Review on Cyber Security for Smart Grid System

[1]Dhanashri P.Bhuse, [2] Ashvini M. Bharambe
[1, 2]Computer Science and Engineering Department,
Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, India

Abstract—The alteration of traditional energy networks to smart grids modernizes the energy industry in terms of dependability, presentation, and manageability by providing bidirectional transportations to work, monitor, and control power flow and quantities. However, communication networks in smart grid fetchgreater than before connectivity with improvedsimple security vulnerabilities and challenges. Smart grid can be a prime target for cyber terrorism because of its critical nature. As a result, smart grid security is already getting a lot of attention from governments, energy industries, and consumers. There have been several research efforts for securing smart grid systems in academia, government and industries. This article provides a comprehensive study of challenges in smart grid security, which we concentrate on the difficulties and suggested solutions. Then, the outline current state of the investigation and future standpoints. With this artifact, students can have a more thorough considerate of smart grid security and the research trends in this topic.

Keywords: *Cyber security, Smart Grid, Network Security in Power Grid, Smart Grid Security.*

I. INTRODUCTION

The integration of electrical distribution system with communication networks forms smart grid where power and information flow is expected to be bi-directional. This transformation of traditional energy networks to smart grids transforms the energy industry in terms of consistency, performance, and manageability by providing bi-directional transportations to work, monitor, and control power flow and measurements. Furthermore, smart grid is expected to automate the systems with the help of advanced communication systems. Along with several benefits the communication networks offers in smart grid, they bring the private power control systems to the public communication networks and associated security vulnerabilities. Smart grid can be a prime target for cyber terrorism because of its critical nature. As a result, cyber security for smart grid is getting a lot of attention from governments, energy industries, and consumers. There have been several research efforts for securing smartgrid systems in academia, government and industries[1].

Conferring to National Institute of Standards and Technology (NIST) conceptual model for smart grid, communication networks connect power system components as shown in Fig. 1. There are seven logical domains: Markets, Service Provider, Operations, BulkPeer group, Transmission, Spreading and Consumer. The first three deal with data collection and power management whereas the last four deal with power and information flows in the smart grid. These domains are connected with each other through secure communication links as shown in Fig. 1.[1]

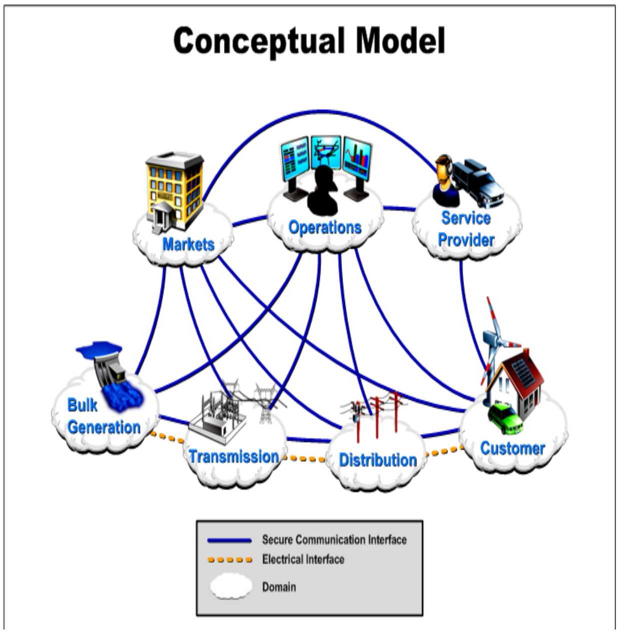

Figure 1: The NIST Conceptual Model For Smart Grid.

The conceptual model presented supports planning and organization of the different, going upassembly of interrelated networks that will compose the Smart Grid. Each domain and its sub-domains encompass Smart Grid actors and applications.The conceptual model must be constant with the legal and monitoring framework and provision its development over time. The standards and protocols recognized in the framework also must align with current and emergentmonitoring objectives and everyday jobs. The concrete model is intended to be a useful tool for regulators at all stages to assess how best to accomplish public policy aims that, along with business purposes, inspire investments in modernizing the nation’s electrical power structure and building aunpolluted energy economy [2].

II. OBJECTIVES FOR CYBER SECURITY IN SMART GRID SYSTEM

The cyber security working group in the NIST SmartGrid interoperability section has recently released an inclusive guideline for Smart Grid cyber security. There are three types of smart grid objectives such as availability, integrity and Confidentiality [3].

