Available online at www.sciencedirect.com

ScienceDirect

Journal of Electrical Systems and Information Technology 5 (2018) 468–483

www.elsevier.com/locate/jesit

Review

Smart grids security challenges: Classification by sources of threats

Abdulrahaman Okino Otuoze [a,b,*], Mohd Wazir Mustafa [a], Raja Masood Larik [a]

[a] *Department of Power Engineering, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia*
[b] *Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, University of Ilorin, Ilorin, Nigeria*

Received 24 December 2016; received in revised form 14 August 2017; accepted 5 January 2018
Available online 7 February 2018

Abstract

Smart grids (SGs) deployments have made power systems operation more efficient by the application of distributed computing schemes in grids' interoperation. However, these schemes have triggered various security issues which are growing to be of major concerns. Physical attacks, cyber-attacks or natural disasters are major notable form of threats to SGs deployment which could lead to infrastructural failure, blackouts, energy theft, customer privacy breach, endangered safety of operating personnel, etc. Hence, the need to critically examine the security issues aimed at preventing possible threats or failures. In this review, various security challenges and threats are discussed with respect to their possible sources of occurrence. These threats are then classified and a framework for achieving more secured SGs is suggested.
© 2018 Production and hosting by Elsevier B.V. on behalf of Electronics Research Institute (ERI). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Keywords: Smart grids; Security; Threats; Sources; Classification

Contents

1. Introduction . . . 469
2. Smart grid security challenges and objectives . . . 471
   2.1. Smart grids security threats and challenges . . . 471
   2.2. Smart grids security objectives . . . 471
3. Related works and some introduced techniques . . . 472
4. Smart grid security threats classification by sources . . . 474
   4.1. Technical sources of smart grids threats . . . 474
      4.1.1. The infrastructural security . . . 474
      4.1.2. Technical operational security . . . 477
      4.1.3. Systems' data management security . . . 478

* Corresponding author at: Department of Power Engineering, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.
E-mail addresses: ooabdulrahaman2@live.utm.my (A.O. Otuoze), wazir@utm.my (M.W. Mustafa), rmlarik@gmail.com (R.M. Larik).
Peer review under the responsibility of Electronics Research Institute (ERI).

Production and hosting by Elsevier

https://doi.org/10.1016/j.jesit.2018.01.001
2314-7172/© 2018 Production and hosting by Elsevier B.V. on behalf of Electronics Research Institute (ERI). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

4.2. Non-technical sources of smart grids threats . . . 478
4.2.1. Environmental security . . . 478
4.2.2. Government regulatory policies and implementation . . . 478
5. The proposed framework . . . 479
6. Conclusions and recommendations . . . 480
Funding . . . 480
Acknowledgments . . . 480
References . . . 480

1. Introduction

Smart girds (SGs) deployments have improved the intelligence of grid system's interoperation by the provision of multi-directional information flow between any two or more units in the system to achieve a revolutionized power industry hence, providing adequate data from metering to substations, distributions, transmission and generations, for increased security, resiliency and efficient control and monitoring of assets and services (Camarinha-Matos, 2016; Farhangi, 2010; Ghansah, 2009; Kumar et al., 2014). The intelligence is achieved by incorporating processors in each component of the power systems, with each component having a robust operating system and independent agents connected to smart sensors linked to its own component or substation to form a large distributed computing platform. This enables it to access its own operating conditions and report to its neighbouring agents via the communications paths, circuit breakers and communication ports for the processors (Amin and Wollenberg, 2005; De Santis et al., 2017; Farhangi, 2010; Gao et al., 2012; Lawrence et al., 2017; Wang et al., 2011).

The conventional power systems are being upgraded worldwide to deliver these advantages which include reliability, security and flexibility in energy distribution, power consumption monitoring, demand side management (DSM), enhanced optimized network traffic, shorter downtimes, minimized failures, reduced grid losses, regulated supply and demand, and generally improved grid operations and services (Calderaro et al., 2011; Clastres, 2011; El-Hawary, 2014; Moretti et al., 2017), etc. With the increased availability of sophisticated computing, communication and measurement technologies, the system's emergency response will be greatly improved. SGs also provide protections which are not provided by the central control systems or the protection schemes (Amin and Wollenberg, 2005; Khelifa and Abla, 2015) for the power infrastructure from the utility end and for smart homes (Abdulrahman et al., 2016; Komninos et al., 2014).

In the popular framework provided by the United States National Institute of Standards and Technology (NIST) in 2010, SG is depicted in a model clearly showing a two-way interaction between units. IEEE had this model modified and explained that the interaction could be enhanced to be multidirectional as shown in Fig. 1 (Scribellito, 2015), and to provide for improvements and easy expansion. The improvements and expansion of SGs systems and networks in

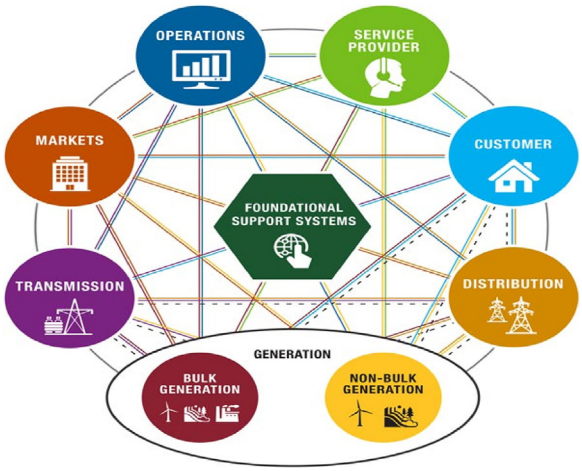

Fig. 1. Modified NIST conceptual model of SG architecture.

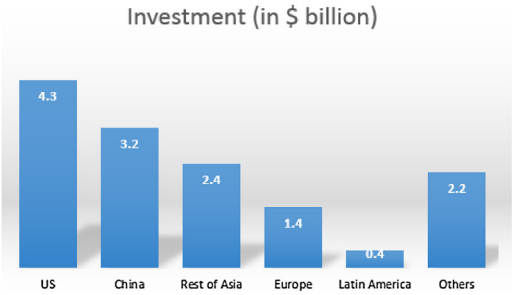

Fig. 2. SGs investment by region as at 2012.

the areas of distributed intelligence and broadband capabilities, have greatly enhanced the efficiency and reliability, climate remediation or any state-defined problem but has on the other hand, posed increased threats (Clastres, 2011; Khurana et al., 2010; Metke and Ekl, 2010; Sanjab et al., 2016). This is due to the huge data collection and transfer in the machine2machine (M2M) interaction and interoperation of the emerging power systems networks.

Also, most electrical power grid systems use the ground wire with an optical fibre, operating efficiently over long distances with reduced losses making it fast, reliable and more secured (Alam et al., 2017; Wang et al., 2011). The optical fibres facilitate the deployment of SGs thus, eliminating the need for additional communication capacity. While supporting the requirements of SG, the TCP/IP protocol currently being deployed failed to provide requisite security for communication among the infrastructural components (Goel and Hong, 2015). In general, the presence of communication nodes has rendered the energy sector more vulnerable to attacks, hence, the need for a real-time operational intelligence of all the interconnected components for improved security, load forecasts, demand side management (DSM), billing information and better utilization of renewable energy systems (Doh et al., 2015; Goel and Hong, 2015; Lawrence et al., 2017; McDaniel and McLaughlin, 2009; Sanjab and Saad, 2016).

In addition, the vulnerabilities could be explored by adversaries to cause system failures in form of possible transmission sequence failure, terrorism, cyber-attacks, vandals, theft, etc. Other possible threats include those of natural disasters and possibly, from some identified system disturbances such as voltage and frequency instability issues (Amin and Wollenberg, 2005; Ghansah, 2009; Goel and Hong, 2015; Khelifa and Abla, 2015; Komninos et al., 2014; Lee and Brewer, 2009; Moslehi and Kumar, 2010; Obi et al., 2014), or even due to inconsistencies in government policies and implementations among other factors.

Several research works on SGs focus on the involvement of consumer in the active operation of the power balance by introducing technical operation systems as well as economic incentives to facilitate flexible demands (Li and Zhang, 2010; Lund et al., 2012). These studies and improvements of the operational securities are very important since the system is complex and the associated infrastructural resources are very expensive. Moreover, heavy investments are been committed worldwide (Fig. 2; Rogers, 2013) and hence, necessary security measures must be taken to prevent damages which may in turn pose danger to either the infrastructures or personnel.

