Smart Grid Cyber Security and Risk Assessment: An Overview

Dharmendra Yadav , Dr. Anjali R Mahajan

Abstract:-A smart-grid for power distribution is a new electrical network based on the digital communication and complete control mechanism which provides energy reliability and energy security for the power distribution networks. It was globally accepted that, it is necessary to improvise the efficiency and reliability of the network for minimizing the distribution loss and security risk. Information and Communication Technologies (ICT) are at the centre of an effective smart grid implementation, but industrial control systems (ICS) and depended operational technology (OT) are also equally important to focus. Above all cyber security risk in smart-grid is a major concern due to large scale of cyber-attack. The fusion on traditional and advance distribution using smart components requires an in depth assessment of risk methods to cater to the both the systems. This paper surveys the risk assessments methods, major challenges and it controls for the various aspects of smart grid to handle the ongoing challenges.

Keywords: *Smart-grid, Risk assessment, Cyber security, Vulnerability, Reliability, Communication.*

I INTRODUCTION

The smart-grid concept was evolved around the year 2003, but the development and deployment of the smart-grid projects are in progress throughout the world. Smart Grids have great potential for the management of energy control in all kind of energy generating and distributing systems such as solar energy, wind energy, bio fuels, geothermal and hydroelectric energy to improve the economy, safety and durability [1]. But the great potential benefits also have high tremendous risks as well and protecting the smart grid systems from cyber security threats is a great challenges [1][2][17].

Smart-grid is a two-way communication network, where the grid operators and users of the system exchange information timely with the help of communication networks and control system. Supervisory Control and Data Acquisition (SCADA) is system in regards and it is being upgraded to "Wide Area Measurement System" (WAMS) for the transmission of line parameters for the dynamic characteristics monitoring. Smart meters refer as "Advanced Meter Infrastructure" (AMI) for smart-grid mechanisms involved in the distribution monitoring to end users. The data that is generated in the smart metering systems can possibly harm its stakeholders. Hence it is important to protect all the stakeholders by providing effective security and controls to the vulnerable elements in the smart metering system. This demands the importance to conduct a risk analysis to evaluate the harms, threats and vulnerabilities that are introduced into this smart modernized systems[5]. Currently there are numerous risk analysis methodologies available; there are many differences among them, and hence selecting an appropriate one is challenging.

Cyber security and risk is an important issue towards the information confidential problems in the communication network [7][17]. All the security measures taken to prevent the disclosure of information to a person or system should authorize correctly. Risk that technical experts perceive to be minor often elicits strong public concerns. Consequently during risk analysis, different perspectives need to be considered. In a smart-grid the definition of security means that the system can accurately measure data collection control centrally in a timely manner and effectively, preferably no transmission error of any incorrect data or tempered data should been sent to the control centre. The smart grid consists of a number of sub-systems that support an underlying grid infrastructure. The failure of a sub-system could cascade into another problem which can be closely related to cyber physical or security impacts. This paper provides a review on smart-grid cyber security vulnerabilities, challenges, risk assessment methods and controls. It also presents current cyber security and risk management works that aim to handle these challenges.

The rest of the paper organized as follows. Section-2 discuss the smart-grid communication system, Section-3 describes the smart-grid reliability for cyber security, Section-4 presents the smart-grid challenges and risks assessment, Section-5 discussed the solutions to the challenges of smart grid risk assessment and Section-6 discuss cyber security risk management and finally in Section-7 it conclude the conclusion of the review.

II SMART-GRID COMMUNICATION SYSTEM.

Smart-grid is a digital communications systems model for data Acquisition, as shown in Figure-1, where one or more regional control centre units integration in a plane to overseeing the operation of power plant and substations data acquisition control.

ISSN: 2278 – 7798

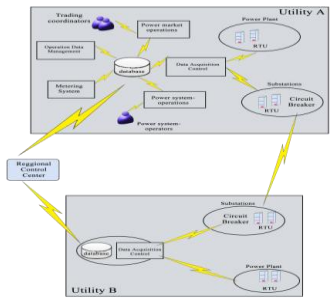

Figure1."Smart-grid Data Acquisition Communication Model" [3].

