Arid Zone Journal of Engineering, Technology and Environment, December, 2017; Vol. 13(6):858-867

Print ISSN: 1596-2490, Electronic ISSN: 2545-5818, www.azojete.com.ng

A REVIEW OF SMART GRIDS DEPLOYMENT ISSUES IN DEVELOPING COUNTRIES

A. O. Otuoze[1]*, A. M. Usman[1], O. O. Mohammed[1] and A. A. Jimoh[2]

[1]Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, University of Ilorin, Ilorin, Nigeria
[2] Department of Electrical and Electronics Engineering, The Federal Polytechnic Offa, Offa, Nigeria
**Corresponding Author's email address: otuoze.ao@unilorin.edu.ng*

Abstract
Smart Grids (SGs) have taken a centre stage in achieving a smarter, more reliable, robust, secured, economically efficient and more environmentally friendly mode of power generation and utilisation. Massive deployment is being recorded in developed worlds. While most of these countries are investing heavily in the development of SGs, well-articulated areas of research and development are key aspects with special emphasis on its security since it involves complex interconnection of units and systems which are expensive to install and maintain. In developing nations, especially those of Africa, realisation of adequate power supply to meeting the ever-growing demand has been a mirage with demand on geometric increase and with every increase largely meaning a drift away from the supply. Hence, attention is focused on capacity expansion in most developing nations rather than SGs deployments especially considering the various challenges militating against the development despite the huge advantages. Although, some of these nations have made tremendous achievements in this regard, the associated challenges have become major source of worry for most of the nations. This paper gives highlights of these issues and possible measures of overcoming them in order to enhance sustainable SGs deployments in developing countries like Nigeria.

Keywords: Smart Grid, Smart Electric Meter (SEM), Power Network, Challenges, Security, Developing Nations

1. Introduction

The quest for an improved power system network worldwide has called for imminent research, investment and upgrade in the power sector. Worldwide, average annual electricity demand is expected to increase more than twice from 1.3% per year in 2015 to about 2.8% by 2020(Smart Grid Top Markets Report 2017). Hence, the deployment of Smart Grids (SGs) for a more efficient operation of the power system. SGs provide a bidirectional communication as well as connect intelligently all power network supply and monitoring devices for a reliable, secured and resilient power delivery (Bigerna, Bollino, & Micheli, 2016; Colak, Fulli, Sagiroglu, Yesilbudak, & Covrig, 2015; Fadaeenejad *et al.*, 2014; Fan and Gong, 2013; Kezunovic, 2011; Li and Cao, 2011; Shuaib, *et al.*, 2015; Smart Grid Top Markets Report 2017). This enables enhanced planning, deployment and possible expansion of the grid (Eissa, 2015; Kezunovic, 2011; Sridhar, *et al.*, 2012).

It was estimated that SG will gulp about $200 billion investments in infrastructure worldwide from 2010 to 2015 and its global market potential will nearly double by 2020 to about US$73 billion in annual revenue and US$461 billion in cumulative profit (Fan & Gong, 2013). Russia, China and India are a few of the developing nations making giant stride in SG deployments (African Economic Outlook 2016; Fadaeenejad *et al.*, 2014). Thailand and India have budgeted US$ 13 billion (for the next 15 years) and USD 5.8 billion (for a five year plan) (Fadaeenejad *et al.*, 2014; Kumar, *et al.*, 2014) to improve their power infrastructure respectively, with Malaysia targeting an

expenditure of $109.0 million by 2016 (World Bank Open Data 2016). Figure 1 shows the investment in SG by region as at 2012 (Rogers, 2013)

