Vulnerability and Forensics associated with the Smart Grid: Cyber Attacks

Oribe Zakareya
Information System Department
Faculty of Computing & Information Technology
King Abdulaziz University Jeddah, Saudi Arabia

ABSTRACT
The entire paper will be considered to be a basic guideline for identifying and maintaining the vulnerability that are associated with Smart Grid technology. This paper will be mainly focusing on cyber attacks however arrangement of other types of disruption can also be experienced by Smart Grid technology. The core components like the grid assets and their classification will be discussed throughout the paper. Besides this the types of cyber attacks will also be classified on the basis of protocols and components that are implemented in smart grid. Along with this the basic attack prevention frameworks will be proposed in this technical writing. For better understanding of the paper tables, figures and equation will be provided here.

Keywords
Cyber assets, Cyber security, data integrity, Digital forensics, FACTS devices, False data injection attacks, Power system control centers, Smart grids, DNP3, SCADA

1. INTRODUCTION
Smart Grid can be defined such a digital technology that uses a two-way communication and information technology can be generated between utilities and its customers. Sensing created along the transmission lines is considered as the generator of smart grid. Although the function of Smart grid is almost similar to the internet but the key difference is that in case of smart grid the entire technology works on electrical grid and responds rapid change of electrical demand. It is capable of expanding the present level of renewable energy generation, transmission and distribution in the context of smart vehicles [1].

Smart gird is also considered as 'System of Systems'. Smart gird is used to reduce the electricity but at the same time the efficacy and transparency of the system is also enhanced. The sensing and measurement capacity of smart grid is superior to internet system but since last few years even after being a highly secured system so smart grid is facing a cyber security attacks repeatedly. Such kind of incident has reflected the security holes of such critical power system infrastructure. This entire paper will discuss about such cyber attacks and related security holes long with a concise description of smart grid functionalities [3].

2. SMART GRID FUNCTIONALITIES
The most widely known Smart Grid functions are as follows,

- Action related to self healing.
- Enhancement of Power quality.
- Preventing cyber attacks.
- Optimization of smarts assets and enhancement of operation efficacy.

3. RISK THREADS AND VULNERABILITIES
In 2003 majority of Midwest and Northeast of US faced a continuous four day blackout by which almost 50 million people were affected. This was a result of cyber system software programming failure.

In mid 2010 'Stuxnet', a computer worm was discovered. This was such a computer worm that was spreading through 'windows operation system'. Most of the Siemens industrial equipment's as well as software were listed under the target of Stuxnet. Not only that

The annual report of Repository that provides information about industrial Security incidents (RISI) shows that almost 35% industrial control System (ICS) security attacks are carried out through remote access. The report also revealed that more than 12 cyber security incidents have been happened within 2004 to 2008. As the smart grid system is comprised of both ICS and SCADA hence the cyber security concern associates with smart grid is on Rapid hike. Due to this reason it can be said that a range of the major cyber physical vulnerabilities associated with Smart Grid have relation with cyber issues hence the Smart Grid Infrastructure

of this page for three addresses. If only one address is needed, center all address text. For two addresses, use two centered tabs, and so on .