A smart grid performs data collection and power distribution in a layered structure. Most of the controlling mechanisms are performed by the regional control system which generally do data acquisition from the metering system and support in data management and power distribution operations. Whereas, substations manage to control the RTUs, HMIs, circuit breaker log storing servers and communication gateways[3].

The enhancement of the smart-grid with GPS provides real-time and accurate measurement of the widely distributed phase measurement units (PMUs) . A reference in GPS, PMU can accurately measure the positive sequence voltages and currents for each phase. Increases the accuracy of the estimate of the situation and notes to enhance the viability of the power network.

A. SCADA - Supervisory Control and Data Acquisition.

SCADA is a core of a substation system for monitoring and control. It helps in achieve higher reliability utilizing distribution automation and remotely control medium voltage through computerization to reduce the maintenance costs. Today, SCADA is a reliable wireless communication using more than one channel, and a powerful integrated solutions is provided remotely using installed electrical equipment by RTUs. In Distribution Management System (DMS) SCADA RTUs is the leading vendors worldwide seamlessly interface with the control canter with a wide range of high performance [20].

B. Communication Network.

The demand of electricity, operational and commercial requirement are need to be considered. Also, need to see requirements of existing and future functionality that supports data communication networks and require a high-performance. Such communications applications form the core of a network of electric automation system. In [36] a hybrid network framework is discussed and it also presents the challenges and risk causes in the electric automation system.

Internet-based virtual private network (VPN), power line communications, wireless communications and satellite communications systems in the electric hybrid network framework can support heterogeneous data requirements to the automation application. A smart electricity grid communications network is expected to be a structured framework for automation of new technologies of communication, and, therefore, to be used in the decision-making process more efficient and direct.

Scalable and smart-grid network systems in a variety of different solutions for the communications networking structures. Advanced metering infrastructure (AMI) solution can be meshed or point-to-point, short or long range wireless broadband local communications coverage[21] . Solutions, such as "WiMax, WLAN, WSN, cellular and LMR", reliability, performance, and as a hedge, depending on the desired use. Wireless communication solutions can be either licensed or unlicensed, again depending on the needs of the utility. For maximum reliability, should be allowed to choose. Each option has its advantages and disadvantages, but what is true and solutions to consistently be a security solution is scalable [22].

III. SMART-GRID RELIABILITY

The legacy cyber business network security techniques are unlikely to be safe and it required internet for data communication and well suited to a smart-grid communications system. Comparatively regular business network systems and smart-grid network communications systems are needed to be protected from cyber attacks[15]. It is important for real-time performance and ensure continuous operation of a system of smart-grid communications. These applications are not originally designed for global business network environment. Therefore, it is necessary for security solutions where they fit, among other things, a control canter and or a sub-station within the communications networks to embrace, and to develop a unique solution in the gaps where traditional business network does not work in cyber security solutions application[28].

Reliability of a smart-grid network relies on the trust, secure and availability of the control over communications application systems[19]. The developed smart-grid communication systems are becoming better control and increasingly sophisticated for allowing and higher reliability[31]. Smart network connection degrees high, it will be necessary to support the new features. Meanwhile, a

ISSN: 2278 – 7798

higher level of connectivity, sophisticated security protocols to deal with cyber security attacks and risks.
The general requirements for a high level of security in relevant to safety requirements are privacy, availability, integrity, authentication and authorization and dependability. In the following section we discuss these requirements.

A. Privacy.

Privacy issues were able to be derived from the privacy of customer data which covers the consumption measurement devices. Consumer data can be used to gain insights into the behavior of a client's information [25].
Smart-grid communications and customer privacy have unintended consequences. Shortly after the smart meter storage, and distribution instructions for use of light acts as a channel of information rich side, customers' habits and behaviors show. Most of the activities, such as viewing TV, they have signatures to detect energy consumption. Financial or political incentive to align the place where history data need to conduct data mining techniques to quickly evolve to match the desires of those who would exploit the information's [29].