A) Availability: Confirming timely and consistent access to and use of information is of the most importance in the Smart Grid. This is for the reason that a loss of availability is the disturbance of access to or use of information, which may further challenge the power delivery.[3]

B) Integrity: Protecting against improper information modification or demolition is to confirm information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or demolition of information and can further make incorrect decision regarding power management.[3]

C) Confidentiality: Protective authorized constraints on dataright to use and discovery is mainly to protect personal privacy and exclusive information. This is in specificcompulsory to prevent unapproved disclosure of data that is not open to the public and individuals. [3]

From the perception of system consistency, obtainability and integrity are the most important security objectives in the Smart Grid. Discretion is the smallest critical for system reliability; however, it isbecoming more important, mostly in coordination including communications with customers, such as request response and AMI networks.

III. REQUIREMENT FOR CYBER SECURITY IN SMART GRID SYSTEM

The tools and information of cyber security are need considerate current and emerging smart-grid architecture, for the greatest part its freedoms and opportunities. Solutions must redirect several key priorities. First, among the modern cyber security effects of secret, dependability, and availability usually acquiresmaximum priority when it comes to power. This is largely because the cyberorganization manages continuous power run in the physical organization and must therefore have high availability. Creationdefinite power is available when needed is more important to most operators than making sure that information about power flows is personal. Second, developers must consider respectableconnotation and scalability. Reliant on where the solution will be working, the grid has varying real-time supplies that make efficiency essential. Mutual use of precisepolicies and networks add to this compulsary. Thetotal time is major regarding ofthe number of devices and the aggregate number of interactions amongst grid entities. Third, creators must include adaptability and solve difficulty. Devices have a trend tolast decades and can erstwhilesurvive cryptographic tools’ lifetimes. So, designs must allow for altered copy and development. Finally, the grid’s widespread, measured, and monitored infrastructure proposalslikely benefits and chances for scheming effective cybersecurity solutions. Such benefits include structured protocols and message connections, formally quantified power flows, presence of trusted third parties, and inherent termination for likelihoods. As with any important system, these material goods are only guidelines. Explanations to specific problems should with judgment consider the appropriate architectural limitations and chances. This is particularly true regarding the grid's ongoing innovation [4].

IV. FEATURES OF SMART GRID SYSTEM

There are various features of smart grid[5].

1) Dependability.
2) Suppleness in network topology.
3) Market-enabling.
4) Platform for advanced services.
5) Demand response support.

V. ADVANTAGES AND DISADVANTAGES FOR CYBER SECURITY

There are various advantages and disadvantages for cyber security [6].

Advantages

1. Care for system against viruses, worms, spyware and other unasked for programs.
2. Protection against data from stealing.
3. Defends the computer from being hacked.
4. Reduces computer cold and crashes.
5. Gives confidentiality to users

Disadvantages:

There are various disadvantages of cyber security [6].

1. Security software can be difficult to configure correctly.
2. The wrong way constituted firewalls may chunk users from carrying out certain actions on the Internet, until the firewall arranged correctly.
3. Creates the system unhurried than before.
4. Need to keep bring up-to-date the new software in order to keep security up to date.
5. Could be expensive for regular user.

CONCLUSIONS

Cyber security in the Smart Grid is a different area of enquiries that has attracted rapidly growing attention in the government, industry and academia. They were presented a complete survey of security issues in the Smart Grid. Also, bring together the conceptual model for smart grid, security objectives and security requirements. . As a result, the Smart Grid needs fine-grained security solutions intended in detail for distinct network applications, making cyber security for the Smart Grid a very successful and inspiring research area in the future.

ACKNOWLEDGMENTS

We would like to thank my honorable Principal Dr. R. P. Singh, my Head of Department, Prof. D. D. Patil, and all the respected teaching faculties of department of computer science & engineering. Also I would like to thank my parents, friend for motivating me in this paper work activity. My special thanks to all the writers of reference paper that are referred by me.

REFERENCES

[1] Danda B. Rawat , Chandra Bajracharya" Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives" IEEE SoutheastCon 2015.

[2] NIST Special Publication 1108, "NIST Framework and Roadmap for Smart Grid Interoperability Standards," Release 1.0, January 2010. [Online Accessed: December 30, 2014] http://tinyurl.com/a2m5kw2.

[3] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Computer Networks, vol. 57, no. 5, pp. 1344–1371, 2013.

[4] M. HADLEY, N. Lu, and A. DEBORAH, "Smart-grid Security Issues," IEEE Security and Privacy, vol. 8, no. 1, pp. 81–85, 2010.

[5] https://en.wikipedia.org/wiki/Smart grid.

[6] https://sites.google.com/site/xinyicyber/the-disadvantages-and-advantages-of-cyber security.