Cyber-Attacks as a Major Flaw in the Deployment of Smart Grid System in Developing Nations

Onawola, H.J, Garba, A., Ridwan, S. & Longe, O.B,
Information Systems Programme
American University of Nigeria
Yola, Nigeria
E-mail: hassan.onawola@aun.edu.ng, Olumide.longe@aun.edu.ng, garba.aliyu@aun.edu.ng, ridwan.salahudeen@aun.edu.ng

ABSTRACT

With the advent of Smart Grids (SG) technology in some countries and resultant security issues associated with the deployment and implementation, implementing cybersecurity plans becomes very vital in the smart grid installations. Smart grid systems have been proposed for developing nations like Nigeria because of its numerous advantages in resolving the challenges of unidirectional flow of information, carbon emission and other factors alike associated with traditional grid system (hydroelectric power). However, with its advantages comes associated risks such as increasing rates of cyber-threats against power and other infrastructures in developing countries such as Nigeria. This paper takes a cursory look into some major issues militating against the deployment of a smart grid system in developing nations. We explore security plans put in place to minimize the effects cyber-attack on smart grid infrastructure. The authors opined that cyber-attacks issues are critical factors for the deployment of smart grid systems by any developing nation if Smart Grids are to enhance reliability and sustainability in energy delivery. We posited that emergence of 5G technology will further enhance the security of the smart grid sand making it more sustainable and manageable.

Keywords: Smart grids, cybersecurity, sustainability, cyber-threats, emergence

iSTEAMS Multidisciplinary Conference Proceedings Reference Format
Onawola, H.J, Longe, O.B, Garba, A. & Ridwan, S. (2019): Cyber-Attacks as a Major Flaw in the Deployment of Smart Grid System in Developing Nations. Proceedings of the 22nd iSTEAMS Multidisciplinary SPRING Conference. Aurora Conference centre, Osogbo, Nigeria. 17th – 19th December, 2019. Pp 95-100. www.isteams.net/spring2019. DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V22N1P8

1. INTRODUCTION

The demand for electricity supply has been a major source of concern to many developing nations and this has been a major source of concern to the generality of inhabitants living in the country. The impact of power failure has affected the nation's economy particularly, firms and industries. Its impact varies from the experience of the dark night to a lot of damages being caused to many electrical appliances and equipment, the damages are due to frequent power failures, small and Medium-sized enterprises are the worst receiving end with respect to power outages. Therefore, to achieve a suitable goal for the power system, the conventional method needs to transform into emerging technology which is the smart grid system. The technology also comes with its own security challenges, but if the security measures and plans are well managed its benefits would be sustained for lengthy periods of time. The essence of power system design and planning is to achieve a reliability target. In order to overcome out of this challenge, the smart grid system has been proposed to be a way out.

A smart grid is a network system that can be intelligently integrated and performs all the actions connected by the users to the grid in order to effectively deliver and provide an economic and sustainable manner to provide and secure electricity supplies. Smart grid technology has been identified to be better, reliable, better power quality, integrate isolated technologies: smart grid enables better energy management, protective management of electrical network during emergency situation, better demand, supply/ demand response, reduce carbon emissions, increased demand for energy but requires more complex and critical solutions with better energy management, smart grids (SG) is a self-healing system and has many advantages over the conventional system of electricity supply, for instance it can intelligently monitor, gives communication and control the electric power supply[1].

One of the key concern is security in a smart grid system [2]. The smart grid also has its own shortcoming, the system lacks adequate intelligent to monitor the functionality of switches from the entry point to the end users meter and this development makes grid vulnerable to hacking by hackers [2]. The consequence of cyber-attacks on smart grid system operation have the conceivable to create a disruption of the power system, can cause severe damage to highly sensitive equipment of SG with great threatening to the safety of human life and properties [3]. The modern communication systems, information technologies and artificial intelligence methods of measurement of operating parameters have significantly improved electric power system in terms of observability, controllability, efficient transmission with great innovations in the area of smart grid development [4].

