International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

Leveraging ICT for Power Delivery and Electrification in Africa: Cyber security, Privacy and Data Protection

Onu Fergus U. and Akpan Abasiam G.
Department of Computer Science, Ebonyi State University, Abakaliki - Nigeria

ABSTRACT

The lack of proper 'security measures' on power installations can cause a major blackout which in turn can lead to a cascaded power failure. Therefore, to protect the critical power system infrastructure and to ensure a reliable power supply to the end users in Africa, smart grid security issues must be addressed with high priority. This paper presents cyber security, privacy and data protection as crucial in maintaining stable and reliable power system operations needed for Power delivery and electrification in Africa. Contingency situations which can be caused by the failure of a critical power system component can be prevented by building a 'secured smart grid' with a less possibility of power grid collapse or equipment malfunction. The paper examined available resources in cyber security, privacy and data protection initiatives to identify common themes and best practices in securing a stable power delivery and affordable electrification of Africa. It was unraveled that cyber security, privacy and data protection are key issues in securing power system infrastructure. Personnel training, online reporting centres, biometric technologies and establishment of a national database were recommended in order leverage ICT for power delivery in Africa.

KEY WORDS: Confidentiality, Cybercrime, Cyber Security, Cyberspace, Database, Data Protection, Electrification, Privacy, Smart Grid, Vulnerabilities

1.0 Introduction

The development of Information and Communication Technologies (ICTs) has given rise to a new space in which relations are conducted and in which the speed and ease with which information and communications exchanged have overcome the barriers of distance and time. Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology – including the Internet – networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalization that provides new opportunities but also entails new challenges, risks and threats. Our society's degree of reliance on ICT and cyberspace is growing daily. Knowledge of its threats, managing the risks and building an appropriate prevention, defence, detection, analysis, response capability, investigation and recovery are essential elements of the Cyber security roadmap in most African countries. Strate [7] defined **Cyberspace** as the notional environment in which communication over computer networks occurs. Therefore, a secure cyberspace is critical to the health of any African economy and to the security of the global economy. In particular, African Governments must address the recent and alarming rise in online fraud, identity theft, misuse of information online and attacks on smart devices that protect and control power grids. In the other hand, Debarati Halder et al. [1] defined **Cybercrimes** as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and groups) and mobile phones. Hence, **"Cyber-security,"** for the purpose of this paper encompasses industry and government defense strategies adopted to curb cyber-criminality in the super highway. Cyber crime has dwarfed the expectations of Governments in Africa as a potential tool to improve Africa's national GDP, job creation, elimination of mass poverty and provision of steady and affordable electricity. Smart cities**,** which is totally dependent on viable internet connectivity, has been violently attacked to the extent that smart grids in most African nations has virtually come to a halt because of the activities of cyber criminals. The activities of these evil agents have been described as the worst threat to the most formidable human innovation after the Industrial Revolution. It is indeed a colossal economic catastrophe for the developing nationals of Africa. This singular act by these agents of the devil has painted African nations black in the eyes of the international community to the extent that electricity transmission and distribution are epileptic. The huge sums of money involved in their dragnets, the absence of a functional legal framework to tackle the menace, the trade has continued to be attractive to new entrants. Worst still, the absence of forensic capability by most African security agencies to address the malady has led many of the cybercriminals to get off the hook and consequently, has encouraged potential scholars who ought to go school to now choose cyber crime as a preferred profession, leading to disastrous misplacement of societal values. This paper describe how smart grid security – cyber security, privacy and Data protection could impact on the provision of affordable electrification in developing nations of Africa.

