INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at www.ijariit.com

Evolving Cyber Security Challenges to the Smart Grid Landscape

Seema Goel
National Law School of India University
goelseema11@gmail.com

Ashish Jindal
Devi Ahilya Vishwavidyalaya
ash.jndl@gmail.com

Abstract: Integrating smart solutions into the existing power infrastructure promises to offer attractive capabilities of dynamic monitoring, measuring and even controlling power flows in real time that can help identify losses and trigger appropriate technical and managerial actions to minimize the damage. With the vision of building a Smart

India, Government of India's National Smart Grid Mission (NSGM) is solely aimed at providing functional resources and financial assistance in planning and implementation of smart grids across the nation. NSGM proposes comprehensive solutions for the development, establishment, operations and management of smart grids, stipulate training & capacity building, strengthen consumer engagement and dispense funding to state-owned DISCOMs.

Smart grid solutions vastly employ information technology in the underlying roots in varying forms of networking and application aspects to enable monitoring and control of the flow of electricity to end users. The extensive incorporation of information technology provides numerous benefits to the grid operations and management, such as increased visibility, predictability, in addition to the regulation of generation and demand to improve efficiency.

However, this enhanced use of information technology to the grid has in parallel introduced the dimension of cybercrime to the smart grid as the grid is now constantly connected to the Internet and can be exploited by hackers by leveraging the wide array of cyber security vulnerabilities. Security of the smart grid is essential to ensure uninterrupted power supply and minimize resulting losses. Compromise of the grid may result in a huge information or business losses by the means of cyber espionage or grid collapse. An uninterrupted power supply lies at the heart of all sectors and failures to the same will result in cascading damages, compelling the establishment of robust smart grids. The paper offers insight into key cyber security threats and vulnerabilities concerning the smart grid technology and proposes protection strategies, methodologies, and technologies to safeguard the smart grid from resulting security damages.

Keywords: Cyber Security, Smart Grid, SCADA, Smart City, Cyber Attack.

I. INTRODUCTION

The Smart Grid is referred to as the evolutionary next-generation power distribution system. Smart Grid will conceptualize the two-way communication channel in contrast to the unidirectional channel existing in the traditional grids to deliver a radical large-scale, highly distributed, and hierarchical communication network.

Different hardware, software and networking the work together in the core of smart grid architecture. This together increases the complexity of the smart grid resulting in an increased array of security vulnerabilities. Cyber-attacks on the smart grids have already been realized and are here to stay. The next sections highlight the growing adoption of smart grids worldwide and the security concerns multiplying in the parallel.

II. THE GROWING IMPORTANCE OF SMART GRID

The power sector in India had an installed capacity of 310 GW as of December 2016[1], which stands fourth largest in the world with even the per-capita consumption yielding one-fourth of the world's average. The prime reason attributing to the low consumption of electricity is the lack of accessibility of the core electrical network to a substantial geography across India. Researchers have estimated that by 2032, the potential demand for electricity may reach to attain a mammoth capacity utilization

of 900 GW. Recently, India announced its projected renewable energy generation target of a significant 175 GW, contributed by 100 GW from solar power, 60 GW of wind power, 10 GW of biopower and 5 GW of small hydropower by 2022 [3]. With this vast reliance on renewable energy to optimize the energy value chain, efficient management plays a key role.

India also recently launched a National Electric Mobility Mission Plan (NEMMP) [4] with a target of 6 million electric vehicles (4 million two-wheelers and 2 million four-wheelers) by 2020 in order to promote hybrid and electric vehicles in the country. Such visionary measures display the criticality and urgency to exalt electrical distribution infrastructure with a smarter system which will control simultaneous charging of multiple electric vehicles from the same feeder. Corresponding support from policy enhancement to strengthen the infrastructure for integration of Electric Vehicles which can store energy during surplus generation and support during moments of the deficit.

The traditional power system in India is faced with the constant challenge of huge transmission and distribution losses across the nation. The reasons may range from the varying weather conditions to dynamic user behaviour. This leads to a variation in the energy demands, at differing levels. Increasing population with high usage of electrical dependent devices ranging from air-conditioners, electric heaters, geysers, microwave oven, CFLs lights etc. stresses the sanctioned electric load capacity. The underlying electrical infrastructure is primarily designed for worst load conditions in order to cater to maximum load requirements, so typically during non-peak hours, the system is typically underutilized. Such utilization and performance issues with the existing electrical architecture lead to the requirement for a smarter and intelligent system that automatically adapts to the underlying variations in electricity generation and consumption.

