

Detection and Prevention of Denial-of-Service in Cloud-based Smart Grid

Abdul Razaq¹, Muhammad Majid Hussain²^a, Waqas Javed³, Tasmiyah Javed and Zulfiqar A. Memon⁴

¹*School of Design and Informatics, Abertay University, Dundee, U.K.*

²*Department of Electrical & Electronic Engineering, University of South Wales, Cardiff, U.K.*

³*Department of Electrical Engineering, University of Engineering & Technology, Lahore, Rachna campus, Pakistan*

⁴*Department of Electrical and Computer Engineering, Ajman University, Ajman, U.A.E.*

Keywords: Cloud based Smart Grid, Denial-of-Service, IDS/IPS, Cyber-security.

Abstract: Smart Grid (SG), components with historical set of security challenges, becomes more vulnerable because Information and Communications Technology (ICT) has its own share of problems while Cloud infrastructure adds yet another unpredicted layer of threats. Scalability and availability, which are strong aspects of the cloud platform making it attractive to users, also attracts security threats for the same reasons. The malware installed on single host offers very limited scope compared to attack magnitude that compromised Cloud platform can offer. Therefore, the strongest aspect of Cloud itself becomes a nightmare in Cloud-Based SG. A breach in such a delicate system can cause severe consequences including interruption of electricity, equipment damage, data breach, complete blackouts, or even life-threatening consequences. We mimic Denial-of-Service (DoS) attacks to demonstrate interruption of electricity in SG with open-source solution to co-simulate power and communication systems.

1 INTRODUCTION

SG promises reduced energy consumption, lower production cost and robust transmission with intelligent distribution. SGs are exposed to a distinctive set of security threats because two different systems of Power Electronics and ICT are integrated to form a system with single core function: “Uninterruptable and Cost-Effective Energy Supply”. At the writing of this draft, not a single country has a true and complete SG setup in place. Beside the ordinary cost issues of installations or upgrading existing systems; critical question of reliability is unanswered. Cyber security for SG is of immense concern because of emerging cyber-threats and security incidents targeting smart grids all over the world. These threats are severe and obvious in SG systems if deployed without appropriate measurements. A cyber-attack at Maroochy Shire resulted in the release of untreated water and attack on Davis-Besse nuclear plant, USA, disabled the safety system (Yang, 2011). Stuxnet worm attack at Iran’s nuclear power station halted the work and a

recent bug termed as ‘HeartBleed’ in OpenSSL has initiated debate in the research community for dedicated security measures and re-assessment of user grade software solutions for multibillion national assets such as power grids.

Existing security measurements are insufficiently scalable, incompatible, or simply inadequate to address the challenges posed by highly complex environments such as smart grid. Below are the possible security threats originated by DoS attacks and general aspects of toolsets to emulate such models in terms of usability, extensibility, and accuracy

1.1 Security and Privacy in Physical Grid

The performance of power grid considerably relies on the actual physical devices and deployed environment; therefore, devices should be critically designed to sustain adverse environmental factors (Stouffer and Falco, 2006) and possible brutal force attacks. Master terminal units (MTUs) and remote

 <https://orcid.org/0000-0002-6255-6966>

terminal units (RTUs) controlling programmable logic controllers (PLCs) from generation to transmission systems require strict timing to control the demand and supply of electricity. Automation in SG is commonly accomplished with Supervisory Control and Data Acquisition (SCADA) system. SCADA devices are real-time or non-real-time (Muhammad and Siddique, 2020) small computer system that manipulates electrical outputs based on the condition of electrical input signals and program logic. In theory, these systems consist of Human Machine Interface (HMI) situated in operation facilities which are part of MTU. MTU is used to monitor RTU which is eventually connected to PLC for automation (Liu and Xiao, 2012). Data communication between RTUs and MTU occurs over wired telephone lines or wireless cellular technologies.

