SURVEY ON SMART GRID CYBERSECURITY THREATS

seminar report submitted
in partial fulfillment of the requirement for award of the degree of

Bachelor of Technology
in
Computer Science & Engineering

By

Ancy Valentina	**(20UECS0049)**
Vadala Deeksha	**(20UECS0982)**
Akshaya K V	**(20UECS0423)**

Mr.P.Elumalaivasan.,M.Tech.,(Ph.D)
Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SCHOOL OF COMPUTING

VEL TECH RANGARAJAN Dr.SAGUNTHALA R&D
INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University Estd u/s 3 of UGC Act, 1956)
CHENNAI 600 062, TAMILNADU, INDIA

December, 2021

BONAFIDE CERTIFICATE

It is certified that the work contained in the seminar report titled ”SURVEY ON SMART GRID CYBERSECURITY THREATS” by ”Ancy Valentina (20UECS0049) Vadala Deeksha (20UECS0982) Akshaya K V (20UECS0423)” has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Signature of Supervisor
Mr.P.Elumalaivasan,M.Tech.,(Ph.D)
Assistant Professor
Computer Science & Engineering
School of Computing
Vel Tech Rangarajan Dr.Sagunthala R&D
Institute of Science and Technology

Signature of Head of the Department
Dr. V. Srinivasa Rao,M.Tech.,Ph.D
Professor & Head
Computer Science & Engineering
School of Computing
Vel Tech Rangarajan Dr.Sagunthala R&D
Institute of Science and Technology
December,2021

DECLARATION

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Ancy Valentina
Date:06/12/2021

Vadala Deeksha
Date:06/12/2021

Akshaya K V
Date:06/12/2021

APPROVAL SHEET

This seminar report entitled SURVEY ON SMART GRID CYBER SECURITY THREATS by Ancy Valentina (20UECS0049), Vadala Deeksha (20UECS0982), Akshaya K V (20UECS0423) is approved for the degree of B.Tech in Computer Science& Engineering.

Signature of Supervisor
Mr.P.Elumalaivasan,M.Tech.,(Ph.D)
Assistant professor
Computer Science & Engineering
School of Computing
Vel Tech Rangarajan Dr.Sagunthala R&D
Institute of Science and Technology

Signature of Seminar Handling Faculty
Dr.C.YOGESH,ME.,Ph.D
Assistant Professor
Computer Science & Engineering
School of Computing
Vel Tech Rangarajan Dr.Sagunthala R&D
Institute of Science and Technology

Date:06/12/2021
Place:Chennai

ACKNOWLEDGEMENT

We express our deepest gratitude to our respected **Founder Chancellor and President Col. Prof. Dr. R. RANGARAJAN B.E. (EEE), B.E. (MECH), M.S (AUTO). DSc., Foundress President Dr. R. SAGUNTHALA RANGARAJAN M.B.B.S.,** Chairperson Managing Trustee and Vice President.

We are very grateful to our beloved **Vice Chancellor Prof. S. SALIVAHANAN, Ph.D.,** for providing us with an environment to complete our seminar successfully.

We record indebtedness to our **Dean & Head, Department of Computer Science & Engineering Dr. V. SRINIVASA RAO, M.Tech., Ph.D.,** for immense care and encouragement towards us throughout the course of this seminar.

We take this opportunity to express our gratitude to Our Internal Supervisor **Mr. P.ELUMALAIVASAN,M.Tech.,(Ph.D)** for his cordial support, valuable information and guidance, he helped us in completing this seminar through various stages.

A special thanks to our **Seminar Coordinator Dr. G. Tamilmani, M.E.,Ph.D** for her valuable guidance and support throughout the course of the seminar.

We thank to our **Seminar handling Faculty Dr.C. Yogesh,M.E.,Ph.D** for the valuable information shared in proceeding with our seminar.

We thank our department faculty, supporting staff and friends for their help and guidance to complete this project.

Ancy Valentina	**(20UECS0049)**
Vadala Deeksha	**(20UECS0982)**
Akshaya K V	**(20UECS0423)**

ABSTRACT

Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On the other hand the smart grid is also getting the most significant applications of the Internet of Things (IoT). On a personal level,you need to safeguard your identity, your data, and your computing devices. At the corporate level,it is everyone's responsibility to protect the organization's reputation,data, and customers. At the state level,national security,and the safety and well-being of the citizens are at stake.

Keywords:Cybersecurity , Smart grid , Internet of things.

LIST OF ACRONYMS AND ABBREVIATIONS

APTS	Advanced persistent attacks
DER	Distributed energy resources
DoS	Denial of service
ICT	Information and communication technologies
IED	Intelligent electronic device
IoT	Internet of things
IT	Information technology
PLC	Programmable logic controller
PMU	Phasor measurement units
RTU	Remote terminal unit

TABLE OF CONTENTS

Page.No

Chapter 1

INTRODUCTION

1.1 Introduction

A cyber attack is any attempt to gain unauthorized access to a computer,computing system or computer network with the intent to cause damage.Cyber attacks aim to disable,disrupt, destroy or control computer systems or to alter,block,delete,manipulate or steal the data held within these systems.Even there is a risk of cybersecurity in the smart grid.