The grid is central to the operation of energy infrastructure and it is expected to mature in coping with future expansion provision. This has mandated development of a defence monitoring mechanism that can efficiently process the complex data in the evaluation of system status, failures or threats identification, prediction of threats, suggestion of remediation while reliably ensuring adequate operational security provisions of the grid (Ghansah, 2009; Goel and Hong, 2015; Khurana et al., 2010; Kosut et al., 2011; Lee and Brewer, 2009; Li and Zhang, 2010; Y. Liu et al., 2011; Sanjab and Saad, 2016; Sanjab et al., 2016; Sha et al., 2016; Yu and Xue, 2016).

In this article, identified threats to SGs deployment are classified and discussed based on technical and non-technical sources of threats. It is hoped that this classification gives explicit framework for easy tracing and curbing of threats in SGs deployment.

The rest of this paper is organized as follows: Section 2 highlights the security challenges as well as the objectives of a well secured SG network while in Section 3, some related works from literatures including techniques adopted in solving some identified threats or failures are presented. Section 4 gives the classification of threats by sources and explanation on each of the selected source of threats. A suggested framework for achieving a secured SG is presented in Section 5 while Section 6 gives the conclusion and recommendation for further works.

2. Smart grid security challenges and objectives

Threats refers to the various possible actions that may be influenced either by artificial or natural means, against a system (Mendel, 2017). These threats do not represent failures but may result in failure if necessary actions are not taken. Hence the need to study the threats and challenges as well as a set objective for a well secured SG.

2.1. Smart grids security threats and challenges

SGs architecture and infrastructure are faced with myriads of security threats and challenges ranging from thefts, cyber-attacks, terrorism, natural disasters, etc. In the event of SG's failure due to any of the threats, possible consequences include power system blackouts (small and large outages), SG IT infrastructure failures, false visualization of the actual system's condition, cascade failures, damaged consumer devices, energy market chaos, endangered human safety, etc.

Various security threats and challenges of smart grid have been highlighted in Goel and Hong (2015), Khelifa and Abla (2015), Lee and Brewer (2009), Li et al. (2010) and Sanjab et al. (2016) and many other research works to include risk of breach of high volume of sensitive customer information by adversaries; thefts, physical components damage, malware propagation in the cyber systems, instantaneous system malfunctioning; distributed control devices vulnerability; lack of physical protection against natural or environmental disasters such as floods, earthquakes, fire outbreaks, tsunamis, explosions, landslides, dangerous radiation leaks, pollutions, dust corrosions; Inadequate control mechanisms in the conventional systems which failed to account for cyber threats; trade-off between security provisions and performance of the systems; ageing infrastructure especially that most of the installations were made several decades ago; Industrial bottlenecks players complexities, etc. Consequently, various sectors are rendered vulnerable by these threats and challenges.

These threats and challenges have prompted research focus towards studying various privacy and security issues by developing techniques for curbing identified threats to improve its security and resilience. Some of these works (Amin, 2000; Anderson, 2010; Calderaro et al., 2011; Delgado-Gomes et al., 2015; Doh et al., 2015; Hasan and Mouftah, 2015; Kezunovic, 2011; Khurana et al., 2010; Lee and Brewer, 2009; Li et al., 2010; Li and Zhang, 2010; McDaniel and McLaughlin, 2009; Metke and Ekl, 2010; Rahman et al., 2015; Russell and Benner, 2010; Sanjab and Saad, 2016; Sanjab et al., 2016; Shahid, 2014; Yip et al., 2014; Zhang et al., 2010) deal with various aspects of the security challenges.

In a broad view, the security challenges can be examined in terms of the authentication, authorization, and privacy of the technologies (Lee and Brewer, 2009; Metke and Ekl, 2010) depending on the security levels; from the technical and non-technical standpoint depending on the source of the security threats; from human and non-human angle according to the cause of threats; from a fault or breakdown of a unit as generation, transmission, distribution or substation operational failure; from natural or non-natural cause according to the factors responsible, etc.; or in terms of deliberate cause e.g. organized crimes involving hacking, rioting, terrorism, cybercrimes, vandals, energy theft, sabotage, coercion, disruption of services, etc. or undeliberate causes e.g. failure of equipment, commanding operation due to false data injection, information leakage to external source (Khelifa and Abla, 2015; Sanjab et al., 2016); or viewed as low, moderate and high based on the impact levels (the effects on systems' operations, assets or personnel) (Lee and Brewer, 2009). The detailed framework explained above is as summed up in Fig. 3.

2.2. Smart grids security objectives

Given the interconnectivity and interdependency of the infrastructures, the demand for reliable and resilient electricity supply system therefore, is key and must be well structured for a safe and efficient energy delivery (Amin, 2000; Ruj and Pal, 2014a). Hence, well-articulated security objectives are generally considered for ensuring an efficient and reliable operation. These objectives must cover all possible expansion and improvement plans for future grids.

Also, the expansion of the grid for large-scale integration of renewable power into the electricity supply such as distributed generation units, is also of utmost priority since it has further increased the security requirements between electricity production and consumer demands (Li and Zhang, 2010; Lund et al., 2012).

A secured SG must therefore, be authentic, available and confidential; possess high level of integrity and efficiency, possess high level of authentication, acceptability, reliability, robustness, flexibility, resiliency (self-healing)

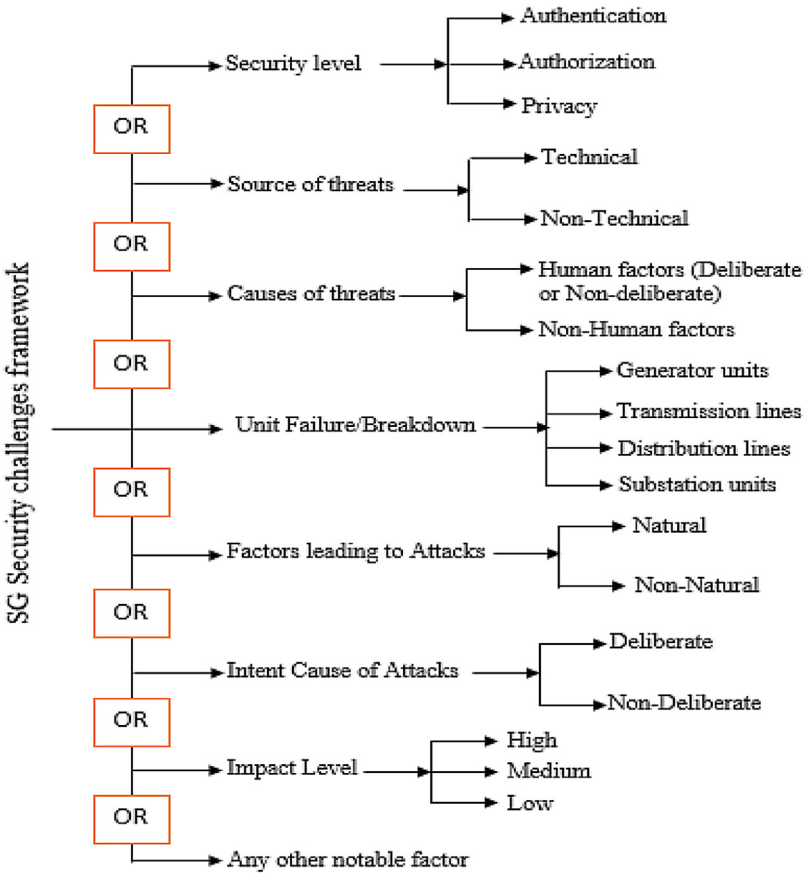

Fig. 3. Framework for identifying smart grid security threats and challenges.

and accommodates maturing electricity markets. In addition, it must have high level of accessibility and observability, controllability, facilitates expanded deployment of renewable energy sources as well as improved system's performance while offering reduction in cost of operations, maintenance and efficient system planning (especially for future expansion) (Amin, 2000, 2008; Amin and Wollenberg, 2005; Bigerna et al., 2015; Doh et al., 2015; El-Hawary, 2014; Gao et al., 2012; Ghansah, 2009; Khan et al., 2016; Khelifa and Abla, 2015; Khurana et al., 2010; Komninos et al., 2014; Lee and Brewer, 2009; Momoh, 2009; Sanjab et al., 2016; Wang et al., 2011; Yu and Xue, 2016).

