Journal of Theoretical and Applied Information Technology
15th December 2021. Vol.99. No 23
© 2021 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SYSTEMATIC REVIEW OF SECURITY IN SMART GRID INFRASTRUCTURE

[1]RASHI SINGH, [2]NASIB SINGH GILL, [3]PREETI GULIA
[1]Research Scholar, DCSA, Maharshi Dayanand University, Rohtak, Haryana, India
[2]Professor, DCSA, Maharshi Dayanand University, Rohtak, Haryana, India
[3]Asssistant Professor, DCSA, Maharshi Dayanand University, Rohtak, Haryana, India
[1]rashimac1@gmail.com,[2]nasibsgill@gmail.com, [3]preeti_gulia2006@yahoo.com

ABSTRACT

Today, a huge enhancement has taken place in our electricity grid system at every level either it is generation, transmission, distribution, or at the consumer side. More and more focuses are on making the grid reliable, efficient, and available all the time. Establishing a framework is a one-time process but maintaining and provides security is life long process and the same is with the smart grid. A smart grid consists of various components, and these components make it more prominent for threats. This paper describes the reasons for the adoption of the smart grid, various security threats in smart meter, Advance metering infrastructure, cloud, communication, and SCADA along with the research work going on these threats. This paper gives a comprehensive research review aiming to help the researchers to explore further possible solutions in making the power grid secure and smarter.

KEYWORDS: Smart Grid, AMI, SCADA, Communication, Cloud, Security of Smart Grid

1.INTRODUCTION

The increasing population and advancement in technology lead to the high demand for electricity. Electric energy emerges as the main source of power. Earlier the main sources of electricity generation are Solar, Coal, Hydrothermal, Geothermal, oil, and nuclear, etc. Although the use of electricity is pollution-free but the generation of electricity from coal, oil, nuclear is releasing various types of pollutants. So, there is a need for generating electricity from renewable and pollution-free sources like solar, wind, hydro, etc. The generation of electricity from these renewable resources is unpredictable and is totally depends on the weather. This leads to work on the technology that has the potential to integrate traditional electricity grid with Internet of Things (IoT) [1].

This technology is known as the smart grid. It is the up-gradation of the traditional electric grid. As in the traditional grid, there is a one-way transmission of energy but in the smart grid, both user and customer are active and support two-way communication. It is also called a knowledge-based grid, or the **Grid 2.0**, through which the whole grid could be remotely monitored and can manage lights, traffic congestion, traffic signs, early detection of power consumption, and power influxes etc. The Smart Grid consists of substations, distribution lines, distribution automation, a network of transmission lines, transformers, smart meters, sensors, cloud computing, software, etc.[2]

The organization of the paper is: Section II. is smart grid components and communication protocols. It discusses the main reasons that lead to the adoption of smart grid, its comparison with traditional grid and smart grid, enlightens the fundamental cyber-security framework and some of the common communication protocols has also been discussed. Section III. explores the threats at various components of the smart grid. Section IV. highlights some of the current issues and limitation. Section V highlights the smart grid security market. Section VI critical Analysis And Future Scope and Section VII Conclusion of the paper.

2. 2. SMART GRID COMPONENTS AND COMMUNICATION PROTOCOLS

a) Reasons for Smart Grid Adoption

1. ***Carbon footprints***: Smart grid seems like a measure to comply with treaties like Paris Environment Treaty, Kyoto Protocol, and others to reduce greenhouse gas emissions.

2. ***Renewable Resources*:** Smart grid supports the generation of electricity from renewable resources like solar, wind, hydro. It facilitates the grid to shift the power generation from renewable resources to non-renewable resources at any time as per the demand.
3. **Economic benefits:** In a smart grid, energy utilization depends on the demand of the customers, so it works on demand and supply equilibrium. The machine learning techniques are used to prognosticate the demand and adjust the generation according to the demand.
4. **More Efficient:** Smart grid helps in increasing the quality and consistency of electricity, as through smart grid one can control the use of electricity during peak hours and non-peak hours. [3]

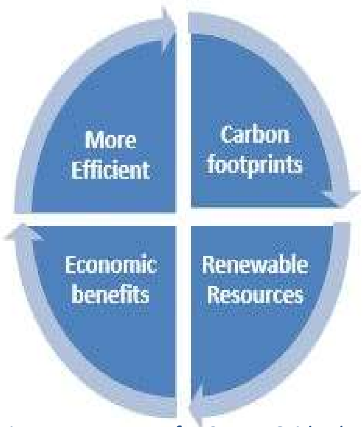


Figure 1: Reasons for Smart Grid Adoption

If we compare the traditional grid with the smart grid we will see the following:[4] However, the integration of the internet of things (IoT) in every field increases its reliability and computability, but along with this IoT exposes devices for cyber threats. According to Symantec's Internet Security Threat Report 2018, on average every hour, there are nine cyber-attack and there is 25% increase in these types of cases every year.