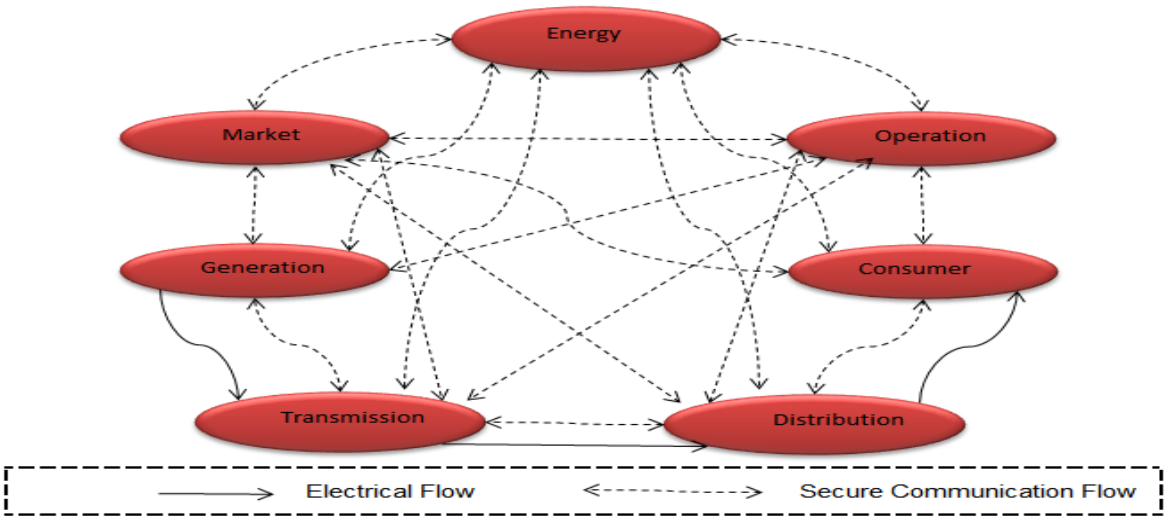

Fig 1: NIST reference Smart Grid Model

Smart Grid is referred to as a complex system including systems that are needed to be understood and interrelated broadly. With respect to this requirement NIST (National institute of Standard and Technology) has contributed in developing an architectural model based on the concepts. This reference model is capable of identifying the seven domains associated with Smart Grid functions like generation, distribution, transmission, operations, service provider, customer and markets. The particular model also incorporates applications that require information exchange which require inter-operability standards.

3.1 Smart Assets

Security (SGIS- Smart Grid Information Security) should focus on cyber terror attacks along with industrial espionage. In order to make the security risk management action more effective the relevant Smart Grid assets have been categorized into various group as follows.

3.1.1 Smart Cyber Assets

This is a comparatively new Smart Asset category that is comprised of a range of new monitoring and controlling devices, communication systems etc. Such kind of smart movements opens up a range of vulnerabilities that are already known to ICT world. Most of the ICT components layers are influenced by such asset types [4].

The ICT component layers can be best described with the help of either OSI (Open Systems Interconnection) model or TCP/IP (Transmission Control Protocol and Internet Protocol) model. The layers in the OSI model are physical, data link, network, transport, session, presentation and application. The TCP/IP model incorporates network access layer, internet layer, host-to-host layer and process layer. These models and the layers are utilized for network communications.

3.1.2 Grid Cyber Assets

The core components comprise the Grid Assets and such type of assets can exist is numerous approach within the modern cyber infrastructures. However the modern types of grid assets like SCADA, Grid operation, C&C Communication Link and Market operation are capable of handling newer type of core component distributed generation. However it must be mentioned that the controlling scope of security measures are comparatively higher in case of Grid Cyber Asset [2]. A sample risk management process with thread taxonomy is provided in figure 2.

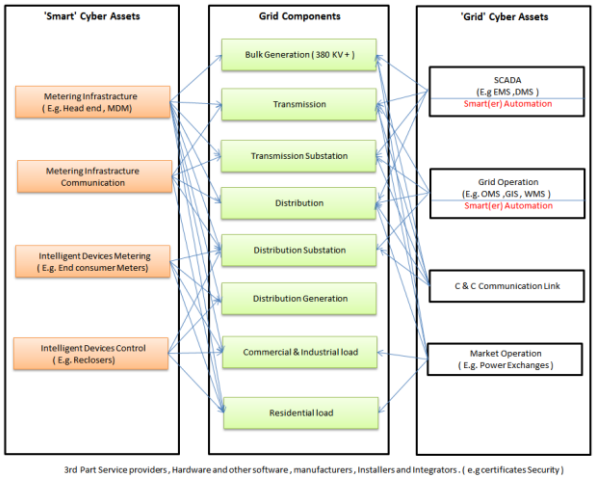

Fig.2 Sample smart grid risk management process with thread taxonomy

3.2 Security Issues associates with Cyber-Physical Smart Grid

As the physical power system and cyber system related to information and communication get coupled under smart grid hence the security issue also becomes more complex. The entire smart grid network is comprised of software, hardware and various types of communication requirements. Basic smart grid architecture is provided in figure 3