1.2 Aim of the Seminar

To focus on cyber-attack types and provide an in-depth of the cybersecurity state of the smart grid. We aim to supply a deep understanding of cyber-security vulnerabilities and solutions and give a guide on future research directions for cyber-security in smart grid applications.

1.3 Scope of the Seminar

Cyber security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked. It encompasses the security considerations that happen during application development and design,but it also involves systems and approaches to protect apps after they get deployed. Cyber security may include hardware,software,and procedures that identify or minimize security vulnerabilities.

1.4 Methodolgy

Cyber Attack Resilience is the capacity of a system to maintain state awareness as a means for detecting cyber attacks,and to proactively maintain a safe level of operational normalcy through rapid system reconfigurations in response to detected cyber attacks that would impact system performance. Maintaining operational normalcy includes containing the immediate consequences of the detected attack and post-attack forensic support based upon the data collected for detecting attacks.

Cryptographic systems : A widely used cybersecurity system involves the use of codes and ciphers to transform information into unintelligible data.

Firewall : Use to block traffic from outside, but it could be also used to block traffic from inside.

An Intrusion Detection System (IDS): IDS is an additional protection measure used to detect attack.

Anti Malware Software and scanners : Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called antiMalware tools are used to detect them and cure an infected system.

Secure Socket Layer (SSL) : It is a suite of protocols that is a standard way to achieve a good level of security between web browser and websites.

Chapter 2

LITERATURE REVIEW

M.H.Cintuglu, O.A.Mohammed, K.Akkaya, A.S.Uluagac 2018 Smart grid CPS testbeds and main capabilities. MITM, Denial of Service, ARP Spoofing, Eavesdropping, Malformed Packet, Precision Insider,Rogue Software, Database Attacks. Smart Grid concept compels to develop proper testbeds to test interoperability and cyber-security vulnerabilities[1].

MZ Gunduz ,R Das 2019 Cybersecurity issues stunting the development of IoT-based smart grid 2018 Device attacks, Data attacks, Privacy attacks, Network attacks, Organized attacks, APTs, Ransomware attack Some interesting challenges not mentioned in the literature. The use of IoT-based technologies in smart grid applications is one of the most important challenges in the development of this system in terms of cyber-security[2].

M.M.Raut, R.R.Sable, S.R.Toraskar 2019 A cybersecurity strategy to detect and counter against cyber attacks in smart grid applications. Rather than applying a simple security approach or deploying a specific security technology,they believe that smart grid cyber-attacks may be mitigated more effectively by combining several security mechanisms through a cyber-security strategy[3].

K. Kimani, V. Oduol, K. Langat 2020 Cyber-security issues stunting the development of IoT-based smart grid.Device attacks, Data attacks, Privacy attacks, Network attacks,Organized attacks, APTs, Ransomware attack. The use of IoT-based technologies in smart grid applications is one of the most important challenges in the development of this system in terms of cyber-security[4].

A cyber-security strategy to detect and counter against cyber attacks in smart grid applications. Attacking cycle steps and details in smart grid. Rather than applying a simple security approach or deploying a specific security technology, they believe that smart grid cyber-attacks may be mitigated more effectively by combining several security mechanisms through a cyber-security strategy[5].

Chapter 3

SEMINAR DESCRIPTION

3.1 Existing System

- Due to the heterogeneous communication architecture of smart grids,it is quite a challenge to design sophisticated and robust security mechanisms that can be easily deployed to protect communications among different layers of the smart grid-infrastructure.
- The traditional electrical power grid is currently evolving into the smart grid.
- A smart grid integrates the traditional electrical power grid with information and communication technologies (ICT).
- Integration empowers the electrical utility providers and consumers to improve the efficiency and the availability of the power system while constantly monitoring,controlling,and managing the demands of customers.

3.2 Advantages

- Protects system against viruses, worms, spyware and other unwanted programs.

- Protection against data from theft.
- Protects the computer from being hacked.
- Minimizes computer freezing and crashes.
- Gives privacy to users

3.3 Disadvantages

- Firewalls can be difficult to configure correctly.
- Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
- Makes the system slower than before.
- Need to keep updating the new software in order to keep security up to date.
- Could be costly for average user.

3.4 Feasibility Study

Smart grid applications have four main stages. These are generation,transmission, distribution, and consumption. Energy has different types such as geothermal heat, flowing water,solar radiation,wind,hydro plants,chemical combustion,and nuclear fission. Generation of electricity is the process of producing electricity from these kinds of energy. Bulk generation system is connected to the distribution system via the transmission system carrying electricity to far distances.

