CYBER SECURITY IN SMART GRIDS (WITH IOT consideration)

MSc Cybersecurity

Shahid Shaik
Student ID: 19188358

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shahid Shaik
Student ID:	19188358
Year:	2021/22
Programme:	MSC in Cybersecurity
Module:	Research Project
Supervisor:	Imran Khan
Submission Due Date:	31/01/2022
Project Title:	Cyber Security in Smart Grids (with IOT Consideration)
Student Name:	Shahid Shaik
Words:	6555

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Shahid
Date:	30/01/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□

You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

CYBER SECURITY IN SMART GRIDS (WITH IOT consideration)

Forename Surname
Student ID

Abstract

Smart grid infrastructures comprise the communication, computing, and measuring services to obtain substantial benefits from the digitization of conventional electrical grids. The rate of information transfer and measuring the field parameters using sensory devices has increased the operational speed of the grid. A smart grid comprises a lot of sensory & intelligent devices and all these devices are controlled by a supervisory system. Integration of intelligent devices and IoTs controlling enhances the information exchange rate, and efficient demand management. However, the integration of IoT devices introduces cyber security threats. This paper entails cyber security concerns and protection measures against cyber security threats. The potential cyber security threats have been addressed first in this report. Then, preventive measures are discussed to reduce the likelihood of cyberattacks. The common challenges that will arise while implementing the cyber security system are also addressed in this report.

1. Introduction

Electrical grids are the intermediate points between generating plants and electrical distribution networks.Generating plants generate the electrical energy at high voltages which are then transmitted to the electrical grids via transmission lines. The electrical distribution network is connected to the grid substation. The electrical substations are categorized as smart grids and conventional grids. With the advancement in technologies numerous automated devices are discovered which are used as an alternative medium for accomplishing manual tasks in the industries. These automated devices do not require any human intervention for accomplishing manual tasks. Generally, these devices are known as intelligent or smart devices.Advanced Metering Infrastructure (AMI) facility at the grid substation assists in real-time analytics and bill creation for the users. All these smart and intelligent devices are based on either machine learning algorithms and IoT technologies. For information transfer from one device to other devices, the internet or networking systems are used (Faquir, Chouliaras, Sofia, Olga, &Maglaras, 2021). The connection of the devices with the internet infrastructure makes the whole system vulnerable to cyber-attacks. This report examines the use of the cyber security system to make the smart grid infrastructure free from cybercrimes.

Electrical energy is generated either by using fossil fuels or renewable sources. Most of the fossil fuels are about to end. So,the entire generation of electrical will depend on the use of renewable energy.The invention of the smart electrical grid has assisted in the efficient management and generation of electrical energy. Cyber attacks are very common threats to the smart grid infrastructure as entire connectivity is linked to the internet services. Physical threats and natural disasters are individual two major threats for smart grid systems. This report is focused on describing the use of the cyber security system to enhance the security of the smart electrical grid. These threats will lead to blackouts, confidential data theft, security breaches, and huge electrical hazards at the grid substation (Otuoze,Mustafa, &Larik, 2018). Therefore, it is crucial to deeply analyze the security system at the smart grids. Security issues related to cyber-attacks andconfidential data theft are critically analyzed with considering the Internet of Things.

1.1. 1.C: Aim and Objectives

The information inside an organization or in a smart grid system can be easily transferred from one terminal to another terminal using the multi-directional data flow system. The main aim of a smart electrical grid is to display the real-time power information of the users to the substation board.Smart grid infrastructures are highly efficient in managing the supply of electricity. A secured smart grid assists in managing the reliable and efficient operation of the electrical supply (Zhang, Huang, &Bompard, 2018). Some of the common objectives of this study report are as follows:

1. Improving the overall security system of the smart electrical grid.

2. Deploying intelligent devices to complete risky tasks inside a smartgrid without the intervention of humans.

3. To minimize the likelihood of confidential data theft present due to the existing vulnerabilities.

4. Securing the entire smart grid from cyber attacks.

5. Developing a cyber-security enable smart grid system for efficient and reliable operation of the electrical grid.

1.2. 1.D: Research Problem

1. What is the need fora Cyber security system in a smart grid?

2. How a conventional smart grid is different from a smart grid?

3. What is the use of the IoT and Intelligent devices in the smart grid system and how do they assist in accomplishing the manual task in smart grids?

4. What are the possible cyber threats and vulnerabilities are present in a smart grid?

5. What is the merits and demerits of a cyber security system in a smart grid?

6. How deeply a cyber attack can impact the operation of the smart grid?

1.3. 1.E: Importance of Study

Smart electrical grids are equipped with numerous intelligent and IoT devices. All individuals working inside the smart grid need to understand the security protocols of a cyber security system. A clear understanding of the security system of the electrical grid will help in assessing the risk portfolio. The presence of cyber threats and the possible vulnerabilities in the smart grid can be easily examined and possible measures can be adopted to reduce the chances of cyberattacks (Ahmed, Lee, Hyun,&Koo, 2019). The working of a smart grid system and cyber security implementation can also be addressed by understanding the operation of smart grid infrastructures.