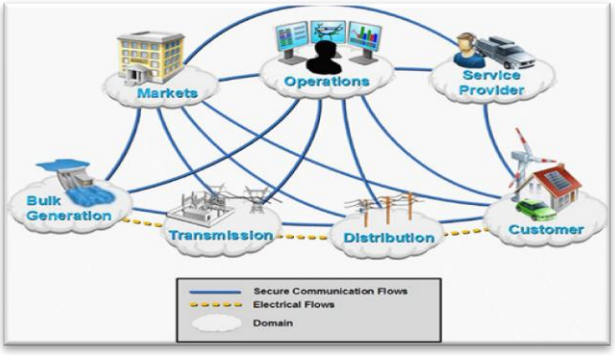

Fig. 3. Basic Smart Grid Architect

4. SECURITY ISSUES ASSOCIATES WITH CYBER- PHYSICAL SMART GRID

A range of security objectives are associated with smart grid and that been classified according to the following groups [4].

4.1 Availability of Data

In order to maintain the consistency of smart grid operation the data security owns the highest significance. The availability of data indicates the timely as well as the reliable access of using information. It must be mentioned in this context that the time availability is dependent on some applications. Few sample applications are provided in the Table 1.

Table 1. Time latency and data availability

Time Requirements	Data Availability for the specific applications
<= 4 ms	Protective relaying
Sub seconds	Transmission wide-area situational awareness monitoring
Seconds	Substation and feeder SCADA data
Minutes	Monitoring noncritical equipment and some market pricing information

4.2 Integrity of Data

Any kind of modification or of exiting data can generate a loss in data integration. The data integrity is termed as the source and quality if available authenticated data. Any kind of intrusion in the cyber domain that has been carried out by attackers might generate such kind of data integrity loss. With the ongoing advancement of smart grid the problem associated with data integrity is increasing [3].

4.3 Data Privacy

In order to maintain the privacy concern of end users implementation of effective security measurement becomes the most significance matter within the smart grid infrastructure [5]. With increasing deployment of latest metering infrastructure the importance of data privacy is getting more attention by the smart grid cyber security experts.

5. IRREGULARITY ASSOCIATED WITH SMART GRID

5.1 Irregularities in the State estimation program

As the load demand is increasing day by day hence in order to avail the power system maximum capacity the safety and reliability of power system must be monitored in each and every operating state. A range of electronic devices are available for much monitoring action but among them Remote Terminal Units (RTUs) are the device that are widely used. Using of state estimation algorithms the bad data can also be detected leading to the estimation with high level of preciseness. Due to the enhancing complexity in smart Grid interconnections the probability of cyber-attacks are becoming higher and consequently the security of state estimation is getting higher degree of significance. A range of available research work have revealed that latest type of cyber security state estimation program have relation with 'False Data Injection Attack'[6].

- **False data Injection Attack:** At the time of operations related to power system State Estimation (SE) is crucial for Automatic generator Control (AGC), Optimal Power Flow (OPF) operation, Contingency Analysis (CA), etc. A conventional power system block diagram is provided in figure 5 which shows the role of SE in ensuring smooth functioning of the operations associated with energy management system. OPF, AGC and CA receive the input from SE for making the important decisions. While carrying out the processing SE obtains data from SCADA. As a result of false data injection attack SE receives wrong data from SCADA and this affects the functioning of the smart grid.

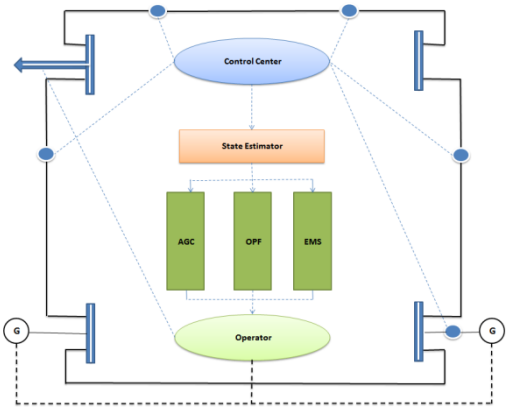

Fig. 5. Conventional Power system Block

States of power systems are considered as the complex voltage magnitudes as well as the angles of each bus. Generally SE estimates the power system state variables by using the meter measurements. Let the state vectors is X and meter measurements is Z.

$$X = [\delta_1\, \delta_2 \delta_3 \ldots \ldots \delta_n V_1 V_2 V_3 \ldots . V_n]^T \quad (1)$$

Here n is the number of state variables.