Table1: Electric Grid vs. Smart Grid

S. No.	Characteristics	Analog	Smart
1.	Source of Energy	Mainly non-renewable	Mostly renewable
2.	Communication	Half Duplex (One side) communication	Full Duplex (two side) communication
3.	Power generation	Centralize	Distributed
4.	Sensors	Very few sensors	Sensors all over the grid
5.	Monitoring	Manual monitoring	Self-monitoring
6.	Area affected due to failure	A large-scale area is affected with power loss.	It is Adaptive and isolated in nature.
7.	Control	Limited control	Universal Control
8.	Consumer involvement	No involvement	Yes
9.	Bidding of price	No	Yes

b) CYBER SECURITY FRAMEWORK

These are the framework that helps to determine security breach in system.

Confidentiality: Ensuring protection from unauthorized access to data, or preserving authorized restriction (password, username, credential establishment etc.). So, that only authorized user can get the information and can't be accessed by unauthorized users.

Integrity: Guarding the data against unauthorized modification or tempering and ensuring authenticity during storing, processing and transition. its purpose is to ensure consistency of the data.

Availability: Ensuring data is available all the time i.e., timely and reliable access of data.

Availability means data is available to authorized user without compromising with security

Availability
Integrity
Confidentiality

Figure 2: Cyber Security Framework

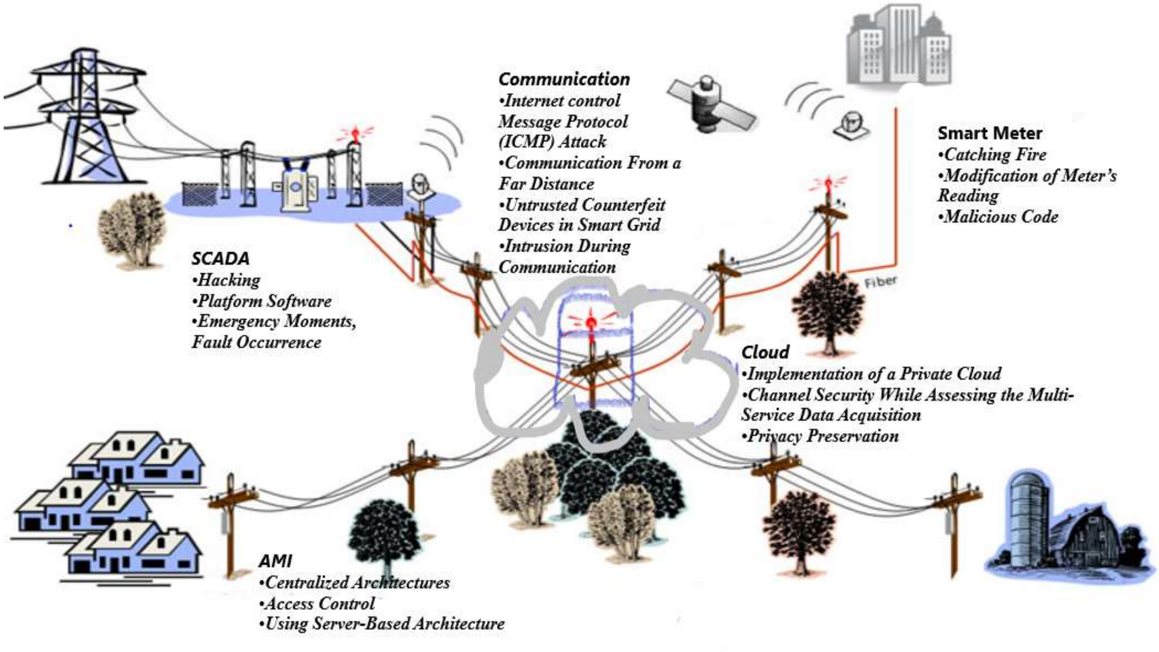
Zigbee	It provide method for security service like frame protection,cryptographic key establishment.
IEC 61107	It is a serial port communication protocol that send ASCII data.
IEEE 1701	It provide plug and play enviornment using ANSCI type 2 optical port.
IEEE 1702	It provide plug and play enviornment using telephone modem communication interface.
IEEE 1703	It is LAN/WAn mode co munication protocol.
IEC 61850	It used Ethernet network interface and support 100 meter distance.
Modbus	It used Serial , Ethernet and support 100 Mbps,1 Gbps data rate.