2. Related Work

2.1. 2.1 Cyber security in smart grids, challenges and solutions

With strong remedies that expand the performance of standard Electrical Grid systems, Micro grid innovation is set to change industrialization. Grid Computing is a digitized communications-based power distribution company. As per [1,] "rising stack and usage requirements maximize energy difficulties." For example, the market is expanding, and troubles include shutdowns, overloads, and under voltage, and electricity show's crucial carbon pollution and, most importantly, having dealt with cyber-attacks. The U.S. is

responsible for nearly 40% of all CO2 outrush from energy systems, which is destructive to the atmosphere. The need for electricity has raised dramatically in both homes and offices areas, as a result of advancements in fast-developing systems that make more use of machines, equipment, and gadgets than ever before. As a result of these factors, the energy need has skyrocketed. The old Power system is inadequate to support operations to industry requirements, but the Smart system is just the next power infrastructure that will ensure that industrial companies have enough electricity. Smart Technology is expected to improve the economy, dependability, and accessibility by integrating sophisticated technologies like telecommunication and enhanced processing capability. The Smart system also includes technology that is linked to 2-way telecommunications and electrical exchanges. It is a well-organized system that inherits traditional electricity generating technologies like biogas, fossil fuels, & coal, and also alternative energies like wind and photovoltaic electricity. It is recognized for distributing and using electricity in a very well manner to a network of digital devices, converters, and equipment. Acceptable, since it employs 2-way interaction to accomplish this mission, while the old power system only utilizes 1-way interaction. The Power System offers consumers speedy and better products with a decreased reaction lag time, allowing the energy issue to be effectively addressed. Meanwhile, the Smart system is not without flaws and challenges, one of the most serious of which is the inability to safeguard the most important piece: data. The causes for this are that the Smarter Power system will often share data because private data may be stored therein (Culler,and Burroughs,2021).

Since multiple home and professional gadgets will be linked through a number of connections to interact and give safety to the systems with different approaches, cyber defense in Power systems is a crucial function. These would be tough challenges that will be addressed through a research article wherein a variety of safety mechanisms will be assessed and studied in order to give remedies to complicated safety concerns.

2.2. 2.2 Cyber security requirements for smart grid

As stated by Frank, Leitner, and Pahi, (2017) it is evaluated that the smart system's security is critical for the proper functioning of this innovative type of electrical infrastructure. In the first step, analysts claim that regulated approaches and methods must be used. Numerous modern digital network regulations have been from the last few months, which conversely

render discovering a detailed link in this abundance of information. The conclusions of research aiming at dealing with this problem by analyzing all regulations that outline safety criteria for the smart systems are presented in this article. Based on a comprehensive analysis of the data, 17 ethical norms were found, which are discussed in this article with an emphasis on the needs and evaluated using assessment methods. In terms of security needs, the links between both the norms have already been examined to determine where they coincide or complement one another and where wholly autonomous. This, combined with the norms' needs-focused explanations, can provide valuable advice on data protection for smart system elements, assisting professionals in selecting the guidelines that are appropriate for their location or a particular situation.

2.3. 2.3 Smart grid security

The Smart Grid System uses data exchange to interact amongst its many elements. 2.4 have a full discussion of its telecommunications.

The study on Smart system network protocols safety encompasses a variety of topics, each of which is broken down into its own department. Misleading implantation threats and transmission bandwidth utilization are explained in the following sections. Table 3.5 displays all the parts as well as the study effort completed within each

As per the views of Liu, Ospina, and Konstantinou, (2020), it is evaluated that Smart Grid power system simulations may be used to test various Power System ideas as well as cyber warfare.

2.5 has a detailed understanding of the Smart Power System model for system security. The investigation on its simulations may be classified into 2 parts. The study discussed in this article includes both hardware & software components simulations. Table 3.6 includes all of the parts as well as the study effort completed within each

2.4. 2.4 Cyber Security Issues for IoT based Smart Grid Infrastructure

Over many years, we've seen an increase in the linking of items of all types that weren't previously had peer interaction. The notion of the Web of Things is formed by these freshly linked items (IoT). The Energy industry is now investigating the potential of online everything. Network control, on the other hand, is not a brand-new phenomenon in this

industry. For management and surveillance, power systems currently have data gathering capabilities, although these are restricted. The convergence of IoT & Smart power systems paves the path for actual information gathering from all locations on the system. Some information that was acquired over time in a consolidated fashion across wide geographical locations may now be obtained locally, at manufacturing or distribution hubs, at an affordable price. It was also the vast quantities of information that can now be collected and processed. The power system is an electrical transmission and logistics system that is improved by computer control, monitoring, and networking capabilities. It allows for a 2, actual interchange of power and data between several participants in the electrical cycle, from the power plant to corporate, industrial, and rural customers. In terms of organizational safety, the energy revolution and the latest electronic grids pose several issues. The utilization of linked items (enabling remote management, surveillance, and administration of the whole life cycle) and the intensification of online trading (manufacturing, transport, and demand are all networked) raises the sensitivity of commercial data systems. Smart power system security is becoming a critical component of guaranteeing the worldwide safety of the world's energy networks. The goal of this paper is to provide a complete review of safety concerns, risks, and remedies in IoT-based micro grids. Their study concentrated on safety flaws, safety needs, and computer hackers in the system in order to identify their influence on the system and provide a roadmap for upcoming internet studies in smart power system apps (Basumallik, Eftekharnejad, Davis, Nuthalapati, and Johnson, 2018,).

2.5. 2.5 Cyber security and privacy in standards for smart grids

Robust data & telecommunication technology are required for the power system to function reliably. Several specifications for the newer type of energy system have been presented in the latest days, making it hard for carriers as well as other smart energy system shareholders to discover papers that are relevant to their specific issues. The goal of this document is to compile a list of all smart energy regulations that address safety problems, as well as data on their composition. A comprehensive investigation was done to attain this aim, which resulted in the discovery of 36 papers on safety and 11 articles on confidentiality.