Standard bodies such as US Department of Energy (DOE), National Institute of Standard and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), Electric Power Research Institute (EPRI), Google, Microsoft, General Electric (GE), North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), ANSI, and hosts of other research institutes, centres and professional bodies, have played important role in ensuring the provision of sustainably deployed SG system. These standard bodies are especially noted for their research contributions and investments in the subject matter (Ghansah, 2009; Kuzlu et al., 2017; Metke and Ekl, 2010). Hence, well-harmonised security objectives for SGs will further enhance its maturity, resiliency and sustainability.

3. Related works and some introduced techniques

So much research efforts are being put in place for enhanced security and resiliency of the SG by researchers across the world using various techniques to curb the challenges posed in various forms. Interestingly, previous works only seek to address an issue or give a broad description with no reported emphasis to sources of threats. Some related works on SG security aimed at proffering solution to some identified threats are discussed below.

A Petri Net (PN) was modelled in Calderaro et al. (2011) with detailed analysis and application of failure identification in SG. The model was however limited to the capture of the details of the protection system in a distribution

system with distributed generations (DGs) for failure identification or detection of faults. Similarly, De Santis et al. (2017) in their study, developed a system for detecting faults in the grid operation of medium voltage feeders in Rome, Italy. They employed hybridization of evolutionary learning and clustering in carrying out a synthesized data-driven model of fault phenomenon.

In terms of security level, Fig. 3 shows the need for an authentication but an improved approach is to provide for a cross authentication. This helps in reliable operation of some key components of the grid as articulated for Advanced Metering Infrastructure (AMI) using Public Key Infrastructure (PKI) technologies (Hasan and Mouftah, 2015; Metke and Ekl, 2010). Also, encryption service for smart grid advanced metering infrastructure (ES4AM) for various encryption approach of the AMI has been proposed and presented in Hasan and Mouftah (2015) while a Dynamic Stochastic Optimal Power Flow (DSOPF) computational algorithm was presented in Momoh (2009) as a tool needed in SG architecture to achieve grid security and efficiency with advanced DSM capabilities while the security and privacy using homomorphic encryption was well articulated in Li et al. (2010).

Increased risk of cascade effects which may propagate from one system to the other, in case of failure(s), is thought to be catastrophic since critical infrastructures of the grid are interdependent (Amin and Wollenberg, 2005; Khurana et al., 2010; Ruj and Pal, 2014b; Scala et al., 2015). In his work, Rahnamay-Naeini (2016) presents Interdependent Networks by Optimum Allocation of Interdependencies for achieving a cascade-resilient system capable of minimizing cascade effects in case of failure, while the effects of targeted attacks in cascading failures were presented in Amin (2000) and Ruj and Pal (2014b). An optimization model for a minimal cost procurement plan for back-start sources for restorative self-healing presented in Qiu et al. (2016). Also, Sha et al. (2016) presented a secure and efficient framework for protecting isolated smart grid devices.

In Xu et al. (2016) and Shahidehpour et al. (2016), enhancements of power grid resilience in the utilization of micro-grids to restore critical loads (e.g. hospitals, street lights, internet and some other communication equipment, etc.) were explored. The works seek to provide for effects of extreme conditions (e.g. flood, earthquake, hurricanes, etc.) on the distribution feeders when the utility power is unavailable. A well-structured defensive islanding for the improvement of grid resilience is also presented in Panteli et al. (2016). Records of failures of distribution apparatus can also be modelled to predict the failures associated with the system for substantial improvement aimed at regulated preventive actions to avoid catastrophic failures as presented in Russell and Benner (2010) and Zhang et al. (2010).

Because communication is key in SG deployments, utilities aim for increased capabilities in communication and data management by improving the intelligence of their infrastructure for the expansion of new applications and processes (Farhangi, 2010; Khan et al., 2016; Sha et al., 2016) in SG security and resilience. Wireless networks with the deployment of 4G worldwide Interoperability for Microwave Access (WiMax) as an effective management solutions for securing the smart grid was presented by Anderson (2010). Internet of Things (IoT) are also being utilized and deployed for smart grids in relation to smart cities, buildings, and home automation network which also help in the monitoring of energy consumption, control and increased safety as well as its resilience (Abdulrahman et al., 2016; Ciavarella et al., 2016; Gubbi et al., 2013; J. Liu et al., 2011; Tuballa and Abundo, 2016; Zanella et al., 2014).

The various Information and Communication Technologies (ICT) basically adopted in these proposed security frameworks by various researchers include the internet, ZigBee, wireless mesh networks, WiMax, 3G, 4G, WiFi and Bluetooth. The suitable method of either optimization or modelling was employed. Also, new emergent technologies such as micro-grids, virtual power plants (VPPs), distributed intelligence techniques, smart metering infrastructure and demand response technology as well as distributed and renewable energy resources are been thought of to make the electricity grid more distributed, flexible for operation and resilient to various security threats (Khelifa and Abla, 2015; Panteli et al., 2016; Schneider et al., 2016; Shahidehpour et al., 2016; Xu et al., 2016) since resilience is always a key consideration for critical infrastructures like power grids (Dong et al., 2015).

Data protection principles aimed at providing adequate privacy for customers as well as the Comprehensive logical interface analysis of all the identified functional priority areas of the cyber-security were carried out and presented in Lee and Brewer (2009) while improvement of customers' data privacy and security from unauthorized parties was modelled in Yip et al. (2014) using Incremental Harsh Function (IHF) in concealing customers' data with no impediment posed on the integrity of the utility company's analysis. State estimation for system monitoring to analyse power grid using values indicated by the meters and power system models to detect errors usually introduced by arbitrary and non-random causes were presented in Y. Liu et al. (2011). Inconsistency robustness technology is proposed where computer memories are tagged and is projected to in the next five years, reduce the vulnerabilities of datacentres (Staff, 2016).

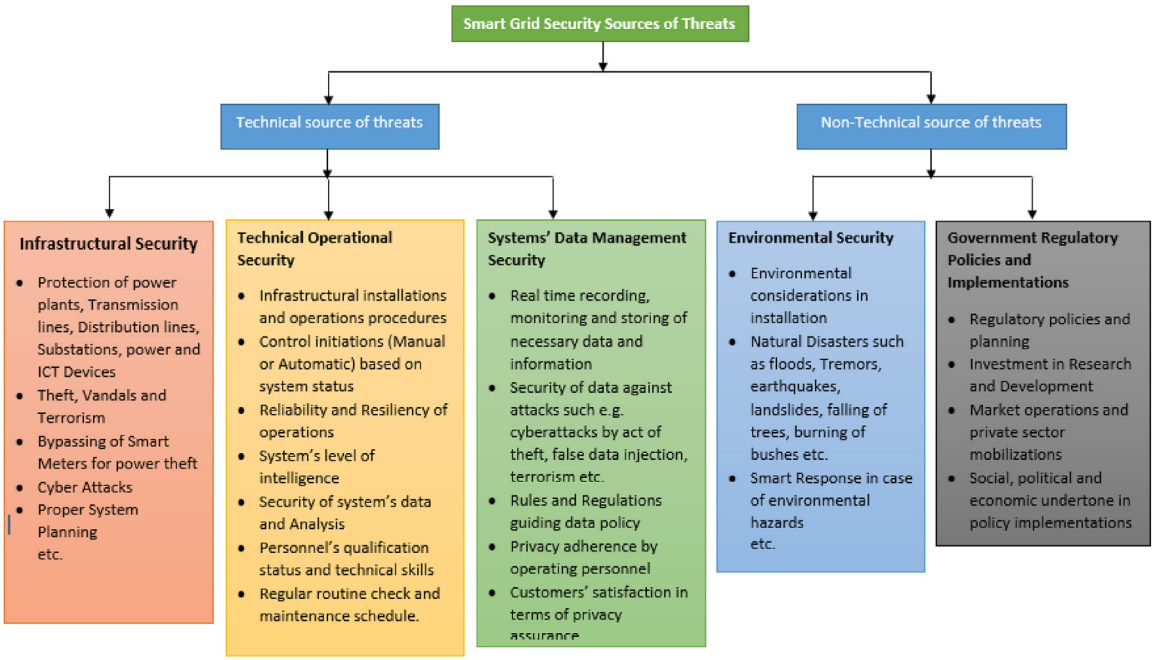

Fig. 4. Classification of SG threats by sources.