Smart grid is an electrical network which uses digital and cutting-edge technologies to meet the dynamic electricity demand of users by effectively and efficiently managing the transmission of energy from various generation sources like wind, solar, coal, nuclear etc. Thus, it helps to minimize environmental impact and operational cost by prioritizing the type of energy like giving precedence of renewable over the non-renewable source. It also helps to maximize system consistency, traceability and stability.

III. BENEFITS OF SMART GRID TECHNOLOGY

The benefits offered by the smart grid notably reduce power losses which are quintessential for successful and sustained energy ecosystem.

Fig 1- Benefits of Smart grid Technology

Smart grid technology helps to monitor, measure and optimize the electricity network management in real time that further assist in identifying the present losses and thus with proper technical and managerial actions, minimize the resulting unavoidable leakages. In addition, Smart grid manages the peak electricity demand by sharing the real-time data with consumers so that they can accordingly manage and shift their consumption. Some of the other benefits for utilities, customer, Government and Regulators is explained above through figure 1.

Although many parts of the world have already started to use a smart grid which is multi-dimensional networks by using their existing transmission and distribution networks with new smart grid technologies and by introducing regulatory developments and investment frameworks. Quick propagation of distributed and renewable generation leads to numerous point of injection and

billion points of consumption which is further become complex due to electric vehicle roll-out and intelligent automation system. It monitors and controls the power flow to match generation in real time or near real time. Currently, traditional grid is already in process of transformation to the smarter grid with the inclusion of automation, communication and IT system. Generally, some of the smart grid application are defined in the below figure 2.

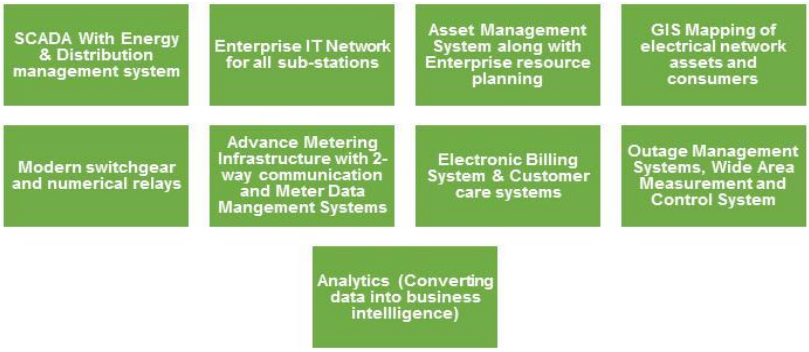

Fig 2 General applications of Smart Grid

India Smart Grid Forum (ISGF) which is non-profit voluntary consortium of public and private stakeholders, was launched in May, 2010 by Government of India with an integrated India Smart Grid Task Force (SGTP) which is an Inter-ministerial group and is serving as focal point for activities related to smart grid technology [2]. National Smart Grid Mission vision says "Transform the Indian power sector into a secure, adaptive, sustainable and digitally enabled ecosystem by 2027 that provides reliable and quality energy for all with the active participation of stakeholders".

As per task force which is defined into following groups which help to provide "Quality power on Demand for all by 2027" is defined Table 1.

TABLE I India Smart Grid Task Force Working Groups

S.No.	Working Group Detail	Activities Involved
1	WG-1	Focus on Trials/Pilots on New Technologies & Ideas
2	WG-2	Focus on loss reduction and theft control including data gathering and analytics, energy accounting
3	WG-3	Focus on access to power to rural areas and reliability & quality of power to urban areas
4	WG-4	Focus on distributed generation and renewable
5	WG-5	Focus on physical cyber security, standards & spectrum

IV INDIA'S ROAD MAP OF SMART GRID

A smart grid allows massive integration of unpredictable and sporadic renewable sources and distributed power efficiently with the inclusion of intelligent control system. Successful implementation of smart grid requires a holistic and integrated approach A transparent and comprehensive plan is in place for smart grid which would help technology development, capacity building, and investment planning. As per smart grid roadmap plan, it is defined in the below table 2 where all three five-year plan are discussed-