Transmission domain is connected to customer domain by distribution domain which could also supply connection to storage systems and distributed energy resources (DERs) to meet electricity need for customers. Practically some security risks ideally need security solution to protect against vulnerabilities and regarding network security in Smart Grids,the networks are the most vulnerable against threats and risks. The threats and risks are the biggest obstacles to maintain the network and system. Practically some security risks ideally need security solution to protect against vulnerabilities and regarding network security in Smart Grids,the networks are the most vulnerable against threats and risks. The threats and risks are the biggest obstacles to maintain the network and system.

Chapter 4

MODULE DESCRIPTION

4.1 Integrity attacks

Integrity attacks aim to modify the con-tent of original data such as customer account data, billing data,voltage and sensor values,control commands, operating status of the devices, also aim to delay and reorder the stream of the messages illegally.

Integrity attacks do not include only illegitimate data modification such as false data injection. So to prevent these types of attacks we Authentication schemes and end-to-end encryption are required to eliminate the aforementioned integrity attacks in smart grid networks. Also,attackers must have authenticated access to the communication networks and sensitive information to initiate a confidentiality or integrity attack.Hence,access control and authentication are crucial to prevent the smart grid from integrity attacks.

4.2 Availability attacks

Availability means that information is accessible by authorized users. Availability attacks prevent and may destabilize authorized access in the smart grid. Availability attacks are also known as DoS attacks.DoS attacks aim to block, damage and delay in data transmission.This causes unavailability in network sources. Availability attacks intend to overload networks by using a variety of techniques,so that the system cannot function properly.Attackers send large volumes of traffic to flood the transmission lines in the network.

This causes legitimate data packets in network traffic to be lost and not to be processed.Smart grid cyber-attacks are generally coordinated to exploit various components to launch simultaneous attacks.A coordinated attack is the most challenging attack type.Since coordinated attacks can exceed usual defense, they require multilayer security solution with robust approaches.Also, coordinated attacks target all of the security objectives, requirements,and smart grid com-ponents. So,the security approaches achieved by analyzing cybersecurity requirements according to network layers will provide effective security solutions for smart grid applications.

Chapter 5

RESULTS AND DISCUSSIONS

Cyber-security is a major and critical issue for IoT-based smart grid applications. Smart grid security issues include data acquisition, and control devices such as PLC,smart meters,IEDs,RTU,and PMUs. There are also network security challenges,including firewalls attack scenarios,countermeasures, encryption,intrusion analysis,forensic analysis,and routers. Classification of cyberattacks for taking into account important factors of information security enables a well-organized and useful way to provide practical solutions for current and future attacks in smart grid applications.

Moreover,due to the characteristics of smart grid applications, specific solutions need to be created for their private necessities. Due to security risks in common IT background,we can infer that nearly all aspects associated with IT technology in smart grid applications have potential vulnerabilities. Therefore,cybersecurity issues in smart grid applications are under research and need deeper investigations to defend against cyber-attacks and vulnerabilities.

Chapter 6

CONCLUSION AND FUTURE ENHANCEMENTS

6.1 Conclusion

Concluding this research, self-awareness related to cyber-attack in Smart Grids is important. The user should be aware of the risks related to the Smart Grid and mitigate them by doing various risk assessments and case studies to provide a further solution in protecting the Smart Grid against different types of cyberattack. The biggest challenge to secure these devices over larger infrastructure. Blockchain technology could help resolve security issues by providing a shared and encrypted ledger that is immutable to changes made by malicious nodes or attackers. It can also be utilized to verify identities and authorize access by storing and recording transactions in the immutable ledger and make data exchanges between distributed gadgets smooth and cost efficient. Therefore,it will provide defense against evolved cyber-attacks.

6.2 Future Enhancements

Evolving security techniques for zero-day attacks. Creating systems that can assist to log information for forensics analysis and audit controls. Establishing new protocols or altering old protocols for the requirements of smart grid applications. Designing global standardization frameworks for secure communication in smart grid applications. Architecting wide-area situational awareness frameworks for cyber-defense solutions.

Reference

[1] M.H. Cintuglu, O.A. Mohammed, K. Akkaya, A.S. Uluagac, A survey on smart grid cyber-physical system testbeds, IEEE Commun. Surv. Tutor. 19 (1) (2018) 446–464, doi:10.1109/COMST.2018.2627399.

[2] MZ Gunduz ,R Das(2019) Cyber-security on smart grid: Threats and potential solutions, Computer Networks Volume 169,14 March 2019, 107094

[3] M.M. Raut, R.R. Sable, S.R. Toraskar, Internet of things(IoT) based smart grid, Int. J. Eng. Trend. Technol. 34 (1) (2019) 15–19. doi:10.14445/22315381/ IJETT-V34P203. [5] V.C. Gungor, D.

[4] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks, Int. J. Crit. Infrastruct. Prot. 25 (2020) 36–49, doi:10.1016/j.ijcip.2020.01.001.

[5] A. Ghosal, M. Conti, Key management systems for smart grid advanced metering infrastructure: a survey,IEEE Commun. Surv. Tutor. 21 (3) (2021) 2831–2848.