. CUPS Server User Interface*

The user interface for SAMBA Server is



*Fig 4.5 b. SAMBA Server User Interface*

**5. TECHNICAL IMPLEMENTATION AND ANALYSIS**

**5.1 OUTLINE**

In this project, we aim to outline IoT applications, advantages and potential risks. In addition, through the implementation and analysis of current existing programs or the development of new programs, a framework is constructed to research and further develop best security practices. Based on the results of the investigation, we provide recommendations to avoid such risks and remedy possible security vulnerabilities. This work will guide regulatory agencies to continue to implement policies and educate end users and entities as well as stakeholders involved in the Internet of Things to develop and apply more appropriate security and privacy measures. We used different tools such as NMAP, Hydra, OpenSSH, Samba and CUP Server to analyze different vulnerabilities in the home router connected to the Raspberry Pi. After scanning for vulnerabilities, we tried to protect them in different ways. We have conducted a risk analysis of what are the risks, how harmful are they, what are the violations, and what measures can be taken to mitigate these risks, what are the challenges.

The security and privacy of the devices, communication channel and network play a fundamental role in fulfilling requirements such as data confidentiality, data protection, authentication, console and network access, etc. Therefore, it is important to review the existing architectural framework and examine how this is possible overcoming the challenges such as scalability, integration problem, data protection and security and how the framework improves security in the IIOT environment and reduces costs.

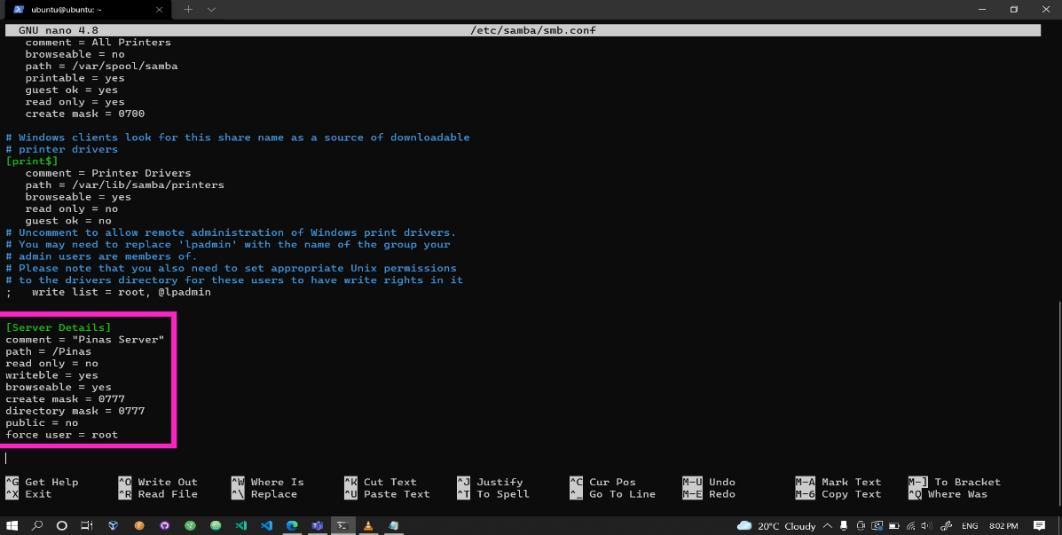
We adopted a descriptive survey methodology to explore the history and background of IoT systems, their security and privacy concerns, and related countermeasures. We have offered our own perspective on the general and extended IoT model and its privacy and security concerns. We have built and studied a cloud / peripheral-supported IoT model that consists of a virtual machine (sensors) and an edge node (Raspberry Pi). This setup was designed to evaluate the model that we have proposed in the following sections of this article. Our work does not provide detailed information on various IoT applications (smart health, smart cities, supply chain, transportation, etc.); their features, advantages and problems, or possible risks or security threats among these applications.

**5.2 TECHNICAL CODING AND CODE SOLUTIONS**

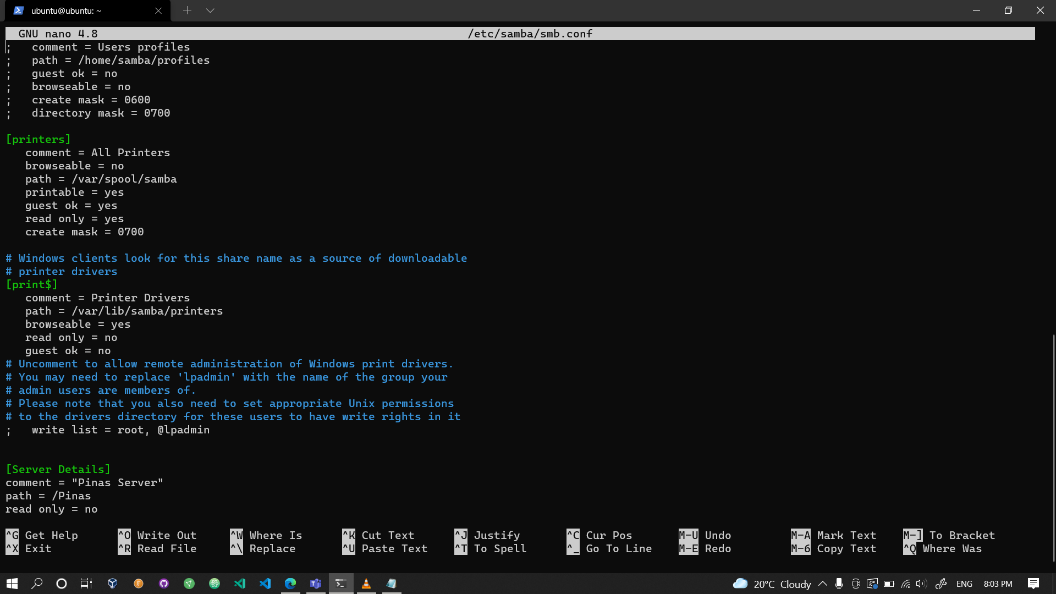
For our home-based router system, we use various tools to scan vulnerabilities such tools are NMAP, Hydra Tool etc. As we know, Samba Server and Cups Server work on a default port number, on changing their port number using Hydra Tool we can increase security.