It is impossible to obtain the state of the system directly hence SE is used so that the states from measurements values can get interfered. There can be a possibility that measurement

values become noisy and increases the presence of errors. The traditional SE formulation is provided in equation (2).

$$\min J(x) = \sum_{i-1}^{m} w_i \ (z_i - h_i(x))^2 \quad (2)$$

Here h (x) is known as the measurement functions representing the measurement of Z.

'w' is the weight and 'm' is the maximum number of measurement.

In absence of error,

$$z_i = h_i(x) \quad (3)$$

When the error is present the equation becomes,

$$z_i = h_i + e_i \quad (4)$$

Here 'e' is representative of error.

If 'e' is present in the measurement which is received from the above equation then it can be assessed that the SE is vulnerable to cyber- attack as smart grid has been deployed. Due the malicious attack the flowing measured data is received by control center.

$$z_i = h_i + e_i + \alpha \quad (5)$$

'α' is considered as attacker vector. A range of research have been carried out in order to prevent all kind of false data intrusion that has been divided in too following three categories :-

- State Estimation vulnerability Analysis
- Analysis of Consequences
- Counter measures development.

With the help of SE estimation errors can be detected in the measurements which will be able to predict the chances of any false data injection attack in the smart grid functionality.

- **Load Redistribution (LR) attack in a power system:** this is nothing but a sub-division of false data injection. Both ED and OPE are highly dependent on the SE output. The LR attack lead to wrong state estimation and consequently the stability of operating conditions get violated [7]. LR attack model is considered as a bi-level programming problem and the equation is provided below :

  $\sum_d \Delta D_d = 0$ (6)

  ΔPL=-SF.KDΔD

  $$-\tau D_d \leq \Delta D_d \leq \tau D_d$$

In the above equation it is demonstrated that when LR attack takes place the demand that is 'ΔPL' either increases or decreases but the total change in the load 'D' remains zero. In other words it can be said that the total changes associated in load remain constant but the demand of load buses get increased or decreased by LR attack in artificial manner. With the above equation the artificial increase or decrease reflected in the load buses helps in detecting the LR attack which can also affect the functionality of smart grid.

5.2 Attacks on Flexible Alternating Current Transmission Systems (FACTS) devices

The function of FACTS devices is to stabilize the power flow of Smart Grids. Along with that the power flow of grid is also regulated by FACTS devices. Load sharing, voltage regulations, power system oscillation mitigation etc are the other vital functions of FACTS devices. Use of FACTS enhances the capacity of network through optimization process of power flow. In this context it must be mentioned that it is not possible for a single FACT device to achieve the optimal power flow required for Smart Grid network due to this an effective level of communication is required among all connected FACTS devices during the power flow operation. Hence it can be state that the communication link become a very important component within smart grid network but such network again make the smart grid network vulnerable to the cyber attacks. However in order to deal with such cyber threats two approach have been invented among then one is agent-based management and another one is improved visualization. A range of security policies and regulations must be implemented in the context of FACTS device coordination process in order to handle the cyber attacks.

5.3 Irregularities associated with Power system Control Centers (PSCC)

The sensors that are comprised of SCADA network provide information to the power system control centers. On the basis of these information the control centers takes intelligence decisions. In the next stage the intelligence decision taken by control center are passed to actuators and there the actions on field devices are performed [8]. The entire process is carried out through a typical power system control loop that is given in figure 6 .