1.1 Cyber Attacks on Smart Grid

In recent years, power system has faced several cyber related attacks which have raised the question regarding the security vulnerabilities and its large scale impact on the critical power system infrastructure. Some significant issues related to cyber-attack on the power grid are discussed:

1. In the middle of 2010, a computer worm ‘Stuxnet’ was discovered which spreads using ‘Windows’ operating system and targets Siemens industrial software and equipment to unstable power system operation [3]. This type of cyber-attack based on the intrusion of computer virus targeting industrial power plant introduces new threads to both cyber and physical systems [3].
2. On September 28, 2003, Italy and some parts of Switzerland faced its largest power supply disruption affecting 56 million people in total [3]. This blackout is restored after 18 hours in Italy resulting huge financial loss. The blackout happened because of the technical difficulties caused by the human error and Ineffective communication within the power grid operators.
3. Another large blackout occurred in the south west Europe due to the human error on November 04, 2006 [6]. Insufficient communication was also an important issue behind the blackout.
4. According to the 2011 annual report of the Repository for Industrial Security Incidents (RISI), around 35% of industrial control system (ICS) security incidents were instigated through the remote access within the cyber system [6]. Power and utility sector faced around 12 cyber security incidents between 2004 to 2008 which is around 20% increase of this type of cyber incidents compared with the previous 4 years [6]. As ICS and SCADA is playing a vital role in a smart grid infrastructure, the cyber security concern in increasing rapidly.

From the above discussion, it can be seen that some major cyber-physical vulnerabilities of the smart grid are related to the cyber issues. Therefore, Smart Grid Infrastructure Security (SGIS) must address the deliberate attacks by the cyber terrorists and industrial espionage, disgruntled employees, user errors, equipment failures, and natural disasters [6]. In order to protect the critical smart grid infrastructure, anomaly detection can play a vital role by identifying malicious data in the network.

2.0 Definition of a Smart Grid

The Smart Grid concept is evolved to make the power grid more energy efficient and intelligent. According to the US Department of Energy, smart grid can be defined as:

> *“Smart grid generally refers to a class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries. They are beginning to be used on electricity networks, from the power plants and wind farms all the way to the consumers of electricity in homes and businesses. They offer many benefits to utilities and consumers -- mostly seen in big improvements in energy efficiency on the electricity grid and in the energy users’ homes and offices.”*

Traditionally, power grid was designed to transport power from the generation plant to the end-users. Therefore, the whole power flow pattern was uni-directional and the control structure was centralized. In order to take advantage of the advanced technology to control power flow and to mitigate the ever growing load demand, new communication techniques and distributed energy resources are being incorporated within the physical power system infrastructure. Integration of distributed generations has introduced bi-directional power flows into the grid. Moreover, energy storage devices, plug-in hybrid electric vehicles, and other advanced physical components of the power system have introduced more complexity into the grid. On the other hand, deployment of the communication network (e.g., SCADA system and Advanced Metering Infrastructure) has provided more stability, reliability, flexibility and efficiency in the operation and control of this complex power system. However, increasingly the vulnerabilities of the physical system are being exposed due to malicious attacks on the cyber-physical smart grid infrastructure. Therefore, there is a need to identify the smart grid security issues related to cyber security.

2.1 Functionalities of a Smart Grid

Smart grid is the modernization of the traditional power grid which should ideally have some advanced functionalities [8]:

- Self-healing
- Motivates and includes the consumer
- Resists attack
- Increases power quality
- Accommodates all generation and storage options
- Enables electrical markets
- Optimizes assets and operates efficiently

Generally, power system is a massive and complex system and very vulnerable in terms of physical or cyber-attack.

2.2 Security Issues of Smart Grid and Associated Risks

According to [6], the security issues of a cyber-physical smart grid comprise of the following issues:

1. The physical components of the smart grid (, *Risk of cascading failures, Increase in potential adversaries, Data Privacy issues*)
2. Control centres and control applications
3. The cyber infrastructures for smart grid stable, reliable, and efficient operation and planning
4. The correlation between cyber-attacks and the resulting physical system impacts
5. The protection measures to mitigate risks from cyber threats

3.0 Protecting Smart Grid from cyber vulnerabilities

In recent years, the vulnerabilities of the smart grid has increased many times due to the wide adoption of communication network in different levels of operation and planning of a power grid. To protect the smart grid, it is important to protect the physical grid from three broad classes of cyber attacks [2] mentioned below:

- Protection from component-wise cyber attack [2]
- Protection from Protocol-wise Cyber Attack [2]
- Protection from Topology-wise Cyber Attacks [2]

3.1 Privacy

Data Privacy deals with the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. The challenge of data privacy is to utilize data while protecting individual's privacy preferences and their personally identifiable information. Moor [4)] attributed privacy as a situation if in a particular condition the individual is protected from intrusion, interference, and information access by others.