*B. Availabilit**y.***

Availability cannot deny access to unauthorized persons or systems or ensuring that authorized users. The blocks of smart-grid systems, such as generation plant, systems controlling, security systems, working stations, engineering workstations, manufacturing execution systems, and components build a synchronize systems for communication between blocks and the outside world. Malicious cyber attacks targets the availability of denial of service (DoS) attacks to delay or even grid network nodes that can be considered to be available for communication and in information exchange it damaged a block transmission of information and network resources. Therefore, it is essential that the impact of DoS attacks on smart-grid and effective countermeasures to evaluate the design of these attacks [15][37].

C. Integrity.

Integrity prevents inadvertently changing of the integrated information systems refers to unauthorized persons.. The objective information integrity is to the transformation of the defense-mail injection, called the message, and the message over the network to another delay. Violating the integrity of security can cause risks and can harm to the equipment or peoples.
The risk of attacks on the integrity of the data-driven power networks is, in fact, true. One of the most notable recent work [27], a new type of attack, called the proposed false data injection attacks. A meter at risk of an attacker already has assumed, and stressed that the attacker can take advantage of a power system configuration to launch attacks injecting false data monitoring canter, which will check the integrity of the data used by the legitimate need to overcome the current power systems.

D.Authentication and Authorization.

Authentication is a true part of the communications system and the identity of a major internal mapping system which is concerned about the determination of the user identity for a known system. Most other security objectives are notably authorization, authentication of users to distinguish between legitimate and illegitimate.

Authorization, described as an access control to a system or people to prevent unauthorized access to the system. In a broader sense, the mechanisms to distinguish between legal and illegal users of all other security objectives, for example, confidentiality, integrity, and so in this sense refers to tighter access control, limiting its ability to issue commands to the plant control system. Violation of authorization may cause security issues.

E. Dependability.

The new design of the smart-grid communications systems is to form a layered framework. Smart-grid network systems, software applications associated with the growth of the power system resulted in numerous fluffiness. It developed a variety of programming languages and platforms extending or usually leads to the development of new and old applications to integrate with legacy systems. Therefore, it cannot be approached in the future smart-grid network security as a new beginning.
Along with the developed systems for smart-grid communications, cyber security infrastructure and monolithic form, is not a viable option. Instead, multi-layer frameworks and advanced methods of control and dependable software and hardware infrastructure, as well as monitoring mechanisms for the protection of the devices at the same time is determined. Dependable software infrastructure as well as to identify and isolate the upper-layer applications can be designed in order to secure an independent cross-layer communication. In addition, the flexibility of the architecture part of the exchange, or to update the system in safe mode and new laws and regulations or in the future due to new developments in the energy market [23].

ISSN: 2278 – 7798

IV. SMART-GRID CHALLENGES AND RISKS ASSESSMENT

Smart-grid technology developments and architecture designing approaches standards are based on the variety of regulations to support the challenges of the future electricity network. This objective of smart-grid network communications architecture, cyber security and cyber security architecture requirements, dependency facilities to promote the heritage and the regulations presented based on industry standards.

To build and operate a secure communications system for smart-grid main challenges include smart-grid networks, security services and security policy and operations differences between the network and security.

A. *Smart-grid Networks.*

The network of smart-grid are interconnected with communication systems but due to the lack of change in the network there are full of vulnerabilities in many built-in security applications and devices. It should not be as important as the smart-grid network model. Cyber security must be built into the solution to smart-grid network layers through the interruption, interception, modification and manufacturing to minimize threats. Where all means of transport for private networks are a tool to maintain a wholly owned, would be reduced by a lot of foreign threats, there would be no access to the Internet for potential intruders. Effective business knowledge communication helps to re-use of the Internet and minimize the secured internet connection which is typically found in a commercial network and these networks are open to all sorts of threats of attack. Among them, a group of cyber-attack enemy cause an interruption of power supply [29] [24].

An internet connection is to be very safe in a smart-grid network. The need of Intrusion detection is, not only to the inner vulnerable points [4][16],whereas internet connects a network of smart-grid network, but it is also a severe prone to attacks point for a wireless network interface[3].