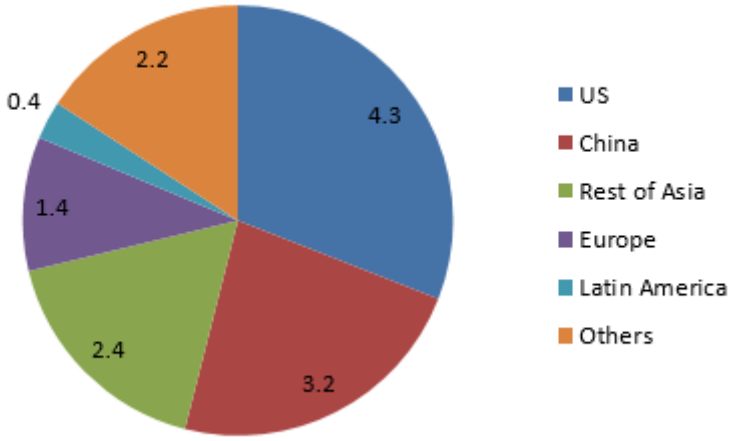

Figure 1: SG Investment by Region as at 2012 (Values in $ billion)

The security issues worldwide are major concerns in this deployment and has necessitated various researches (Amin, 2012; Gharavi and Hu, 2013; Giani, *et al.*, 2012; Li, *et al.*, 2014; Wei, *et al.*, 2011). Although, the general security issues of SG deployment are overwhelming but as developing nations hope to widen investments in SGs with many other countries in the region springing up for power network upgrade, there are peculiar security issues regarding the deployments.

This paper presents some of the worrying challenges militating against the deployment of SGs in the region, giving a brief account with peculiarity to developing nations from Sub-Saharan Africa, using Nigeria as example. The issues raised are pointer to the impending security challenges which slowed the pace of SG deployments in developing nations.

The rest of this paper is organised as follows. Section 2 presents the related issues emanating from the Demand-Supply gap while section 3 discusses issues related to the deployment of Smart Electricity Meters as well as cases of electricity thefts. Cyber-attacks, vandalization, infrastructure theft and terrorism are discussed in section 4 and section 5 presents the highlights of issues concerning poor research and investments. In section 6, low budgetary allocations, poor regulatory policies and corruption are briefly discussed as they affect SGs deployments while section 7 gives the conclusion and recommendation for further study.

2. Demands-Supply Gap

Most developing nations have suffered shortage of electricity for years, with a wide gap in the demand and supply (Gaur and Gupta, 2016; Kemausuor, *et al.*, 2011; Kessides, 2013). Also, many of the Nations lack requisite access to electricity; some are however, able to provide 100% access of electricity to its citizens while others especially the Sub Saharan Countries are lagging far behind (World Bank Open Data 2016) as shown in figure 2.

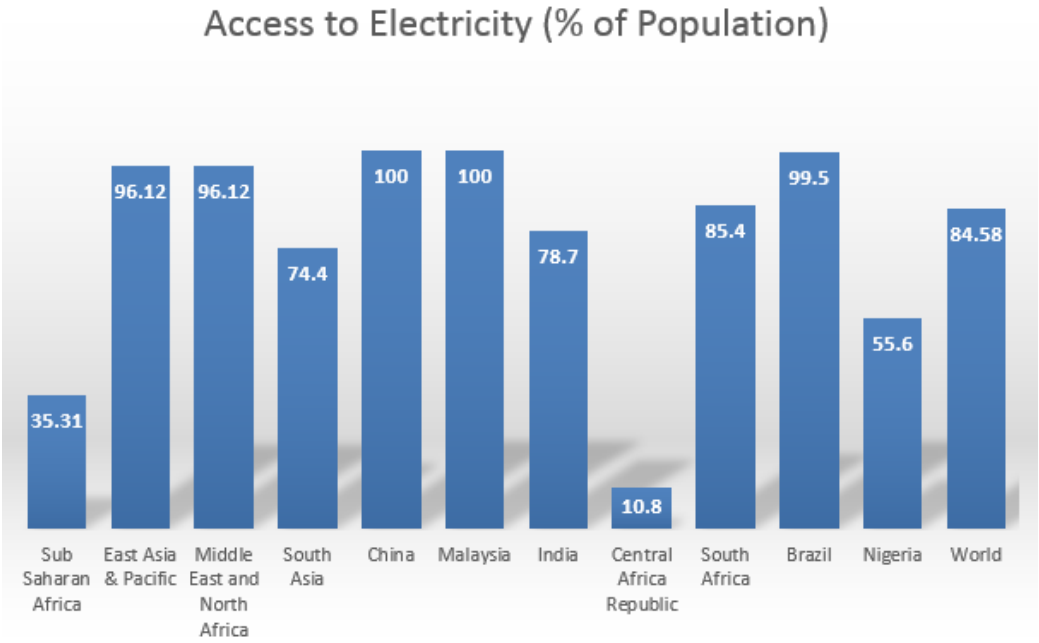

Figure 2: Access to Electricity (% of Population) of selected Regions and Countries as at 2012