Some of Coding which we did are

*Fig 5.2 a. Sample configuration of SAMBA Server*



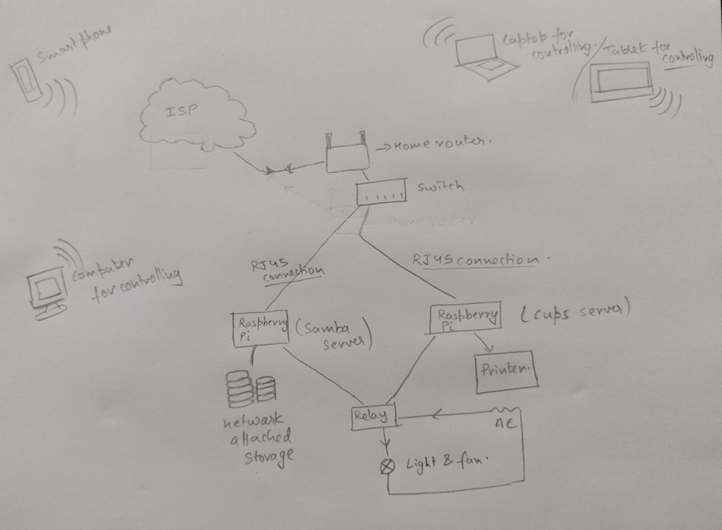
*Fig 5.2 b. Samba Server Configuration*



*Fig 5.2 c. Printer Configuration*

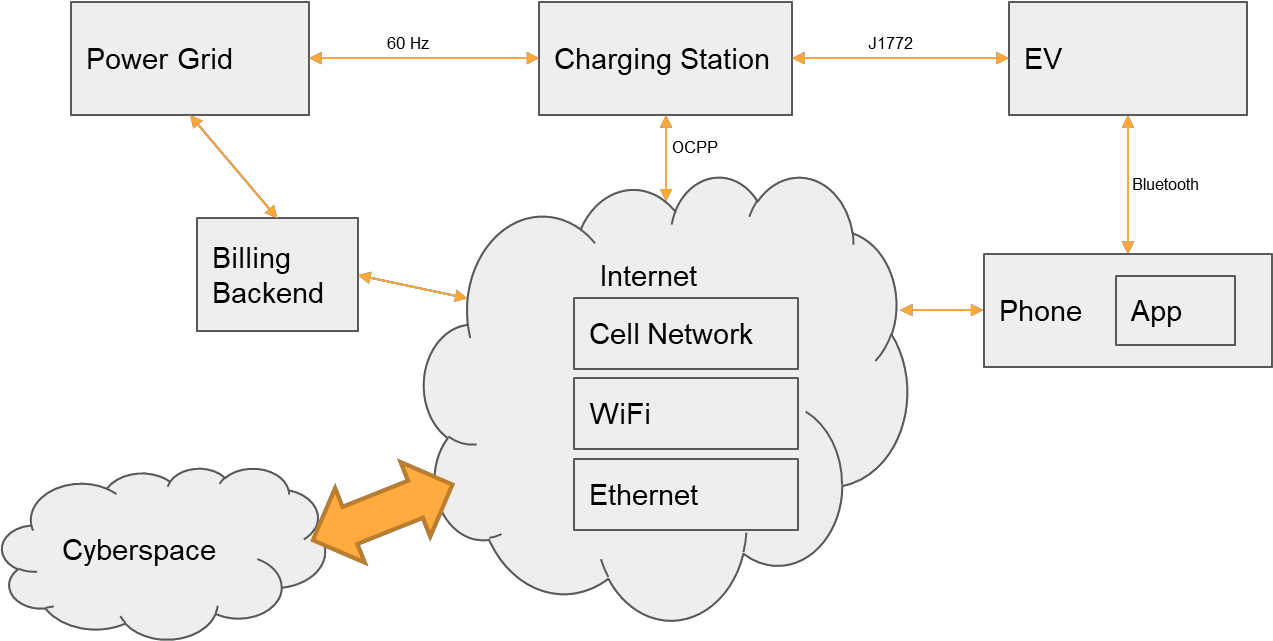
**5.3 WORKING LAYOUTS OF FORMS**

The working layout for home-based router system is-



*Fig 5.3 a. Working Layout for Home-Based Router*

The working layout for EV based system is-

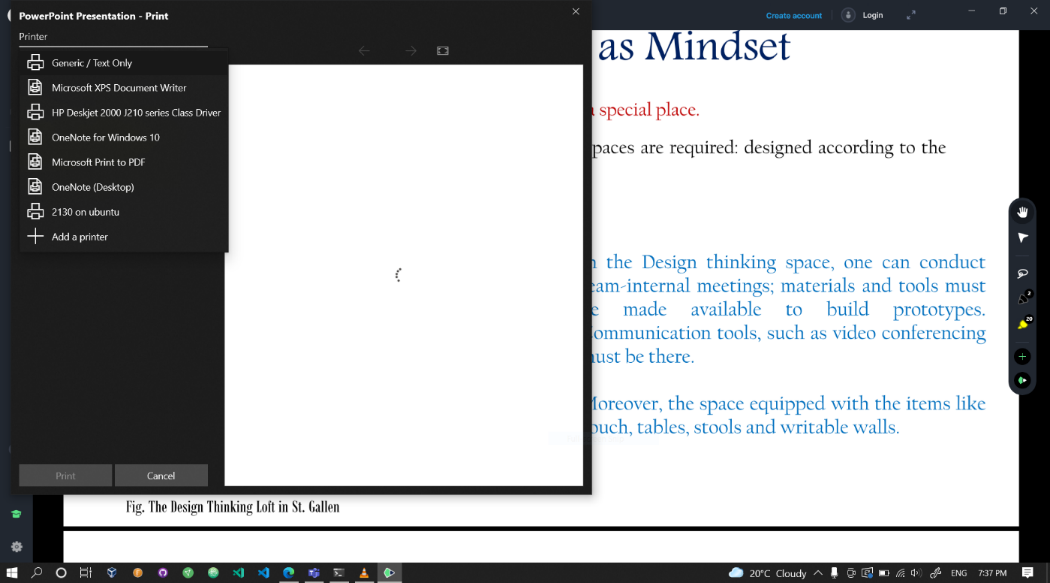


*Fig 5.3 b. Working Layout for EV system*

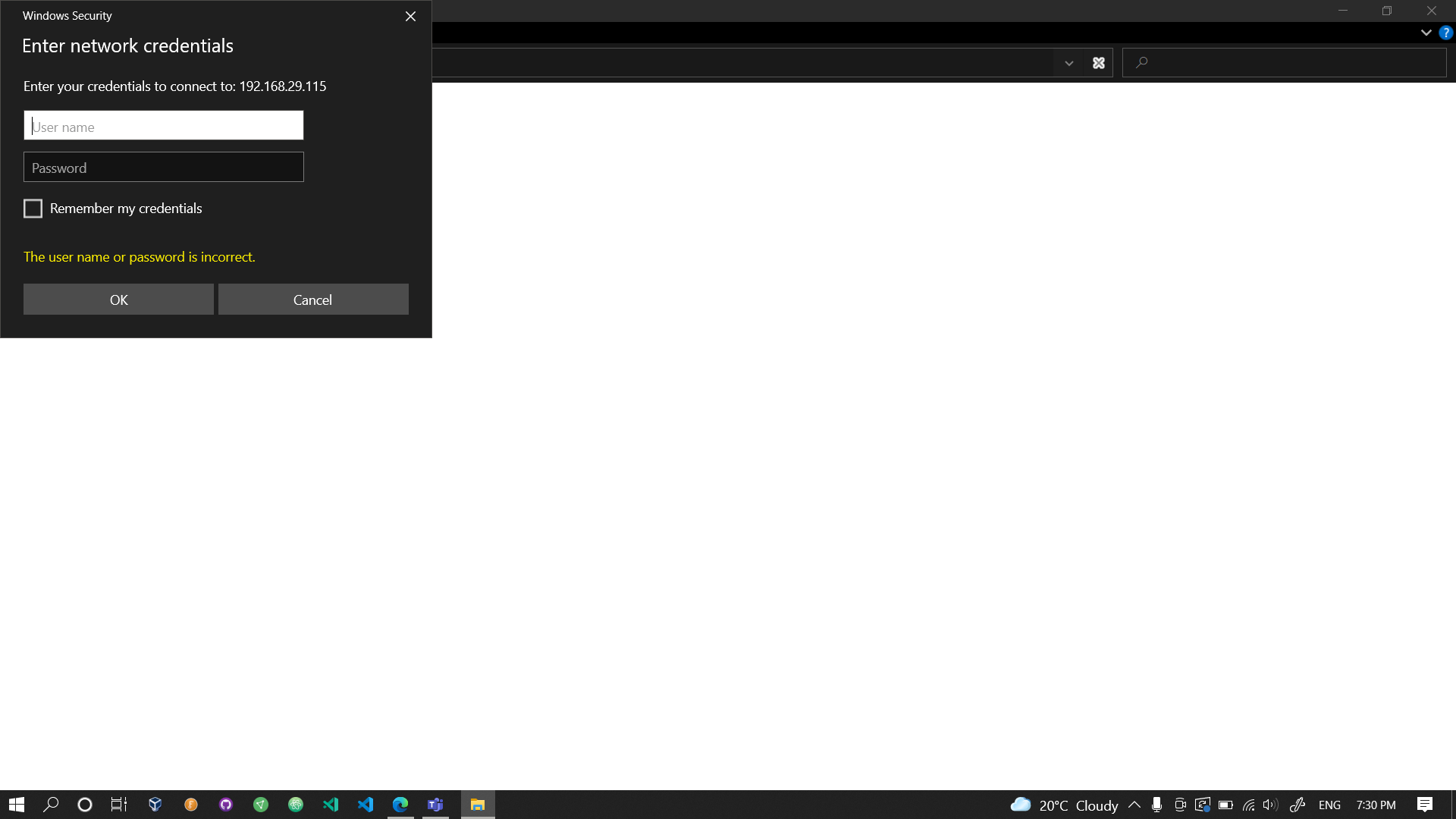
**5.4 TEST AND VALIDATION**

For EV based system, we find out that there are various attacks that can took place on EV components. Some of them include attacks on power grid, protocol vulnerabilities, charging station vulnerabilities, potential attacks including MitM attack, DDoS attack, Packet Replay attack and eavesdropping and many more. All these are the attacks which we found while studying about Electric Vehicle.

For Home-based Router system, our final objective is to host printer on local network so that it can be accessed by any device which was registered on home router.

****

*Fig 5.4 a. Printer hosted on local network*

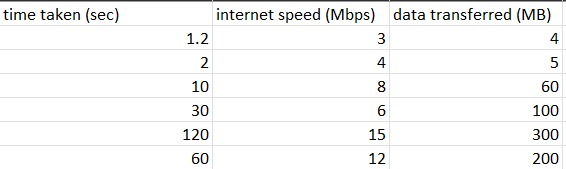


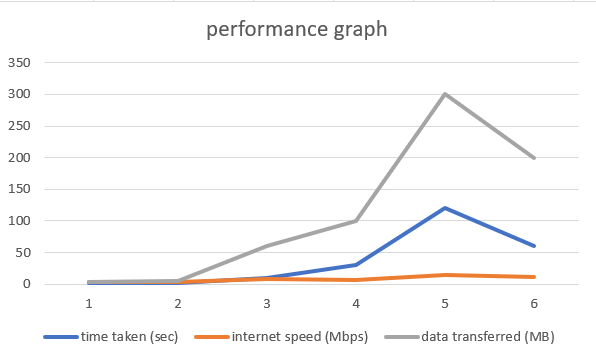
*Fig 5.4 b. Connecting to NAS Server*

**5.5 PERFORMANCE AND ANALYSIS**

This is the graph representing the performance of the server. The blue line shows the time taken for the testing, the orange line shows the internet speed and the red line represents the data transferred per second on the server. This is analysis which we made for our home-based router system.