TABLE II India Smart Grid Five Year plan

	Description	12th Plan (2012-17)	13th Plan (2017-22)	14th Plan (2022-2027)
1	Power for ALL	Electrification of Household by 2017	24 hour supply in all urban areas	24 *7 power supply to all categories of consumers across the country
2	Loss Reduction	Reduction of AT & C losses in all distribution utilities to below 15%	Reduction of AT & C losses in all distribution utilities to below 12%	Reduction of AT & C losses in all distribution utilities to below 10%
3	Smart Grid Rollouts	Smart Grid Pilots and development of microgrids	Smart Grid roll-out in all urban areas and	Smart Gird roll out nationwide and development

		in 1000 villages/industrial parks/commercial hubs	development of microgrids in total 10,000 villages/industrial parks/commercial hubs	of microgrids in total 20,000 villages/industrial parks/commercial hubs
4	Policies and Tariffs	Implementation of dynamic tariffs & demand response program for select categories of consumers	Open access to consumers in metros and select urban areas	Open access to all consumers
5	Green Power and Energy Efficiency	Energy efficiency programs for lighting & HVAC in Metros & State Capital	Energy efficiency programs for lighting & HVAC in Urban Areas	Dynamic energy efficiency programs nationwide
6	Electric Vehicles & Energy Storage	EV charging stations in Urban areas and along selected highways and Introduction of energy storage system on trial basis	EV charging stations in all urban areas and strategic locations on highways and large roll-outs of energy storage systems	EV charging stations in all urban areas along all state and national highways

At different geographical locations in India, Ministry of Power and India Smart Grid Task Force [5] had shortlisted 14 Smart Grid pilot projects and 1 smart city R & D platform to be executed in power sector. These pilot projects will provide impetus with a business case, regulatory and policy framework for the much larger context in the next phase with features like Advance Metering Infrastructure (AMI), Outage Management System (OMS), Integration of renewable energy and peak load management. For these projects, Government of India average estimated the cost of each pilot projects would be US$ 10 million out of which half grant will be shared by Government of India.

V HOW SMART GRID TECHNOLOGY EVOLVED

The pillar and strength of the smart grid are the integration of two-way communications between utilities and consumers through advanced metering infrastructure (AMI), or "smart meters". AMI is thus designed to provide knowledge of energy parameters which are pricing, demand, power and quality in real time or near real time. In such a case, it becomes perplexing for the utility to make an accurate directing for the return on investment for the technology already deployed. Like all technological advancements happening in the field of energy efficiency, smart grid has significant benefits to offer which need to take care with following things and it is highlighted in figure 3.

Recently, many smart grid projects which involve deployment of components like smart meters, distribution management system etc. are adopted by State-owned utilities in Andhra Pradesh, Assam, West Bengal, Madhya Pradesh, Maharashtra, Tamil Nadu, Uttar Pradesh, Himachal Pradesh and Punjab are also making headway towards a smart grid era through the restructured APDRP of the Government of India. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment.