In this way, Electricity generating companies must add data to their list of their assets. These assets include, for example, customers' bills, meter readings, customer's credit card numbers etc. These assets added must be seclude from third parties who may post as an intruder or attacker. By doing this, a reliable and affordable power generation will be achieve.

3.2 Data Protection

According to SNIA organization in 2013, data protection can be defined as:

> *"Data Protection is the assurance that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable requirements. For data in power stations to be protected for reliable power delivery, we need to reliance on backup, restoration, replication and disaster recovery."*

Investigations as ascertain by SNIA organization shows that data in smart power stations can be protected through backup, restoration, replication and disaster recovery. Protecting power assets through these means can ginger reliable and affordable electrification Africa.

Conclusion and Recommendations

In recent years, the numbers of cyber attacks are increasing rapidly. The intelligent cyber terrorists with detail and advanced power system knowledge may be able to create an integrity, availability or confidentiality attack on power networks. Protection of smart grid from cyber attack is not only a concern of the Engineers, Researchers and the Utility operators; it is also the responsibility African governments to ensure the security of this national critical infrastructure. To achieve this, the following recommendations must be taken into consideration:

- Training of African Police in Cybercrime Prevention and Forensic Science for crime policy and control.
- Establishment of a national online reporting centre.
- Deployment of Biometrics and device fingerprinting supported by secure gateways and quality encryption.
- Urgent need for establishment of a single national database to gather and compile cybercrime data.

When this is done, a steady and affordable electrification will be a reality in Africa.

References

1. Debarati et al., "Cybercrime and the victimization of women: Laws, Rights and Regulations" Hershey, PA, USA: IGI Global, 2011, ISSBN: 978-1-60960-830-9.

2. Dong et al., "Protecting Smart Grid Automation Systems Against Cyber attacks," IEEE Transactions on Smart Grid, vol.2, no.4, pp.782,795,Dec.2011.

3. McMillan, R. (2010,sept.) Siemens: Stuxnetworm hit industrial systems. Available: http://www.computerworld.com/article/.../siemens--stuxnet-worm-hit-industrial-systems.htm....

4. Moor, J., "How to invade and Protect Privacy with computers.'' The Information Web. Ed. Carol c. Grould Boulder: West view Press, 1987, 57-70

5. Robert et al., (2013, Aug.) *Data Protection Law in the USA.* Available:

http://a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf

6. Sridhar, S. (2012), "Cyber–Physical System Security for the Electric Power Grid," Proceedings of the IEEE, vol.100, no.1, pp.210-224, Jan.2012.

7. Strate, L.,"The varieties of Cyberspace: Problems in definition and delimitation''. Western Journal of Communication. 63 (3): 322-3,Sept.1999

8. The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements", August 2010.

Fergus Uchenna Onu holds a Ph.D in Data Communication and Computer Networks, a Master's degree in Computer Science (EBSU–Nigeria) and a Bachelor of Engineering in computer science and Engineering (ESUT-Nigeria). He has a flare for software development and computer programming and languages. He works as a senior lecturer in the Department of Computer Science, Ebonyi State University, Abakaliki Nigeria. He has authored over 30 journal articles addressing various IT concerns.

Abasiama Akpan holds a bachelor Degree in Computer Science (Calabar), Master's degrees in information Technology (Lagos), Geographic information system (Port Harcourt) and a Master of Business Administration (Lagos). Currently, he is a Doctoral research student, in the Department of Computer Science, Ebonyi State University, Abakaliki- Nigeria. He has an inclination towards the domain of information security. He is an avid reader of texts on trending technologies. He enjoys writing and considers it as way of disseminating knowledge.