In all the works reviewed and many other related works, little or no consideration is given to the identification or classification of the various sources of SGs threats for enhanced preventive and correctives measures. Increased caution must therefore, be taken as the deployments widen. In the next section, classification of the possible sources for which threats can emanate to pose challenges to SG operation is presented and discussed.

4. Smart grid security threats classification by sources

Having identified various threats and challenges faced by the grid system, the threats must be well-defined and an encompassing approach towards the operational security provisions must be laid and followed. Hence, the need to study the sources of threats. Although, the threats can be viewed from many perspectives as presented in Fig. 3, the classification studied in this work is based on technical and non-technical view.

The identified threats are grouped based on various identified sources as depicted in Fig. 4. The figure gives a comprehensive overview of each of the given classification and it is very vital for the deployment of a well-secured and resilient system. This classification can further be modified as the figure has not given an exclusive classification, rather, a model which is opened for suitable modification and reclassification into possible smaller units for a well-coordinated preventive and corrective measures.

4.1. Technical sources of smart grids threats

This classification as presented, is based on the identified threats which can be traced to the technical aspects of SGs. Three key aspects of the technical sources of these threats are identified and these are infrastructural security, technical operational security and systems' data management security.

4.1.1. The infrastructural security

SGs infrastructure is a very complex system which are geographically, logically and economically distributed; interconnecting users, power plants, utilities, transmissions, distributions, substations, transformers, etc. as well as Advanced Metering Infrastructure (AMI), the associated communication and ICT devices such as combination of wireless, fibre optic, power line carrier (PLC), and traditional cable or Ethernet, hence, making SGs, a highly intelligent

system (Goel and Hong, 2015) and as such, the security of the infrastructure becomes critical. Some attacks on electric grid resulting in infrastructural failures were reported in Goel and Hong (2015) to include cybersecurity breach, cascade failures, blackouts, etc.

The AMI is more vulnerable as it is central to SG operation. AMI security (AMI-SEC) task force was reported to have developed some consistent and standard security guidelines, though last updated since 2009, for the implementation of AMI solutions including meter data management system (MDMS) down till smart meter interface (Mendel, 2017).

The demand for energy is ever-increasing worldwide and to effectively cater for the increased demands, existing generation, transmission and distribution capacity require improved expansive integration and coordination for a secured and efficient supply (Yu and Xue, 2016). Hence, the need to adequately analyse security issues for critical systems e.g. the physical components of the infrastructure and sophisticated software security against digital attacks (Yu and Xue, 2016).

Articulated future phase investments in infrastructure, maintenance and system upgrade could be the solution to the potential threats in optimizing the management of demand, decentralized productions, and several other applications as adequate security provisions for sensors and devices, network securities and the grid structure will help in ensuring sustainable systems for SG deployments (Clastres, 2011; El-Hawary, 2014; Wasserman and Cramer, 2016).

4.1.1.1. Advanced Metering Infrastructure security. AMI is an integral component of SG infrastructure and consists of smart meters, communication networks, data management systems exploiting bidirectional communication from the utilities through to customers for information interchange as well as integration of collected data into software application platforms for proper control response, dynamic pricing and regulations (Chakraborty and Shaniia, 2016; Greer et al., 2014; Hu et al., 2015; Mohassel et al., 2014; Wasserman and Cramer, 2016). They are of different designs and provide near real-time monitoring of power consumption (Greer et al., 2014).

The AMI architecture are more susceptible to cyber-attacks (Goel and Hong, 2015) given the fact that it consists of network of sensors, meters, devices and computers for data recording and analysis. As a result, the security of SG will have to cater but not limited to the Advanced Metering Infrastructure (AMI), Wide area situational awareness, IT Network integration, Interoperability, Demand response, customer privacy and efficiency (Gao et al., 2012). The attacks have majorly been targeted at AMI especially the Smart Meter (SM) component, for electricity theft.

The AMI security requirements as it relates to the entire system as well as its personnel and third parties' privacies were developed by Advanced Security Acceleration Project – Smart Grid (ASAP – SG) and NIST led Cyber Security Coordination Task Group (CSCTG) as contained in Lee and Brewer (2009). SG commonly used standard frameworks provides for comprehensive security measures for the various architecture (Greer et al., 2014; Kuzlu et al., 2017).

4.1.1.2. Smart meters and power theft. Smart meters (SMs) are advanced energy meters employed as replacements for the conventional analogue meters to measure customer's energy consumption by providing additional information to the utility company and the customers themselves unlike in the case of conventional energy meters (Alahakoon and Yu, 2016; Depuru et al., 2011; Nikovski et al., 2013). Other enhanced functions of SMs are failure and outage notification, remote command operations, load control for demand response purposes, power quality monitoring, energy theft detection, automatic notification and interaction with other intelligent devices as well as improving environmental conditions by emission reduction through efficient power consumption (Alahakoon and Yu, 2016; Mohassel et al., 2014; Nikovski et al., 2013). By 2020, Number of SMs deployed worldwide is anticipated to be well over 1 billion (International Trade Administration's Top Market Report). SMs penetration is projected to climb from about 30% to 53% at the end of the years 2016 and 2025 respectively (Navigant Research, 2016).

One of the major reasons for attacks on smart meters is power theft, a worldwide phenomenon and very catastrophic to utilities due to its capability of inflicting heavy losses from both technical and financial points of view (Hu et al., 2015; Jiang et al., 2014). It is a notable threat to SGs implementation. Hence, the need for SMs for a real-time monitoring, recording and control of pricing and consumption data for both consumer and utility. SMs are deployed to securely communicate the stored data to the AMI. They are gradually being deployed worldwide owned to its advantages in shaping more accurately, consumers' energy consumption.

The deployment of SMs as a key component of AMI has solved the issues of lingering power theft to some extent, since customers' SMs can easily be detected when offline or perhaps, in case of complete or intermittent bypass. Although, it has come under serious threats mainly by cyber-attacks leading to data manipulations thereby constituting major challenges in the implementation of SGs.

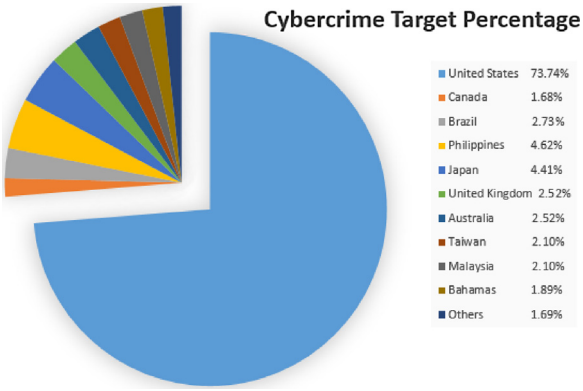

Fig. 5. Countries being targeted by cybercrime (% of estimates) as at 2015.

Various reasons for power theft, means of power theft detection and the mitigations (technical and non-technical approach) have been largely studied using various propositions and models (Depuru et al., 2011; Gaur and Gupta, 2016; Jiang et al., 2014; Kate and Rana, 2015; Mohammad et al., 2013; Mohassel et al., 2014; Nikovski et al., 2013; Patil et al., 2013; Sahoo et al., 2015; Sharma et al., 2016; Solanki et al., 2016), etc.

Lack of proper infrastructure for synchronizing SMs with the existing ones might interrupt the introduction of smart meters and when successfully installed, are extremely attractive targets for hackers, who basically explore the vulnerabilities to compromise the system for example by manipulating their energy costs or fabricate generated energy meter readings depending on the motive(s) of the attacker, hence the need to ensure adequate restrictions on the data by formulation of security guidelines for collection, transmission, storage, and maintenance of the energy consumption data.

4.1.1.3. Cyber-attacks. Cyber-attacks are arguably the most discussed attacks on smart grids due to the vulnerabilities of the infrastructure to digital attacks. It is capable of leading the system to total collapse (Delgado-Gomes et al., 2015), if not properly guarded against. A number of significant vulnerabilities of the Smart Grid have been identified in Dennis and Keogh (2009). Any significant attack is capable of misleading the utilities in making wrong decisions about usage and capacity as well as possibly blind them from impending problems or on-going attacks (McDaniel and McLaughlin, 2009).