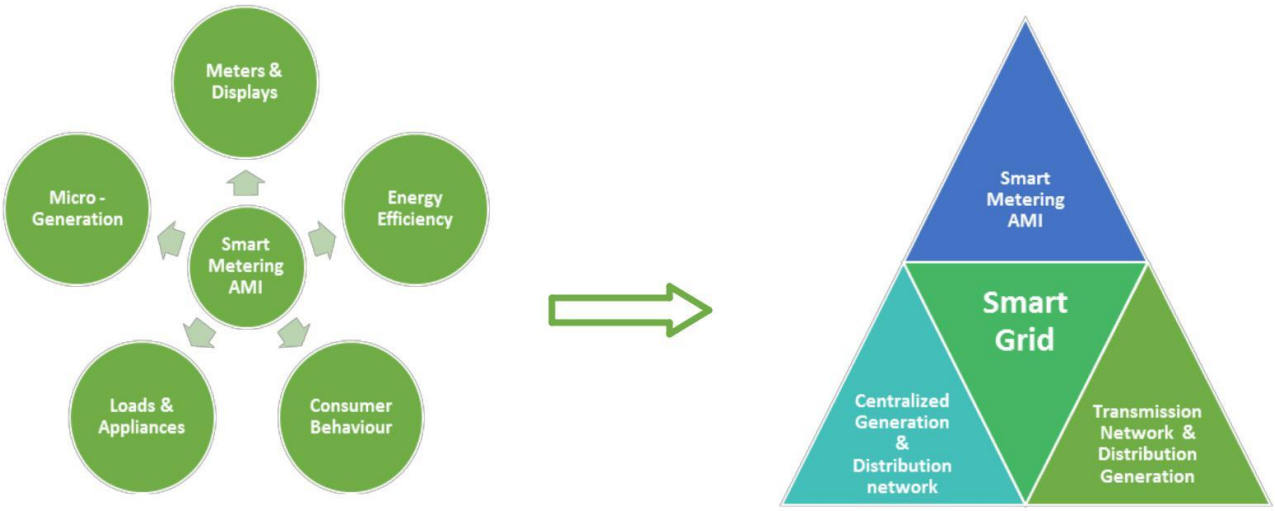

Fig 3 – Fundamental building block of Smart Grid

Overall, development of smart grid is essential it globally achieving energy security, economic development, and climate change mitigation. The rapid expansion of smart grid is somehow led to a diffusion of roles and responsibilities among government and industry actors and to reduce overall expense on technology and demonstration and policy development. The broad aspects of smart grid include generation, transmission, and distribution. Since the smart grid is a journey from conventional electrical system to the smarter grid system and that is happening in phased manner and for this capacity building and investment planning from all stakeholders will timely implementation of this technology through length and breadth of the country. There is a need for a strong institution that can drive smart grid development in India. One designated entity should be made responsible for the smart grid roadmap including implementation roadmaps, technology selection guidelines, standards guidelines, capacity building programs etc.

VI ROLE OF IT IN SMART GRIDS

Smart Grids are a one stop solution to the shackles of transmission and distribution challenges distressing the traditional grids and highly rely on information technology at the core and support diverse protocol stacks for a variety of applications.

With the aim of efficiently serving the diversified needs of industrial, commercial and home entities, smart grids deploy closely knitted interfaces and advanced control methods like advanced metering infrastructure and phasor measurement units.

According to the logical model framework for Smart Grid [12] proposed by the National Institute of Standards and Technology (NIST), US, the Smart Grid consists of seven logical domains as illustrated in figure 4 below:

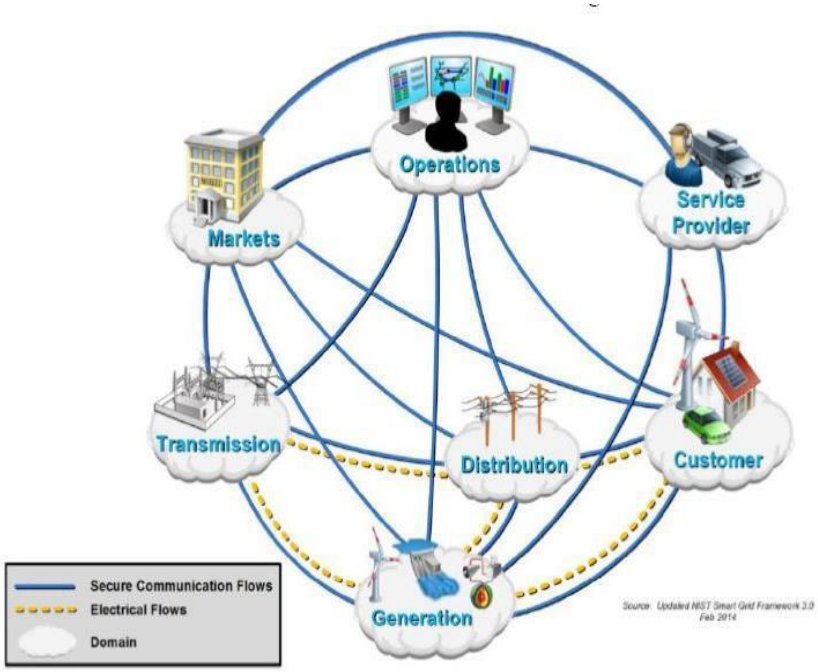

Fig 4: Smart Grid Domains

The various actors stay interconnected with an underlying backbone of the internet to ensure the dynamic requirements of the smart grid landscape. Smart Grid Operations are managed using a Command-and-Control Center that delivers advanced capabilities including outage analysis, integrated workforce management, real-time monitoring of dynamic energy demands, detailed visualization dashboards.