1.2 Security and Privacy in Information and Communications Technology

ICT provided necessary communication means and protocols for control and data exchange in SG. Security of interconnected devices and subsystems is important, but it should not result in a degraded and unreliable system. Efficiency and reliability should be achieved with only secure and complete open solutions (Hahn and Member, 2013). The (Bou-Harb, 2013) investigated communication in distributed networks and smart meters. They suggest that distributed devices and applications should follow design objectives including device authentication, data confidentiality, message integrity, prevention mechanism for cyber-attacks and facilitating communication overhead.

Historically (Galloway and Hancke, 2013), control in industrial automation was done mechanically with hydraulic controllers or manually. These mechanical components were upgraded once electronics such as transducers, relays and hard-wired control circuits became available. This changed to new dimensions when small microcontrollers were introduced which would allow smaller size and ability to connect over wire or wireless. Electronics based digital systems are able to remotely control and monitor various power grid components with various connectivity means and communication protocols. These communications protocols are commonly referred to as fieldbus protocols. Various protocols and technologies are being used in traditional power grids for networking purpose such as ModBus, ModBus+, ProfiBus, ICCP, DNP3, PROFINET, INTERBUS, WorldFIP, etc. It is important to note

that all these were designed without considering cyber security. Existing deployed communication protocols were developed under the umbrella of IEEE, IEC and DNP3. IEC 60870-5 and DNP3 are considered most widely used protocols in the automation industry. IEC is typically used in European countries and recognized by IEEE 1379 standard which is used in Asia and North America (Liu and Xiao, 2012).

1.3 Security and Privacy in Cloud-based Smart Grid

Cloud virtualization presents a logical view of resources while encapsulating heterogeneity, complexity, and distributed characteristics with unified interface. Cloud computing provides virtually aggregation of dispersed resources beside remote accessibility. The emerging technologies in Cloud based platforms present feasible solution for processing and storage thriving domains such as SG. Cloud-Based capability will allow ordinary resource limited devices in SG with low power CPU and limited memory to execute resource intensive security protocols. It is also important to note that Cloud platforms are prone to open access and anonymous attacks.

Data and software in cloud resides on network which poses a unique set of security and privacy challenges to the system. A survey conducted by (Bera, 2015) provides comprehensive discussion on Cloud applications for SG in contrast to conventional solutions that exist without Cloud. Traditional solutions need point to point physical connection whereas cloud can provide virtual control of any node without any real physical connection or media. Similar (Genge and Beres, 2014) survey on existing cloud-based solutions for SG without any details on security criteria concludes that security in cloud storage, communication paths between Cloud with Grid and security within SG are basic system requirements.

The (Markovic, 2013) provided comprehensive survey on cloud in SG. An interesting comparison is provided between conventional and smart grids and how cloud solutions can effectively apply in integration, reduced control latency, virtualized energy sources and load management. Study conducted on Los Angeles SG to address S&P in this development investigates software layers on various levels in cloud settings. The similar work is investigated by (Simmhan, 2011) and emphasis on data mining and aggregation of 1.4 million power customers in municipality of United States of America. Reporting, transporting, and storing huge

data (Bigdata) without native support of encryption can result in poor performance on Cloud platform. SG user applications should address privacy threats while utilizing datasets obtained continuously which represent user behaviour.

A comprehensive report published by (Akyol, 2012) under the umbrella of Department of Defence, United States concluded that power grids will eventually deploy cloud computing and this shift will be gradual only if the cyber security challenges are addressed. Report further recommends that utility providers must comply with NIST 2010 and NIST 2011 cyber security requirements analysis and design methodologies. A mechanism implemented on Eucalyptus open-source platform by (Baek, 2014) based on ID, encryption and proxy validation provides an ideal solution. However, cascading of trust layers can prove to be dangerous if cooperating layer is compromised. Proposed Smart-Framework is interesting as far as it fulfils the trust criteria.

The (Alcaraz, 2011) investigated this in very details of SCADA and how a virtual secure blanket can efficiently execute console to hardware commands with cryptic and efficiently. This virtual control not only provides access to resources but also guarantees scalability and availability with re-routing solutions for communication infrastructure. However, introducing virtual control layer over critical physical instalments would introduce latency which can result in fatal consequences. Recently, (Armando, 2014) investigated smart metering data in cloud with attribute-based control model. They have used open-source Energy Home platform for proposed security framework. Solution partially addresses the security access problem assuming that data transportation and storage is secured.