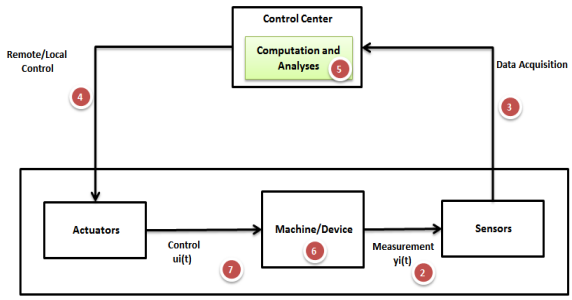

Fig. 6. Typical Power system control loop

The data integrity attack has an inherent relationship with PSCC attack and in such cases the denial of service attack (DoS) and time based attack are also found, such kind of attack corrupt the information.

The generation side of power system is associated with Automatic Voltage regulator (AVR), Automatic Generation control (AGC).

- **Cyber attacks on AGC:** as the load keep chaining with time hence on order to keep the balance between powers outputs generated from different plants AGC is installed. Through AGC the system frequencies can be monitored easily and the decision regarding the load demand balancing can be taken easily [3]. The both frequencies that are

associated with secondary frequency control loop are measured and is passed to the other connected devices via wide area communications such as IEC 61850. The entire communication process of power system unit is controlled by point to point communication arrangements like DNP 3.0. However a range of securities issue also lies their and that must be addressed in order to maintain the feasibility entire power grid operation. Reachability Framework approach is such an approach that have been developed in order to deal with such cyber attacks related to AGC. According to this approach a range of policies have been developed via which a power grid can be followed in case of power grid disruption by attackers and the type of AGC identification can be identified. The threat models that have been developed in order to control the attacks have considered mainly two types of attacks- 'min attacks' and 'max attacks'. The manipulations of 'Area Control Errors' performed such type of attacks. The attacker mainly targets the sensor measured value, manipulation of such values directly affect the operation conditions of the systems [8].

- **Cyber attacks on GC:** In some cases as a result increasing load changes in generator the output power become lager in comparison to mechanical input power. Such kind of phenomenon generates deviation in speeds and fall in frequency. The sensor then detect fall in generator speed. Although GC owns an high rate of dependence on local measurement but as most of the modern generator use standard type of communication protocols corresponding information sharing with operation center hence the dependency of GC on local measurement get lowered. Any kind of cyber attack is lead to disruption of the physical power grid system and GC plays the most crucial role in stabilization process of generator operation.

6. PROTECTION PROCEDURES OF SMART GRIDS FORM CYBER ATTACKS

6.1 Digital Forensics

Various kind of statistical, mathematical as well as computer science data that are collected for the purpose of identification, analysis and interpretation of digital evidences are referred as Digital forensic. The most updated digital forensic methods own the capability of finger print extraction from various kinds of digital media with the help of finger print cameras. The computer network forensic is also capable of extracting data but through wireless networks like IEEE 802, form this aspect the Electric Network Frequency can be termed as the figure print in case of smart grid [7].

6.2 Smart Grid Forensics

The studies of Smart Grid Forensics are mainly used for identification purpose of electricity security attacks. This type of forensic studies is also capable of digital audio verification, video recordings related to crimes and addressing of both cyber and physical vulnerabilities associated with smart grid. An in detail consumption information can be tacked through smart meters as well as my Advanced Metering Infrastructure (AMI). Smart Grid forensic is also capable of carrying out cyber-crime related investigation such as hacking, cyber terrorism etc [11]. Not only the man made deserters, natural disaster can also be treated through Smart grid forensics. For example the power system failure investigation that has to be carried out after any kind of natural disaster can also be handled effectively through the application of Smart Grid Forensics [9].