3. Research Methodology

Comprehensive research methodology and 2-way flow of data might very well widen the possibility for concessions of security and vulnerabilities of consumer privacy, as well as negotiations of private details and interferences of data security." As the links hubs grow, so does the count of entrance points and pathways that enemies could manipulate. "Risk refers to the possibility for an unpleasant event originating from foreign or domestic variables, as assessed by the probability of events and the related implications," according to the paper (Gunduz,. and Das, 2020). The whole day, their aim is to assist health personnel in making the best decisions for every patient. The innovation and quality incorporated in their NGS, panels, and FISH products demonstrate their commitment to advance the development of genetic medical care. They function in such a way that inherited genetic characteristics services may continue to evolve and improve the lives of patients by utilising fast, accurate, and simple-to-use genetic analysis technologies established for researchers. Pestle assessment is an excellent example of a contrast. A method for addressing important external factors that may have an influence on a business. Levels and technological advancements are examples of technological aspects. In the tourism, forestry, and agricultural industries, such factors must be taken into account. Political parties deal with legal issues. Shareholder planning is a crucial talent that ambitious individuals use to acquire acceptance from others. The investor participation technique is being utilized to identify the key people who must be convinced.

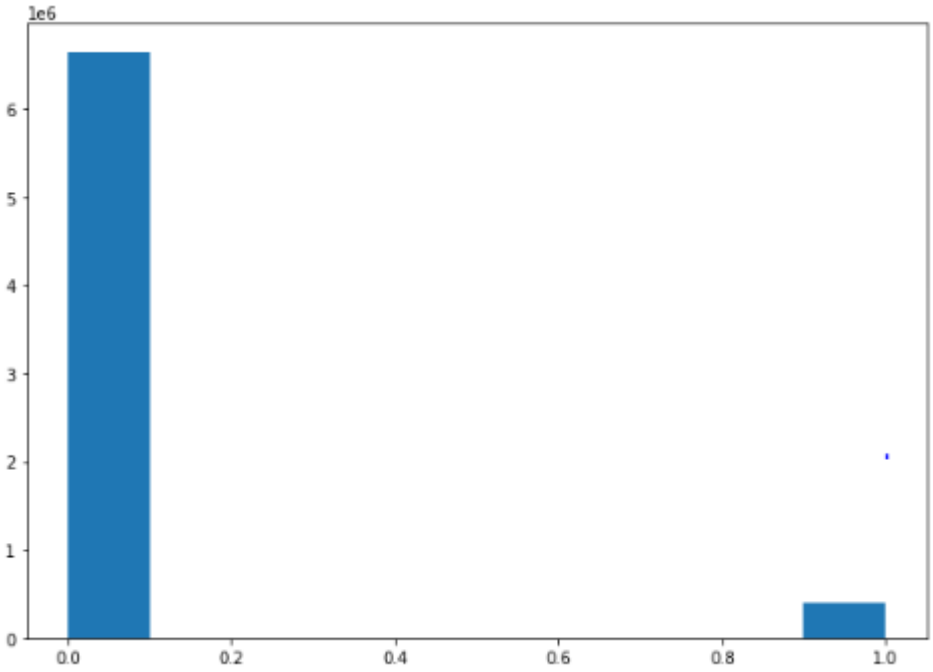
4. Design Specification

The techniques and/or architecture and/or framework that underlie the implementation and the associated requirements are identified and presented in this section. If a new algorithm or model is proposed, a word based description of the algorithm/model functionality should be included.

Cyber Security Data Analysis

The dataset is collected from the IEEE Data-port site. The dataset comprises the previous record of cyber security characteristics of various electrical grid system. The grid system which has been exposed to cyber attack are included in this dataset. The attribute "Target" have two class labels where "1", represents a successful cyber attack, and "0" represents an unsuccessful cyber attack.

The proportion of successful, and unsuccessful cyber attacks in the dataset are as follows



A predictive model is developed using the decision tree algorithm for detecting the potential threat based on successful characteristics of the cyber security systems.

```
print(auc_dtree)
print(f1_dtree)
print(prec_dtree)
```

```
1.0
1.0
1.0
```

The precision, Recall, and Accuracy of the predictive model is 1.

5. Implementation

5.1. Implementation of Cyber Security in Power Grids

The integration of modern information and communication system in the traditional smart grid has transformed the conventional distribution system of electricity. The use of advanced and IoT-based infrastructure at electrical grids made the entire system vulnerable to cyber-attacks. The cyber layer of a smart grid handles the communication, data exchange, and data computation work. Both the cyber layer and the physical components of a smart grid system are tightly coupled to perform the integrated tasks efficiently. Cyber system implementation in an electrical grid is a sequential process. It involves three major steps such as 1. Risk & Threat Assessment, 2. Exploration, 3. Implementation (Mitigation & Restoration). There are numerous sub-steps are also between the aforementioned three major steps (Faquir, Chouliaras, Sofia, Olga, & Maglaras, 2021). This section of the report entails types of

potential cyber threats, risk analysis, and the process of implementing the cyber security system in electrical grids.

5.2. The architecture of Electrical Smart Grid

An electrical power system comprises electrical generation, transmission, and distribution as three major activities and an electrical grid serves as the central management point of these activities. The cyber layer of a smart grid system handles data exchange, communication, and computation operations of all these electrical activities. An ideal architecture of a smart grid system is shown in the picture below. The smart grid architecture is an integration of numerous software tools and hardware components. The sensory and communication technology at the smart grid provides significant advantages to consumers as well as utilities. These intelligent devices at the smart grid assists in reducing the utility bills, and automatic control devices. Smart grid infrastructure also assists in managing the decentralized electric generation unit also.