Confidentiality, authentication and privacy of data critical for grid reliability and efficiency must be guaranteed to prevent unauthorized modifications through the infrastructure (Moslehi and Kumar, 2010). Examples of notable cyber-attacks are the reports of cyber-attacks on US power system network when it was said to have been penetrated by spies (Gorman, 2009; Klimburg, 2011), also, Estonia, Georgia, Lithuania, Kyrgyzstan, Ukraine, Kazakhstan, the United Kingdom have been reportedly targeted (Klimburg, 2011). Reports of cyber-attacks abound across various facet of the world's infrastructure. Fig. 5 (Saravanakumar et al., 2016) shows the cyber-attack target by countries with United States dealt a major blow of the threats.

Distributed cyber-security systems are therefore designed to monitor the architecture in maintaining data integrity (Esnaola et al., 2016; Goel and Hong, 2015; Sanjab and Saad, 2016; Sanjab et al., 2016).

While physical destruction by a deliberate or non-deliberate action, infrastructural theft and power theft are common threats to the operation and safety of SGs, the customers' most worry is possible breach of privacy and malicious control of personal devices and appliances (Goel and Hong, 2015; Sanjab et al., 2016). The deployment of Google Power Meter (Singh et al., 2016) capable of receiving real time energy consumption statistics providing access via a customized online web page for the plots and analysis, monitoring of day-to-day consumption pattern has pushed customers for a further rethink and unease about the security of their energy consumption data which may further reveal their activities to impending adversaries (Goel and Hong, 2015; Khurana et al., 2010; McDaniel and McLaughlin, 2009); for example, they can exploit poorly configured firewalls to insert a malicious data into the control units (Sanjab and Saad, 2016).

Cyber-attacks on SG can lead to a devastating impact which could result in cascading failures of critical infrastructure and disruption in the economy since critical infrastructure rely on power supply (Amin, 2000; Onyeji et al., 2014). Fig. 6 (SEIT, 2017) shows SG attacks on the energy sector are far higher (at 53%) and above average of all sectors.

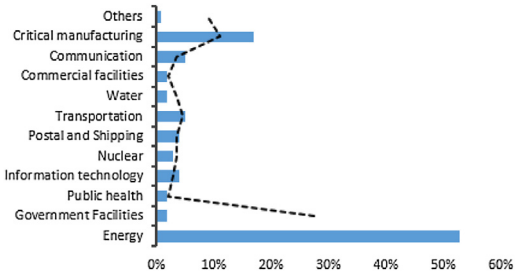

Fig. 6. Percentage cyber-attacks by sectors.

Research focus on how these attacks can be mitigated are now based on provision of meter bots, distributed DoS attacks, usage loggers, SM rootkits, meter-based anti-viruses for improved security (McDaniel and McLaughlin, 2009) and new approaches are currently being developed. The U.S. DOE and the electricity industry have jointly invested $7.9 billion between 2009 and 2015 in projects for modernization of systems in SG implementation, improve cyber security and enhance interoperability (Konstantinou et al., 2016) while India budgeted $5.8 billion in similar vain to span the deployment plan from 2012 to 2017 (Kumar et al., 2014). Global Smart Grid cybersecurity is expected to gulp about $1.8 billion and $3.2 billion in 2017 and 2026 respectively (Navigant Research, 2017).

4.1.2. Technical operational security

The complexity of the grid necessitates secured operational schemes. This is because failures may likely have greater effect since critical infrastructures depend on secured and reliable electricity operations and supplies for energy and control (Amin, 2000; Amin and Wollenberg, 2005; Lightner and Widergren, 2010). Some of the coordination in the operation of the system is under computer control but some part of the operations also require on-field attention of operators at the utility control centres, especially during emergencies in some cases (Amin and Wollenberg, 2005).

Technical operational security covers infrastructural installations and operational procedures, control initiations (Manual or Automatic) based on system status, reliability and resiliency of operations, system's level of intelligence, security of system's data and Analysis, personnel's qualification status and technical skills, regular routine check and maintenance schedule, etc.

In a resilient grid system, timely recognition and diagnosis of problem conditions are key factors for preventing spread of disturbances (Arefifar et al., 2013). This is considered by the use of some notable practical approach, analytical tools and technologies based on advances in the fields of computation, control, and communications to provide solutions for power grids and other infrastructures in locally self-regulating and automatically reconfigure in the event of failures, threats, or disturbances (Amin and Wollenberg, 2005) for uninterruptible operations.

Since faults could also occur due to failure of protective devices, there is the need to design the system to be self-healing by ensuring acceptable fault tolerance level (Goel and Hong, 2015; Rahnamay-Naeini, 2016; Yu and Xue, 2016) and provision of requisite redundancy to achieving a reliable operational security (Goel and Hong, 2015; Yu and Xue, 2016). The underlying principle behind self-healing and distributed control of an electric power system involve treating the individual components as independent intelligent agents by building a processor into each of the component of the substation interacting, monitoring, and cooperating (Amin, 2008; Rahman et al., 2015) to achieve optimal operation. The design includes modelling, computation, sensing and control.

The Quality of Service (QoS) routing in smart grid as studied and presented comprehensively in Li and Zhang (2010) by an algorithm which addressed both the requirements as well as secure the smart grid will help in improving the resiliency since it provides for both Quality of Service in terms of up-time and the real time market value. Working with professional bodies for a comprehensive recovery strategy from failures has also been suggested (Amin, 2008; McDaniel and McLaughlin, 2009; Mendel, 2017) as a viable way of maintaining resilience of the power grid.

If distributed sensing and control is organized in coordination with the internal structure existing in a complex infrastructure and the physics specific to the components they control, these agents promise to provide effective local oversight and control without excessive communications, supervision, or initial programming. These agents exist in every local subsystem and perform pre-programmed self-healing actions that require an immediate response (Amin and Wollenberg, 2005). A maturity assessment aimed at making the grid adaptable to myriads of conditions as they

unfold was discussed in Jin et al. (2015). Thus, a systematic approach will give a concentrated solution to all identified modes of propagation of threats.

In its effort to further improve and strengthen all necessary measures towards improving SG deployment, its reliability and security, the DOE, United States held special Smart Grid Communication programme on Research and Development (R&D) Roadmap on August 30–31 in Washington DC (Department of Energy, 2016).

4.1.3. Systems' data management security

This aspect covers real time recording, monitoring and storing of necessary data and information, security of data against attacks, rules and regulations guiding data policy, privacy adherence by operating personnel, customers' satisfaction in terms of privacy assurance, etc.

The critical data of Generations, Transmissions, Distribution networks, consumer's load profile and performance parameters as well as the features of their control equipment must be collected, analysed and simulated to evaluate the systems' reliability and maintainability for existing systems to model for new installations and upgrades. The study must be carried out to identify all the security threats, vulnerabilities and security provisions.

The growing concerns over the possibilities of privacy breach by the utility companies in possibly revealing customers' data is a major concern for customers. Although, SMs have however changed the nature (and likely, the volume) of SM data frauds or attacks, compromising the meter by remote penetration and control of recorded and stored data may be a source of very sophisticated attacks capable of allowing indistinct changes to customer's usage and falsely indict targeted victims or depending on their intention, launch large-scale attacks on the main grid (Depuru et al., 2011; McDaniel and McLaughlin, 2009).

4.2. Non-technical sources of smart grids threats

The non-technical sources of SGs threats examine those factors which could militate against the deployment or operation. Such factors include natural or man-inflicted environmental hazards such as earthquakes, floods, falling of trees, bush burning, etc.; Government regulatory policies, planning and implementations; or even market operations and private sector mobilizations, etc. Although, considering the causative mode, some factors are considered non-technical but may require technical approach in tackling it.

4.2.1. Environmental security

Provision of environmental security is very crucial in SGs implementation as it helps control and avoid potential catastrophic effects on the infrastructures due to any of the natural or artificial inflicted environmental hazards such as floods, tremors, earthquakes, landslides, falling of trees, burning of bushes, etc. by articulating smart response. Smart response based on environmental considerations is basically achieved by sending appropriate threat alert based on received data and providing alternate feeder for critical infrastructure in such emergencies. Although, this aspect of SGs security is classed under non-technical in this study, some aspect of it has both technical and non-technical implications.

The system's response to failure, in its ability to within the shortest possible time, restore service (by using an improvised alternative feeder as may be applicable) or provide sufficient data which will aid systems' operators in restoring the service is of utmost priority in SGs. This is basically achieved through automated switching to restore service in the event of outages or failure. Some of the factors militating against resiliency as highlighted in Goel and Hong (2015) and Sharifi and Yamagata (2016) are Natural disasters, extreme temperatures, peak and fossil oil depletion, volatility of global energy markets, terrorism, sabotage, vandalism, etc. The 2012 hurricane sandy in US leading to a total loss of $70 billion leaving about 8 million customers without electricity is a perfect example (Panteli et al., 2016) while obvious scenarios are being recorded in countries ravaged by vandals, terrorism and war e.g. Syria, Iraq, Afghanistan, Nigeria, etc.