One of the most contributory factors militating against SG deployment is the wide gap of supply compared to the demand as reported for Ghana, South Africa, Pakistan, India, Nigeria etc. (Gaur and Gupta, 2016; Kemausuor *et al.*, 2011; Kessides, 2013) and many developing nations. This impact negatively on the economy, which include but not limited to low international competitiveness and exports, increased poverty level, killing of local manufacturing sectors and hence low country's growth in terms of GDP (Kessides, 2013) are the major consequences of the low or irregular power supply. With this poor access to electricity, SG deployment is hindered since constant energy supply critical to the present-day world (Akorede, *et al.*, 2017) cannot be guaranteed to serve both individual and community needs. Also, countries who are yet to deploy this technology to a reasonable level are likely going to concentrate on improving their generation capacity even though urgent deployment of SG will help in the efficient management of the system especially by improved monitoring, control and metering.

3. Roll out of Smart Electric Meters and Electricity Theft

Smart electric meters (SEMs) are installed to help measure energy flow values and transmit the energy consumption data to both the utility and customer as well as making the data available via Advanced Metering Infrastructure (AMI), for billing, planning, and control actions (Geelen, *et al.*, 2013; Jiang *et al.*, 2014; Siano, 2014). The SEMs offer huge advantages in energy billing, monitoring and management, energy saving, improved metering by reducing power theft, enhancing revenue generation, effective demand side management and security (Abdulrahman, *et al.*, 2016; Amin, 2012; Smart Grid Top Markets Report 2017). The AMI is a key component of SGs deployment. It employs the use of smart meters (SMs) at substations and customer ends (Shuaib *et al.*, 2015). It is a subsystem of the SGs which provides bidirectional communication between the SMs and the utilities by helping in real-time transmissions of consumption data, control commands and pricing information usually at specified interval (Jokar, 2016; Shuaib *et al.*, 2015). The

introduction of AMI digitalises the electricity metering system compared to the old mechanical meters (Fatemieh, *et al.*, 2010; Jiang *et al.*, 2014). Since early 2000s, SMs have been deployed around the globe as key element of SGs.

The prime functions and applications of SMs include real-time energy consumption data capture, remote and local reading capability, fast outage detection and supply management, remote controlled access, integrated ability to other commodity supplies, interoperability within the SGs, device and energy status capture, demand response, faster diagnosis of faults, electricity theft detection and support for distributed generations (DGs) (Alahakoon and Yu, 2016; Altmann *et al.*, 2011; Fatemieh *et al.*, 2010; Jiang *et al.*, 2014).

Globally, 313 million SEMs were reportedly installed as at 2013 and could rise to about 1.1 billion in 2023 (Shuaib *et al.*, 2015). 852 million SEMs was projected to be installed worldwide by 2018 (O'Malley, 2014). In 2013, Zimbabwe Electricity Supply Authority (ZESA) reportedly installed about 573,667 units targeting installation of 800,000 units by 2018. Uzbekistan, India and Pakistan have been enjoying some support by Asian Development Bank in the financing of their SMs project (Metering.com Data).

In effort to fast-track the roll out of SEMs, Nigeria introduced Credited Advanced Payment for Metering Implementation (CAPMI) scheme in partnership with EcoBank, but the scheme met a stiff opposition due to the unwillingness of customers to finance the installation using their own money. Later, CAPMI was terminated since it could not achieve its aim. Complacency by the distribution companies (Discos) was also a major reason expressed in some other quarters as cases were reported where consumers managed to pay the power distribution companies (DISCOs) for SEMs and are not promptly supplied and installed by the DISCOs. In most of these cases, consumers have to wait for at least, 15 months before being supplied. Sometimes, they even have to bribe their way out. This has led to consumers being continuously charged on estimated billing, which eventually leads to cheating on the consumers; and the consumers also look for way to engage in energy theft. Nigeria's Kaduna Electricity Distribution Company (KEDC) promised its manufacturing plant in Kaduna will help the company roll out 500,000 SEMs to meet its set target by 2021. Overall, reports show that the Discos have only managed to deploy a few of hundred thousand which is very poor in a country as big as Nigeria (Metering.com Data).