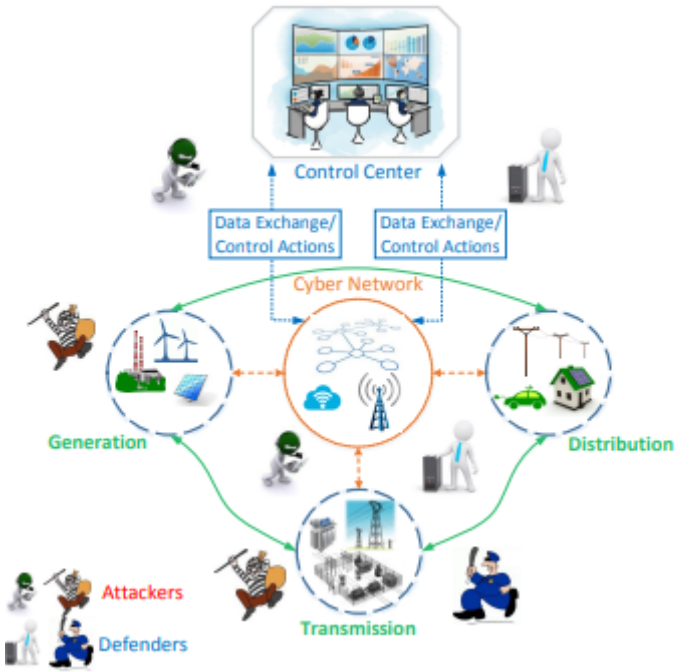


Figure 1: Smart Grid Architecture

5.3. Need of Cyber Security in Smart Grid

The smart grid is a modern technology-enabled infrastructure that monitors and manages the major activities of an electrical grid automatically or with minimum human intervention. This is used to keep track of grid conditions, energy utilization, and generation, as well as

automate many of the company's processes. The smart grid's objectives and purposes include, but are not limited to:

- Enhancing the electrical grid's resiliency.
- Enhance its overall effectiveness
- Reduced distribution and production costs
- Allow for electricity grid monitoring in real-time.

As shown in the picture below, the continuous black bold line depicts the flow of information between two or more departments on the smart grid (İsa, 2021). However, the flow of electricity is shown by the dashed bold line. Intelligent devices and smart instruments both are used at each terminal of smart grid infrastructure to automate and efficiently manage the grid operation. Advanced metering infrastructure (AMI) which are microprocessor-enabled electric meters that communicate with utilities and customers in real-time about the amount of energy used, grid conditions, and electricity costs, is one of these technologies.

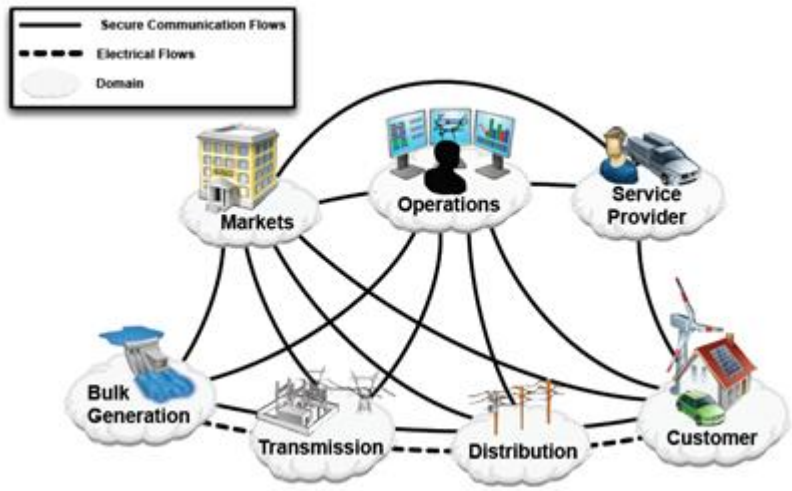


Figure 2: Electrical and Information flow between two units in Smart grid architecture

.

6. Evaluation

Threat Evaluation processes have been completed. The chosen advanced methods must be open source technology to ensure that the Overall System is safeguarded by practical and cost-effective innovations that support and collaborate in a consistent way. Connectivity with older operational databases is a requirement for the chosen alternatives. Furthermore, the use

of open-source technology means that the Cyber Defense program may grow, develop, and adjust to change difficulties as they occur. Management is usually faced with the problem of deploying effective responses while also dealing with restricted resources and the need to accommodate new ways of doing business and increased competition (Huseinović, Mrdović, Bicakci, and Uludag, 2020). As a result, management must prioritize Security Infrastructure that provides:

- Comprehensive surveillance.
- Adaptability, technical support for older devices.
- Transition to smart technologies.
- A robust accounting, recording, and publishing framework.
- Cost-efficient.
- Agreement with appropriate standards.
- Decreased sophistication.
- Connectivity with current processes.

.

Use visual aids such as graphs, charts, plots and so on to show the results.

6.1. Experiment / Case Study 1

Implementation of Cyber Security in Power Grids

The integration of modern information and communication system in the traditional smart grid has transformed the conventional distribution system of electricity. The use of advanced and IoT-based infrastructure at electrical grids made the entire system vulnerable to cyber-attacks. The cyber layer of a smart grid handles the communication, data exchange, and data computation work. Both the cyber layer and the physical components of a smart grid system are tightly coupled to perform the integrated tasks efficiently. Cyber system implementation in an electrical grid is a sequential process. It involves three major steps such as 1. Risk & Threat Assessment, 2. Exploration, 3. Implementation (Mitigation & Restoration). There are numerous sub-steps are also between the aforementioned three major steps (Faquir,

Chouliaras, Sofia, Olga, & Maglaras, 2021). This section of the report entails types of potential cyber threats, risk analysis, and the process of implementing the cyber security system in electrical grids.

