Role of Cryptography in Smart Grid Security

Vibhuti Vats
Mody University of Science and Technology
v.vats98@gamil.com

Stuti Nagwanshi
Mody University of Science and Technology
stutinagwanshi@gamil.com

Nisheeth Saxena
Mody University of Science and Technology
Nisheethsaxena.cet@modyuniversity.ac.in

Abstract. The power system's efficiency and reliability can be improved by the latest invention of the "Smart Grid". Smart Grid being one of the biggest technology and so useful and powerful is also facing some of the crucial and dangerous security threats from everywhere round the globe. It plays an important role in modern energy infrastructure. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently, and how to process a huge amount of data received from these devices. Cryptography can be used to counter smart grid security threat to a large extent.

Keywords: *Smart grid, Power system, Cyber security, Cryptography.*

*****

1 Introduction

"Power System" is one of the most essential, complicated, and smart network we have in today's technology world. This system have components such as circuits, wires, towers, transformers, sensors, and cables interlinked to give us undisrupted power supply from source to destination to transfer the information efficiently. The power system is more of a mechanical system and has very less association with electronics system like sensors and communication. But our new technology "Smart Grid" improves the performance of the power communication system by involving new and better steps and methods to supply the power. This can be happening only because smart grid uses sensors communications, calculation, and control in to make the system work for itself using intelligence in the form of control through feedback or in other words by practicing two way communication. Yes, smart grid uses two ways communication that is it transfers the communication from both the ends of the path be it the receiver or the transmitter [1].

The National Institute of Standards and Technology (NIST) recounted the smart grid as the combination of the traditional power grid with the current latest development in information and communication technologies. This is because smart grid accounts all the required parameters and sectors for an efficient and safe power supply that too "Two Way" power supply.

1 The "Smart" Grid

The term Smart Grid refers to the next generation power grid that generates, transmits, distributes and manages the flow of the power transmitted also managing the electricity and also upgrading the system again and again. And all these tasks are done by the smart grid with the help of the latest technologies of computing and communication sector. In other terms smart grid is a way to set-up a two-way communication between two parties where the flow of power is done from both the sides instead of one which used to happen in the earlier power grids available to us.

Even the governments are also promoting this and helping to take it to the next level so as to improve it and make most use out of this [9].

Being so advanced and technologically ahead smart grid helps in increasing the performance of the power suppliers as well as to the end users by optimizing their power consumption. But due to the heavy dependency on communication networks and computing techniques smart grids are now more prone to be a target of the usual cyber attacks [9].

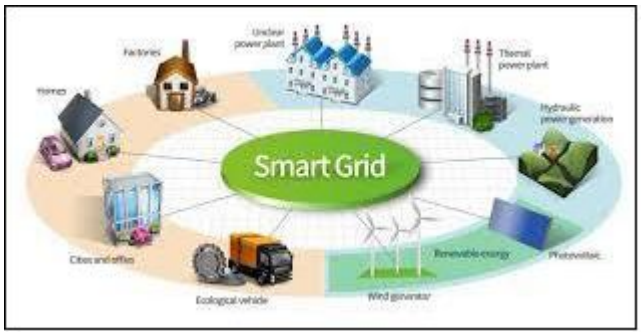

Fig: Smart Grid [9]

For smart grid the supervising is done by executing a smart appraising systems network, as well as smart meters for communicating with the basic system. In its modern, the grid consists of four extensive components:

1) Electric energy is being produced in different manners, e.g., by scorching fossil fuels, counting nuclear reaction, trapping water (hydro-electric dams), wind, Solar, and tidal forces.

2) Transference moves electricity through a very high voltage framework.
3) Distribution steps down current and gives out for utilization.
4) Exhaustion, i.e., industrial, commercial and residential sectors, uses the electric energy in a collection of ways.

Smart grid basically consists of two components:

A. System Components:

The main system components of the smart grid are daily Electrical apparatus, Renewable Energy resources, Smart meter, Service Providers and Electric Utility Operation Center.

i) Electrical Household Devices assures efficient power consumption by all electrical household appliances because of the fact that these devices are able to interact with smart meters through Home Area Network (HAN).

ii) Renewable energy resources like solar and wind energy give the opportunities to generate electricity on their own using these renewable resources.

iii) Smart Meter is a stand-alone embedded system. It contains a microcontroller that has both volatile and non-volatile memory, both analog and digital wharf, tiers, sequential time clock and serial communication facilities [4].