B. Security Services.

The management and maintenance of a secure smart-grid, equally important, and the development of a solution to integrate the smart-grid will be safe. Security services operators are to recognize control and manage security risks in the smart-grid network communications. High-performance security services, mobility, security and cost-effective system integrates the expertise which includes a smart-grid network access. Security services can be designed to best suit their needs and their usefulness in achieving organizational objectives. Figure-2 presents a typical security services, smart-grid network communications [26]. People, processes, policies and technologies on the basis of each organization describes a framework for cyber security operations.

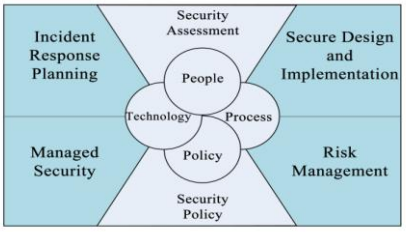

Figure-2: "Security Services of Smart-grid"[26]

C. Security Policy and Operations.

A smart-grid network reliability of components and the proper operation of many of these depends on the proper connectivity. Interrupted by an attacker access to an electronic component, and configure in smart-grid network system look like one of the other ingredients and a report or alarm conditions might attempt. That adversary might attempt to attack one of the easiest types of DoS attacks, where the adversary by authorized devices to communicate from one device to prevent excessive consumption of resources.

Many industries and researchers will be involved in the operation of a smart-grid network. Then the smart-grid communication network distributed intelligence entities are added, it will be necessary to determine the status of these entities in the remote authentication and authorization from one organization to another entity. Great care must be taken to safety organizations have policies and practices do not conflict with these other institutions will have to ensure interoperability. A smart-grid network of organizations operating in at least the minimum of a set of operational security policy is formally approved and documented as industry standards [30].

D. Risks Assessment.

The main objective of risk assessment is to identify threats and cyber security vulnerabilities and determine their impact[9][10]. The risk assessment results in terms of safety and security controls should be used in the determination of an intelligent network selection. Risk assessment implements both top-down and bottom-up approach for the assessment[33]. In addition, existing methods of risk assessment is divided into quantitative and qualitative

ISSN: 2278 – 7798

approaches. And the probability of a threat to the effect that the use of quantitative metrics. This often proves difficult circumstances as a result of a shortage of reliable data and subjective, qualitative approach, which will also take advantage of other sources of information that are not easily quantifiable can be used instead, as the threat may be able to view graphics and game theory models[8]. A database of risk assessment standards, approaches and tools are maintains by European Network and Information Security Agency (ENISA)[34].

ICT dealt with information security risk assessment is defined in the conventional system, the risk assessment of intelligent networks is still in its infancy. System stakeholders, utility providers, manufacturers and system developers, and intelligent network of risk assessment remains a huge challenge for several reasons: the areas of risk assessment, focused mainly on conventional as well as ICT systems[6][13], or is the traditional power network[35][36]. This means that the smart grid cyber security risk assessment for the safety aspects that must be met.

It was observed that risk assessment is addressed in small number in most of the designed framework for critical infrastructures. A high level of security guidelines applicable for smart grid security and assessment is developed by NIST for the U.S[12], but it is not provided any general approach for risks assessment in cyber security. But no specific methodology is recommended for selecting the appropriate measures that highlighted the importance of a comprehensive risk assessment. Performance and Risk-based Integrated Security Methodology (PRISM) based security management guideline is developed for the European Commission to perform risk assessment for energy grid [18]. With any of the security controls in place SGIS proposed risk assessment assuming that the future of the smart grid which takes a clean-slate approaches[14][11]. As a result, the system undergoes a transformation, which is growing into the power grid set up in such a way that it does not reflect smart grid. Therefore, as a practical cyber risk management policy must deal with the many challenges of a complex combination of legacy systems and new technologies[7].

V. SOLUTIONS TO THE CHALLENGES OF SMART GRID RISK ASSESSMENT

We are in an ongoing investigation by the smart grid-related programs will look for the challenges in the implementation of a risk assessment.