6.2. The architecture of Electrical Smart Grid

An electrical power system comprises electrical generation, transmission, and distribution as three major activities and an electrical grid serves as the central management point of these activities. The cyber layer of a smart grid system handles data exchange, communication, and computation operations of all these electrical activities. An ideal architecture of a smart grid system is shown in the picture below. The smart grid architecture is an integration of numerous software tools and hardware components. The sensory and communication technology at the smart grid provides significant advantages to consumers as well as utilities. These intelligent devices at the smart grid assists in reducing the utility bills, and automatic control devices. Smart grid infrastructure also assists in managing the decentralized electric generation unit also.

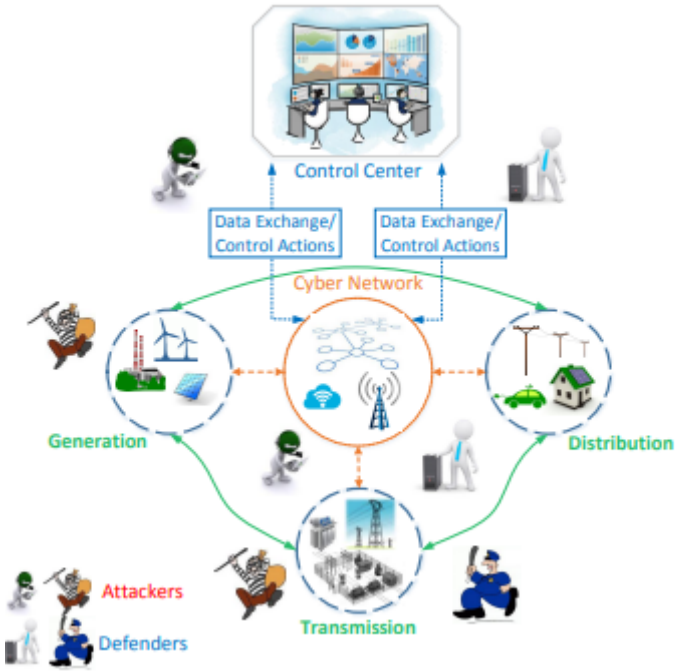


Figure 1: Smart Grid Architecture

6.3. Experiment / Case Study 2

Need of Cyber Security in Smart Grid

The smart grid is a modern technology-enabled infrastructure that monitors and manages the major activities of an electrical grid automatically or with minimum human intervention. This is used to keep track of grid conditions, energy utilization, and generation, as well as automate many of the company's processes. The smart grid's objectives and purposes include, but are not limited to:

- Enhancing the electrical grid's resiliency.
- Enhance its overall effectiveness
- Reduced distribution and production costs
- Allow for electricity grid monitoring in real-time.

As shown in the picture below, the continuous black bold line depicts the flow of information between two or more departments on the smart grid (İsa, 2021). However, the flow of electricity is shown by the dashed bold line. Intelligent devices and smart instruments both are used at each terminal of smart grid infrastructure to automate and efficiently manage the grid operation. Advanced metering infrastructure (AMI) which are microprocessor-enabled

electric meters that communicate with utilities and customers in real-time about the amount of energy used, grid conditions, and electricity costs, is one of these technologies.

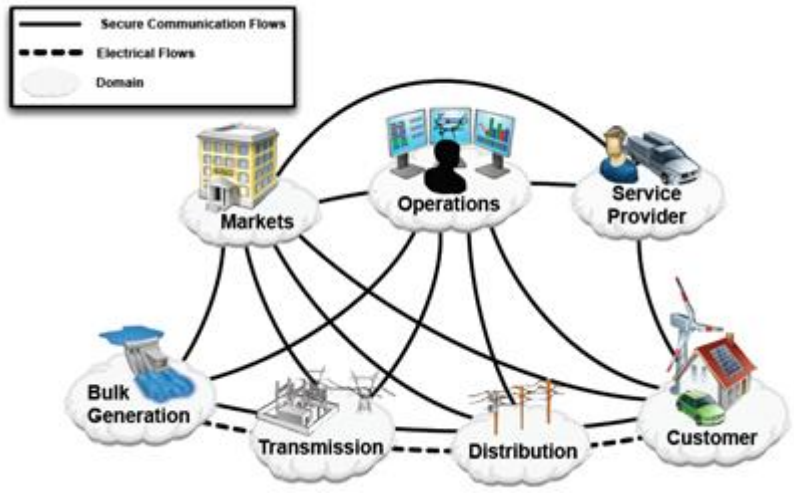


Figure 2: Electrical and Information flow between two units in Smart grid architecture

6.4. Experiment / Case Study 3

Potential Cyber Threats in Electrical Grids

Information security is associated with the potential threats of Smart Grid technology and its information infrastructure. There is a wide range of research being done to find potential answers to security issues with Smart Grids. There is a going concern about cyber security with the rise of using intelligent and IoT-based devices on the electric grid. The cyber-crimes are mainly associated with the communication system. The rise of cyber attacks motivates cyber associates to enhance the privacy and security of the communication system. Almost all aspect of the smart grid is vulnerable to cybercrimes. However, threats associated with communication are very significant (Yin, Liu, Nkenyereye, & Ndibanje, 2019). Each of these smart gadgets, which are designed for real-time contact, will present a new attack vector that might be abused if not handled carefully. The potential threats at a smart grid are as follows:

- As the complexity of the smart grid increases, the susceptibility to potential attackers and the likelihood of human-made error increases.