c) **COMMUNICATION PROTOCOLS FOR SMART GRIDs**

Table 2: Various Threats W.R.T Network Layer

Network Level	**Confidentiality**	**Integrity**	**Availability**
Physical Layer	Eavesdropping	Smart Meter Tampering Attack	Jamming Attacks,
MAC Layer	Traffic Analysis, ARP-Spoofing, Man in the middle Attacks	MITM Attacks, Attacks on ARP	DDoS, Spoofing, MITM Attacks
Transport Layer	Data-Injection, Man in the middle Attacks, IP-Spoofing, Password Purloining	Covert, Injection of malicious code, Disguising the communication, Replay, Wormhole	Buffer Attacks (overflow/ flooding) DDos Attacks, Wormhole, MITM
Application Layer	Data Injection Attack	-	HTTP Flooding, Buffer Overflow, LDoS,

a


Communication
•Internet control Message Protocol (ICMP) Attack
•Communication From a Far Distance
•Untrusted Counterfeit Devices in Smart Grid
•Intrusion During Communication
Smart Meter
•Catching Fire
•Modification of Meter's Reading
•Malicious Code
Fiber
SCADA
•Hacking
•Platform Software
•Emergency Moments, Fault Occurrence
Cloud
•Implementation of a Private Cloud
•Channel Security While Assessing the Multi-Service Data Acquisition
•Privacy Preservation
AMI
•Centralized Architectures
•Access Control
•Using Server-Based Architecture

3. THREATS AT VARIOUS COMPONENTS OF SMART GRID

In this section we review some of the vulnerabilities, risk associated and their countermeasure of each component of the smart grid.

The smart grid is broadly divided into five components i.e Smart Meter, Advance Metering Infrastructure (AMI), Cloud, Communication, and SCADA as shown in figure 3.

1. Smart Meter

It measures the electricity consumption units and communicates bidirectional with advance metering infrastructure. This smart grid component is nearest to the consumer so more prone to attacks. Some of the common miss-functionality with smart meter is:

•**Catching Fire-** As smart meters are not made up of non-tempered material. On a daily basis, there is news of catching fire of smart meter.

[5] In this paper, security threats due to catching fire are discussed and a distributed algorithm has been proposed to protect the smart meters from catching fire. A Guard meter has been installed at each microgrid level and a controller that communicates with SM. The temperature sensors are installed at a smart meter that is used to sense the temperature of SM periodically. An algorithm is designed which checks the temperature of the smart meter Temp (SM) and compares it with a threshold temperature Temp if Temp (SM) <Temp, then the smart meter work normally otherwise a “Disconnect” message will be sent to smart meter and the current configuration will be saved. The temperature of the Smart meter is tested periodically. The complexity of this algorithm is O(n2).

•**Modification of Meter’s Reading-** There are cases when attacker modifies the meter’s reading.

[6] have used a hash function for generating unique cryptographic keys. These keys can be stored in the Smart meter itself in encrypted form and one copy is with the service provider. These keys are generated through a pseudo-random generator. In this paper, the length of the key is 128 bits which will generate 2^{128} unique keys. The advance encryption standard (AES) and rivets cipher 4 (RC 4) also support the 128-bit length of the key. To validate this key encryption method, they used 100 actual meter numbers of the Kenyan utility company and use a hashing function to provide a key. The 11-digit meter number was converted as a string of characters. Before applying the hash function the time is concatenated with the meter number. The hash value is computed using secure hash algorithm (SHA-512). The first 128 bits of the obtained hash value were chosen and used as a key. All consecutive smart meter keys were compared to check whether they are similar or successive meter keys can help in retrieving another smart meter key. But the result shows all keys are unique and no consecutive meter keys have any similarities.