Electricity theft, high cost of SEMs, billing irregularities via the conventional meters by the DISCOs resulting in over-billing of customers coupled with the bureaucratic procedures involved in SEM installations are some unfortunate challenges against smooth deployment of SGs. Often, DISCOs fail to read the conventional meters while they bill customers and since electricity is highly unstable, they seem to be making higher revenues compared to having customers with SEMs and hence, would rather frustrate the efforts on SEMs distributions. A development to which Nigeria's Electricity Regulatory Commission (NERC) has repeatedly threatened sanctions but has done little or nothing to sanction erring DISCOs. Hence, posing appalling challenges to the deployment of SGs in a country like Nigeria.

One of the major source of loss for utility companies is electricity theft causing them huge losses and preventing further investment plans (Sharma, *et al.*, 2016). Unpaid electricity bills, billing irregularities, smart meter manipulations and cyber-attacks, corruption of employees (e.g. misappropriation of funds, illegal procurement, sale and installation of prepaid meters, helping customers in meter bypass etc.) and other related fraudulent activities militating against SG deployments. SEMs have come under series of electricity theft techniques including bypass, cyber-

attacks etc. Electricity theft has evolved as the major security challenge worldwide as huge losses are being reportedly incurred by utility operators and governments. Each year, utilities reportedly lose more than $25 billion worldwide (Jiang *et al.*, 2014) causing every player high dissatisfaction. As a palliative measure, some governments reportedly grant subsidies to enable utility companies keep customers' bills low (Mohammad, *et al.*, 2013; Sharma *et al.*, 2016). About $25 billion is reportedly lost to power theft globally on yearly basis (Jiang *et al.*, 2014; Sharma *et al.*, 2016). In some Sub-Saharan African, South-East Asia, Latin America and Middle east, huge losses in various range have been reported (Gaur and Gupta, 2016; Jamil and Ahmad, 2014; Jiang *et al.*, 2014; Nikovski *et al.*, 2013) and many cases are either partially reported or left unreported.

Government subsidies, encouragement of local production as in the case of KEDC, adequate database of customers, proper regulatory policies for monitoring and control by government and utility companies will help in SEMs deployments and monitoring against power thefts. Engineers and Researchers are continuously working on various techniques for curbing the menace of electricity theft.

4. Cyber-Attacks, Vandalization, Infrastructure Theft and Terrorism

Cyber-attacks are global phenomenon affecting countries, companies, institutions, security agencies, infrastructures etc. They are capable of inflicting heavy damages to both physical or the programmes on which the control relies. SG is made vulnerable to cyber threats by the fact that it is dependent on information technology (Stefanov and Liu, 2014; W. Wang & Lu, 2013; X. Wang & Yi, 2011). Globally, an estimated sum of US$445 billion is spent yearly in combating cyber-crimes (Khodaei *et al.*, 2016; Lala and Panda, 2001) with many developing nations budgeting little or nothing to fight cyber-crimes. So, the deployment of SG must be accompanied with well-structured cyber-security for a secured and resilient system. Various approaches have been proposed to curb cyber security threats and attacks as contained in (Genge, *et al.*, 2015; Kreutz, *et al.*, 2016; Lala and Panda, 2001; Mo, *et al.*, 2012; Stefanov and Liu, 2014; Wei, *et al.*, 2011) etc.

Vandalism and theft of infrastructure are other aspects requiring key research to be able to determine the exact value loss. In Africa, various reports dominate pages of newspapers daily on either theft of power infrastructure or its vandalization. The recent Niger Delta attacks on oil and gas infrastructure has led to shortage of gas supply which is a major impetus to power generating companies. The Guardian Newspaper reported that estimated $14bn is required for the damage caused (The Guardian 2015). While Nigeria, Mozambique, Zimbabwe, South Africa have also reported various cases and losses due to vandalism and theft (APANews.net; ThisDay Newspaper April 19 2016; ThisDay Newspaper May 9 2016). Several developing nations face similar fate.

