Cyber-Infrastructure Connections and Smart Gird Security

Alex R Mathew

Abstract*: The architecture of the smart grid combines the communication grid and physical power grid in a sole huge network. Smart grid has various security threats like cyber-attacks, physical attacks or natural disasters. The mentioned threats can lead to the breach of the user's privacy, failure of the infrastructure, energy theft, blackouts endanger the safety of the operators among many more. For this reason, there is need to ensure that the smart grid cyber security is adequate to prevent any of these threats. Adequate security will as well ensure that the smart grid operates adequately as it is viewed that is by providing safe, reliable and uninterrupted supply of power to the consumers with a regular flow of end to end information that are all secure. The smart grid environment will ensure that the electric power infrastructure is modern. This is majorly by combining the present functionalities and the future ones with the upgraded requirements to the users.

***Keywords*: Network communication, smart grid, cyber security, threats.**

I. INTRODUCTION

The smart grid security is important because it allows the operation of the power system to be more reliable. Ensuring that the smart grid is secure will guarantee that the collapse of the grid is not any possible since only robust equipment will be used. In the past days, there has not been a proper smart grid security and this brought about several blackouts some of which could even result to cascading malfunctions. For this reason, it is very essential to ensure that this power system infrastructure is protected at all times. This will ensure uninterrupted and reliable supply of the power to the consumers.The smart grid environment ensures that the electric power infrastructure is modern. This is majorly by combining the present functionalities and the future ones with the upgraded requirements to the users. Cyber systems need to be integrated to ensure that the smart grid is possible. Integration of the cyber system with the traditional power systems has not only made the grid more energy efficient but modernized too. However, the integration of the cyber system has also introduced some vulnerabilities like cyber-attack challenge that make the national infrastructure even more fragile as well as the satisfaction of the users. ICT features, and the traditional power supply system, the security concerns related to cyber systems must be ensured to keep the smart grid effective at all times. Even

This is the main reason why smart grid security is more essential, as it ensure that the components of the power systems are not damaged and that every user is safe at all times.Because smart grid is only possible through integration of cyber systems,

though smart grid is expected to greatly advance the users' experience of power distribution, communication and control of consumption, there are security risks that the system comes along with like cyber-attacks, physical attacks or natural disasters. Majorly in the information system and network communication sectors. This therefore affirms that the cyber security when it comes to smart grid is vital.

II. METHODOLOGY

SMART GRID CYBER SECURITY

The smart grid is adding new ICT features to the existing electrical powers systems. It is therefore vibrant that smart grid will greatly advance the electricity dissemination and consumption control to benefits the users, the grid operator and the electricity suppliers. Yet, the improved services and procedure will come with a cost of subjecting the whole electricity network to new dangers mainly in the security sector of information systems and network communication. Conversely, it will as well introduce various new security perils in the system [7]. Every user depends on the electrical power grid for electricity supply. This dependence of electricity brand the electrical power grid a vital asset. Disrupting this power supply has a huge impact to the entire society. Because of this, security of the electrical power grid is very essential. The smart grid will launch even more new security challenges that are connected to the automation of the system, collection of data, communication requirements and new technologies. The network of the smart grid is its pillar. This is because it connects the various features of the smart grid together as it enables a two-way communication amid the network. And thus, several steps like ensuring the security of the data, stable power supply as well as secure flow of information with no breach will have to be given more attention.

III. POWER SUPPLY BLOCK DIAGRAM

Power supply block diagram aids in regulating the power supply that comes from the transformer centers or substations to the users.

Revised Manuscript Received on August 30, 2019.
* Correspondence Author

Alex R Mathew*, Department of Computer Science and Engineering, Cybersecurity Awareness Training, Information Technology, India.

The power is stepped up or down and rectified and converted to AC and later to DC by the filter.