*Table 5.5 1. Computation of Performance*





*Fig 5.5 a. Performance Graph*

**5.5 SUMMARY**

In future work, more research should be conducted on encryption security methods that are more capable of running on resource-constrained IoT devices (lightweight encryption). It will help ensure that users with different experiences can use and set up IoT systems stably, even though many of these IoT devices have insufficient consumer interfaces. In addition, there is an urgent need to standardize data collection and sharing procedures performed by IoT devices connected to the Internet. Such standards will reduce the number of unpredictable vulnerabilities and related attacks on disparate platforms. We study the benefits and risks associated with the Internet of Things. With all the many benefits, risks can be exploited to harm end users by allowing unauthorized access to sensitive personal data, enabling attacks on the system, and posing risks to personal safety. As devices supporting the Internet of Things are launched on the market, we need to provide them with appropriate security measures which affect the user-friendliness, the operation, and the integration into existing systems. We hope, with the help of researchers, to build a dynamic security framework to mitigate, not necessarily eliminate, security and privacy risks, and to be smart enough to adapt to changes in new communication technologies and different application delivery scenarios.

**6. PROJECT OUTCOME AND APPLICABILITY**

**6.1 OUTLINE**

After performing research, testing, and validating, now we produced possible outcomes which we get on studying as well as by performing various tasks. Outcomes are especially important for any work as they give us idea about what we have done, what we missed out, and how can we overcome the flaws which were generated while testing and studying.

For our EV based work, we produced various attacks that could take place and harm end users security and privacy.

For our Home-based router system, we scan various vulnerabilities and risk associated, did risk analysis and finally we tried to mitigate them so that it cannot harm anyone.

**6.2 KEY IMPLEMENTATIONS**

Key implementations of EV based research work is we first studied about EV and its emerging technologies. What are various attacks and risks associated with it. After analyzing risk associated with EV and various IoT devices used in EV we came up with various mitigation approaches. These is how our work flow is goes.

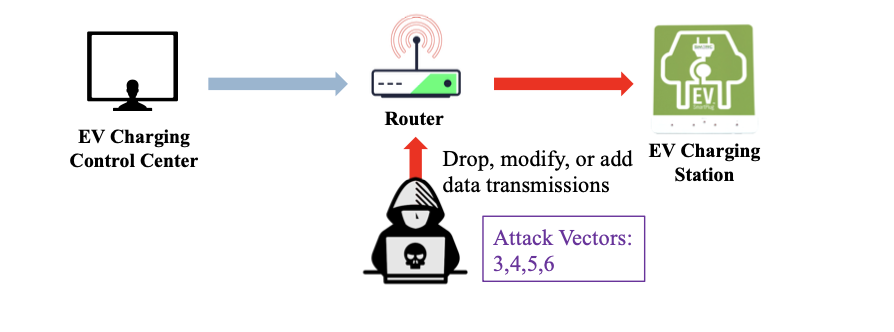
Key implementation of Home-Based Router System is here made a connection including Samba Sever, Cups Server, Raspberry Pi to use printer using all the connections and there on scanning vulnerabilities. We also use NMAP and Hydra Tool to apply more security by changing port number as well so that no user from public network can access the system. Only devices which are registered with on home device can access the printer system.