- Communication networks used to connect with other networks frequently have a similar likelihood of being vulnerable and hence they might impact many domains of the smart grid system.
- Using the software tools, numerous hardware components at the smart grid are interconnected with each other. Huge interconnections of devices increase the chance of "malicious code" or "DOS" intrusions.
- An increase in the number of communication nodes also increases the number of entry points for cyber attackers.
- Extensive data is collected and stored due to the two-way communication that raises the risk of data breaches.

6.5. Frequent Security Risk in Smart Grids

Numerous potential threats can cause extensive harm to smart grid infrastructure. These dangers could represent substantial threats to individuals' privacy, such as sensitive information about customers being stolen or the firm being shut down permanently. The risk associated with cyber-attacks is not limited to the internet services but cyber risk affects the entire distribution system of the electric grid. Some common security risks at smart grids are as follows:

1. Phishing: Phishing is a type of unethical cybercrime and its execution is very simple. Hence, it is the primary phase of a cyber-attack that can put consumers at risk. Intruders collect consumer information from bills, and utility payment receipts and the raw information collected from the sources processed to extract crucial information. Attackers may use the extracted information for fraudulent emails and illegitimate communication to the consumers. Consumer data can be traded with unknown sources and these activities may affect consumers financially as well as mentally.

2. Malicious Code Spreading: This is regarded as a major threat to the infrastructure enabled with smart devices such as the smart grid. The proliferation of malicious code is a major activity under this attack. The smart and intelligent devices at smart grids are affected by the spread of the malware introduce at any network node (Ustun, Farooq, & Hussain,

2019). The operation of devices is manipulated and controlled by the intruders once the malicious code is active on the smart grid system.

3. Denial of service: It is a strategic cyber attack and it can be used by the attackers at a ecific time. The major smart grid services available whether smart grid stands a risk of being attacked with a DoS attack. The connectivity services in the smart grid must be secure and reliable. Distributed architecture system is used at a smart grid to spread a connection to the innumerable devices over a broader region, the device must be inter dependable.

6.6. Cyber Security Challenges in Electrical grids

In recent times, huge variability in the generation and demand of electricity is noticed. This change in electricity demand is influenced by the digitization process of power grids. Power grids are the major component of the electricity transmission system, and hence evaluation of security challenges at power grids is crucial. Some of the major challenges in power grids affecting cyber security is as follows:

1. Information Security: The fundamental concept of information security is backed by the CIA (Confidentiality, Integrity, and Availability). The information security system is differently managed in the case of the power sector. In conventional cybersecurity systems only confidentiality and integrity parameters are sufficient to secure the flow of information. But, in the case of the power sector, availability is a major parameter. The power grids are affected by the longer blackout of electricity. If the power blackouts last longer, the more difficult the power grid restoration process is.

2. Balancing Generation and Consumption: The frequency of generated electrical energy is 50 Hz and 60 Hz. Electricity generation and consumption is an important factor to stabilize the power generation frequency. Power generation frequency is higher when the consumption of electricity is less than generated power. The Reserve capacity of the plant is used to maintain the frequency equilibrium at the power generation unit.

3. Decentralized Electricity Generation: The exploitation of renewable energy sources for the generation of electricity empowered many individuals to decentralized energy generation. Many household owners generate electrical energy for their consumption. But in case of excess generation, the additional unit of electricity can be transmitted to the nearest grid. The use of the AMI at the grid efficiently manages the unit received from the household owner.

The security system of the individuals is not secured as much security present at the grid station. So, the software tools and physical components used by the individuals are not more secure.

4. Dynamics of Physical Network: The lifetime of power devices installed at grid stations is very high. ICT (Information and Communication Technology) devices having shorter development cycles are more vulnerable to cyber attacks as these are used for many years.

6.7. Implementation of Cyber Security

Identified risk at the smart grid is solved by implementing cyber security solutions. Cyber security implementation at the smart grid protects the entire infrastructure against potential vulnerabilities. The communication network at the smart grid is most vulnerable to threats.