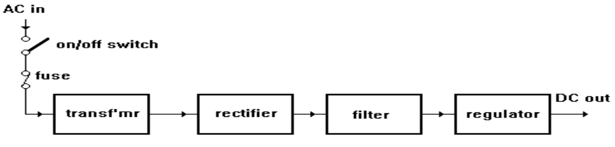

Figure 1: Power Supply Block Diagram

With smart grid, the block will need addition of some ICT technologies to ensure that the power moderation from the substations is automatic and that any information from its communication network cannot be attacked at any time. This block plays a huge role in ensuring aims of smart grid power supply system is achieved. However, it requires tight security to ensure that its automatic power regulation and generation is not interrupted. A system that detects any kind of intrusion should be adopted to the block to make its security more efficient.

IV. ALGORITHM:

Like any other system, smart grid will need techniques that will aid in detection of anomalies. Algorithm will be used to reduce the data and improve the work of detecting anomalies in a form of knowledge-based guidelines. To ensure that the important power system infrastructure have been protected, an inclusive framework e.g. neural network based on probability need to be developed. This will aid in detecting relays from attacks on data. The figure below illustrates a security-based framework smart grid.

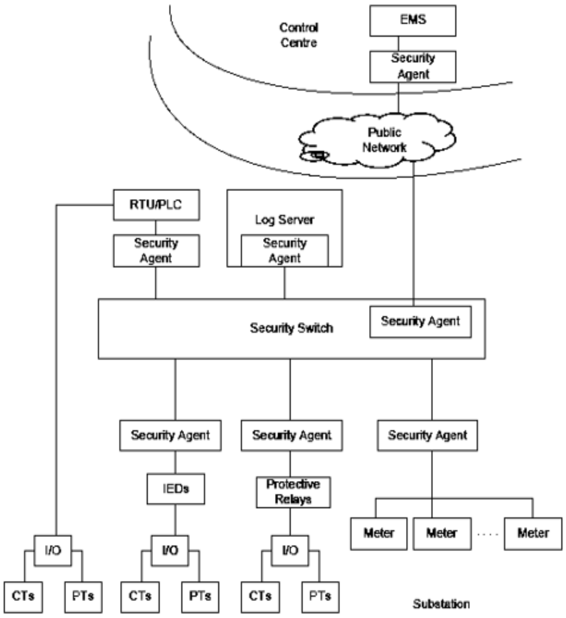

Figure 2: A Security-Based Framework For Smart Grid Systems.

While choosing and using the requirements to use in this framework, the directions of the architecture is essential to ensure that it works well with the technology in place and other systems. Also, strategic placements of the requirements like smarts meters strengthen the security. The encryption algorithms can as well be applied to ensure data transferred in the whole network remains safe [9]..

V. FLOW CHART

While developing and analyzing the suitable framework for these security issues, having a draft of how the system ought to work is essential as well. In this case, a flow chart will provide a presentation of how the effective security framework will work from monitoring the real time data communication to detecting any anomalies that may arise.

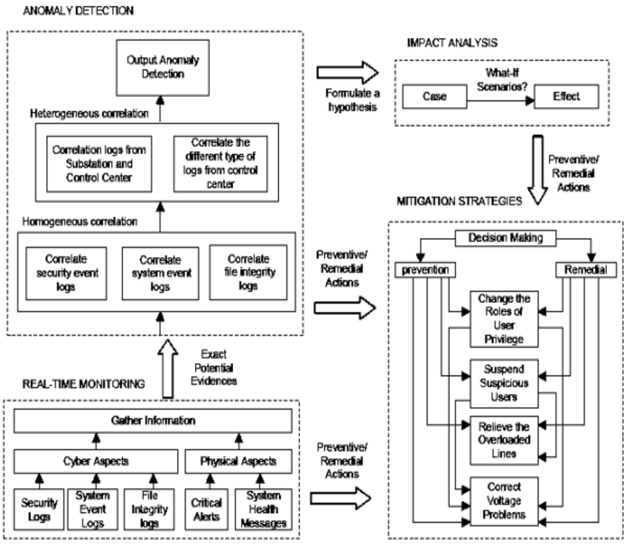
ANOMALY DETECTION
Output Anomaly Detection
Heterogeneous correlation
Correlation logs from Substation and Control Center
Correlate the different type of logs from control center
Homogeneous correlation
Correlate security event logs
Correlate system event logs
Correlate file integrity logs
Formulate a hypothesis
IMPACT ANALYSIS
Case
What-If Scenarios?
Effect
Preventive/ Remedial Actions
MITIGATION STRATEGIES
Decision Making
prevention
Remedial
Change the Roles of User Privilege
Suspend Suspicious Users
Relieve the Overloaded Lines
Correct Voltage Problems
Preventive/ Remedial Actions
Exact Potential Evidences
REAL-TIME MONITORING
Gather Information
Cyber Aspects
Physical Aspects
Security Logs
System Event Logs
File Integrity logs
Critical Alerts
System Health Messages
Preventive/ Remedial Actions