**6.3 SIGNIFICANT PROJECT OUTCOMES**

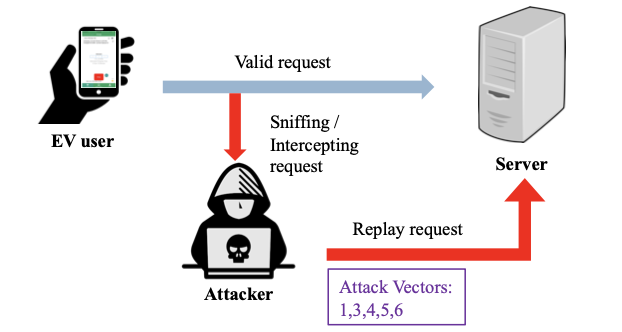
**6.3.1 EV PROJECT OUTCOMES**

For our research on EV and its charging technologies, we found various attacks on different components of EV. The attacks are-

1. Cyberattacks Against the Power Grid - Stuxnet, a covert malware released by the US and Israel against Iran in 2010, was perhaps the first hack targeting vital infrastructure systems. The virus caused damage to equipment at Iranian nuclear refining facilities, interrupting the country's refinement efforts. Its deployment was primarily motivated by the desire to avert conflict, notably nuclear warfare, between Israel and Iran. While the initiative was a political success, many people see it as the opening of Pandora's Box, ushering in a new era of cyberattacks.
2. Vehicle Vulnerabilities - The goal of this is to go over the dangers and vulnerabilities that have been connected with non-EV and EV to this point. While their propulsion, systems are dissimilar, their control, safety, and infotainment systems are comparable.
3. Charging Station Vulnerabilities - Charging stations are vulnerable to a wide range of threats. To manage charging, execute invoicing, and update systems, most charging stations use wireless connectivity. Wi Fi, cellphone, Bluetooth, and RFID are examples of communication technologies. EV chargers, like EVs, may now be called IoT devices thanks to the integration of networking. Because it is an IoT device, it is vulnerable to a wide range of assaults.
4. Protocol Vulnerabilities - The majority of the charging station ecosystem is made up of OCPP-based technologies. The fact that ISO standards are expensive to get and OCPP is free source is a major issue and reason for OCPP's dominance in the charging protocol war. The high expense of ISO standards reflects in my capacity to locate providers. The majority of the vulnerability analysis was devoted to identifying and addressing OCPP flaws. OCPP v1.5, which was published in 2012, is the version present in practically all charging stations today. OCPP 2.0, a newer version, was released in April of 2018 and is not included in the scope of this evaluation.
5. Man-in-the-Middle Attack - An attacker can intercept communication between the EV charging control center and drop, edit, or add data transfers.

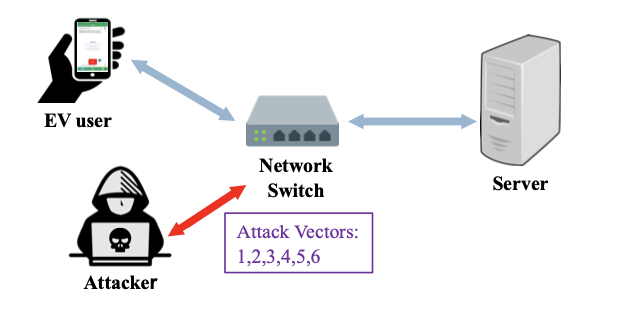


*Fig 6.3.1 a. Man-in-the-Middle Attack on EV*

1. Packet Replay Attack - The activity captures and duplicates or delays legal data transfers, leading in changed messages or fraudulent communication channels for the demand response automation system (DARS), or collects private EV user information. 

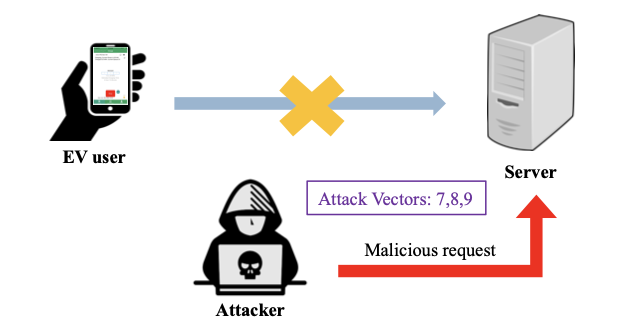
*Fig 6.3.1 b. Packet Replay Attack on EV*

7. Address Resolution Protocol Spoofing –



*Fig 6.3.1 c. Address Resolution Protocol Spoofing on EV*

8. Denial-of-Service Attack-



*Fig 6.3.1 d. Denial-of-Servive Attack on EV*

MITIGATION STRATEGIES FOR EV-

There are several ways that the threat of a cyberattack against the grid can be mitigated. The two strategies of increasing grid security are through:

1. Charging Infrastructure

2. Power Grid

**6.3.2 HOME-BASED ROUTER PROJECT OUTCOMES**

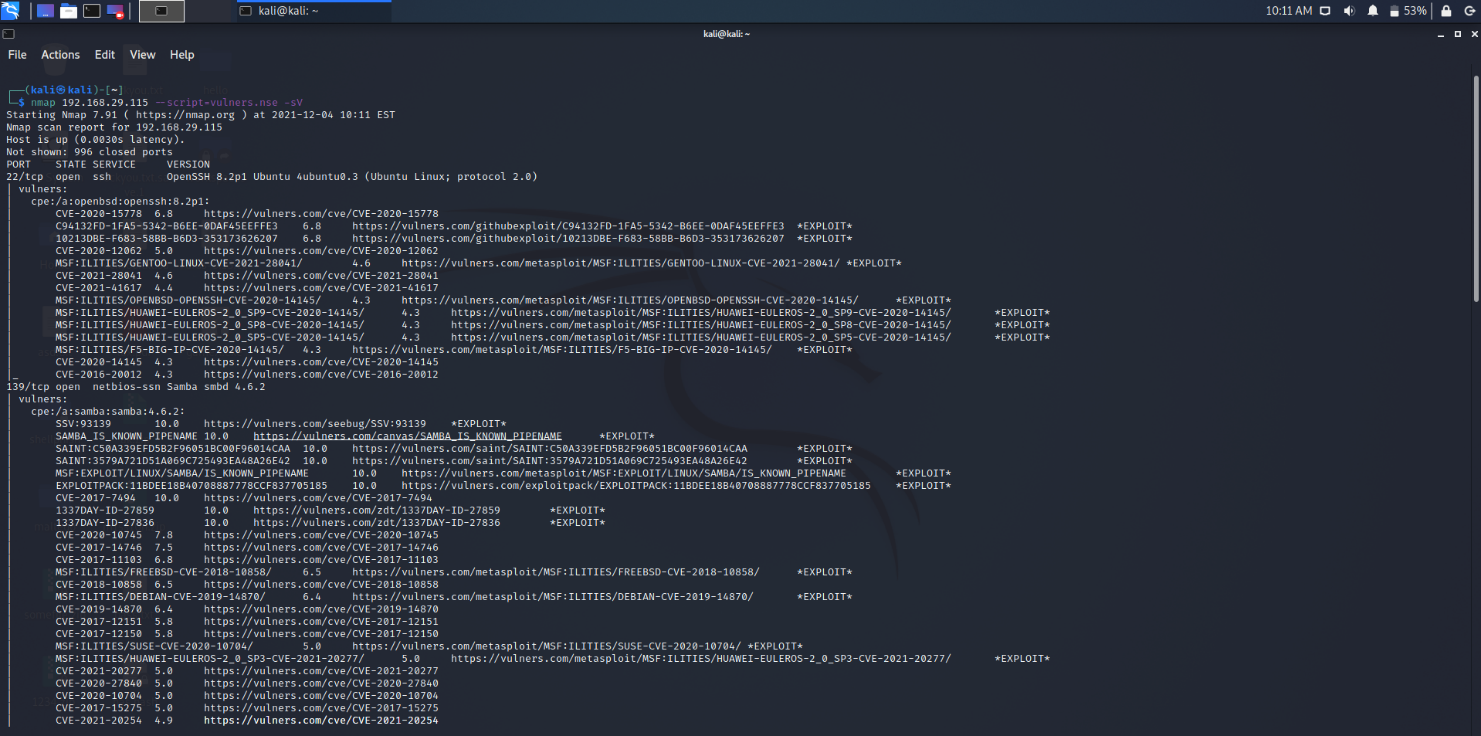
There are various vulnerabilities that we found from home-based router system are-