Terrorism can come in form of physical attacks on infrastructure or cyber-attacks. The attacks could be perpetuated by some terror groups such as ISIS, ISIL, Boko-haram and Al-Shabab or militancy in form of Niger Delta Avengers (in Nigeria) or any other form of insurgency. They can be carried out in form of war between states e.g. the war between Russia and Ukraine, Israel and Palestine. Usually, the effects are so enormous that reportage is limited to causalities in terms of human lives lost rather than infrastructure. Terrorism has cost the global economy huge sum of money (difficult to properly estimate) and given the rising insurgency in most developing nations, SG deployments is threatened by terrorism.

5. Poor Research and Investment

Research and development (R&D) in sub-Saharan Africa is at a notable low profile and with SG deployment requiring several billions of dollars, continuous research is needed for a sustainable deployment. SG research and investment in developed and emerging economies are on a steady growth due to the high commitment in research and general investment. Developing nations must emulate same for improvement in research and investment (both in human and capital resources). This will enhance deployment efficiency and reduce the overall operational and maintenance overheads. In addition, research institutions too must key into doing lots of works in coming up with results that will enhance deployment of SGs in developing economy.

6. Low Budgetary Allocations, Poor Regulatory Policies and Corruption

Considering the cost of deployments of SGs, the low budgetary allocations of many developing nations is another barrier. SG projects engulfed $14.9 billion in 2013 (Gonzalez, 2014). The current economic downturn worldwide which has sent many developing nations to recession automatically means low budgetary for the power sector (African Economic Outlook 2016). Priority must however be given to some key aspects of SGs deployment since it helps run the power system more efficiently.

Poor regulatory policies and implementation in most region of the developing nation is also worthy of note as a barrier to SG deployment because consistency and a well-driven policy are key to sustainable implementations. The regulatory bodies like the Nigerian Electricity Regulatory Commission (NERC) is docile in carrying out its primary responsibility of regulating the power industries. The major stakeholders (the Generating, Transmitting and Distributing companies) are not playing by the rules. The regulators must be bold enough to heavily sanction any erring stakeholder. They must be compelled to research into the future. Major deadlines must be set and met as contained in laid regulatory policies as it relates to SGs deployment.

Furthermore, corruption has become a way of life of government officials and some highly placed private individuals in most developing nations to such an extent that in some quarters, open war is being declared to curb the menace as evident in Nigeria. Corruption also contributes a lot to power theft increase as discussed earlier. Increased budgetary allocations, good and consistent regulatory policies and a stiff penalty against corruption by the government will be helpful in SGs deployments.

7. Conclusion and Recommendations

Various threats militating against SGs deployments in developing nations have been briefly highlighted and discussed. Some of the ways by which SG deployments can be successful in these countries include understanding the basics and needs for SGs, increased public and private sector investments, research investments as well as well-structured regulatory policies and implementation. Investors must be made to play by the laid down rules. The regulatory bodies must be bold enough to carry out its statutory duties and sanction erring or compromising investors in accordance with the laid down law. Government must create enabling environments for businesses to thrive by addressing various agitations that often lead to public unrest. Power infrastructure must be jealously protected against theft and vandalism. Government must create public awareness on the need for citizen to jealously protect public infrastructures. Further research can be done by

identifying and classifying each of the source of threats for extensive research aimed at finding lasting solutions to factors militating against massive deployment of SGs.

REFERENCES

Abdulrahman, AT., Isiwekpeni, OH., Surajudeen-Bakinde, NT., and Otuoze, AO., 2016. Design, Specification and Implementation of a Distributed Home Automation System. *Procedia Computer Science*, *94*, 473-478.

African Economic Outlook, 2016. "Sustainable Cities and Structural Transformation".Accessed September 12, 2016 via http://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/AEO_2016_Report_Full_English.pdf.

Akorede, MF., Ibrahim, O., Amuda, SA., Otuoze, AO., and Olufeagba, BJ. 2017. Current status and outlook of renewable energy development in Nigeria. *Nigerian Journal of Technology*, 36(1), 196-212.