Figure 3: Flow Chart

This flow chart explains an overview of how the smart grid security system will communicate, detect and handle any attack that is detected while the power supply remains safe and uninterrupted [5].

VI. RESULT ANALYSIS AND DISCUSSION

Generally, smart grid is a huge and a more complex system that is so vulnerable as it has many attacks both cyber attach and physical attack. However, implementing the said security measures example applying the appropriate cyber systems to the power supply block diagram will advance functionalities such as self-healing. This implies that the system will be able to resume to its working stability even after being interrupted. And because this functionality also controls high level of decentralization, blackout is thus prevented. Deployment of the appropriate algorithms and requirements in the system will give the smart grid system ability to resist attacks [1]. This way, the grid infrastructure will be protected as it serves the users. The information communication networks involved from both ends of the system are very essential, more like the backbone of the smart grid system which needs to be secured. The proposed measures will aid to ensure that the applied framework is secure enough to give the required security. While security of the implemented cyber system is given much attention, physical security is also important to ensure the power generation, transmission, distribution and control are all effective and that users do not get challenges with the improved technology. Also, smart grid incorporates many new technologies that make in more complex. This is another reason why its security needs to be upfront to not allow any potential adversaries. With every feature and new technology added to the smart grid system increases the number of nodes.

This means that the entry points are also increasing and if any of
them can give access attackers will be right in the system. So, as the complexity of the smart grid system increases, its security ought to increase as well to ensure its safety from attackers [2]. Also, these attacks can result to sudden failure of the smart grid if attacked. This is another reason as to why the nodes, from all points need to be secure to retaliate the attacks. Additionally, smart grid systems tend to collected a lot of information compared to the traditional power supply system. These information flow from end to end and back and should be kept private. If any intrusion happens, the data will lose its confidentiality posing risk of other related attacks to the system.

Actually, smart grid cyber security is so vital to ensure that the system is effective as expected. Providing safe, uninterrupted and reliable power supply. This will be achieved if the cyber security and physical security are attained to ensure that the features of the smart grid, availability of data, confidentiality of data and data integrity are all achieved and thus no attacks [10]. With new technologies, appropriate requirements, right security measures like use of algorithm, and a suitable security-based framework, all anomalies and attack attempted will be detected and corrected instantly.

VII. CONCLUSION

For the grid to be made smarter, various inventive like the ones mentioned above, use of algorithms to ensure a fit security-based framework, need to be taken globally. The measures will modernize the grid as well as improving the functionality of the entire system making it more stable, efficient and reliable. However, of the measures taken, security issues need to be looked at with more attention. This is because, all the desired qualities of the smart grid will be possible only if the security of the system is achieved and maintained. Managing the huge system with several nodes if there is adequate security, from the attackers will also be less of a worrying job. With adequate security, the users will be able to get stable and uninterrupted supply of power. Also, it is essential to note that an accurately designed framework in contrast to the cyber-attacks need to address all the possible cyber-crimes that may be related in an intricated cyber physical electricity grid infrastructure. This means that the focus should not only be on cyber-attacks but should as well consider the unintended ICT related variances like human operator error, equipment failures, software errors and natural disaster problems.