1.4 Denial-of-Service Threats in Smart Grid

(He and Chan, 2014) proposed a mechanism based on MicaZ and TelosB motes to resist DoS attacks against adversaries and legitimate insiders. They suggest that public key infrastructure (PKI) is valid solution for uninterrupted service; however, deployment of PKI is directly proportional with cost for large scale networks such as SG. Different security protocols have been suggested depending upon the applications' scalability and resources on board. (Lu and Wang, 2010) reviewed the security threats of DoS in DNP3 and classified these into three types: network availability, data integrity and information privacy, and evaluated their feasibility and impact on the smart grid.

(Liu, 2013) investigated DoS attacks on load frequency control (LFC) in SG while analysing dynamic performance of communication channels connected to RTUs in power systems. Case-studies of simulated DoS attacks were modelled as a switched (on/off) power system and two-area LFC theoretical model was built for different attack-launching instants. It has been concluded that adversaries can make power system unstable via DoS attacks if communication channels of RTUs are jammed. Similar work by (Liu and Chen, 2013) also investigated jamming threat but for wireless networks in the power systems. They suggested that traditional anti-jamming techniques can serve the purpose with additional measurements. A local controller with channel hopping is proposed to reduce possible DoS threats.

In (Manandhar, 2014) investigated theory of false data injection (DoS) attacks in power systems and proposed Kalman Filter (KF). They suggest that DoS attacks can be averted with linear quadratic estimation (KF) detectors for sensors in SG such as PMUs which measure current phase and amplitude in power systems. The projected values by KF and incoming instant values can be compared to detect an anomaly in the system.

Recently, (Sgouras, 2014) presented qualitative assessment of DoS attacks with simulation in OMNeT++ and INET framework. They examined performance of AMIs, routers and utility servers under such situation. An attack on AMI would result in minor consequences connected to single entity whereas similar scenarios for utility server would cause drastic effects during peak hours. Similar work was conducted by (Yi, Zhu, 2014) to demonstrate the impact of DoS in ICT without involving power grid simulation. They termed DoS attack as puppet attack which would penetrate in the system like warm and continue to congest the communication channels with false data until the network is exhausted.

1.5 Cloud based Intrusion Detection System and Intrusion Prevention System in Smart Grid

Intrusion Detection System (IDS) with Intrusion Prevention System (IPS) or combined Intrusion Detection and Prevention System (IDPS) is a system which is meant to detect and prevent the unwanted activity. In a cloud environment where infrastructure and resources are in the form of services, a system of IDPS should also adopt service-oriented design. (Patel, 2013) presented a systematic review of existing IDPS techniques and how they are

insufficient for Cloud platform. Classic IDPSs are unable to address security challenges that are presented in mix-network-topology, multi-user, and mixture of software layers in Cloud platforms. (Mohamed and Adil, 2013) adopted to monitor system calls generated by virtual machine's programs to the hypervisor. This approach is limited to and false alarm would be huge problem if legitimate, but not-document application is executed. This technique also suffers with typical system overloading and lower throughput problem as monitoring all the systems calls and their call sequence.

In Cloud computing IDS has its applicability on Virtual machine level. The (Alina, 2013) proposed a multilevel protection mechanism, the system consists of front-end control and IDS on virtual machines. Authors claim to reduce number of false alarms with efficient detection of real threats. This approach short falls if trust system is compromised, a similar attack reported but with different weigh will be undetected. Recently, (Li and Sun, 2012) proposed anomaly-based solution with neural settings for artificially sensing the activity. Neural configuration helps to distribute the workload of IDS to spread algorithm across Cloud rather chocking a single machine. This technique of load balancing is natural as far as all entities share the same interest and participate with resources and time. The (Vaid and Verma, 2014) proposed IDPS based on user behaviour to detect malicious activities, the proposed system is meant to be implemented as SaaS layer of cloud. In (Maiti and Sivanesan, 2012) presented simple but practical implementation of Cloud based intrusion detection system. The presented idea provides a simple yet robust example how cloud-based security service can leverage on vast resources for resource limited system.