Deploying a wide array of communication infrastructure and protocols within the smart grid network allows for the smooth communication amongst heterogeneous devices. Interoperable wired and wireless network technologies support reliable data transmission between the various entities in the smart grid with maximum reliance on high bandwidth and low latency for an efficient smart grid communication network. The comparison [6] of the maximum threshold data rates and coverage ranges of the commonly employed communication protocols in the smart grid architecture is shown in Table III.

Table III: Comparison of Smart Grid Communication Technologies

Technology	Standard/protocol	Max. theoretical data rate	Coverage range
Wired communication technologies			
Fiber optic	PON	155 Mbps–2.5 Gbps	Up to 60 km
	WDM	40 Gbps	Up to 100 km
	SONET/SDH	10 Gbps	Up to 100 km
DSL	ADSL	1–8 Mbps	Up to 5 km
	HDSL	2 Mbps	Up to 3.6 km
	VDSL	15–100 Mbps	Up to 1.5 km
Coaxial Cable	DOCSIS	172 Mbps	Up to 28 km
PLC	HomePlug	14–200 Mbps	Up to 200 m
	Narrowband	10–500 kbps	Up to 3 km
Ethernet	802.3x	10 Mbps–10 Gbps	Up to 100 m
Wireless communication technologies			
Z-Wave	Z-Wave	40 kbps	Up to 30 m
Bluetooth	802.15.1	721 kbps	Up to 100 m
ZigBee	ZigBee	250 kbps	Up to 100 m
	ZigBee Pro	250 kbps	Up to 1600 m
WiFi	802.11x	2–600 Mbps	Up to 100 m
WiMAX	802.16	75 Mbps	Up to 50 km
Wireless Mesh	Various (e.g., RF mesh, 802.11, 802.15, 802.16)	Depending on selected protocols	Depending on deployment
Cellular	2G	14.4 kbps	Up to 50 km
	2.5G	144 kbps	
	3G	2 Mbps	
	3.5G	14 Mbps	
	4G	100 Mbps	
Satellite	Satellite Internet	1 Mbps	100–6000 km

Established standards (Table IV) define the communication specifications for integration of distributed components of the smart grid to achieve efficient operations.

Table IV: IEEE and IEC standards for Smart Grid

Key Power Grid and Communications standards	
IEEE P2030	Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications and Loads
IEC 61850	It is a standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems to be able to communicate with each other.
IEC 60870	Defines controlling electric power transmission grids and other geographically widespread control systems (Supervisory Control And Data Acquisition) by use of standardized protocols, equipment from many different suppliers can be made to interoperate
IEC 61968	A series of standards that define interfaces for the major elements of an interface architecture for Electrical Distribution Management Systems
IEC 61970	A series of standards deals with the application program interfaces for energy management systems (EMS) and the exchange of information to systems external to the control center environment
IEEE 1379	A uniform set of guidelines for communications and interoperations of remote terminal units (RTUs) and intelligent electronic devices (IEDs) in an electric utility substation

IEEE 1547	This standard provides a uniform standard for interconnection of Distributed resources with electric power systems. It provides requirements relevant to the performance, operation, testing, safety Considerations, and maintenance of the interconnection.
IEEE 1646	This standard defines communication delivery time of information to be exchanged within and external to substation integrated protection, control, and data acquisition systems

VII MANAGING THE GRID'S CYBER SECURITY

The Smart Grid communication network acts a carrier for enormous usage data from a huge spectrum of connected devices to manage dynamic energy loads. Cybersecurity becomes indispensable in the context of energy management and delivery in the smart grid, and cyber-attacks on the same can impact the wider economy. Energy leadership has demonstrated an increasing concern over smart grid cyber security due to the potential of devastating consequences included but not limited to blackouts, power overloads, device breakdowns, data tampering, and the rippling effects to everyday lives.

Due to the presence of multiple entry points, smart grids lie at the risk of increased attack periphery. The cyber threat landscape for smart grids is expanding notably affecting all interconnected components across generation, transmission and distribution channels in some or the other way.