Geographic Information System (GIS) based instantaneous data is key in this analysis especially in relation to natural disasters forecast and analysis which are used in determining environmental threats alert.

4.2.2. Government regulatory policies and implementation

As opportunities widen in SGs technologies and services, the conventional utility increasingly faces challenges all due to the requirement of new technologies, policies, increasing demands and business models involved in transforming

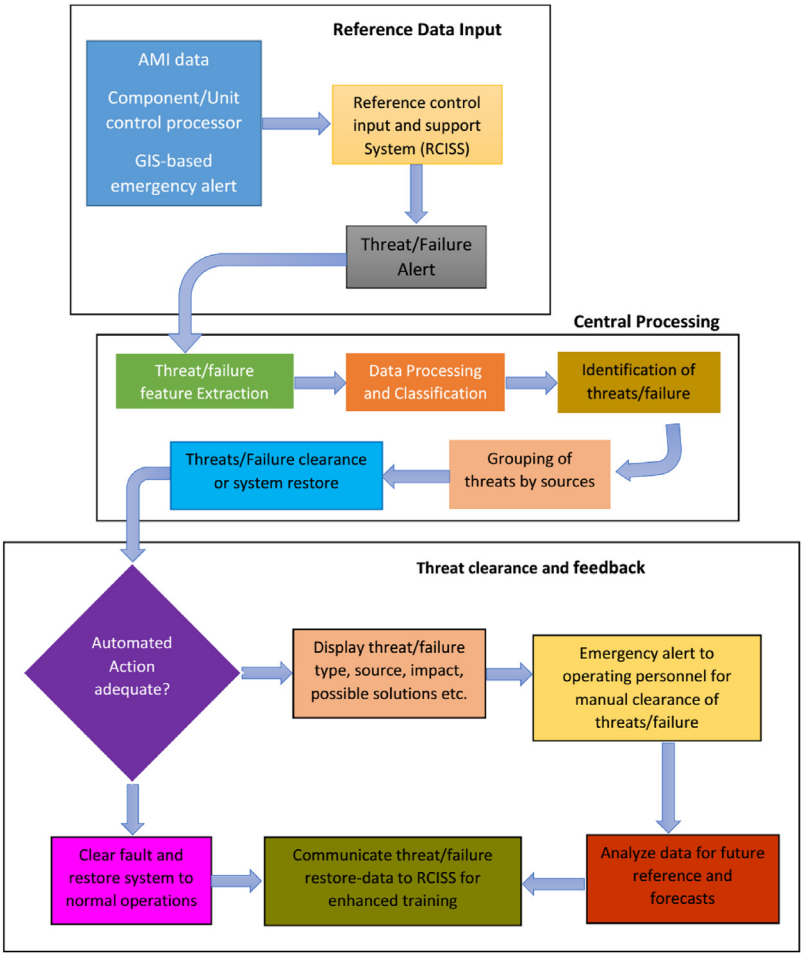

Fig. 7. Conceptual framework for SG security threats identification and clearance based on sources of threats.

to SGs era (Wasserman and Cramer, 2016). Therefore, governments' involvements in providing requisite regulatory policies to aid smooth market operations and private sector mobilizations is key to achieving the set objectives of SG deployment. Technical, social, political, environmental, legislative and economic undertone could prove to be enough a militating factor against achieving a desired deployment except with requisite commitment of governments with proper policy implementations.

The governments' duties in this context is also expected to include public awareness for consumer supports since consumers are key players of the energy sector as their consumption patterns as well as their cooperation with the operators will go a long way in attaining smooth operations. Hence, governments at all levels must play their parts in ensuring timely policy supports and implementations. Also, they have a deep role to play in the areas of Investing in Research and Development. This must be a well-planned roadmap to be respected by successive governments to ensure consistency in the deployment.

5. The proposed framework

Power infrastructures are expensive to procure and complicated in its installation, hence, requires a comprehensive security provision for every potential threat which could result in failure of any unit, systems or even cause cascade effects across the infrastructure. It is therefore pertinent to develop a real-time and maturing intelligent operational security system of all the interconnected components for enhanced security and resiliency.

In the conceptual framework, shown in Fig. 7, a holistic view, based on the sources of threats, for identification and clearance of detected threat is presented. This framework is entirely concentrated on using the technique of threat tracing to the source, for a comprehensive, though complicated, but a more efficient means of combating the dangers posed by the identified threats.

As boldly indicated in the figure, at the reference input, alert from AMI data, sensors or GIS-based system are crossed checked with the control and support system unit to determine any threat.

At the central processing stage, which could be analogous to a control centre, necessary feature needed from the data are extracted, classified, identified and grouped for efficient system clearance and restore. The threats clearance and feedback stage takes care of the output data and provides data for further analysis and reference input to the Reference Control and Support System (RCISS). This system cannot be exclusively captured for all cases before operations or in a single operation but involves intelligent data gathering and analysis with time. Therefore, the proposed framework is opened for further modifications and improvements with time.

6. Conclusions and recommendations

This paper has discussed various SG security threats and challenges as well as giving a classification which could be refined and constantly updated to give a better model for addressing the security and resiliency issues right from the source of threats. With proper verification, application of suitable models, analysis, simulations and optimization tools, the system network can be made to adapt to various conditions; and this should be largely taken care of in both planning and operational stage for a robust, optimized, well-secured and resilient grid system (as the response to threats, source of such threats, impact and even nature of the threats will easily be traced, quantized (where possible) and processed for onward field response, monitoring and control, long before the threats could manifest).

Also, extensive research is required by government agencies, academia, industries, professional bodies and relevant corporate bodies in the evaluation of SG security and privacy issues to enhance Customers' trust and awareness. Therefore, various stakeholders must invest in SG deployment with its security and resiliency issues as priority.

Future work may consider providing suitable models for tackling Smart Grid security threats by source classification for the desired resiliency as well as developing a robust simulation tool for threats sensing and response, for a stabilized system.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Acknowledgments

I sincerely acknowledge Universiti Teknologi Malaysia for providing access to various subscribed online databases which are very helpful for this research. My supervisor, Prof. Mohd Wazir Bin Mustafa, is also duly acknowledged for his advice and guide in getting this work prepared.

References

Abdulrahman, T., Isiwekpeni, O., Surajudeen-Bakinde, N., Otuoze, A., 2016. Design, specification and implementation of a distributed home automation system. Procedia Comput. Sci. 94, 473–478.

Alahakoon, D., Yu, X., 2016. Smart electricity meter data intelligence for future energy systems: a survey. IEEE Trans. Ind. Inform. 12 (1), 425–436.

Alam, S., Sohail, M.F., Ghauri, S.A., Qureshi, I., Aqdas, N., 2017. Cognitive radio based smart grid communication network. Renew. Sustain. Energy Rev. 72, 535–548.

Amin, M., 2000. Toward self-healing infrastructure systems. Computer 33 (8), 44–53.

Amin, M., 2008. Challenges in reliability, security, efficiency, and resilience of energy infrastructure: toward smart self-healing electric power grid. Paper presented at the Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, 1–5.

Amin, S.M., Wollenberg, B.F., 2005. Toward a smart grid: power delivery for the 21st century. IEEE Power Energy Mag. 3 (5), 34–41.

Anderson, M., 2010. WiMax for smart grids. IEEE Spectr. 47 (7), 14.

Arefifar, S.A., Mohamed, Y.A.-R.I., EL-Fouly, T.H., 2013. Comprehensive operational planning framework for self-healing control actions in smart distribution grids. IEEE Trans. Power Syst. 28 (4), 4192–4200.

Bigerna, S., Bollino, C.A., Micheli, S., 2015. Overview of socio-economic issues for smart grids development. Paper presented at the 2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), 1–6.

Calderaro, V., Hadjicostis, C.N., Piccolo, A., Siano, P., 2011. Failure identification in smart grids based on Petri net modeling. IEEE Trans. Ind. Electron. 58 (10), 4613–4623.

Camarinha-Matos, L.M., 2016. Collaborative smart grids – a survey on trends. Renew. Sustain. Energy Rev. 65, 283–294.