A researcher (Tupakula, 2011) elaborated design suggestions for virtual machine based IDPS targeted for IaaS. Proposed design will require continuous monitoring of operating systems calls and application logging, this method is not ideal for systems with strict timing needs and limited resources untill data mining techniques are adopted. Researchers (Mehmood and Habiba, 2011) presented a comprehensive discussion on different solutions for Cloud security. Authors have suggested that IDS should utilize multiple or hybrid solutions for effective detection in Cloud security challenges. Recently, (Prajapati, 2014) critically investigated classical solutions and concluded that databases of incident used to detect anomaly have low reliability. This approach drastically increases the database size and can introduce latency in monitor and detector

functionality. (Sathya and Vasanthraj, 2013) also investigated Cloud based pattern matching IDPS and have introduced multilevel detection system. Their solution can suffer from overloading as auditing and logging will require ample resources and monitoring each activity will reduce overall system throughput.

In section 1 evaluate existing work in literature review that encircles challenges presented in SG system from power systems to communication technologies and cloud. Section 1 also describes possible security threats originated by DoS attacks and general aspects of toolsets to emulate such models in terms of usability, extensibility, and accuracy. Section 2 represents a proposed technique. Finally, work in progress is presented in section 3 with simulation of DoS in SG system for protected and insecure settings before concluding with discussion and future directions.

2 PROPOSED TECHNIQUES

In this section, we propose techniques to simulate DoS attack and methodologies adopted to address this attack (Abdul and Huaglory, 2016). Power and network architecture is presented with specifications of physical components and link layouts with functional configurations. Several solutions were evaluated as described in the literature review section. Most of these solutions simulate SG with a combination of network and power simulators (PS) based on commercial and open-source tools.

Our proposed simulation uses NeSSi2 due to its open-source license and ability to simulate power and IP networks as a single application. NeSSi2 is a scenario and profile-based simulation tool. Each network in NeSSi2 consists of at least one scenario which is eventually profiled depending upon required simulation. A scenario defines type of profiles that can be deployed on each node of the network. Multiple profiles can be deployed on a single node within a single scenario. A profile is a component to provide a specific set of functionalities incorporating single or various features relevant to power and IP network simulation, which can be deployed onto SG nodes. Finally, profiled scenario requires a simulation component which allows the mapping of power and network domains while linking the corresponding entities. NeSSi2 is capable to generate various attack scenarios and traffic analysis.

Figure 1 presents the high-level topology of proposed SG simulation for both networks. Power network is represented on the left side with the corresponding IP network presented on the right side.

Power network consists of one generator and two consumption subnets representing insecure and secure grid configurations. Parallel IP network also consists of similar topology with server as a main subnet connected to insecure and secure subnets. Mapping between power and IP network is configurable on node level within the simulation.

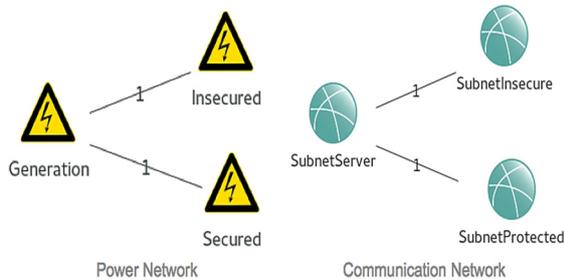


Figure 1: Proposed SG network topology.