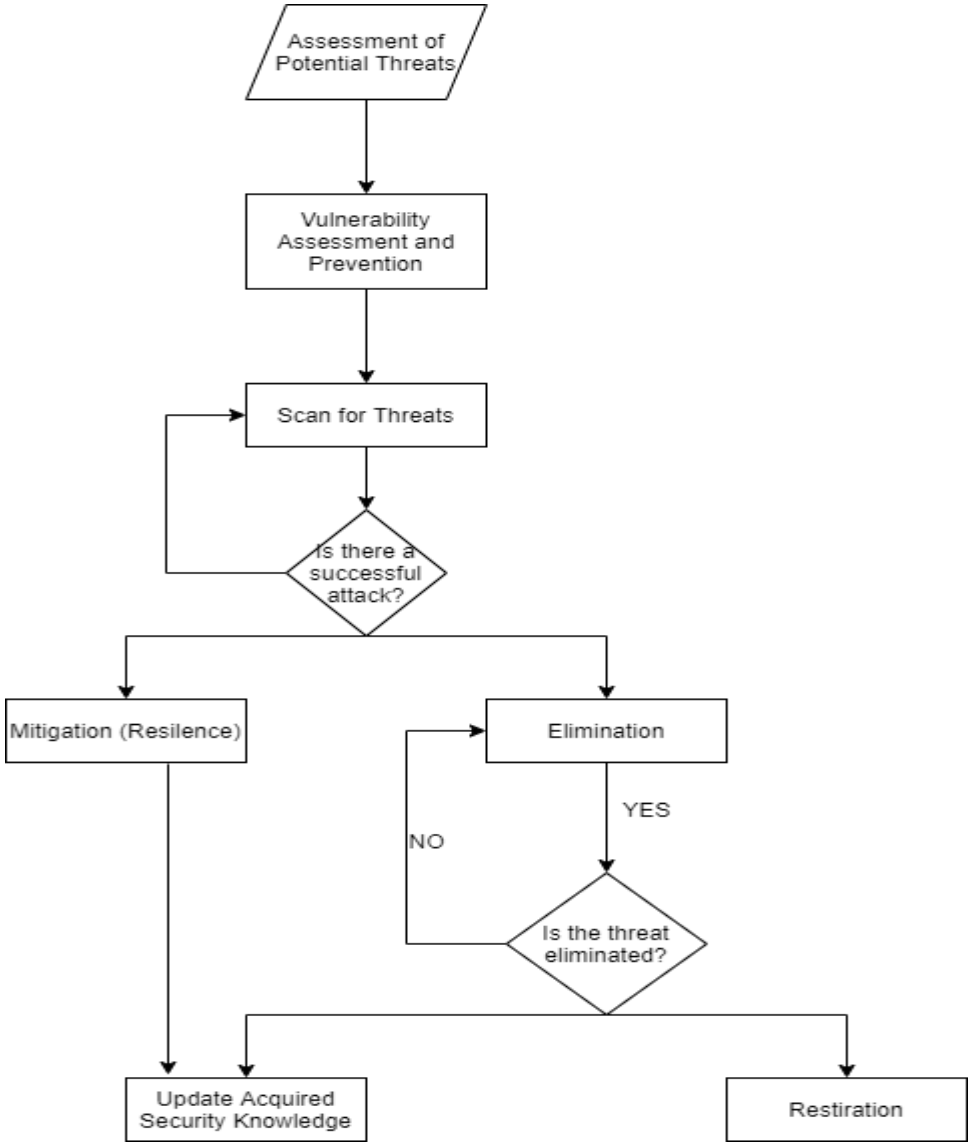


Figure 3: Flow Chart for Implementation of Cyber Security at Smart Grid

The proposed cyber security implementation at the smart grid is shown by the above flow chart. Threat evaluation of the smart grid is the initial step for the implementation of the cyber security system. After evaluation of the threat, potentially vulnerable nodes of the communication network are assessed and preventive action is taken. Any successful attempt of threat is identified during the assessment process. In case of a successful attempt of a cyber attack, a mitigation or elimination process is implemented.

The potential security solution that is provided to prevent cyber-attacks are as follows:

1. Encryption: Encryption is a technique used to scramble the input message in such a way that intermediate sources are not able to decipher the message. Using VPN (Virtual Private Networks) and AES (Advanced Encryption Standards) will assist in reducing the overall

cyber risks. When a VPN system is used to connect with the internet, the intruders will not be capable intercept the data stream.

2. Malware Protection: Malware protection is used at the smart grid as the combination of software tools as well as hardware devices are installed. A private key is obtained from the manufacturer during the certification of software. The reason an embedded system is secure is that it is only exposed to run software that is supplied by the manufacturer and requires a manufacturing key to validate the software, whereas general-purpose systems support third-party software such as antivirus software, which is constantly updated (Le, Anwar, Loke, Beuran, & Tan, 2020).

3. Network Security: VPN (Virtual Private Networks) can be used to connect with the internet as the use of VPN will prevent the cybercriminals to decipher the original message from the sender end. Numerous security assistance such as encryption and secured data transmission is provided by VPN services.

4. Risk Assessment: Annual assessment of cyber security is crucial to detect the potential vulnerable nodes threats present at the smart grid.

6.8. Discussion

The many structural parts of the Digital Grid's Power systems, such as Functional Controllers, Intelligent Sensors, SCADA devices, and Power stations, all require data protection. Of obviously, all Smart Power System users are affected by the requirement for Data Protection. The necessity for Data Security extends to the Generating, Transportation, and Distributing areas, as shown below, and a range of components in those areas must be secured. When a Data Security strategy is applied in every area, a strong, unified Cyber Defense safety is achieved. A complete Cyber Defense program should be designed when the proper Threat Evaluation processes have been completed. The chosen advanced methods must be open source technology to ensure that the Overall System is safeguarded by practical and cost-effective innovations that support and collaborate in a consistent way. Connectivity with older operational databases is a requirement for the chosen alternatives. Furthermore, the use of open-source technology means that the Cyber Defense program may grow, develop, and adjust to change difficulties as they occur. Management is usually faced with the

problem of deploying effective responses while also dealing with restricted resources and the need to accommodate new ways of doing business and increased competition (Huseinović, Mrdović, Bicakci, and Uludag, 2020). As a result, management must prioritize Security Infrastructure that provides:

- Comprehensive surveillance.
- Adaptability, technical support for older devices.
- Transition to smart technologies.
- A robust accounting, recording, and publishing framework.
- Cost-efficient.
- Agreement with appropriate standards.
- Decreased sophistication.
- Connectivity with current processes.