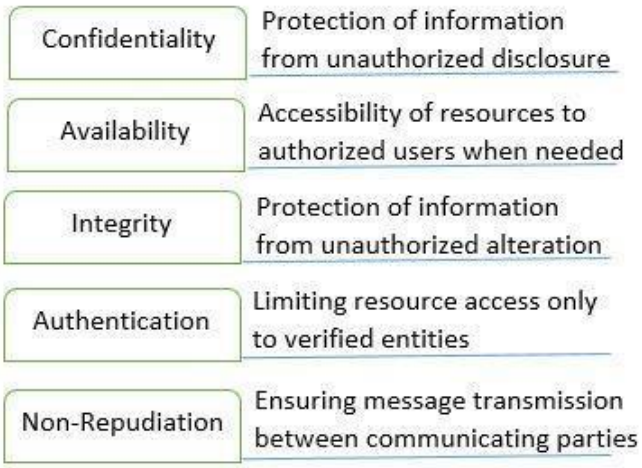

Fig 5: Pillars of Information Security

Cyber security solutions must address premeditated attacks such as internal breaches and industrial espionage along with unintended compromises of the ICT infrastructure due to accidental consumer errors, equipment failures, and natural disasters. Figure 5 depicts the pillars of cyber security stand well applicable to the critical infrastructure landscape of the smart grid architecture.

VIII CYBER-ATTACKS ON THE SMART GRID

Every digital component introduces attack points in the smart grid ecosystem. Nations worldwide are faced with the increasing cyber-attacks on the smart grid both in terms of volume and complexity. Ukraine's power outage in December 2016 was due to a cyber-attack as quoted by Reuters [7]. Experts in other nations including India have also stated a growing concern over smart grid security. The Ministry of Power (MoP) displayed a commitment to safeguarding national power grids from Cyber Attacks under the directions received from National Critical Information Infrastructure Protection Centre (NCIIPC) and Indian Computer Emergency Response Team (CERT-In) [8].

The underlying communication network acts as the backbone of the Smart Grid infrastructure that binds the different components together by provisioning two-way communication between them. This network follows a distributed architecture to support a vast number of heterogeneous electronics nodes by employing varied technologies and protocols, thus introducing complex security challenges for each interface involved.

Cyber threats evident to the smart grid architecture can be categorized as

1. Sniffing and Eavesdropping

The sniffing process is a common methodology implemented by hackers either to steal information indirectly or to acquire the technical specifications of the network in order to craft further attacks. Authors in [9] provide a comprehensive study on the practical aspects of eavesdropping on the Smart Grid by capturing and monitoring network traffic in order to obtain underlying data by using SmartRF Packet Sniffer, ZenaSniffer, KillerBee framework and a few Python modules.

2. Denial of Service (DoS)

These attacks are conducted with the aim of rendering the resources temporarily unavailable to the intended users by overwhelming the underlying communication and computational infrastructure. Distributed Denial of Service attacks is identified DoS attacks that usually involve a huge number of infected machines, recognized as bots to generate simultaneous load on the targeted infrastructure. DoS attacks in a smart grid can realize on the physical, MAC or TCP/IP layer of the network architecture.

3. Malicious Data Injection

An attacker may leverage underlying vulnerabilities in the configuration of a smart grid infrastructure and inject malicious data that will misrepresent the state estimation process without being detected by any of the existing techniques. Researchers have demonstrated that showed that an attacker can systematically and efficiently construct attack vectors in both scenarios, which can not only change the results of state estimation but also modify the results in a predicted way. [10]

4. Spoofing

These attacks involve a malicious party impersonating another device or user on a network. Researchers have established that the GPS receivers in many sensor devices, including synchrophasor are vulnerable to GPS time-base spoofing attacks making it possible to drift the time reference of the PMU local clock in the order of tens of microseconds in several minutes, causing the phasor measurements to become entirely unreliable. [11]

Successful spoofing attacks may result in incorrect calculation of clock offsets in order to render erroneous estimates of the actual power load, leading to overall inaccurate monitoring that ultimately reflects on power stability and line fault likelihoods.

5. High-level Application Attacks

A wide array of internet and intranet web based applications provide the interface for communicating with the underlying infrastructure such as the configuration interfaces, management consoles, end user web interfaces. The high-level applications attacks against any component or application in the system will cause unexpected physical damages. Such attacks may impact the fundamental power flow measurement, state estimation, Energy Management System (EMS), etc. By attacking the state estimator that determines the real-time prices, the attacker can influence the revenues of a real-time market. The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.