1. DDoS Attack

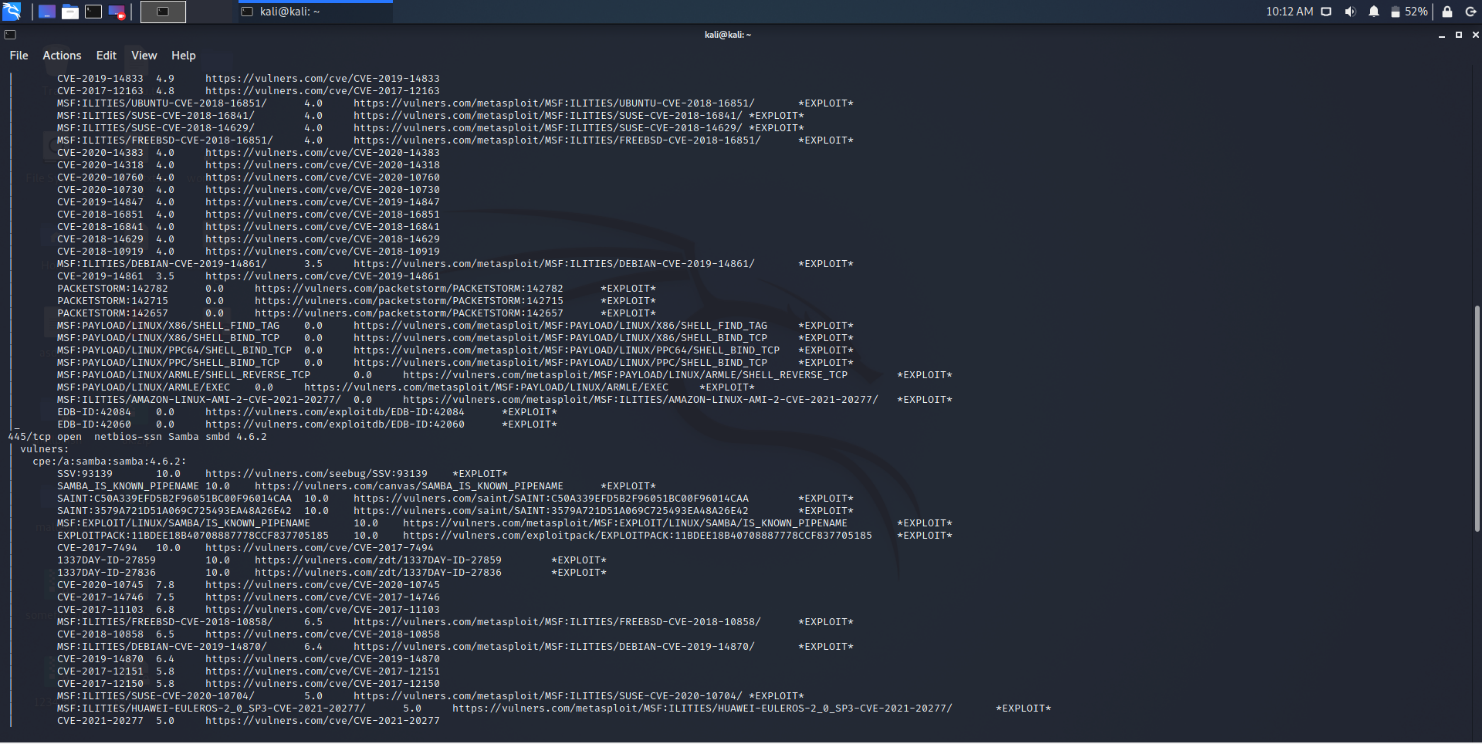
2. Man-in-the-Middle Attack

3. Keystroke Capture or Keylogging

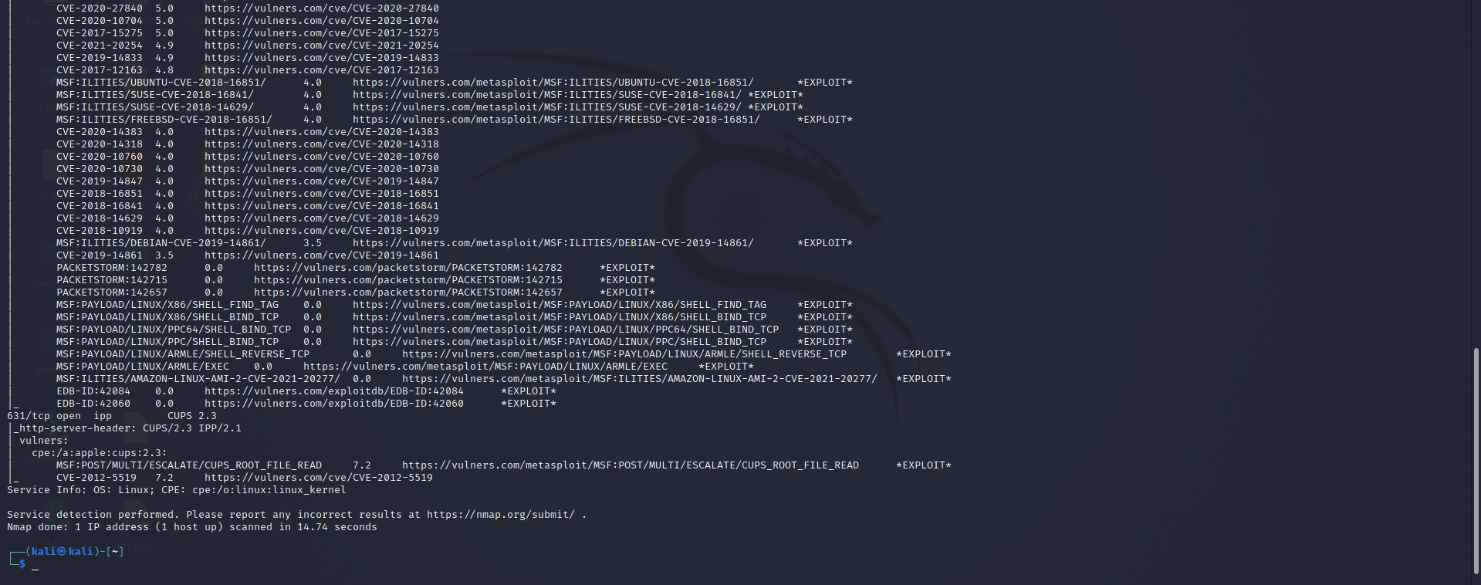
4. Network Sniffing

****

*Fig 6.3.2 a. Scanning vulnerabilities in Router system*

****

*Fig 6.3.2 b. Scanning vulnerabilities in Router system*

****

*Fig 6.3.2 c. Scanning vulnerabilities in Router system*

Mitigation Approach –

1. We will change port number of SSH, SAMBA, CUPS Server to provide basic security from threats.

2. We’ll applying Machine id filter to prevent unauthorized access to our network.

**6.4 PROJECT APPLICABILITY**

As we know, EV is gaining popularity now in India and from a long ago was a part of developed countries, so our research on EV, its risk associated, mitigation approaches will help companies to overcome these issues as well as make end users aware about the flaws that EV and its components have.