7. Conclusion and Future Work

The existing energy grid is insufficient to meet business requirements, but the Smart power grid is it's the next generation of energy grid that will guarantee that industry sectors have enough energy. Obtaining the support of powerful owners may help them to acquire significantly more resources, increasing the likelihood that their plans will prosper. Creating a list of stakeholders is the first step in any Investor Strategic planning. Models of Smarter Power grid networks can be used to evaluate various Electrical concepts as well as cyber terrorism. Cyber defense in power sources is a necessary feature since several residential and commercial devices will be interconnected through a variety of linkages, providing security to the platforms using various techniques. 2.5 understand the Intelligent Electric Grid paradigm in depth for security protocols. Computerized administration, surveillance, and network technology increase the power network, which is an energy distribution and logistics framework. Their research focused on the system's security issues, security demands, and cybercriminals in order to determine their impact on the system and create a framework for future studies in intelligent energy apps. The confluence of IoT and smart energy systems

provides the way for real-time data collection from all points across the grid. The main cause of concern is Smartphone, which are at the heart of this power grid. It's a sophisticated system that incorporates not just many systems, linkages, and activities, but also technological factors like information and communications technology and the power source. Smart phones are the major area of concern because cyber-crimes are related to all portions of the digitized network areas, especially power distribution devices. The Federal Institute of Standards and Technology has identified four significant challenges in cyber security. Device protection, programming, and access agreements, connection and safety hazards, and security measures are among them. Develop training and educational that adhere to the firm's, local, state, and national policies and statutory structures. An emergency request for the security of electrical networks has been issued by the US National Defense organization, the Canadian Electrical System Protection Division, and the US Department Of energy. Information safety is important by several structural properties of the Virtual Grid's Energy systems, including Operational Controller, Smart Devices, SCADA equipment, and Power generators.

References

Ahmed, S., Lee, Y., Hyun, S. H., & Koo, I. (2019). Mitigating the impacts of covert cyber attacks in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders. Energies, 12(16), 3091.

Albayati, A., Abdullah, N.F., Abu-Samah, A., Mutlag, A.H. and Nordin, R., 2020. A serverless advanced metering infrastructure based on fog-edge computing for a smart grid: A comparison study for energy sector in iraq. Energies, 13(20), p.5460.

Aravinthan, V., Balachandran, T., Ben-Idris, M., Fei, W., Heidari-Kapourchali, M., Hettiarachchige-Don, A., Jiang, J.N., Lei, H., Liu, C.C., Mitra, J. and Ni, M., 2018, June. Reliability modeling considerations for emerging cyber-physical power systems. In 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS) (pp. 1-7). IEEE.

Basumallik, S., Eftekharnejad, S., Davis, N., Nuthalapati, N. and Johnson, B.K., 2018, April. Cyber security considerations on PMU-based state estimation. In Proceedings of the Fifth Cybersecurity Symposium (pp. 1-4).

Beloglazov, A. and Buyya, R. (2015). Openstack neat: a framework for dynamic and energy-efficient consolidation of virtual machines in openstack clouds, *Concurrency and Computation: Practice and Experience* 27(5): 1310–1333.

Culler, M. and Burroughs, H., 2021. Cybersecurity Considerations for Grid-Connected Batteries with Hardware Demonstrations. Energies, 14(11), p.3067.

Faquir, D., Chouliaras, N., Sofia, V., Olga, K., & Maglaras, L. (2021). Cybersecurity in smart grids, challenges and solutions. AIMS Electronics and Electrical Engineering, 5(1), 24-37.

Feng, G. and Buyya, R. (2016). Maximum revenue-oriented resource allocation in cloud, *IJGUC* 7(1): 12–21.

Frank, M., Leitner, M. and Pahi, T., 2017, November. Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/ DataCom/CyberSciTech) (pp. 38-46). IEEE.

Gomes, D. G., Calheiros, R. N. and Tolosana-Calasanz, R. (2015). Introduction to the special issue on cloud computing: Recent developments and challenging issues, *Computers & Electrical Engineering* 42: 31–32.

Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, p.107094.

Hossain, E., Khan, I., Un-Noor, F., Sikander, S.S. and Sunny, M.S.H., 2019. Application of big data and machine learning in smart grid, and associated security concerns: A review. Ieee Access, 7, pp.13960-13988.

Huseinović, A., Mrdović, S., Bicakci, K. and Uludag, S., 2020. A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access, 8, pp.177447-177470.

İsa, A. V. C. I. (2021). Investigation of Cyber-Attack Methods and Measures in Smart Grids. Sakarya University Journal of Science, 25(4), 1049-1060.

Jaatun, M.G., Moe, M.E.G. and Nordbø, P.E., 2018, June. Cyber security considerations for self-healing smart grid networks. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-7). IEEE.

Kune, R., Konugurthi, P., Agarwal, A., Rao, C. R. and Buyya, R. (2016). The anatomy of big data computing, *Softw., Pract. Exper.* 46(1): 79–105.

Le, T. D., Anwar, A., Loke, S. W., Beuran, R., & Tan, Y. (2020). GridAttackSim: A cyber attack simulation framework for smart grids. Electronics, 9(8), 1218.

Liu, X., Ospina, J. and Konstantinou, C., 2020. Deep reinforcement learning for cybersecurity assessment of wind integrated power systems. IEEE Access, 8, pp.208378-208394.

Otuoze, A. O., Mustafa, M. W., &Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. Journal of Electrical Systems and Information Technology, 5(3), 468-483.

Sukumara, T., Sudarsan, S.D., Starck, J. and Vittor, T.R., 2017. Cyber security–security strategy for distribution management system and security architecture considerations. CIRED-Open Access Proceedings Journal, 2017(1), pp.2653-2656.

Ustun, T. S., Farooq, S. M., & Hussain, S. S. (2019). A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard. IEEE Access, 7, 156044-156053.

Yin, X. C., Liu, Z. G., Nkenyereye, L., & Ndibanje, B. (2019). Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach. Sensors, 19(22), 4952.

Zhang, Y., Huang, T., &Bompard, E. F. (2018). Big data analytics in smart grids: a review. Energy informatics, 1(1), 1-24.