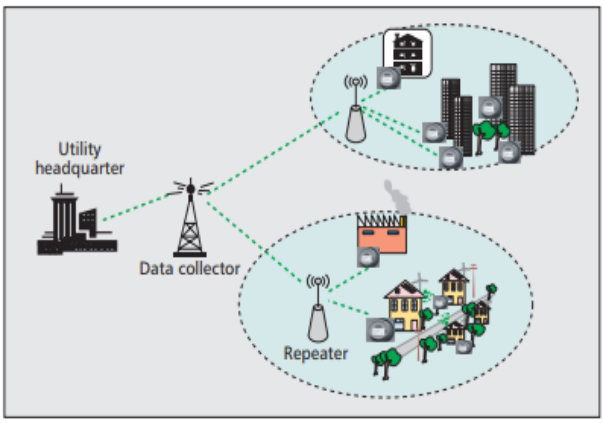

Fig 7. Smart Meters and AMI

6.3 Protection process to get rid of component wise cyber attack

In order to project smart gird a range of security framework have been proposed that includes agents like alarm management, data long management and reporting, continuous traffic data analysis and continuous collection of network traffic patterns along with end-to-end security control. In order to detect any kind of abnormality in the smart grid the Rough Classification Algorithm can be used [10] A sample security agent based frame work of smart grid against cyber attack has been provided in figure 8.

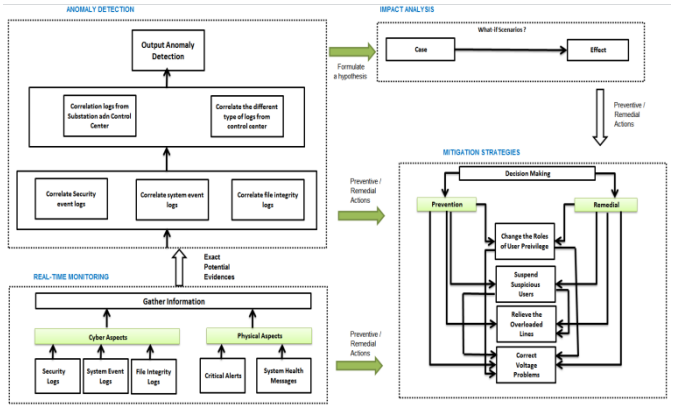

Fig 8. A basic framework for irregularities detection in smart grid

The above framework given in the figure reflects about SCADA based security framework which is based on anomaly detection and real time monitoring. The particular framework ensures reliable and cost effective protection against cyber attacks.

6.4 Protection Process to Get Rid of Component Wise Cyber Attack

When a large numbers of stakeholders are present within an smart grid network then firewalls, authentications etc become incapable of providing the required level of cyber security and for this reason a range of different communication protocols are used among all the FACTS devices for the purpose of

effective automated operation of smart grids. Although most of the smart grid network is associated with Distributed networking protocols but the advancement of technology have made DNP also vulnerable to cyber attacks hence a range of data set that are based on security rules have been proposed of such DNP 3 devices [9].

Distributed Network Protocol or DNP3 is referred to as an IEEE-1815 standard. It is a primary protocol which is deployed in the functionality of smart grid. DNP3 is very much reliable and a better protocol and is implemented in delivering the measurements from a client based in a field to a server based at a center [14].

6.5 Using of detection algorithms

In this context of smart grid, to resist any kind of cyber attacks using of detection algorithms is a compulsory thing which must be use in this type of case. There are several algorithms that have been used for this purpose such as DPRAODV algorithm, S-DES Cryptographic algorithm & using of TDMA protocol for packet loss & avoidance. All are connected to each other's in order complete one task. S-DES Cryptographic algorithm is able to provide better security to the larger network. This algorithm is already exists & tested many times. In this algorithm constant bit rate application is used which is able to produces constant packets through the protocol which must be user defined. It is basically used to secure data at the time of transmission within a network by using it along with the key allocation based on time which should be implemented in this case. DPRAODV algorithm is used for the detection of prevention and reactive AD-HOC on the basis of demand of distance vector. Black hole attack can also be detected with the help of this algorithm. To complete the process these two existing algorithm should be used followed by the last step which includes TDMA protocol for the purpose of packet loss & avoidance for preventing any kind of cyber attack. In this step, the constant packets produced through constant bit rate application according to the S-DES Cryptographic algorithm which is used through the user defined protocol. An IP network will also be simulated by using the Rocket-fuel topology which uses routers for the purpose of tracing [13].