Alahakoon, D., and Yu, X. 2016. Smart electricity meter data intelligence for Future Energy Systems: A survey. *IEEE Transactions on Industrial Informatics*, 12(1), 425-436.

Altmann, M., Schmidt, P., Landinger, H., Michalski, J., Brenninkmeijer, A., Buscke, I., and Barquín, J., 2011. Effect of smart metering on electricity prices. *Study for the European Parliament, 130*.

Amin, SM., 2012. *Smart grid security, privacy, and resilient architectures: Opportunities and challenges.* Paper presented at the Power and Energy Society General Meeting, 2012 IEEE.

APANews.net. Mozambican power utility loses US$8m to energy theft, vandalism. Accessed May 16, 2017 via http://apanews.net/en/news/mozambican-power-utility-loses-us2018m-energy-theft-vandalism.

Bigerna, S., Bollino, CA., and Micheli, S., 2016. Socio-economic acceptability for smart grid development–A comprehensive review. *Journal of Cleaner Production*, 131, 399-409.

Colak, I., Fulli, G., Sagiroglu, S., Yesilbudak, M., and Covrig, CF., 2015. Smart grid projects in Europe: Current status, maturity and future scenarios. *Applied Energy*, 152, 58-70.

Eissa, M., 2015. Protection techniques with renewable resources and smart grids—A survey. *Renewable and Sustainable Energy Reviews*, 52, 1645-1667.

Fadaeenejad, M., Saberian, AM., Fadaee, M., Radzi, M., Hizam, H., and AbKadir, M., 2014. The present and future of smart power grid in developing countries. *Renewable and Sustainable Energy Reviews*, 29, 828-834.

Fan, X., and Gong, G., 2013. Security challenges in smart-grid metering and control systems. *Technology Innovation Management Review*, *3*(7), 42.

Fatemieh, O., Chandra, R., and Gunter, CA., 2010. *Low cost and secure smart meter communications using the tv white spaces.* Paper presented at the3rd International Symposium on Resilient Control Systems (ISRCS), 2010.

Gaur, V., and Gupta, E., 2016. The determinants of electricity theft: An empirical analysis of Indian states. *Energy Policy*, 93, 127-136.

Geelen, D., Reinders, A., and Keyson, D., 2013. Empowering the end-user in smart grids: Recommendations for the design of products and services. *Energy Policy*, 61, 151-161.

Genge, B., Kiss, I., and Haller, P., 2015. A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, 10, 3-17.

Gharavi, H., and Hu, B., 2013. *Dynamic key refreshment for smart grid mesh network security.* Paper presented at the Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES.

Giani, A., Bent, R., Hinrichs, M., McQueen, M., and Poolla, K., 2012. *Metrics for assessment of smart grid data integrity attacks.* Paper presented at the Power and Energy Society General Meeting, IEEE.

Gonzalez, M., 2014. Smart Grid Investment Grows with Widespread Smart Meter Installations. *Tech. Rep.*, Accessed on September 16, 2016 via http://vitalsigns.worldwatch.org/sites/default/files/vital_signs_smart_grid_final_pdf.pdf.

Jamil, F., and Ahmad, E., 2014. An empirical study of electricity theft from electricity distribution companies in Pakistan. *Pakistan Development Review,* 53(3), 239.

Jiang, R., Lu, R., Wang, Y., Luo, J., Shen, C., and Shen, XS., 2014. Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 19(2), 105-120.

Jokar, P., 2016. *Detection of malicious activities against advanced metering infrastructure in smart grid.* University of British Columbia.

Kemausuor, F., Obeng, GY., Brew-Hammond, A., and Duker, A., 2011. A review of trends, policies and plans for increasing energy access in Ghana. *Renewable and Sustainable Energy Reviews*, 15(9), 5143-5154.

Kessides, I. N., 2013. Chaos in power: Pakistan's electricity crisis. *Energy Policy*, 55, 271-285.

Kezunovic, M., 2011. Smart fault location for smart grids. *IEEE Transactions on Smart Grid*, 2(1), 11-22.