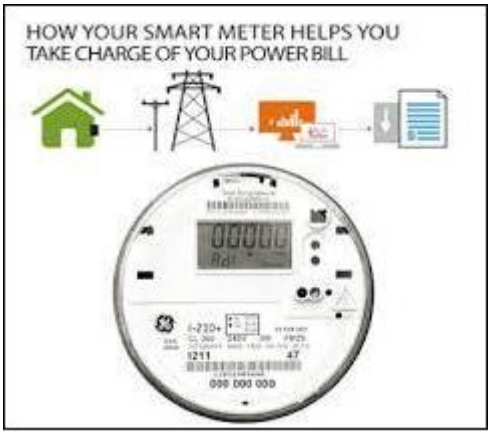

Fig: Smart Meter [16]

iv) Electric Utility Center regulates the power consumption by interacting with smart meters. It sends all the utilization associated information to smart meters and collect power utilization reports with respect to the hours used.

v) Service Providers it generates contracts with users related to their power consumption and to cater electricity for personal equipment. It interacts with domestic devices via messages given by the smart meter [4].

B. Network Components:

It assimilates two types of transmission: Home Area Network (HAN) and Wide Area Network (WAN). The HAN connects all the home appliances across the home with the smart meter for further communication using ZigBee, wired or wireless Ethernet or Bluetooth. A WAN on the other side, is an enormous network that associates the smart meters, service providers and electric utility [4].

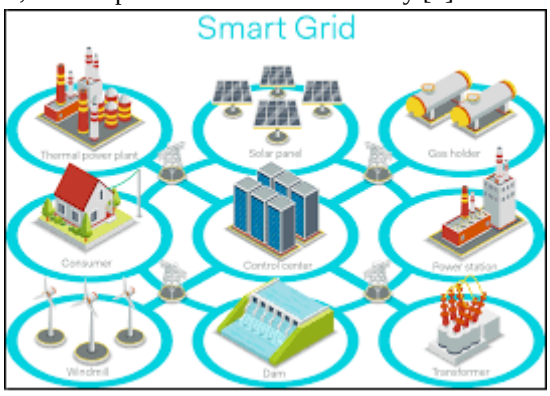

Fig: Smart Grid [10]

The Goals and Challenges of Smart Grid Objectives

The current power grid has more than 9200 electric developing units, 1,000,000 plus megawatts of developing capacity associated by using 300,000 miles of communication lines.

The basic requirement of electricity is it must be used as soon as it is developed. And the present grid is so much successful in this task to be fulfilled. However, we can't and we shouldn't ignore the fact that the grids are being over burdened now and because of that reliability of the grid is at stake.

Also being it so efficient the smart grid beats everything in terms of its efficiency and that makes it one of the best technologies and efficient one in the field of power supply.

Also in United States of America the electricity is produced by burning of coal which in turns leads to immense increase in the global warming. So by using renewable resources for this power generation we can reduce the extent of global warming caused by burning of coal.

The most important factor is the security. The grid is so much prone to cyber attacks that its security becomes its most important aspect to be taken care of [12].

Challenges

The communication network in the smart grid is refined as it combines number of devices that communicate with each other. And thus it makes it vulnerable to be prone to cyber attacks.

Cyber Security Model

There are three main aspirations that cyber security targets on in any network's security and that is confidentiality, integrity and availability, that is, availability of power with virtue of information and confidentiality of customer's information.

Confidentiality

The network only is liable for the conservation of the user's knowledge. The user must be given this information that their data is secured and protected in this network. And if not then the user should be provided with the proper information about the attacker.

Integrity

We also have to make the user feel safe and tension free that their messages will be received in an authenticated manner only. The network must ensure that the information is pure and not tempered.

Availability

One of the main reason we are using this smart grid technology is availability. Because at the end of everything all we need is to grant continuous power supply to the end user and match their obligations with at most sincerity.

The cyber infrastructure of smart grid consists of electronic information and communication systems and services along with the information stored in these systems and services. The infrastructure includes both the hardware and software too. Their primitive objectives are to process, store, and communicate data. This is completed using a control system that is Supervisory control and data acquisition (SCADA). The SCADA is a neutral system [12].

SCADA

Our power distribution system uses centralized control systems which are called as (SCADA). It is used for checking and supervising process.

SCADA system comprises of the following blocks mentioned below:

(i) Processed data is presented by HMI (human machine interface)
(ii) There is a supervisory computer which is responsible to collect all the data and use it for processing.
(iii) It comprises of remote terminal units (RTUs)
(iv) Programmable logic controller (PLC)
(v) Communication infrastructure

The SCADA systems are connected to internet or by certain specific lines by the help of power system communication in the smart grid. The vendors are using off the shelf products as part of the SCADA systems. These products are like the personal computers we use at home and thus are susceptible to attacks and different threats.

A SCADA system is required in the grid structure. It is used for two purposes; the public transport system and the public control system.

The cyber security basically can be attacked in the following three steps:

(i) The SCADA system is controlled over by the attacker,
(ii) The attacker identifies the suitable system to launch an attack
(iii) Attacker initiates the attack.