•**Malicious Code-**[7] This paper focused on the seriousness of malicious attacks on smart meter data due to the easy availability of data. They proposed a novel approach to detect malicious code such as minor Trojan, or fleshing of the screen embedded in the system. The detection method is divided into two sub-modules. First is the data collection module, which collects the energy consumption information of the central processing unit (CPU) module inside a smart meter. The power consumption by the CPU helps to detect if there is any malicious code inside a meter or not. If there is malicious code then more power is consumed by the CPU to run those malicious codes. Resistance is placed in between the power module and the CPU module to calculate the current in the circuit. The resultant is in the form of time series. Long-short term memory (LSTM) is used for processing and analyzing this time series data. The model is implemented with the tensor flow of python and comparison is done with traditional machine earning algorithms. The experimental results demonstrate the method the proposed method detects malicious code with an accuracy of 92%.

3 .ADVANCE METERING INFRASTRUCTURE *(AMI)*

In the smart grid, the measurement of energy consumption is held at AMI for predicting the demand of electricity and pricing of consulted electricity. Hence AMI could be a point for intruders to reach all this information. Some of the threats could be:

•**Centralized Architectures-** If the data is centralized then it is easy to assess the data by an intruder, manipulate the data, and theft the data. In order to protect the data, a distributed approach is needed.

[8] In this paper, a hierarchical and distributed intrusion detection system (HD-IDS) is proposed. HD- IDS monitors the AMI environment for early detection of false data injection attacks so that any misshaping could be prevented by taking necessary preventive measures. It is applied on each levels either it is i.e. home area network (H-IDS) that includes a home gateway, Residential area network (R-IDS) that includes residential gateway or the last level that is fog network (F-IDS) that includes fog operational center. There is a communication link between each IDS. The stochastic Markov chain process is used to analyze the smart meter’s behaviour. The authenticity of the algorithm has been tested on real-world traces of the Toronto electricity board.

And it came out that it is more efficient to keep data distributed.

•**Using Server-Based Architecture-**[10] have proposed a Server-less infrastructure, for making it highly reliable, secure, cheap price, less complex, and maintainable. All the system components such as-computational power, the API proxy, security storage, database is managed by the cloud service provider. Some of the technologies used in this paper are for computational power- AWS Lambda, for API Proxy- Amazon API Gateway, for storage- Amazon S3, for the database- Amazon Dynamo DB, for archive –Amazon Glacier. This model can be further extendable by investigating on security aspects of this proposed system.

3. CLOUD

The Smart grid is interdependent on cloud computing. Most of the smart grid applications like energy management, bill generation, data unit consumed user's personal data, electricity forecasting all store in the cloud. Data storage, Data analytics, Data monitoring are three basic utilizations of cloud-based service. It offers fast response, better management, fast computing, and cost-effectiveness. Along with the huge benefit of the cloud, it brings huge risk to the security of data. [11] Here some of the threats have been discussed.

•**Implementation of a Private Cloud-** For the sake of security and privacy private cloud computing is preferred but due to the small size of the private clouds, it is very challenging to support heterogeneous activities of such small size cloud networks. On the other hand, a third party is also involved in real-time monitoring of the smart grid. Although private cloud computing ensures the privacy of customers with the existing technology it is very hard to provide security along with the involvement of third party. [12]

•**Channel Security While Assessing the Multi-Service Data *Acquisition*-**While the data is transmitting to the cloud the problem arises while assessing the multi-service data acquisition.

[13] have proposed a lightweight security algorithm for collecting information on motley services data accession (i.e., of electricity, gas, water, and heat meters). The main concept is “four meters for civil use". It is an integration of multiple meters, but the problem arises in remotely accessing each reading separately. The proposed framework uses the channel security isolation method based on subcarrier isolation. In this model, the broadband power line is divided into multiple subcarriers. Firstly, the total required bandwidth is calculated Btotal and compared with the broadband power line communication (BPLC) total bandwidth capacity C. if Btotal <=C then allocates bandwidth according to requirement otherwise distribute bandwidth proportionally. To validate their model, they experiment by taking channel 1 as normal and channel 2 use channel security isolation algorithm. The data of packet loss rate and delay are tested. The comparative study shows the isolation degree of channel 1 is 0.2 whereas channel 2 has a 1.0 isolation degree.