Detailed configuration of proposed power network based on is shown in figure 2. The power grid consists of green generation based on solar panel with output of 5147W. Two step-down transformers with varying current of 380kV to 220kV are in place between generation and consumption which depict transmission and distribution. These swing bus profiled transformers are eventually connected to two consumption local grids: “Secure” and “Protected.” As solar generation is considered unreliable, depends on surrounding environment, a swing bus is used between the links from solar panel to transmission transformer. Swing bus accommodates system losses by emitting or absorbing active/reactive power to/from the system. The transformer connected to insecure subnet is profiled with line failure profile to simulate the unviability of load during power interruption. Line failure profile of NeSSi2 allows simulating the load unavailability in target power line between required time intervals. This line failure profile only accepts a single power link and can be mapped to one instance of application. Consumption subnets further consists of one transformer and two smart houses. These smart houses are capable to simulate load consumption and are mapped to corresponding IP nodes in IP network for communication simulation. Smart houses are capable to emulate load usage depending upon time, weather, and number of persons.

Configuration of proposed 100Mbps IP network is presented in Figure 3. Main subnet or Server subnet is connected to two subnets labelled as Insecure Subnet and Secure Subnet. Server node with Server subnet is profiled as Echo server application serving both connected subnets.

Server subnet is connected to insecure subnet without any protection mechanism in place, whereas, secured subnet is connected via front-end firewall. Moreover, secured subnet deploys additional firewall at client's interface level in case router has been compromised by malicious activity. DoS attacks simulated via BOT component are presented in both insecure and secure subnets. The firewall alone is not a sufficient solution; an Intrusion Prevention System (IPS) along with Intrusion Detection System (IDS) must be carefully designed and deployed side-by-side for complete protection. NeSSi2's firewall and packet sniffer profiles are very limited which results in restricted functionality.

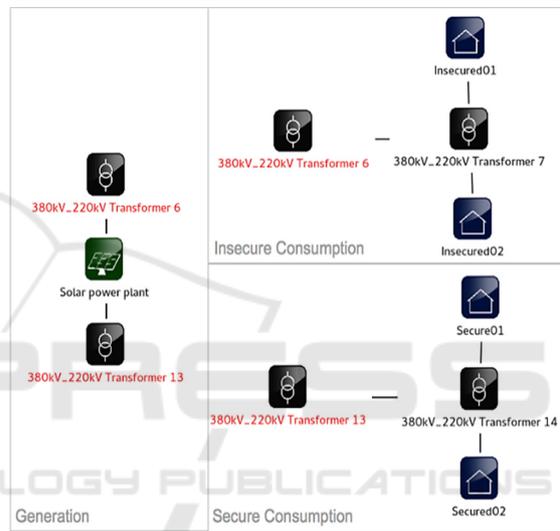


Figure 2: Power network layout.

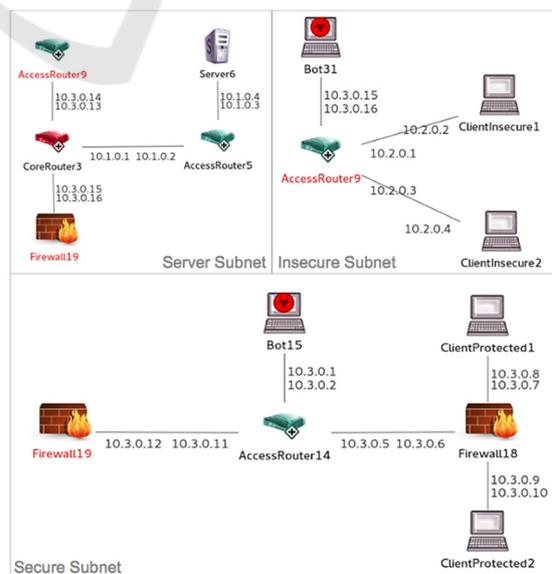


Figure 3: IP network layout.

3 SIMULATIONS OF DENIAL-OF-SERVICE ATTACKS AND DETECTIONS IN SMART GRID

All nodes of IP network are configured with default load (echo client/server) at the beginning of simulation, but the packet flow is increased to demonstrate the packet loss which is turn depicts the DoS. DoS or inability to serve the legitimate incoming requests is a phenomenon where system’s capacity has reached its maximum throughput and prompts to unavailability of given service. Ability to handle DoS attacks is crucial due to the power electric grid’s strict availability requirements. Botnet attack is emulated in both secure and insecure networks for DoS attack. The BOT profile of NeSSi2 is limited to only specify the attack start time and can only target single IP node. All these IP nodes are mapped to smart houses in a power network with a one-to-one relationship, which means that a house in a power grid has a counterpart IP client in an IP network.