A. Smart Grid Security Guidance (SG).[2]

Smart Grid Security Guidance is an Austrian smart rid security guidance project developed for the assessment of cyber security. This method is based on the definition of a national reference structure, and run the legacy systems and can be applied to both the near-term future developments. Conceptual analyses of the risks for the future development of existing systems, which are complemented by practical security measures are evaluated.

B. EMC[2]

Schmittner et al.[3] proposed and developed a safety analysis technique as EMC[2] based on the extension of FMEA analysis and funded by Artemis . It objective is to targets to analyze the impact of cyber attacks on the safety measures. This project is embedded in multi-core systems mostly found implemented in the automotive industry. It will enable us to directly compare the safety and security incidents, threats and support analysts actors, among others, the incentives and the ability to determine the action. While the aspects of this project is to study the safety and security for embedded systems based on the technique of smart-grid network components and sub-systems can be tailored to the specific analysis.

C. *HyRiM - Hybrid Risk Management.*

Hybrid Risk Management project is for utility Providers. The utility networks can be applied to the development of novel techniques for risk analysis. One aspect of the project are part of a study investigating the effects of cascading, and through which electricity grid corresponds to the effects of events in the transport system. HyRiM are based research and smart grid, which is connected to each other and the power of ICT networks and sub-system consists of more than necessary.

D. SECCRIT - Secure Cloud computing for Critical Infrastructure IT.

Secure Cloud computing for Critical Infrastructure IT project provides high-assurance of ICT services, including services that enhance critical infrastructure, in order to study how to support the implementation on the Cloud. A cloud-specific threat and vulnerability services should be applied to the catalog for developed and understand the risks associated with migrating to Cloud. Cloud assess the risks associated with the use of similar challenges as those for the smart grid, there are a number of organizations in relation to the risks of the complex responsibilities.

E. SPARKS - Smart Grid Protection Against Cyber Attacks.

Smart Grid Protection Against Cyber Attacks projects focus on the cyber security and smart-grid network of resistance is being investigated with appropriate methods of risk assessment. The project will make a special contribution to the attack scenario simulation and modelling, and a

ISSN: 2278 – 7798

cyber-attacks on the smart grid can be used to understand the potential impact.

VI. CYBER SECURITY RISK MANAGEMENT

Smart-grid's is a reformation of the electrical system, along with two-way movement of electricity and information, information technology (IT) and telecommunications infrastructure has become a severe infrastructure in the energy sector. Global cyber security strategy for Smart-grid is to alleviate these conditions and infrastructure development as well as domain-specific solutions for the different parts of a common strategy to ensure effectiveness.

Therefore, management and infrastructure, and to protect the components risks of these systems will also have to get more and more diverse energy sector. This is required to achieve the level of security that the architectural design. "Smart-grid Cyber Security Coordination Task Group" (CSCTG) established by NIST, which is now more than 200 volunteers in the public and private sectors which includes academia, regulatory and federal agencies are working to mitigates the cyber security risks.

The establishment of a cyber-security strategy, generally requires the needs of a risk management framework for Smart-grid. Both the sectors are in this framework and the risk management is based on the existing approach. The risk management framework on smart-grid and its domains and sub domains, such as houses and businesses, is expected to produce the effect of the threat, vulnerability, and threat to the information set out to combine the processes.

The additional risks to the smart-grid can be due to as follows:

- Due to the complexity of the grid and weaknesses and the potential attackers mistakenly, increase exposure to increase the present imperfections.
- Interconnection networks are more prone to common vulnerabilities.
- Communications disturbances and the introduction of harmful software vulnerabilities that can cause denial of service (DoS) or compromise the integrity of systems and software.
- Increase the number of access points and pathways for prospective adversaries to exploit.
- The prospective to endanger the confidentiality of data, among other things and breach of customer privacy.