Khodaei, A., Wu, L., Aminifar, F., Bahramirad, S., Parvania, M., Qiu, F., and Kwasinski, A., 2016. Guest Editorial Power Grid Resilience. *IEEE Transactions on Smart Grid,* 7(6), 2805-2806.

Kreutz, D., Malichevskyy, O., Feitosa, E., Cunha, H., da Rosa Righi, R., and de Macedo, DD., 2016. A cyber-resilient architecture for critical security services. *Journal of Network and Computer Applications,* 63, 173-189.

Kumar, VA., Pandey, KK., and Punia, DK., 2014. Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. *Energy Policy,* 65, 126-133.
Lala, C., & Panda, B., 2001. Evaluating damage from cyber attacks: a model and analysis. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans,* 31(4), 300-310.

Li, H., Lu, R., Zhou, L., Yang, B., and Shen, X., 2014. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Systems Journal,* 8(2), 655-663.

Li, Q., and Cao, G., 2011. Multicast authentication in the smart grid with one-time signature. *IEEE Transactions on Smart Grid,* 2(4), 686-696.

Metering.com Data. Analysis: Prepaid electricity metering in Africa. Accessed May 21, 2017 via https://www.metering.com/features/analysis-prepaid-electricity-meters-africa/.

Mo, Y., Kim, THJ., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B., 2012. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1), 195-209.

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

Nikovski, DN., Wang, Z., Esenther, A., Sun, H., Sugiura, K., Muso, T., and 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. Springer. 379-389.

O'Malley, L., 2014. The Evolving Digital Utility: The convergence of energy and IT. Accessed September 20, 2016 via https://www.marsdd.com/news-and-insights/the-evolving-digital-utility/.

Rogers, R., 2013. Smart Grid and Energy Storage Technologies Spread. Accessed on 16th February, 2016 via http://www.worldwatch.org/smart-grid-and-energy-storage-technologies-spread.

Sharma, T., Pandey, K., Punia, D., and Rao, J., 2016. Of pilferers and poachers: Combating electricity theft in India. *Energy Research & Social Science,* 11, 40-52.

Shuaib, K., Trabelsi, Z., Abed-Hafez, M., Gaouda, A., and Alahmad, M., 2015. Resiliency of Smart Power Meters to Common Security Attacks. *Procedia Computer Science,* 52, 145-152.

Siano, P., 2014. Demand response and smart grids—A survey. *Renewable and Sustainable Energy Reviews,* 30, 461-478.

Smart Grid Top Markets Report 2017. – A Market Assessment Tool for US Exporters. Accessed on May 17, 2017 via http://trade.gov/topmarkets/pdf/Smart_Grid_Top_Markets_Report.pdf.

Sridhar, S., Hahn, A., and Govindarasu, M., 2012. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE,* 100(1), 210-224.

Stefanov, A., and Liu, CC., 2014. Cyber-physical system security and impact analysis. *IFAC Proceedings Volumes,* 47(3), 11238-11243.

The Guardian 2015. Niger delta oil pipeline vandalism estimated to cost $14bn a year. Accessed on Tuesday 10 November, 2015 via https://www.theguardian.com/environment/2015/nov/2010/niger-delta-oil-pipeline-vandalism-estimated-to-cost-2014bn-a-year.

ThisDay Newspaper April 19 2016. Rescuing Discos from Vandalism. Accessed January 23rd, 2017 via https://www.thisdaylive.com/index.php/2016/2004/2019/rescuing-discos-from-vandalism/.

ThisDay Newspaper May 9 2016. Vandalism and the Power Sector. Accessed April 10, 2017 via https://www.thisdaylive.com/index.php/2016/2005/2009/vandalism-and-the-power-sector/

Wang, W., and Lu, Z., 2013. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks,* 57(5), 1344-1371.

Wang, X., and Yi, P., 2011. Security framework for wireless communications in smart distribution grid. *IEEE Transactions on Smart Grid*, 2(4), 809-818.

Wei, D., Lu, Y., Jafari, M., Skare, PM., and Rohde, K., 2011. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid,* 2(4), 782-795.

World Bank Open Data 2016. Accessed September 15, 2016 via http://data.worldbank.org/.