This simulation is executed for 1000 ticks and failure or interruption of electricity and communication is simulated between 105-350, 500-600 and 800-900 ticks (time intervals). A tick is the smallest possible time interval (event) in NeSSi2. The actual time length depends on the simulation, simulation mode and underlying hardware platform. The solar panel model is set to produce 5147W peak production whereas smart houses are simulated for 5

persons each with 0.90% consumption of received load.

Figure 4 provides simulation statistics of 1000 tick of server’s echo response to secure and insecure subnet nodes. The communication packets are presented along vertical axis whereas horizontal axis present numbers of ticks or simulation time itself. Interruption of insecure subnet is visible between failed intervals with less density of packets compared to tick intervals for secure subnet. The successful or uninterrupted communication between server and secure subnet can be verified in figure 5 which demonstrated the continuous request sent by a secure client.

Communication of insecure client is presented in Figure 6. Packet drop statistics marked with cyan colour simulates the failure scenario when client was under attack from BOT and failed to process the echo packets. Successful echo request is marked in yellow colour whereas packets in magenta colour represent forwarded packets. The successful and drop packets can be compared with server’s statistics which illustrates the fewer number of packets during failed communication of insecure client. These failed intervals can also be cross-checked in figure 7 which presents the load statistic of insecure smart house. The mapping between insecure client and smart house is done prior to simulation and smart house is profiled with smart house consumption profile along line failure profile on transformer link level. The corresponding IP client is profiled with echo client and device failure.

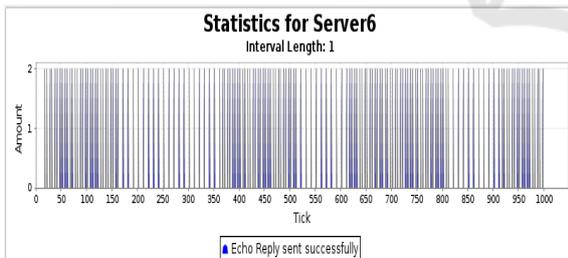


Figure 4: Server communication - secure and insecure subnets.

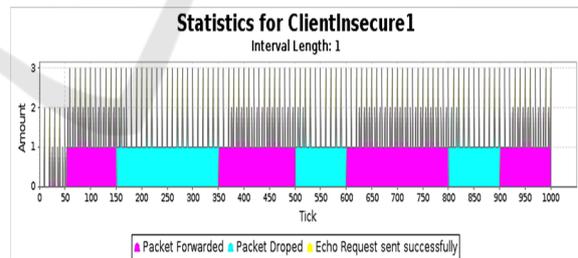


Figure 6: Insecure IP client.

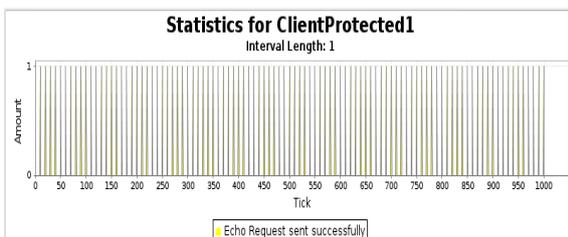


Figure 5: Secure IP client.

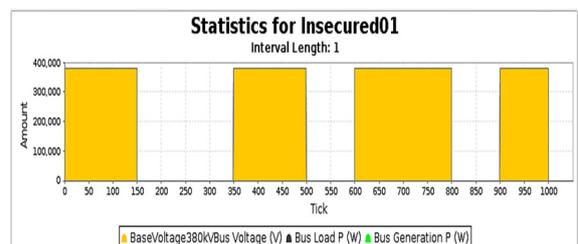


Figure 7: Power interruption of insecure house.