4. COMMUNICATION

A vast amount of data is transmitting to and forth through a web of communication channels to keep the grid functional.
This transmitted data is vulnerable to cyber-attacks. Here, some of the studies have been done.
•Internet control Message Protocol (ICMP) Attack-

[15] have shown the extent to which a cyber-attack can hamper the smart grid and the data collection regarding power use. A commercial Multiline EPM 6100 Power Quality Meter is connected with two bulbs (385- watt load) and its power consumption is noted for four days. An ICMP ping-based cyber-attack is done on the communication channel for the next four days. After day four there is a 1.77% reduction in power consumption. Here it seems a low value but when applied to the database of the Pacific Gas & Electric company, then the total loss of revenue due to this cyber-attack is $18.6 million per month which is a significant financial loss.

•Communication from a Far Distance-
[16] have come up with a solution to overcome the problem that was hard to reach smart meters which were far from clustered areas. Approx. 1% Smart meter located in remote areas which is liable to account for the half cost of entire smart meter network. They have proposed a wireless long-range communication using long range (LoRa) technology. It uses low power, low rate but supports long-range communication (up to 22 km). The whole system is composed of two parts-

Figure 4: Communication Sequence

securing the meter through the LoRa technique and key management. The smart meter reading is sent to the data collector through the communication channel. The smart meter has a secret key that is assigned when it is deployed. On the periodically base reading is sent to the data collector. Here this reading is encrypted with the help of key management protocol. At every transaction between data collector and smart meter, a unique key is assigned so that no intruder can manipulate or read the data in between. All this can be understood through the following steps: -

- Connection request
- Connection confirmation
- Authentication request,
- Authentication result,
- Send reading request,
- Response to a reading request,
- Disconnect request,
- Disconnect confirmation.

The efficiency of the system is shown by the experiment.

•**Untrusted Counterfeit Devices in Smart Grid-** [17] The paper discusses the effects of counterfeit device in smart grid. They divided the devices into 2 broad categories: resource-rich () and resource-limited devices (). The paper utilizes two techniques to detect counterfeit devices in the smart grid. First is system call tracing by using ptrace and library interposition to know the type and amount of system calls are invoked while communicating. The purpose of these two techniques is 1) To compare the system calls of genuine grid and grid containing the counterfeit device to identify the variation of system call activity through both methods; 2) they also draw the statistical correlation of the system call invoked by the genuine and counterfeit devices.

•**Intrusion During Communication-** [18] While data is being communicated from one system to another in the form of signals there are possibilities of data intrusion either by adding extra noise or outliers. This paper designs an algorithm named Kalman filter. The Kalman filter removes the noise and destructive effects from the signal. Further, an x2- Detector technique is applied on the output signal of the Kalman filter effect to distinguish attacks from noise to prevent false alarming in case of the presence of noise in the manipulated signal. This approach is 99.73% effective in detecting DOS, Scaling, Random attacks, and false alarming. (Intrusion Detection on Critical Smart Grid Infrastructure)

5. SCADA SYSTEMS

The smart grid has a centralized control system named Supervisory Control and Data Acquisition (SCADA). SCADA is a system that reports, monitors, measures, and control real-time situations. The data consists of switch position, voltage, current, circuit breaker, and apparatus alarms. Attackers are always keen to get all this information for the sake of attack/collapse the smart grid. Some of the attacks have been discussed here.

•**Hacking**-Hacking is a very common threat to the smart grid. Sometimes the hacker hacks the system for the sake of publicity among peer groups and in some cases, it may be revengeful activity. On the basis of the nature of attacks, these are classified into three categories - topology wise, protocol wise and component-wise attacks.

•**Platform Software-** It includes three types of threats- denial of service (DoS), lack of intrusion detection, presence of malware. The DOS attack on SCADA software may lead to delay in system operation, prevent authorized entry to software, disruption of service. The lack of intrusion detection may lead to deletion of data, loss of system availability, or inappropriate use of control commands. The malware in the system can cause degradation of service, loss/modification of data, or degradation in performance of the system so the presence of malware protection software is essential for the proper functioning of not only SCADA software but for the whole smart grid. This paper introduced two techniques. One is to safeguard SCADA from DOS attacks and the second technique is to remove sniffers from the system. They analyze the transistor-transistor logic (TTL) to detect the DoS attacks. However, message digest (MD) -5 algorithm and Promiscuous mode detection is used to detect and remove sniffer. [19]

•**Emergency Moments, Fault Occurrence**- This paper has discussed those emergency moments when it is hard to provide a robust and reliable supply of electricity. To ensure the increase in quality of power supply they discussed the importance of satellite telemetry connectivity technology. The satellite telemetry connectivity technology is used to monitor and control measurement systems present at the customer side. In an emergency situation, it is hard to establish a communication channel between SCADA present at the Distribution Operation Center (DOC) and devices installed at the customers' side which leads to no telecommunication coverage. This loss of telecommunication coverage will result in a huge techno- financial loss. The satellite telemetry comes as a channel for communication between DOCs -cloud-metering equipment at the customer's side [20].