6.6 Hypothesis

The base of this context is discussed as per below To resist cyber attacks, They have to develop a cyber security by applying SCADA with the help of logical study of different subjects which are identified as the dealing subjects in this case as per the definition, classification of crimes & other measurement. So the main objective is to design a framework from the existing researches and models which will be tested and implemented for detecting and mitigating the vulnerability and assessing the forensics with respect to the cyber attacks taking place within the smart grid functionality

6.7 Contribution of this whole work

The contribution of this whole work is very much effective as they can able to figure out the vulnerabilities by the location in terms of architecture which is associated with the probability of cyber attack as per below.

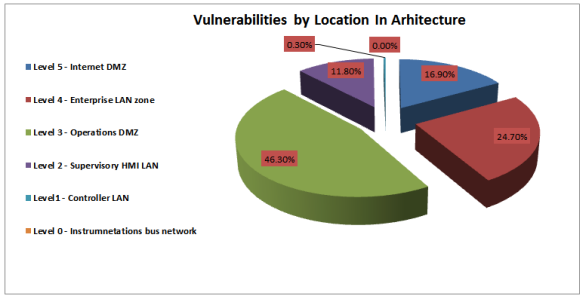

Fig 9. The pie chart shows the vulnerability of the smart grid systems in different area due to continuous attacks.

The above stastistics represents the analyssis of vulnerability for the continous attacks in the smart grid security sytems which has been exposed by several cyber attacks from various perspectives which has resulted in the form of critical system failures.

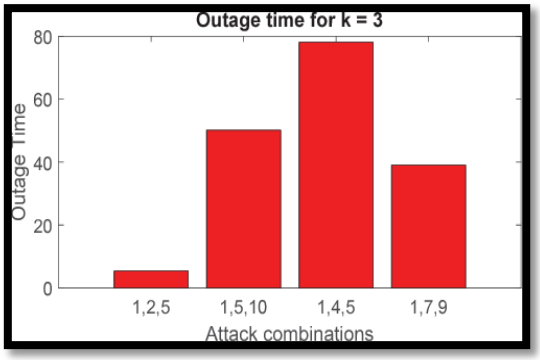

Fig 10. The statistical reprsentation of the analysis of vulnerability of cyber attack in terms of smart grid cyber security system (Source: Kabalci & Yasin, 2016)

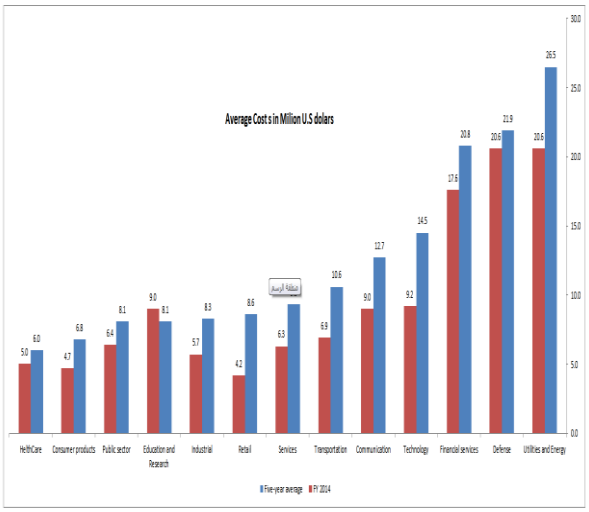

Fig 11. This is the graphical representation of the average annual cost behind cyber crime in industrial sector (in dollars) (Source: Yan *et al.*, 2017)

From the above graph, they can also get an idea about the cost of this system to get secure data transition process in respective field as well. So, it can be said that as the contribution of the whole work is import for our society to resist more cyber attack before taking place in future in this digitally advanced world with the help of this technology also.

The contribution of this whole work is very much effective as they can able to figure out the vulnerabilities by the location in terms of architecture which is associated with the probability of cyber attack as per below.