REFERENCES

1. AlMajali A, Viswanathan A, Neuman C (2012) Analyzing resiliency of the smart grid communication architectures under cyber attack. In: Proceedings of the 5th workshop on cyber security experimentation and test, Bellevue, 6 Aug 2012
2. P. McDaniel and S. McLaughlin, “Security and Privacy Challenges in the Smart Grid,” IEEE Security Privacy Magazine, vol. 7, no. 3, pp. 75–77, 2009. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5054916
3. L. Snider, “Xcel smart grid costs blow up, PUC orders more transparency,” 2010. [Online]. Available: http://www.coloradodaily.com/cu-boulder/ci 14346139#axzz17mrIQg00http://www.smartgridnews.com/artman/publish/Business Policy Regulation News/Boulder-SmartGridCity-Cost-Overruns-How-Bad-is-it-Really-1868.html
4. Li H, Gong S, Lai L, Han Z (2012) Efficient and secure wireless communications for advanced metering infrastructure in smart grids. IEEE Trans Smart Grid 3(3):1540–1551
5. Y. Jiaxi, M. Anjia, and G. Zhizhong, Cyber Security Vulnerability Assessment of Power Industry. IEEE, 2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper. htm?arnumber=4142474
6. D. Watts, “Security and Vulnerability in Electric Power Systems,” in 35th North American Power Symposium 2003, 2003, pp. 559–566. [Online]. Available: http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.69.4104&rep=rep1&type=pdf
7. R. Berthier, W. H. Sanders, and H. Khurana, “Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions,” in 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 350–355.
8. Wang S, Cui L, Que J, Choi D, Jiang X, Cheng S, Xie L (2012) A randomized response model for privacy preserving smart metering. IEEE Trans Smart Grid 3(3):1317–1324
9. Zhang Y, Wang L, Sun W, Green RC, Alam M (2011) Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans Smart Grid 2(4):796–808
10. Zonouz S, Rogers K, Berthier R, Bobba R, Sanders W, Overbye T (2012) SCPSE: securityoriented cyber-physical state estimation for power grid critical infrastructures. IEEE Trans Smart Grid 3(4):1790–1799

AUTHORS PROFILE

Ph.D. in Computer Science and Engineering (Cyber Security)
Certified Information Systems Security Professional- CISSP - (ISC)2
Microsoft Certified Solutions Expert – MCSE - (Microsoft)
Certified Ethical Hacker – CEH- (EC-Council)
Cisco Certified Network Associate (CCNA) – (Cisco)
Computer Hacking Forensic Investigator - CHFI- (EC-Council)
IBM Certified Ecommerce Specialist
ZAP Certified Web Designer
Security+ (CompTIA)
ECSA (EC-Council)
CPSA(CREST)
Memberships:
IEEE, Cisco, EC Council, CompTIA, IBM, Microsoft, CSTA.

Alex's areas of expertise include Cyber Security, Ethical Hacking, Cyber Crimes and Digital Forensics Investigation. He is a Certified Information Systems Security Professional and the founder of several cyber security awareness initiatives in India, Asia, Cyprus and Middle East. With over 20 years’ experience of consulting and training has developed a large skill set and certification set. He was instrumental initiating and organizing a number of conferences. He has 100+ publications with IEEE, ACM and Scopus Indexed International Journals. Dr.Alex has received a number of awards including the Best Professor, Best Presenter etc. He is a frequently invited speaker and panelist, reviewer at International conferences related to Cyber Security, Technology, Innovation and education. Alex's profile describes a confident and outgoing individual who enjoys the company of other people. He has a persuasive, open style with others, and develops interpersonal relationships quickly and relatively easily. His levels of self-confidence mean that he rarely doubts his abilities in a social situation, although he may find it a little harder to deal with practical or impersonal situations. Alex's communicative and open style means that he tends to be trusting of others, or at least confide information more readily than many other personality types. Because of his social orientation, however, he finds it rather difficult to deal with rejection by other people, thriving as he does on their positive attention. His current research activities are directed towards Cyber Security, Internet of Things (IoT), Security in Next Generation Networks, Smart Technologies, Cybercrimes Investigations.