Table 3: Attacks Occurred in Different Components

S. No	Parameters/Attacks	SM	AMI	Communication	Cloud	SCADA
1	Temperature	✓	✓			✓
2	Malicious Code	✓	✓	✓		✓
3	ICMP		✓			
4	Trojan	✓	✓			✓
5	DoS	✓	✓	✓	✓	✓
7	Data /Pilferage of data	✓			✓	

6. ISSUES AND LIMITATIONS

Although Smart grid is an ongoing technology, that is booming with new technologies day by day. A lot has been done, and a lot is to be done, on the basis of analysis of current development. Here we have studied some of the papers and try out to find some of the research gaps that will help out the researchers.

Table 4: Issues and Limitations in Existing Work

S.No	Publish year	Description	Research gap	Techniques
1.	2020 [5]	• A distributed algorithm is proposed to protect SM from fire. • A Guard meter is installed at micro grid level and a controller. • The temperature sensors are used to sense the temperature of SM periodically.	• The temperature of SM is tested periodically. • The complexity of this algorithm is O(n^2) which can be optimized.	• Distributed Algorithm
2.	2020 [10]	• A Server less infrastructure is proposed. • All the system components such as-Computational power, The API proxy, security storage, database is	• It can be extended by investigating on security aspects of this proposed system. A demo can be built to compare with existing model.	• For Computational power- AWS Lambda •For API Proxy- Amazon API Gateway

		managed by cloud service provider.		• For Storage-Amazon S3 • For database-Amazon Dynamo DB • For Archive – Amazon Glacier.
3	2020 [9]	• The paper came out with a new access control contract scheme (ACC) to make smart grid more trustworthy and use distributed approach.	• Trust management system can be applied for better security.	• Blockchain
4	2020 [6]	• Hash function is used with first 128 bit key	• By introducing recursive method while applying hash function. • Various new subsets of hash value can be made while selecting the keys (hash function).	• AES • RC 4
5	2019 [15]	• This paper shows the extent to which a cyber-attack can hamper the smart grid and the data collection regarding power use.	• Experiment could be done with various attacks.	• ICMP Ping flood attack • A commercial Multilin EPM 6100 Power Quality Meter
6	2019 [13]	• This paper uses a concept "four meter for civil use". • It collects information of multi service data acquisition (i.e., of electricity, gas, water and heat meters).	• Various multiplexing techniques can be used for sharing bandwidth	• Channel security isolation algorithm.
7	2019 [8]	• 3 level security is provided HAN, RAN, and FAN	• Edge computing	• Fog computing

8	2019 [7]	• Malicious code detected by studying the power consumption of CPU module.	• Accuracy could be increased above 92%. • Different machine learning algorithm could be used.	• Long Short-Term Memory (LSTM) network
9	2018 [16]	• For long way communication LoRa technique is used and the data is secured through encryption key.	• key encryption method like hashing	• LoRa communication technique • Key encryption technique

7. SMART GRID SECURITY MARKET

According to compounded annual growth rate (CAGR), it is expected that there will be 30% increase in total expenditure from USD 7.8 billion to USD 79 billion on cyber security through 2020.[22]

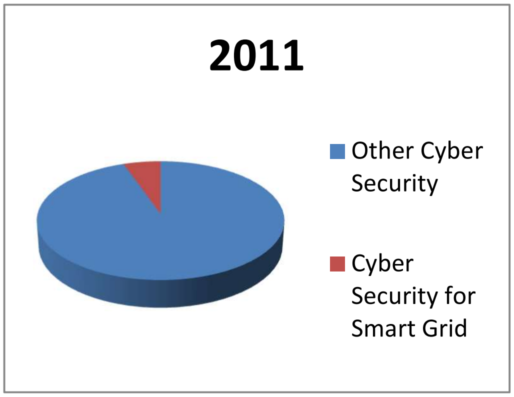


Figure 6: Security Issues in 2011

8. CRITICAL ANALYSIS AND FUTURE SCOPE

The issues related to security are occurring day-by-day, and in anticipation the technology and techniques of security are also upgrading in terms of overcoming existing issues/limitations. There are several techniques like encryption (end-to-end encryption), DES, Steganography, etc. to secure the data while data synchronizes to and forth between various components of smart grid. Various new technologies like blockchain, cloud computing, and fog computing can be used for data storage and computation. Moreover, machine learning can be applied to predict/ analyze the generation of the electricity. So that, the demand and supply