IX SECURITY RECOMMENDATIONS FOR SMART GRID

1. Stronger Defense Mechanism

Mitigating the evident vulnerabilities can be achieved by adopting the traditionally proven Defense in Depth principle that adopts a multi-layered approach by employing different security mechanisms at each layer. This mechanism behind this approach is to distribute the risk across various layers so that if one layer of defense gets penetrated, another layer of defense stands actively to hopefully discourage the attacker from probing further.

2. Secure Key Management

Security in the overall process of key management starting from generation, to distribution, including updating if any, and finally destruction is crucial for the overall grid security posture. Devices connected to the Smart Grid should support reliable cryptographic capabilities, including the ability to support symmetric ciphers for authentication and/or encryption. Public-key cryptography may be supported either in hardware by means of a cryptography co-processor or, as long as it is performed infrequently or in software.

3. Cybersecurity Risk Assessment

The objective of cyber security risk assessment is to evaluate various information assets to identify underlying vulnerabilities and threats and determine their impact in the instance of a cyber-attack. The conclusion of the risk assessment frames the required security requirements and dictates the selection of security controls for the smart grid. Top-down, bottom-up, qualitative and quantitative approaches should be used to implement risk assessment.

4. Awareness and Training

Security awareness and training formulate the building blocks of smart grids enhanced security.

Effective training programs need to be designed based on individuals' roles and responsibilities to enhance awareness on the existing potential vulnerabilities. Such awareness would cater to a safer smart grid due to pinned understanding of security issues.

5. Incident Response

Incident response refers to the capability to resume normal operations in the event of disruption of Smart Grid information system operations. Incident response planning involves the preparation of incident specific policies and procedures to enable the smart grid to recover smoothly and swiftly in case of an incident. In the absence of an effective incident management plan, an incident may result in a disruption in the operations of vital business functions including ICT systems, employees, customers and others.

REFERENCES

[1] Central Electricity Authority, Ministry of Power; Executive Summary of Power Sector, Ministry Of Power. New Delhi: Central Electricity Authority, 2016. Print. December 2016.

[2] India Smart Grid Forum, Smart Grid Vision and Road Map for India. New Delhi: India Smart Grid Forum & Ministry of Power, Government of India, 2013. Print. August 2013.
[3] National Institution for Transforming India, Report of The Expert Group On 175 GW RE By 2022. New Delhi: NITI Aayog, Government of India, 2016. Print. January 2016.
[4] Ministry of Heavy Industries & Public Enterprises, Government of India. National Electric Mobility Mission Plan 2020. New Delhi: Department of Heavy Industry, Government of India, 2012. Print.
[5]"ISGF". Indiasmartgrid.org. N.P., 2017. Web. Jan. 2017.
[6]M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN", Computer Networks, vol. 67, pp. 74-88, 2014.
[7]2017.http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA.
[8]2017.http://www.business-standard.com/article/government-press-release/power-ministry-committed-to-safeguard-national-power-grids-from-cyber-attacks-116111701433_1.html.
[9]C. Valli, A. Woodward, C. Carpene, P. Hannay and M. Brand, "Eavesdropping on the Smart Grid", Australian Digital Forensics Conference, 2012.
[10]Y. Liu, P. Ning and M. Reiter, "False data injection attacks against state estimation in electric power grids", ACM Transactions on Information and System Security, vol. 14, no. 1, pp. 1-33, 2011. [11]I. Akkaya, E. A, A. Lee and P. Derler, "Model-Based Evaluation of GPS Spoofing Attacks on Power Grid Sensors".
[12] National Institute of Standards and Technology, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security", 2010.
[13] Ondrej Linda, Milos Manic and Todd Vollmer "Improving CyberSecurity of Smart Grid Systems Via Anomaly Detection and Linguistic Domain Knowledge," 5th International Symposium on Resilient Control Systems, Aug. 2012.
[14] V. C. Gungor, D. Sahin, T. Kocak, S, Ergut, C. Buccella, C. Cecati and G. H. Hancke "Smart Grid Technologies: Communication Technologies and Standards," IEEE trans.on Industrial
Informatics, Vol. 7, no. 4, pp. 529-539, Nov. 2011
[15] Skopik, F. 2012. "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures."
International Journal of Smart Grid and Clean Energy 1 (1): 22-8
[16] Mashima, D., and Cardenas, A. 2012. "Evaluating Electricity Theft Detectors in Smart Grid Networks." In Research in Attacks, Intrusions, and Defenses, Berlin: Springer-Verlag Berlin Heidelberg.