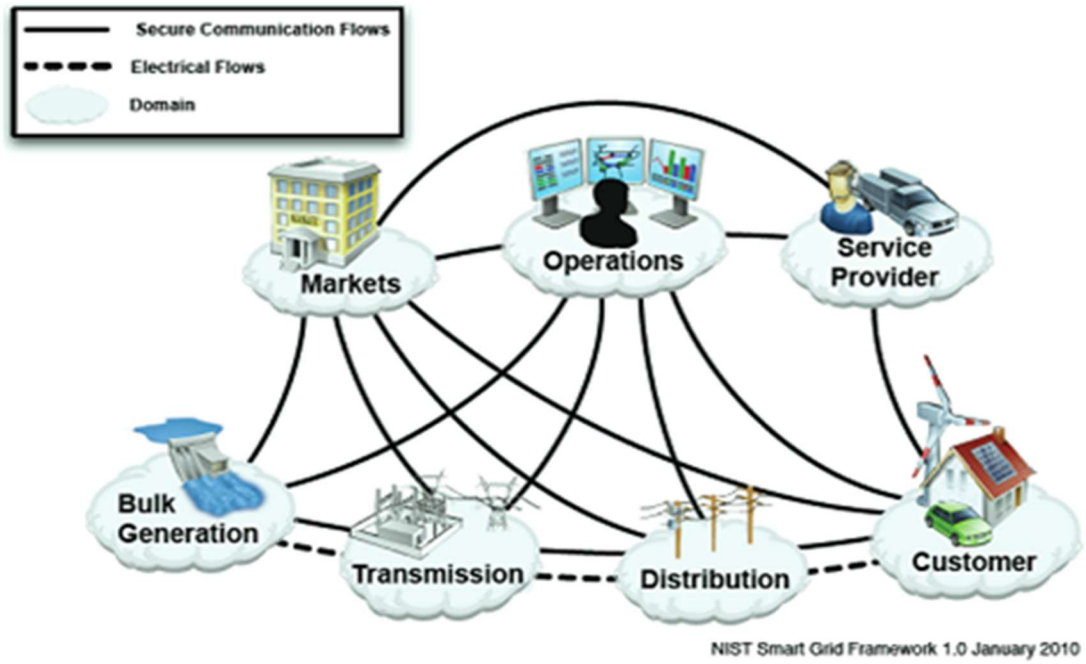

Figure 1. A conceptual model of Smart Grid

Source International Telecommunication Union (Geneva,18-21 Dec.2011.
Smart -0-34 Rev.4.Accessed 13th July,2019

It is very important to take cognizant of the following factors, the environment where the technology is to be deployed i.e. environment impact assessment(EIA) [5]. Again is there market and commercial prospect for the technology? Are the end-users ready to key into the new technology; are the policies and regulatory framework friendly? The internet of things (IoT) plays an important role in the deployment [1]. The concept of Smart grid technology is to provide a secure, reliable source of electricity generation which is considered to be more efficient way of providing energy to the end-users and to also allow the use of renewable energy for electricity sustainability, this is in contrast with the traditional way of electricity supply [6]-[7]. It is however anticipated that emergence 5G will further enhance some the challenges and make the smart grid easier to manage and affordable. The aim is to provide security plans and measures for the implementation of Smart Grid Intelligent System as a reliable means of electricity supply for developing like Nigeria.

2. RELATED WORKS

SGs has been considered to have more advantages than the traditional grid used by most of the developing nations but the challenges of deploying SGs has been a major setback for its deployment [8]. SGs is an emerging technology that has the potential to the modernized electricity power supply in developing the nation with the benefits of providing quality electricity supply to the generality of people, to achieve this goal some critical issues concerning its deployment have to be resolved [9]. The deployment of smart grids have been good but it has generated lots of security challenges which if not properly handled may ripen into cyber-attacks, energy theft, infrastructural failure, privacy breach and other challenges alike [10]. According to the International Energy Agency (IEA) using energy more efficiently has the capability to restrain carbon IV oxide emission for the next 20 years than using hydroelectric power [5].

In this modern technology very powerful computer machines, specifically, Artificial Intelligence are now being deployed in solving very difficult situations that arise in the area of power system operation, diagnosis, design and event planning [11]. The smart grid system report of 2018 shows that the incidence of cyber-attacks has dramatically increased over the last decade [3]. Appropriate cybersecurity controls are to be installed in every smart grids infrastructure to sustain cyber-attacks incident and avert interference of attacks to critical energy transfer functions [12]. Findings have shown that there are numerous threats of cyber-attacks incident specifically targeting smart grids and other critical infrastructure [13]. One of the reasons why SG is vulnerable to attack is because the technology of SG contains a big-data and proximity to attach is high [8].

Based on the above-related works the authors opined that in order to address the problem of cyber-attacks on Smart grid, security plans are required to be built into SG infrastructure right from its inception and provide adequate security measures to guide against vulnerabilities in the system before, during and after the installation SG infrastructure. Additionally, the practice of mitigating effect systems can be very useful in lessening the impact of cyber-attack.

3. PROPOSED MEASURES FOR SECURITY CHALLENGES IN SGS

Installation of SGs are very expensive and required skillful personnel, provision adequate security for its protection is very important in order to avert a total failure as a result of cyber-attack, related verses and enhanced high reliability, security and resilient in the system.