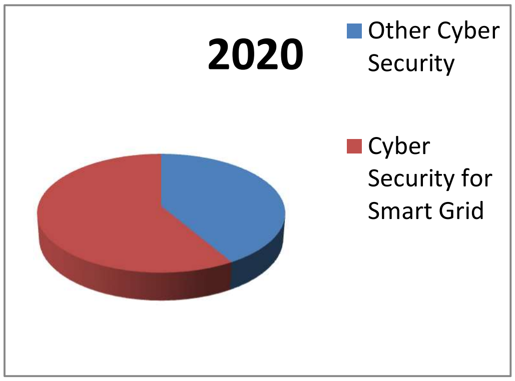


Figure 7: Smart Grid Security Market

equation can be maintained. But the existing work is easily tempered and accessible without any authorized validation/verification. In future, the authors of the present study will try to extend existing work with the latest technology/tools/techniques.

4. CONCLUSION

Indeed, the smart grid is successful in becoming a part of this generation but security threats cannot be underestimated. Recognizing and eliminating such problems (like data loss, manipulation in bills, hackers, zero-day, malware, etc.) before any security breach happens is very essential since the presence of any single loophole can lead to threats to the smart grid. This paper provides an overview of existing threats in various smart grid components. Each component is having its own and different types of threats so the method used to cope up with these threats will also be different. This paper revels the existing research gaps/future scope that are very important to fulfill the requirements for providing the security to the grid. However, continuous research is going on in this field but it still needs more efforts to solve these threats.

REFERENCES

[1] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A Methodology for Security Classification applied to Smart Grid Infrastructures," Int. J. Crit. Infrastruct. Prot., vol. 28, p. 100342, 2020, doi: 10.1016/j.ijcip.2020.100342.

[2] N. Kumar and G. Singh, "Energy efficient load optimization techniques for smart grid with futuristic ideas," Int. J. Eng. Adv. Technol., vol. 9, no. 1, pp. 4327–4331, 2019, doi: 10.35940/ijeat.A1778.109119.

[3] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," IEEE Trans. Power Syst., vol. 21, no. 2, pp. 548–558, 2006, doi: 10.1109/TPWRS.2006.873129.

[4] H. P. T. T. Frp, "6XPPDU \ RI 5HVHDUFK RQ 6HFXULW \ DQG 3ULYDF \ RI," pp. 39–42, 2020, doi: 10.1109/CCNS50731.2020.00017.

[5] R. Marah, I. El Gabassi, S. Larioui, and H. Yatimi, "Security of Smart Grid Management of Smart Meter Protection," 2020 1st Int. Conf. Innov. Res. Appl. Sci. Eng. Technol. IRASET 2020, 2020, doi: 10.1109/IRASET48871.2020.9092048.

[6] L. K. Kiarie, "Key Generation for Electrical Smart Meters using Hash Functions," pp. 0–3.

[7] H. Wang, J. Li, T. Zhang, H. Ying, J. Han, and X. Ji, "Malicious Code Detection on Smart Meters - A Side-Channel Based Approach," 2019 IEEE 3rd Inf. Technol. Networking, Electron. Autom. Control Conf., no. Itnec, pp. 808–812, 2019.

[8] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid," ICC 2019 - 2019 IEEE Int. Conf. Commun., pp. 1–6, 2019.

[9] Z. Abou, E. Houda, A. Hafid, and L. Khoukhi, "Blockchain Meets AMI: Towards Secure Advanced Metering Infrastructures," 2020.

[10] A. Al-Naser and W. M. El-Medany, "A proposal for server-less cloud-based infrastructure for a smart metering system in the Kingdom of Bahrain," 2018 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2018, pp. 1–4, 2018, doi: 10.1109/3ICT.2018.8855729.