VII. CONCLUSION

Smart-grid as a service provider framework requires comprehensive cyber security solutions. It requires security solutions for the communication based on the traditional schemes security such as authentication, PKI mechanism and trusted computing mechanism and it is also clear that standards-based smart-grid communications infrastructure requires the state-of-the-art security to ensure the use of communication protocols. Smart-grid networks of the future for many of the new requirements can only be met through the support of a wide range of ICT infrastructure will be able to respond. This changes the importance of cyber issues: safety and reliability of the electricity network has been in the focus of security considerations, until now, cyber attacks as well as emerging risks to consider in the future. ICT is focusing in the areas of risk that cannot be immediately applied to smart-grid networks. Even specific security for the smart-grid is exists for the cyber risk assessment and special challenges associated with the networks, such as the relationship between safety and security risks, mix of legacy systems and novel systems are often failed, or unable to understood the potential cascading effects. Many research works are in progress to meet the current challenges. Smart-grids are a common target of these efforts, understanding and support smart grid stakeholders and assessing vulnerabilities and cyber threats, and cyber and energy security assessment processes by integrating systems to provide guidelines for effective risk management.

REFRENCES.

[1]. Yu, W.,Xue, Y., Luo, J., Ni, M. , Tong, H. and Huang, T. "An UHV Grid Security and Stability Defense System: Considering the Risk of Power System Communication", IEEE Transactions on Smart Grid, Volume-99, pages-1, Feb. 2015.

[2]. Rui Wang, "Research on information security strategy and risk management for smart grid", IEEE China International Conference on Electricity Distribution (CICED), Page 1392-1396, Sept. 2014.

[3]. Christoph Schmittner, Thomas Gruber, P.P., Schoitsch, E.: Security Application of Failure Mode and Effect Analysis (FMEA). 33rd International Conference on Computer Safety, Reliability and Security (SafeComp), 2014

[4]. Xiao Liang,Kunlun Gao, Xiaokun Zheng and Ting Zhao "A Study on Cyber Security of Smart Grid on Public Networks", IEEE, Green Technologies Conference, Pages 301-308, 2013.

[5]. Rani Yesudas, Roger Clarke, "A Framework for Risk Analysis in Smart Grid", Springer International Publishing,978-3-319-03964-0, Computer Science Volume-8328,pp 84-95, 2013.

[6]. Brasca. C., Ciapessoni. E., Cirio. D., Pitto. A., Sforna. M. and Morini. A. "Extended risk analysis of power and ICT systems", IEEE Conference on Innovative

ISSN: 2278 – 7798

Smart Grid Technologies Europe (ISGT EUROPE), Pages: 1-5, 2013.

[7]. Wenye Wang, Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges", Elsevier Computer Networks, Vol-57, Pages-1344–1371, 2013.

[8]. Mohammad Hossein M, Quanyan Zhu, T Alpcan, Tamer B, and Jean-Pierre H, "Game theory meets network security and privacy", ACM Computing Surveys. 45(3), July 2013.

[9]. Farzan. F.Jafari. M.A., Wei. D., Lu. Y., "Cyber-related risk assessment and critical asset identification in power grids", IEEE Innovative Smart Grid Technologies Conference (ISGT), Page(s): 1 - 5, 2014.

[10]. Buhari. M., Kopsidas. K., Tumelo-Chakonta. C. and Kapetanaki. A., "Risk assessment of smart energy transfer in distribution networks" IEEE Innovative Smart Grid Technologies Conference Europe (ISGT-Europe),Page(s):1-6,2014.

[11]. CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, December 2013.

[12]. NIST, NISTIR 7628 – Guidelines for Smart Grid Cybersecurity, 2013.

*[13]. Federal Office for Information Security (BSI)(*http://www.bsi.bund.de/gshb),IT *Baseline Protection Catalogs, 2013.*

[14]. CEN-CENELEC-ETSI Smart Grid Coordination Group, Reports in response to Smart Grid Mandate M/490, 2012.

[15]. X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu: Securing smart grid: cyber attacks, countermeasures, and challenges, IEEE Communications Magazine, vol. 50, no. 8, pp. 38–45, August 2012.

[16]. P.-Y. Chen, S.-M. Cheng, and K.-C. Chen: Smart attacks in smart grid communication networks, Communica- tions Magazine, IEEE, vol. 50, no. 8, pp. 24–29, August 2012.

[17]. Ye Yan, Yi Qian, Hamid Sharif and David Tipper, "A Survey on Cyber Security for Smart Grid Communications", IEEE Communications Surveys & Tutorials, Vol. 14, No. 4, Fourth Quarter 2012.