3.1 Cyber-attacks

The Internet of things is one of the technologies used in smart grids and its operations are done via an open internet that is prone to attack by the hackers thus manipulating the information between the real-time production and the utility consumption, which will have a negative impact on the end users[14],however It is a known fact that what is good today might not be good for tomorrow, therefore the challenge of cyber-attacks can be minimized by building a state-of-the-art cybersecurity capability into smart grid infrastructure and networks as they develop in anticipation for future situation. The design of such a smart grid should for the next generation to give adequate resilient to the system with controls instilled into it [3].

3.2 Planning

Avoidance of system failure by implementing cybersecurity plans in anticipation of cybersecurity attacks, additionally, this requires a sustainable holistic planning approaches, in doing this, the participation of major stakeholders like end users who uses the utilities, developer, service providers in fighting this menace is very key.Smart grid infrastructure should be provided with automated control switches (sensors) which also serves a self-healing system to protect the critical infrastructure of the smart grid.

3.3 Risk Analysis and Cost Analysis

In transiting from conventional grid to smart grid necessary protection needed to be provided, hence the call for risk analysis to evaluate the critical infrastructure of SG, threats and vulnerability impact to SG and users. Therefore, a system must be put in place to review and update the risk analysis from time to time to ensure the security of all SG infrastructures.

3.4 Mitigating effects systems

Mitigation is a process of making an attack less severe, dangerous and reduces the impact of attack, therefore, introducing mitigating effect measures can go along to solve the challenges of cyber-attacks, done by concurrently carrying out mitigation that lessens the likelihood of an attack and mitigation that lessen the consequence of an attack occurring [15]

3.5 Technology

Provision and applications of technology can be a technology that easily interfaces and synchronize with other applications to allow easier transformation from one generation to another i.e. from 4G-5G and has the ability to adapt dynamic conditions with the ability to control and secure other equipment on the grid system.

4. CONCLUSION AND FUTURE WORK

Building in cybersecurity into SG during the design, construction and installation stages is imperative to avert cyber-attacks in the SG infrastructure, its consequence can give rise to failure and unstainable system. However, in this research work, we discussed some measures that could be put in place to guide against a cyber-attacks scenario in the smart grid system. Future review of this study will further give more insight on the mitigating factors that can lessen the effects of cyber-attacks on the smart grid system.

REFERENCES

[1] "Smart-Grid-Challenges-Opportunities-For-Malaysia.pdf." .
[2] Overview of Smart Grid System," ResearchGate. [Online]. Available: https://www.researchgate.net/publication/235951354_Overview_of_Smart_Grid_System. [Accessed: 08-Jul-2019].
[3] "Smart Grid System Report," p. 93, 2018.
[4] F. Li et al., "Smart Transmission Grid: Vision and Framework," IEEE Trans. Smart Grid, vol. 1, no. 2, pp. 168–177, Sep. 2010.
[5] R. L. Ottinger, "UN Environment Guide for Energy Efficiency and Renewable Energy Laws," p. 389.
[6] T. Vijayapriya and D. P. Kothari, "Smart Grid: An Overview," SGRE, vol. 02, no. 04, pp. 305–311, 2011.
[7] D. O. Johnson, J. O. Petinrin, and S. F. Oyelekan, "Integration of Distributed Energy Resources in Smart Grid System," vol. 2, no. 6, p. 10, 2017.
[8] A. O. Otuoze, A. M. Usman, O. O. Mohammed, and A. A. Jimoh, "A Review Of Smart Grids Deployment Issues In Developing Countries," . ISSN, vol. 13, p. 10.
[9] A. Elizabeth, W. Samuel, A. Felix, and M. Simeon, "Smart Grid Technology Potentials in Nigeria: an Overview," vol. 13, no. 2, p. 10, 2018.
[10] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," Journal of Electrical Systems and Information Technology, vol. 5, no. 3, pp. 468–483, Dec. 2018.
[11] R. P. Nath and V. N. Balaji, "Artificial Intelligence in Power Systems," p. 7.
[12] C. Hawk and A. Kaushiva, "Cybersecurity and the Smarter Grid," The Electricity Journal, vol. 27, no. 8, pp. 84–95, Oct. 2014.
[13] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment," Journal of Advanced Research, vol. 5, no. 4, pp. 481–489, Jul. 2014.
[14] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," IEEE Access, vol. 7, pp. 62962–63003, 2019.
[15] E. B. Rice and A. AlMajali, "Mitigating the Risk of Cyber Attack on Smart Grid Systems," Procedia Computer Science, vol. 28, pp. 575–582, 2014.