[11] M. Mahmud Hasan and H. T. Mouftah, "Cloud-centric collaborative security service placement for advanced metering infrastructures," IEEE Trans. Smart Grid, vol. 10, no. 2, pp. 1339–1348, 2019, doi: 10.1109/TSG.2017.2763954.

[12] Y. Ma, F. Zhao, X. Zhou, and Z. Gao, "Summary of cloud computing technology in smart grid," Proc. 2018 IEEE Int. Conf. Mechatronics Autom. ICMA 2018, pp. 253–258, 2018, doi: 10.1109/ICMA.2018.8484418.

[13] Z. Yin, S. Dou, H. Bai, and Y. Hou, "Light-Weighted Security Access Scheme of Broadband Power Line Communications for Multi- Source Information Collection," 2019 IEEE 3rd Inf. Technol. Networking, Electron. Autom. Control Conf., pp. 1087–1090, 2019.

[14] H. Yang, S. Liang, H. Li, and C. Security, "Privacy-preserving HE-based clustering for load profiling over encrypted smart meter data," 2020.

[15] S. Kumar, H. Kumar, and G. R. Gunnam, "Security Integrity of Data Collection from

Smart Electric Meter under a Cyber Attack," Proc. - 2019 2nd Int. Conf. Data Intell. Secur. ICDIS 2019, no. Epm 6100, pp. 9–13, 2019, doi: 10.1109/ICDIS.2019.00009.

[16] Y. Cheng, H. Saputra, L. M. Goh, Y. Wu, C. S. Tower, and F. Way, "Secure Smart Metering Based on LoRa Technology."

[17] L. Babun, H. Aksu, and A. S. Uluagac, "A Framework for Counterfeit Smart Grid Device Detection," pp. 0–1, 2016.

[18] F. Akbarian, A. Ramezani, M. T. Hamidi-Beheshti, and V. Haghighat, "Intrusion Detection on Critical Smart Grid Infrastructure," Proc. - 2018 Smart Grid Conf. SGC 2018, pp. 1–6, 2018, doi: 10.1109/SGC.2018.8777815.

[19] S. Shitharth and D. P. Winston, "A novel IDS technique to detect DDoS and sniffers in smart grid," IEEE WCTFTR 2016 - Proc. 2016 World Conf. Futur. Trends Res. Innov. Soc. Welf., vol. 5, no. 8, pp. 434–440, 2016, doi: 10.1109/STARTUP.2016.7583897.

[20] R. Burian and H. Alvarez, "Robustness and Reliability in Smart Grid Solutions," 2019 IEEE 7th Int. Conf. Smart Energy Grid Eng., pp. 59–62, 2019.

[21] Last assessed on (15 February 2021)https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-24-cyber-security-threat-landscape).

[22] Last assessed on (21 April 2021) https://www.marketsandmarkets.com/Market-Reports/smart-grid-security-market112912959.html

[23] Smart Meter [Available Online] https://www.google.com/url?sa=i&url=https%3A%2F%2Fpestechenergy.com%2Fevents-and-news%2Fgoodbye-digital-meters-and-hello-to-smart-meters-reap-the-benefits-of-advanced-metering-infrastructure-ami%2F&psig=AOvVaw0LmeK7v-2_OgZeZOC&ust=1630923883712000&source=images&cd=vfe&ved=2ahUKEwiV4ZyHz-fyAhWatWMGHcUeA9IQjRx6BAgAEAk Last accessed on 29 July 2021.

[24] N. Kumar and G. Singh, "A Novel Algorithm to Improve the Power Quality for the Smart Grid and Integration with the Optimization Framework". International Journal of Engineering Trends and Technology, 69(9),272-280. DOI:https://ijettjournal.org/archive/ijett-v69i9p233.

[25] Irawan, Y., Fonda, H., Sabna, E., & Febriani, A. (2021). Intelligent Quality Control of Shrimp Aquaculture Based On Real-Time System and IoT Using Mobile Device. International Journal of Engineering Trends and Technology, 69(4), 49–56. https://doi.org/10.14445/22315381/ijett-v69i4p208

[26] Kaushik, N., Bagga, T., & Aggarwal, R. K. (2020). Comparative Study on IoT Technologies - Short & Long Range. International Journal of Engineering Trends and Technology, 68(12), 37–42. https://doi.org/10.14445/22315381/ijett-v68i12p207