Chakraborty, A.K., Shaniia, N., 2016. Advanced metering infrastructure: technology and challenges. Paper presented at the 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 1–5.

Ciavarella, S., Joo, J.Y., Silvestri, S., 2016. Managing contingencies in smart grids via the Internet of things. IEEE Trans. Smart Grid 7 (4), 2134–2141, http://dx.doi.org/10.1109/TSG.2016.2529579.

Clastres, C., 2011. Smart grids: another step towards competition, energy security and climate change objectives. Energy Policy 39 (9), 5399–5408.

De Santis, E., Rizzi, A., Sadeghian, A., 2017. A learning intelligent system for classification and characterization of localized faults in smart grids. Paper presented at the 2017 IEEE Congress on Evolutionary Computation (CEC), 2669–2676.

Delgado-Gomes, V., Martins, J.F., Lima, C., Borza, P.N., 2015. Smart grid security issues. Paper presented at the 9th International Conference on Compatibility and Power Electronics (CPE), 2015, 534–538.

Dennis, D., Keogh, M., 2009. The Smart Grid: An Annotated Bibliography of Essential Resources for State Commissions. National Association of Regulatory Utility Commissioners, https://www.smartgrid.gov/files/The_Smart_Grid_Annotated_Bibliography_Essential_Resources_fo_200909.pdf (accessed on 25.07.16).

Department of Energy, 2016. Smart Grid Communication Programme on Research and Development (R&D) Roadmap, https://secure.inl.gov/SmartGrid/Default.aspx (accessed on 20.10.16).

Depuru, S.S.S.R., Wang, L., Devabhaktuni, V., 2011. Smart meters for power grid: challenges, issues, advantages and status. Renew. Sustain. Energy Rev. 15 (6), 2736–2742.

Doh, I., Lim, J., Chae, K., 2015. Secure authentication for structured smart grid system. Paper presented at the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015, 200–204.

Dong, X., Lin, H., Tan, R., Iyer, R.K., Kalbarczyk, Z., 2015. Software-defined networking for smart grid resilience: opportunities and challenges. Paper presented at the Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 61–68.

El-Hawary, M.E., 2014. The smart grid – state-of-the-art and future trends. Electr. Power Compon. Syst. 42 (3–4), 239–250.

Esnaola, I., Perlaza, S.M., Poor, H.V., Kosut, O., 2016. Maximum distortion attacks in electricity grids. IEEE Trans. Smart Grid 7 (4), 2007–2015, http://dx.doi.org/10.1109/TSG.2016.2550420.

Farhangi, H., 2010. The path of the smart grid. IEEE Power Energy Mag. 8 (1), 18–28.

Gao, J., Xiao, Y., Liu, J., Liang, W., Chen, C.P., 2012. A survey of communication/networking in Smart Grids. Future Gener. Comput. Syst. 28 (2), 391–404.

Gaur, V., Gupta, E., 2016. The determinants of electricity theft: an empirical analysis of Indian states. Energy Policy 93, 127–136.

Ghansah, I., 2009. Smart grid cyber security potential threats, vulnerabilities and risks. In: California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047.

Goel, S., Hong, Y., 2015. Security Challenges in Smart Grid Implementation Smart Grid Security. Springer, pp. 1–39.

Gorman, S., 2009. Electricity grid in US penetrated by spies. Wall Str. J. 8.

Greer, C., Wollman, D.A., Prochaska, D.E., Boynton, P.A., Mazer, J.A., Nguyen, C.T., FitzPatrick, G.J., Nelson, T.L., Koepke, G.H., Hefner Jr., A.R., 2014. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. Tech. Rep. NIST SP-1108r3. The National Institute of Standards and Technology.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. 29 (7), 1645–1660.

Hasan, M.M., Mouftah, H.T., 2015. Encryption as a service for smart grid advanced metering infrastructure. Paper presented at the 2015 IEEE Symposium on Computers and Communication (ISCC), 216–221.

Hu, Z., Mohagheghi, S., Sartipi, M., 2015. Efficient data acquisition in advanced metering infrastructure. Paper presented at the 2015 IEEE Power & Energy Society General Meeting, 1–5.

International Trade Administration's Top Market Report, January 2017. Smart Grid Top Markets Report – Update, http://trade.gov/topmarkets/pdf/Smart_Grid_Top_Markets_Report.pdf (accessed on 29.07.17).

Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., Shen, X.S., 2014. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci. Technol. 19 (2), 105–120.

Jin, X., Li, X., Qi, W., Zhao, Q., Jia, H., Huang, H., Zeng, Y., Liu, Y., 2015. Maturity assessment model of smart grid project. Paper presented at the 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), 2015, 2752–2757.

Kate, P.G., Rana, J.R., 2015. ZIGBEE based monitoring theft detection and automatic electricity meter reading. Paper presented at the 2015 IEEE International Conference on Energy Systems and Applications, 258–262.

Kezunovic, M., 2011. Smart fault location for smart grids. IEEE Trans. Smart Grid 2 (1), 11–22.

Khan, F., ur Rehman, A., Arif, M., Aftab, M., Jadoon, B.K., 2016. A survey of communication technologies for smart grid connectivity. Paper presented at the 2016 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), 256–261.

Khelifa, B., Abla, S., 2015. Security concerns in smart grids: threats, vulnerabilities and countermeasures. Paper presented at the 3rd International Renewable and Sustainable Energy Conference (IRSEC), 2015, 1–6.

Khurana, H., Hadley, M., Lu, N., Frincke, D.A., 2010. Smart-grid security issues. IEEE Secur. Priv. 8 (1), 81–85.

Klimburg, A., 2011. Mobilising cyber power. Survival 53 (1), 41–60.

Komninos, N., Philippou, E., Pitsillides, A., 2014. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun. Surv. Tutor. 16 (4), 1933–1954.

Konstantinou, C., Sazos, M., Maniatakos, M., 2016. Attacking the smart grid using public information. Paper presented at the 17th Latin-American Test Symposium (LATS), 2016, 105–110.

Kosut, O., Jia, L., Thomas, R.J., Tong, L., 2011. Malicious data attacks on the smart grid. IEEE Trans. Smart Grid 2 (4), 645–658.

Kumar, V.A., Pandey, K.K., Punia, D.K., 2014. Cyber security threats in the power sector: need for a domain specific regulatory framework in India. Energy Policy 65, 126–133.

Kuzlu, M., Pipattanasompom, M., Rahman, S., 2017. A comprehensive review of smart grid related standards and protocols. Paper presented at the 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG), 2017, 12–16.

Lawrence, T.M., Watson, R.T., Boudreau, M.-C., Mohammadpour, J., 2017. Data flow requirements for integrating smart buildings and a smart grid through model predictive control. Procedia Eng. 180, 1402–1412.

Lee, A., Brewer, T., 2009. Smart grid cyber security strategy and requirements. In: Draft Interagency Report NISTIR, 7628.

Li, F., Luo, B., Liu, P., 2010. Secure information aggregation for smart grids using homomorphic encryption. Paper presented at the First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, 327–332.

Li, H., Zhang, W., 2010. QoS routing in smart grid. Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010, 1–6.

Lightner, E.M., Widergren, S.E., 2010. An orderly transition to a transformed electricity system. IEEE Trans. Smart Grid 1 (1), 3–10.

Liu, J., Li, X., Chen, X., Zhen, Y., Zeng, L., 2011. Applications of internet of things on smart grid in China. Paper presented at the 13th International Conference on Advanced Communication Technology (ICACT), 2011, 13–17.

Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14 (1), 13.

Lund, H., Andersen, A.N., Østergaard, P.A., Mathiesen, B.V., Connolly, D., 2012. From electricity smart grids to smart energy systems – a market operation based approach and understanding. Energy 42 (1), 96–102.

McDaniel, P., McLaughlin, S., 2009. Security and privacy challenges in the smart grid. IEEE Secur. Priv. 7 (3), 75–77.

Mendel, J., 2017. Smart grid cyber security challenges: overview and classification. e-mentor 1 (68), 55–66.

Metke, A.R., Ekl, R.L., 2010. Security technology for smart grid networks. IEEE Trans. Smart Grid 1 (1), 99–107.

Mohammad, N., Barua, A., Arafat, M.A., 2013. A smart prepaid energy metering system to control electricity theft. Paper presented at the International Conference on Power, Energy and Control (ICPEC), 2013, 562–565.