Home-Based Router system helped the end users as it provides them with the following functionalities-

1. Portability - Now end users do not need to carry hard disk with them to operate the server.
2. Security - Not able to work on new mac address if we implement mac filtering, hence increasing security.
3. Storage Solution - We can have a huge amount of storage in a very cheap cost.
4. Easy to access - It can be accessed through internet so can be accessed easily through any device which is registered on home device.
5. If RAID system is implemented then the risk of data loss will be mitigated.

These are some of the project applicability which will help the users with their work providing more ease to them.

**6.5 INFERENCE**

IoT is a technology which is growing and growing and it never stops. The demand for IoT devices never going to stop but always increases. But with this increasing demand, their safety should not be compromised. After analyzing all the outcomes, we came to a single conclusion that with the increase in cyberattacks, companies should keep in mind what they are producing, what can be their effect on customers life, what can be done so that security and privacy is not compromised. IoT is a never-ending technology and so its flaws.

**7. CONCLUSIONS AND RECOMMENDATION**

**7.1 OUTLINE**

The Internet of Things (IoT) is a new key technology that will pave the way for the next generation of industrial production systems. IoT will be a critical component of the Future Internet. It is unique due to its sensing and actuating capabilities. It serves as a link between the real and virtual worlds. Today's IoT systems have not been sufficiently enhanced to meet the desired functional requirements, and they pose security and privacy risks. Attacks on cyber physical systems, in particular, can cause physical harm and endanger human life. However, a slew of information security and privacy issues have emerged that must be addressed before implementing IoT. Our research focuses on IoT security and privacy issues, as well as mitigation approaches and case studies. Here we try to figure out various challenges faced by IoT devices and thereby analysing some of the mitigation approaches. We also try to analyse some of the recent case studies to get in depth knowledge.

**7.2 LIMITATION AND CONSTRAINTS**

Talking about limitation of our work, as our work is a research work limitation is not that it cannot fulfill any particular function. Research work is said to be totally successful if it can help the people to get better understanding about the topic. In our research work, we tried to incorporate every thing so that end users get the better understanding and try to incorporate it in their lives. But somewhere we lag to add some more latest IoT device issues, their mitigation approaches. There are many smart devices which people use without even knowing how they cam harm their security and privacy.

**7.3 FUTURE ENHANCEMENTS**

In future, we are accepting to add more and more recent case studies, some latest IoT devices with their challenges, the risk incorporated in them and how to mitigate them. We also try to add some more risk assessment strategies which can help companies to overcome the attacks, threats and breaches.

These are our future work which we are looking forward to complete and update it with our work so that it can help more and more end users and companies

.

**7.4 INFERENCE**

An IoT system is a network of smart devices that work with users to create smart services. It generally groups together a large number of devices interacting using several technologies and communication protocols. Over the past decade, IoT systems are increasingly prone to various security issues, such as malicious access to services and network attacks. These problems caused considerable damage and affected the secrecy, integrity and availability of information. By studying about IoT, we came to a conclusion that IoT is gaining popularity all over the world and humans are getting dependent on IoT devices to a great extent. With these growing needs companies are focused on developing more IoT devices rather than focusing on its functionality, security and privacy concerns. Because of these growing needs, security is compromised which leads to various attacks, threats, vulnerabilities etc. It is very important for companies to look into these issues and try focusing more on major concerns rather than producing more and more.

**REFERENCES**

1. Aqeel-ur-Rehman, Sadiq Ur Rehman, Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan: *Security and Privacy Issues in IoT.*

2. JOHN SOLDATOS: *SECURITY RISK MANAGEMENT FOR THE INTERNET OF THINGS TECHNOLOGIES AND TECHNIQUES FOR IOT SECURITY, PRIVACY AND DATA PROTECTION*.

3. Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achuthan and Venkat P. Rangan:

*IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process*.

4. <https://www.tylercybersecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment>.

5. src.nist.gov/glossary/term/risk

6. <https://www.attilasec.com/blog/what-are-the-risks-associated-with-industrial-iot>

7. <https://www.investopedia.com/articles/professionals/021915/risk-management-framework-rmf-overview.asp>

8. <http://www.icthub.pk/blog/biggest-iot-security-issues/index.html>

9. Glenn Sean Morrison: *Threats and Mitigation of DDoS Cyberattacks Against the U.S. Power Grid via EV Charging.*

10. <https://www.intellectsoft.net/blog/biggest-iot-security-issues/>

11. <https://www.infoguardsecurity.com/95-of-websites-risk-operating-on-outdated-software-with-known-vulnerabilities/>

12. <https://www.ponemon.org/>

13. <https://www.financialexpress.com/money/man-in-the-middle-cyber-attacks-leading-to-surge-in-security-breach-incidents-amid-pandemic/2258462/>

14. <https://securityintelligence.com/articles/florida-water-supply-poison-iot-security/>

15. <https://duo.com/blog/the-2019-state-of-the-auth-report-has-2fa-hit-mainstream-yet>

16. Yu-Wei Chung, UNIVERSITY OF CALIFORNIA, Los Angeles: *Electric Vehicle - Smart Grid Integration: Load Modelling, Scheduling, and Cyber Security*