4 DISCUSSION AND CONCLUSIONS

Virtualization technologies in SG focus on availability, aggregation and accessibility of computing, storage, and network resources; without consideration of security. A shift to cloud-based SG is focused on the deliverability of services with respect to cost and throughput. However, security threats within these architectures not only remain the same but it is even more severe when deployed in a critical system of SG. Security in Cloud-based SG is complex because of its multi-layered nature. Which entity should be responsible for threat handling? Is it applications, devices, services, or infrastructure providers?

DoS is an instinctive security threat which include hardware failure to service interruption. Efficiency to revert DoS without considerable change in QoS is important both during under-attack and afterwards. Detection and prevention are a set of a single security function divided into two conceptual sub-functions: IDS and IPS. These two distinguishable methods offer first line of defence in the event of DoS attack. DoS and IDPS are also directly proportional in terms of resources. The more intense the DoS attack, the greater the resources of processing and data mining techniques are required for IDPS. Cloud based security-as-a-service technique for IDPS overcomes this classic limitation.

We examined the importance of SG for future energy requirements followed by detailed security challenges that are presented in Cloud Based SG systems. We demonstrated DoS attack and how this can cause the interruption of electricity while simulating the power and IP networks in parallel. We also simulated ICT configuration for SG security that can withstand DoS attack while ensuring the uninterrupted communication and power. Finally, we suggested that simulators for critical systems such as SG should be able to simulate defence techniques, including firewalls and IPS/IDS practices to avert possible attacks.

REFERENCES

- Akyol, B. A., 2012. Cyber security challenges in using cloud computing in the electric utility industry. *Pacific Northwest National Laboratory*.
- Alcaraz, C., Agudo, I., Nunez, D., Lopez, J., 2011. Managing incidents in smart grids a la cloud. *IEEE 3rd International Conference on Cloud Computing Technology and Science*. pp. 527-531.
- Armando, A., Carbone, R., Chekole, E. G., Petrazzuolo, C., Ranalli, A., Ranise, S., 2014. Selective Release of Smart Metering Data in Multi-domain Smart Grids. *Intl. Workshop on Smart Grid Security*. pp. 48-62.
- Baek, J., Vu, Q., Liu, J., Huang, X., Xiang, Y., 2014. A secure cloud computing-based framework for big data information management of smart grid. *IEEE Transactions on Cloud Computing*. pp.233-344.
- Bera, S., Misra, S., Rodrigues, J. J., 2015. Cloud Computing Applications for Smart Grid: A Survey. *IEEE Transactions on Parallel and Distributed Systems*. pp. 1477-1494.
- Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., Assi, C., 2013. Communication security for smart grid distribution networks. *IEEE Communications Magazine*. pp. 42-49.
- Galloway, B., Hancke, G. P., 2013. Introduction to Industrial Control Networks. *IEEE Communications Surveys & Tutorials*. pp.860-880.
- Genge, B., Beres, A., Haller, P., 2014. A survey on cloud-based software platforms to implement secure smart grids. *49th International Universities Power Engineering Conference*. pp. 1-6.
- Hahn, A., Member, S., Ashok, A., 2013. Cyber-Physical Security Testbeds: Architecture, Application and Evaluation for Smart Grid. *IEEE Transactions on Smart Grid*. pp. 847-855.
- He, D., Chan, S., Zhang, Y., Guizani, M., Chen, C., Bu, J., 2014. An enhanced public key infrastructure to secure smart grid wireless communication networks. *IEEE Network*. pp. 10-16.
- Hussain, M. M., Siddique, M., Raees, A., Nouman, M., Javed, W., Razaq, A., 2020. Power management through smart grids and advance metering infrastructure. *6th IEEE International Energy Conf*. pp.767-772.
- Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C. L. P., 2012. Cyber Security and Privacy Issues in Smart Grids. *IEEE Communications Surveys & Tutorials*. pp.981-997.
- Liu, S., Liu, X. P., Saddik, A. E., 2013. Denial-of-Service (dos) attacks on load frequency control in smart grids. *IEEE PES Innovative Smart Grid Technologies Conference*. pp. 1-6.
- Liu, H., Chen, Y., Chuah, M. C., Yang, J., 2013. Towards self-healing smart grid via intelligent local controller switching under jamming. *IEEE Conference on Communications and Network Security*. pp. 127-225.
- Lonea, A. M., Popescu, D. E., Tianfield, H., 2012. Detecting DDos attacks in cloud computing environment. *International Journal of Computers, Communications & Control*. pp. 70-78.
- Li, Z., Sun, W., Wang, L., 2012. A neural network based distributed intrusion detection system on cloud platform. *IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*. pp. 75-79.
- Lu, Z., Lu, X., Wang, W., Wang, C., 2010. Review and evaluation of security threats on the communication networks in the smart grid. *Milcom Military Communication Conference*. pp. 1830-1835.
- Maiti, A., Sivanesan, S., 2012. Cloud controlled intrusion detection and burglary prevention stratagems in home

