Configuration Manual

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		
Programme:	MSC in Cybersecurity	**Year:**	2021/22
Module:	Research Project		
Supervisor:	Imran Khan		
Submission Due Date:	31/01/2022		
Project Title:	Cyber Security in Smart Grids (with IOT Consideration)		

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):	

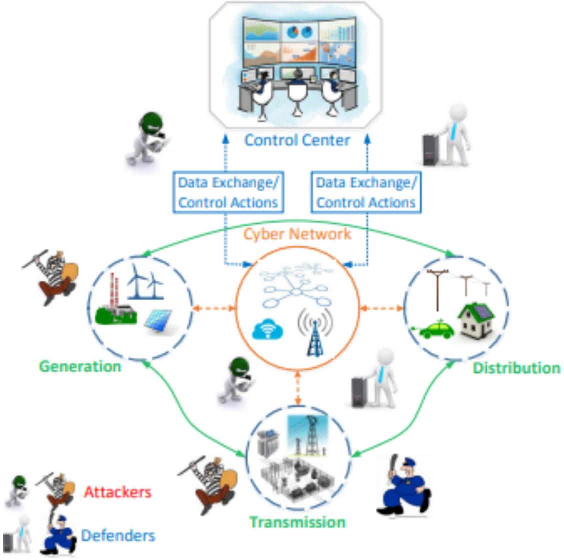
Configuration Manual

Shahid shaik
19188358

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.



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.

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

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.

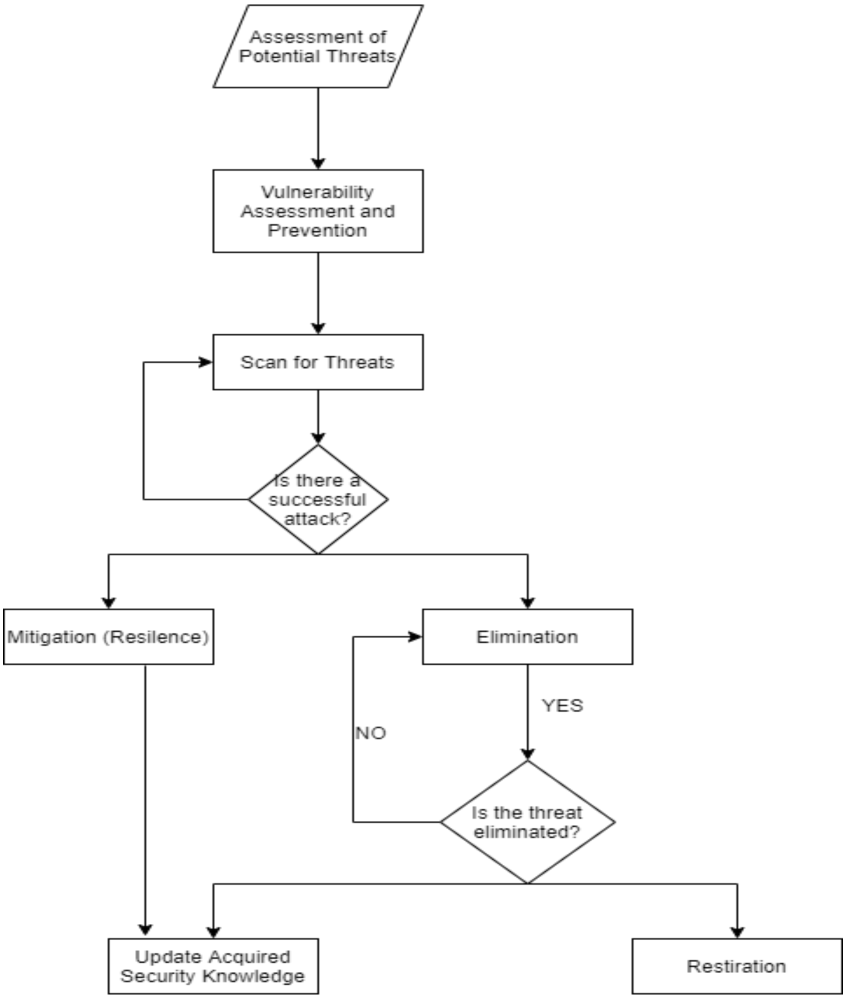

Assessment of Potential Threats
Vulnerability Assessment and Prevention
Scan for Threats
Is there a successful attack?
Mitigation (Resilence)
Elimination
YES
NO
Is the threat eliminated?
Update Acquired Security Knowledge
Restiration

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.

References

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.