7. CONCLUSION

In conclusion it can be stated that although a range of security frame work have been developed in order to protect the smart grid form cyber attack but with ongoing time the nature of attack is also herring richer and due to this reason each and every security options are getting updated rapidly. Although the Smart Grid forensic is getting popular but still has to be improved further. Cyber security has become most crucial aspect within the Smart Grid infrastructure [12]. Smart grid forensics is a powerful and an emerging security component of power system, which is mostly used for the cyber-security purposes. Major challenges being faced with the use of SMART GRID FORENSIC technology is to handling the enormous amount of big data and information. Apart from that, smart grid forensic technology is mostly use for identifying an individual who is associated with or involved in electricity theft and/or with the cyber attack. Moreover, this particular system software is particularly useful for acquiring information related with the natural-disasters related failures, like earthquakes, hurricanes and other natural disasters. Keeping eyes on those beneficial impacts of smart grid forensics, it can be stated that, this particular power system cannot be used without violating the confidentiality issues related with the users' privacy [15].

In order to respond effectively to incident strategies for IT forensic investigation, SCADA forensics model can be considered crucial. There are certain steps needed to be followed for conduction of a successful digital forensic investigation. The basic steps for the same include preservation, examination, identification, extraction, as well as, documentation of the digital evidences. The major purpose of the mentioned investigation is to establish in court of law that substantial evidence has been obtained correctly in order to provide standard legal backing

8. REFERENCES

[1] Arxiv.org,2018.[Online].Available:https://arxiv.org/ftp/arxiv/papers/1401/1401.3936.pdf. [Accessed: 29- May- 2018].

[2] Pdfs.semanticscholar.org,2018.[Online].Available:https://pdfs.semanticscholar.org/19cb/57b2e83d6a473966e961bd39d563a785e8c7.pdf. [Accessed: 29- May- 2018].

[3] Ab Rahman, Nurul Hidayah, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo. "Forensic-by-design framework for cyber-physical cloud systems." IEEE Cloud Computing 3, no. 1 (2016): 50-59.

[4] Zhu, Yihai, Jun Yan, Yufei Tang, Yan Lindsay Sun, and Haibo He. "Joint substation-transmission line vulnerability assessment against the smart grid." IEEE Transactions on Information Forensics and Security 10, no. 5 (2015): 1010-1024.

[5] Kabalci, Yasin. "A survey on smart metering and smart grid communication." Renewable and Sustainable Energy Reviews 57 (2016): 302-318.

[6] Lin, Hui, Adam Slagell, Zbigniew Kalbarczyk, Peter Sauer, and Ravishankar Iyer. "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids." IEEE Transactions on Smart Grid (2016).

[7] Rawat, Danda B., and Chandra Bajracharya. "Detection of false data injection attacks in smart grid communication systems." IEEE Signal Processing Letters 22, no. 10 (2015): 1652-1656.

[8] Jokar, Paria, Nasim Arianpoo, and Victor Leung. "A survey on security issues in smart grids." Security and Communication Networks 9, no. 3 (2016): 262-273.

[9] Wang, Kun, Miao Du, Yanfei Sun, Alexey Vinel, and Yan Zhang. "Attack detection and distributed forensics in machine-to-machine networks." IEEE Network 30, no. 6 (2016): 49-55.

[10] Wang, Kun, Miao Du, Yanfei Sun, Alexey Vinel, and Yan Zhang. "Attack detection and distributed forensics in machine-to-machine networks." IEEE Network 30, no. 6 (2016): 49-55.

[11] [11] He, Haibo, and Jun Yan. "Cyber-physical attacks and defences in the smart grid: a survey." IET Cyber-Physical Systems: Theory & Applications 1, no. 1 (2016): 13-27.

[12] Yan, Jun, Haibo He, Xiangnan Zhong, and Yufei Tang. "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks." IEEE Transactions on Information Forensics and Security 12, no. 1 (2017): 200-210.

[13] Keerthana, J.K., Kala, I., Mahadev, M., Nousheen, S.M. and Pavithra, A., 2017. An Enhanced Dynamic Probabilistic Based Broadcasting Scheme for MANET.

[14]]www.DNP3.org

[15] Boyer, S.A., 2018. SCADA supervisory control and data acquisition. The Instrumentation, Systems and Automation Society.

[16] Sridhar, S., Hahn, A., & Govindarasu, M. (2012, January). Cyber attack-resilient control for smart grid. In *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES* (pp. 1-3). IEEE.