- automation systems. *2nd Baltic Congress on Future Internet Communications*. pp. 182-186.
- Manandhar, K., Cao, X., Hu, F., Liu, Y., 2014. Combating false data injection attacks in smart grid using Kalman filter. *International Conference on Computing, Networking and Communications*. pp. 16-20.
- Markovic, D .S., Zivkovic, D., Branovic, I., Popovic, R., Cvetkovic, D., 2013. Smart power grid and cloud computing. *Renewable and Sustainable Energy Reviews*. pp. 566-577.
- Mehmood, Y., Habiba, U., Shibli, M. A., Masood, R., 2013. Intrusion detection system in cloud computing: challenges and opportunities. *2nd National Conference on Information Assurance*. pp. 59-66.
- Mohamed, H., Adil, L., Saida, T., Hicham, M., 2013. A collaborative intrusion detection and Prevention System in Cloud Computing. *AFRICON Conf*. pp. 1-5.
- Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J. C., 2013. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*. pp. 25-41.
- Prajapati, N. M., Mishra, A., Bhanodia, P., 2014. Literature survey - IDS for DDoS attacks. *Conference on IT in Business, Industry and Government*. pp. 1-3.
- Sathya, G., and Vasanthraj, K., 2013. Network activity classification schema in IDS and log audit for cloud computing. *International Conference on Information Communication and Embedded Systems*. pp. 502-506.
- Simmhan, Y., Kumbhare, A. G., Cao, B., Prasanna, V., 2011. An analysis of security and privacy issues in smart grid software architectures on clouds. *IEEE International Conf. on Cloud Computing*. pp.582-589.
- Stouffer, K. K. K., Falco, J., 2006. Guide to Supervisory Control and Data Acquisition (SCADA) and Other Industrial Control System Security. *NIST Guide to Industrial Control Systems (ICS) Security*.
- Sgouras, K. I., Birda, A. D., Labridis, D. P., 2014. Cyber-attack impact on critical Smart Grid infrastructures. *Innovative Smart Grid Technologies*. pp. 1-5.
- Tupakula, U., Varadharajan, V., Akku, N., 2011. Intrusion detection techniques for infrastructure as a service cloud. *IEEE 9th International Conference on Dependable, Autonomic and Secure*. pp. 740-751.
- Vaid, C., Verma, H. K., 2014. Anomaly-based IDS implementation in cloud environment using BOAT algorithm. *Proceedings of 3rd International Conf. on Reliability, Infocom Technologies and Optimization*. pp. 1-6.
- Yang, Y., Littler, T., 2011. Impact of cyber-security issues on smart grid. *IEEE PES Innovative Smart Grid Technologies Conference Europe*. pp. 1-7.
- Yi, P., Zhu, T., Zhang, Q., Wu, Y., Li, J., 2014. A denial-of-service attack in advanced metering infrastructure network. *IEEE International Conference on Communications*. pp. 1029-1034.
- Abdul, R., Huaglory, T., Bernardi P., Hong, Y., 2016. Simulating smart grid cyber security. *Taylor and Francis group: Smart Grid Networking, Data Management, and Business Models*. pp. 97-116.