[18]. A Reference Security Management Plan for Energy Infrastructure. Prepared by the Harnser Group for the European Commission under Contract TREN/C1/185/200. 2010. Available at http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf

[19]. Shipman. C.M., Hopkinson. K.M. and Lopez, J., "Con-Resistant Trust for Improved Reliability in a Smart-Grid Special Protection System", IEEE Transactions on Power Delivery,Volume-30,Issue-1,Page(s): 455 - 462, 2014

[20]. S. Hong, and M. Lee, "Challenges and Direction toward Secure Communication in the SCADA System," IEEE Eighth Annual Communication Networks and Services Research Conference (CNSR 2010), pp.381-386, 2010.

[21]. L. Wenpeng, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in IEEE Transmission and Distribution Conference and Exposition, pp.1-4, 2010.

[22]. P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in IEEE Power and Energy Society General Meeting,pp. 1-7, 2010

[23]. N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "Trust infrastructures for future energy networks," in IEEE Power and Energy Society General Meeting 2010, pp. 1-7, 2010.

[24]. L. Husheng, M. Rukun, L. Lifeng, and R. C. Qiu, "Compressed Meter Reading for Delay-Sensitive and Secure Load Report in Smart Grid," in First IEEE International Conference on Smart Grid Communications (SmartGridComm2010), pp. 114-119, 2010.

[25]. G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 232-237, 2010.

[26]. A. R. Metke and R. L. Ekl, "Smart Grid Security Technology," in Innovative Smart Grid Technologies (ISGT2010), pp. 1-7, 2010.

[27]. Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. ACM Conference on Computer and Communications Security (CCS 09), Sept. 2009.

[28]. J. Fan, S. Borlase, "The evolution of distribution," IEEE Power and Energy Mag., vol. 7, pp. 63-68, 2009

[29]. P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security & Privacy, vol. 7, pp. 75-77, 2009

[30]. R. J. Thomas, "Putting an action plan in place," IEEE Power and Energy Mag., vol. 7, pp. 26-31, 2009.

[31]. Xindong Liu, Shahidehpour. M., Yijia Cao, Zuyi Li and Wei Tian, "Risk Assessment in Extreme Events Considering the Reliability of Protection Systems" IEEE Transactions on Smart Grid, Volume-6, Issue-2,Page(s):1073-1081, 2014.

[32]. V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," Computer Networks, vol. 50, pp. 877897, 2006.

[33]. NIST, Smart grid cyber security strategy and requirements, NISTIR 7628.

[34]. ENISA, Inventory of risk management/risk assessment methods and tools. http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory.

[35]. NERC, Security guidelines for the Electricity sectors: vulnerability and risk assessment.

[36]. ISA, Security for industrial automation and control systems: concepts, terminology and models.

[37]. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defence mechanisms," SIGCOMM

ISSN: 2278 – 7798

Comput. Commun. Rev., vol. 34, no. 2, pp. 39C53, 2004.

Dharmendra Yadav received the B.E and M.Tech degrees in Computer Technology and Computer Science respectively. He is pursuing PhD from G H Raisoni College of Engineering, research Centre under Nagpur University . He is IRCA ISO 27001:2013 Lead Auditor on Information Security from British Standards Institute. He is National EC Member of ISTE .He is currently an Assistant Professor in Computer Science and Engineering department at Govt. College of Engineering and Technology Bikaner, India.

Dr. Anjali R Mahajan , currently working as Head of Department ,Govt. Polytechnic, Nagpur, completed her B.E. in Computer Science and Engineering from Government College of Engineering, Amravati in the year 1994, M.E in Computer Science and Engineering from Sant Gadge Baba Amravati University in the year 2002 and Ph.D. in Computer Science and Engineering from Sant Gadge Baba Amravati University. Dr. Mahajan has to her credit several publications in National, International Journals and National, International conferences. Dr. Mahajan is recognized guide for ME by research and Ph.D in Computer Science and Engineering.Dr. Mahajan is Life Member of ISTE, CSI and member of IEEE.

ISSN: 2278 – 7798