Mohassel, R.R., Fung, A.S., Mohammadi, F., Raahemifar, K., 2014. A survey on advanced metering infrastructure and its application in smart grids. Paper presented at the 27th Canadian Conference on Electrical and Computer Engineering (CCECE), 2014, 1–8.

Momoh, J.A., 2009. Smart grid design for efficient and flexible power networks operation and control. Paper presented at the Power Systems Conference and Exposition, 2009. PSCE'09, 1–8.

Moretti, M., Djomo, S.N., Azadi, H., May, K., De Vos, K., Van Passel, S., Witters, N., 2017. A systematic review of environmental and economic impacts of smart grids. Renew. Sustain. Energy Rev. 68, 888–898.

Moslehi, K., Kumar, R., 2010. A reliability perspective of the smart grid. IEEE Trans. Smart Grid 1 (1), 57–64.

Navigant Research, 2016. Market Data: Smart Meters, https://www.navigantresearch.com/research/market-data-smart-meters (accessed on 28.07.17).

Navigant Research, 2017. Cybersecurity for the Digital Utility, https://www.navigantresearch.com/research/cybersecurity-for-the-digital-utility (accessed on 28.07.17).

Nikovski, D.N., Wang, Z., Esenther, A., Sun, H., Sugiura, K., Muso, T., Tsuru, K., 2013. Smart meter data analysis for power theft detection. Paper presented at the International Workshop on Machine Learning and Data Mining in Pattern Recognition, 379–389.

Obi, P.I., Chidolue, G., Okonkwo, I.I., 2014. Protection and control of power system – a review. Int. J. Adv. Res. Technol. 3 (5), 158–166.

Onyeji, I., Bazilian, M., Bronk, C., 2014. Cyber security and critical energy infrastructure. Electr. J. 27 (2), 52–60.

Panteli, M., Trakas, D.N., Mancarella, P., Hatziargyriou, N.D., 2016. Boosting the power grid resilience to extreme weather events using defensive islanding. IEEE Trans. Smart Grid PP (99), 1–10, http://dx.doi.org/10.1109/TSG.2016.2535228.

Patil, S., Pawaskar, G., Patil, K., 2013. Electrical power theft detection and wireless meter reading. Int. J. Innov. Res. Sci. Eng. Technol. 2 (4), 1114–1119.

Qiu, F., Wang, J., Chen, C., Tong, J., 2016. Optimal black start resource allocation. IEEE Trans. Power Syst. 31 (3), 2493–2494.

Rahman, M., Mahmud, M., Pota, H., Hossain, M., 2015. A multi-agent approach for enhancing transient stability of smart grids. Int. J. Electr. Power Energy Syst. 67, 488–500.

Rahnamay-Naeini, M., 2016. Designing cascade-resilient interdependent networks by optimum allocation of interdependencies. Paper presented at the 2016 International Conference on Computing, Networking and Communications (ICNC), 1–7.

Rogers, R., 2013. Smart Grid and Energy Storage Technologies Spread, http://www.worldwatch.org/smart-grid-and-energy-storage-technologies-spread (accessed on 16.02.16).

Ruj, S., Pal, A., 2014a. Analyzing cascading failures in smart grids under random and targeted attacks. Paper presented at the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications.

Ruj, S., Pal, A., 2014b. Analyzing cascading failures in smart grids under random and targeted attacks. Paper presented at the 28th International Conference on Advanced Information Networking and Applications (AINA), 226–233.

Russell, B.D., Benner, C.L., 2010. Intelligent systems for improved reliability and failure diagnosis in distribution systems. IEEE Trans. Smart Grid 1 (1), 48–56.

Sahoo, S., Nikovski, D., Muso, T., Tsuru, K., 2015. Electricity theft detection using smart meter data. Paper presented at the Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society, 1–5.

Sanjab, A., Saad, W., 2016. Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective. IEEE Trans. Smart Grid 7 (4), 2038–2049, http://dx.doi.org/10.1109/TSG.2016.2550218.

Sanjab, A., Saad, W., Guvenc, I., Sarwat, A., Biswas, S., 2016. Smart Grid Security: Threats, Challenges, and Solutions. arXiv:1606.06992.

Saravanakumar, S., Raja, S., Anjali, A., Indhumathi, P., Sathiya, M., Thamaraiselvi, V., Vijayalakshmi, S., 2016. Design of modern GSM for emergency alerts using proteus. Int. J. Appl. Eng. Technol. 2 (4), 8–12.

Scala, A., Pahwa, S., Scoglio, C.M., 2015. Cascade failures and distributed generation in power grids. Int. J. Crit. Infrastruct. 11 (1), 27–35.

Schneider, K., Tuffner, F., Elizondo, M., Liu, C.-C., Xu, Y., Ton, D., 2016. Evaluating the Feasibility to Use Microgrids as a Resiliency Resource.

Scribellito, A., 2015. About IEEE Smart Grid Domains & Sub-domains, http://smartgrid.ieee.org/resources/2073-domains (accessed on 23.08.16).

SEIT, 2017. Identifying Smart Grid Vulnerabilities Due to Cyber Attacks, https://www.unsw.adfa.edu.au/school-of-engineering-and-information-technology/identifying-smart-grid-vulnerabilities-due-cyber-attacks (accessed on 01.08.17).

Sha, K., Alatrash, N., Wang, Z., 2016. A secure and efficient framework to read isolated smart grid devices. IEEE Trans. Smart Grid PP (99), 1–13, http://dx.doi.org/10.1109/TSG.2016.2526045.

Shahid, A., 2014. A cyber-physical approach for stochastic hybrid control and safety verification of smart grids. Paper presented at the 2014 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA), 721–725.

Shahidehpour, M., Li, Z., Liu, X., Cao, Y., 2016. Microgrids for enhancing the power grid resilience in extreme conditions. IEEE Trans. Smart Grid PP (99), 1, http://dx.doi.org/10.1109/TSG.2016.2579999.

Sharifi, A., Yamagata, Y., 2016. Principles and criteria for assessing urban energy resilience: a literature review. Renew. Sustain. Energy Rev. 60, 1654–1677.

Sharma, T., Pandey, K., Punia, D., Rao, J., 2016. Of pilferers and poachers: combating electricity theft in India. Energy Res. Soc. Sci. 11, 40–52.

Singh, A., Fernandes, J., Yadav, M., Patil, N., Charadva, M.M., 2016. Wireless multiuser real time LCD display using short message service based on GSM technology. Int. J. Adv. Found. Res. Sci. Eng. 2, 173–177.

Solanki, V.K., Katiyar, S., BhashkarSemwal, V., Dewan, P., Venkatasen, M., Dey, N., 2016. Advanced automated module for smart and secure city. Procedia Comput. Sci. 78, 367–374.

Staff, C., 2016. Future cyberdefenses will defeat cyberattacks on PCs. Commun. ACM 59 (8), 8–9.

Tuballa, M.L., Abundo, M.L., 2016. A review of the development of Smart Grid technologies. Renew. Sustain. Energy Rev. 59, 710–725.

Wang, W., Xu, Y., Khanna, M., 2011. A survey on the communication architectures in smart grid. Comput. Netw. 55 (15), 3604–3629.

Wasserman, A., Cramer, S., 2016. Opportunities for governors to align electricity markets with state energy goals. Electr. J. 29 (8), 27–32.

Xu, Y., Liu, C.C., Schneider, K., Tuffner, F., Ton, D., 2016. Microgrids for service restoration to critical load in a resilient distribution system. IEEE Trans. Smart Grid PP (99), 1, http://dx.doi.org/10.1109/TSG.2016.2591531.

Yip, S.-C., Wong, K., Phan, R.C.-W., Tan, S.-W., Ku, I., Hew, W.-P., 2014. A Privacy-Preserving and Cheat-Resilient electricity consumption reporting scheme for smart grids. Paper presented at the International Conference on Computer, Information and Telecommunication Systems (CITS), 2014, 1–5.

Yu, X., Xue, Y., 2016. Smart grids: a cyber-physical systems perspective. Proc. IEEE 104 (5), 1058–1070.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M., 2014. Internet of things for smart cities. IEEE Internet Things J. 1 (1), 22–32, http://dx.doi.org/10.1109/JIOT.2014.2306328.

Zhang, P., Li, F., Bhatt, N., 2010. Next-generation monitoring, analysis, and control for the future smart control center. IEEE Trans. Smart Grid 1 (2), 186–192.