These SCADA systems are most prone to attacks. Automation is required to prevent the attackers from gaining control of SCADA system. Cyber security coordination task group (CSCTG) has been established by the NIST, which addresses and evaluates processes resulting in thorough cyber security policies for smart grid.

The risks assessed by the CSCTG consist of the following:

(i) Weak point and openings to attackers due to complexity of the grid.
(ii) Cascading errors due to interconnected networks
(iii) DOS (denial of service) attacks
(iv) Attack on consumer privacy to excessive data gathering
(v) Attacks from annoyed employees and terrorists
(vi) The number of entry points for an attacker increases as number of nodes increases [12].

2 Cryptography

The importance of information and communication system in today's world for the society and economy is increasing with the increasing data that is transmitted and stored on those systems. But at the same time these data and information of communication system is becoming very vulnerable to the cyber threats and cyber- attacks such as unauthorized access and use, unauthorized alteration and updating and destruction of the data and information of the user. The hiding of information is called encryption, and on the other side when this hidden information is unhidden by the network that is known as decryption. A cipher is used for this encryption and decryption process [4].

To hide any data two techniques are used mainly which are named as cryptography and Steganography. Here, we are discussing about cryptography only. It is the science of protecting the data, which means converting the data into unreadable form so that only the person who is supposed to get the information may only read the information and no one else can access it unauthentic. It uses mathematics to encrypt and decrypt the data so as to secure it from any misappropriation.

Basic Terms of Cryptography

It is the technology to secure our data in which our data gets converted to a form which can't be understood and is not readable. It actually refers to the methodology of concealing the content of messages, to secure it from the people who

are not supposed to get the information right. The word Cryptography came from a Greek word "Kryptos", which contains the meaning hidden, and "graphikos" means writing.

The information that we intend to secure and save from others is called as "Plaintext". Plaintext can be of any form it can be text, pictures, executable programs, and numerical data. The plaintext for example is the text the sender has before encryption or the data that receiver receives after decryption.

The transmitted text is called as cipher text, its meaning is meaningless data or unclear text that nobody can understand, accepts the one who tends to be the receiver. This text is transferred from the network. There are various algorithms used and applied for the conversion of plaintext to cipher text. Cipher is the algorithm which is used to transform plaintext to cipher text. Basically, it is the conversion of readable and understandable data to meaningless data. And this conversion of plaintext to cipher text is called "encryption".

The Key is the input to the encryption algorithm, and this value must be independent of the plaintext provided. This input is used to convert plaintext to cipher text. Also different keys generate different cipher text. And on the other side, the inverse of the key will be used inside the algorithm instead of using the key [4].

Goals Fulfilled

Cryptography is the technology that basically is used to protect our data. And in that process fulfills various goals, which are listed below:

1. Cryptography helps keeping the data and communication signals as confidential and secured by ensuring that no one else can understand it or misuse it.
2. The data which is being transferred can only be read by people with proper identity hence maintaining the authentication of the document.
3. It also maintains data integrity by ensuring that the data transferred can't be changed and is as same as it was before the sender sent it.
4. It also ensures that the message is actually sent by the sender and is received by the specific and correct receiver, so that the receiver can't claim that the message wasn't sent.
5. Cryptography manages access control too. It is a process in which unauthorized use of resources is being prevented. This is done by setting some permission levels which are used to check the access control to the resources. By which we can ensure that the access is given to correct user or not.

Types of Cryptography

There are basically two types of cryptography:

1. Symmetric Key Cryptography

It is also known as private-key cryptography. In this type of cryptography a secret key is generated and provided to the sender as well as the receiver. If the cryptography is used to send some secret message between the two parties, both the sender and receiver must have the secret key to access the data.

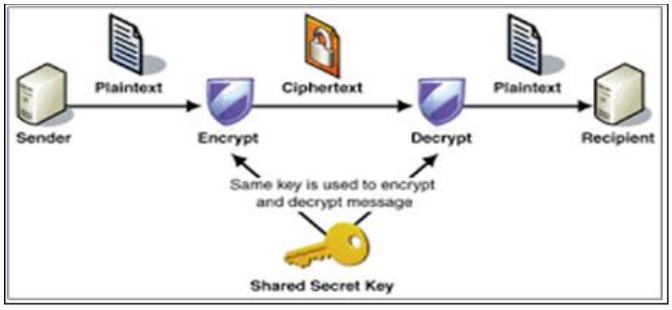

Fig: Symmetric Key Cryptography [11]

2. Asymmetric key Cryptography

This two-key system is also known as the public key system, in which one key is used to encrypt the sender's data and the other mathematically related key is used to decrypt the data on the receiver's end. In this the computer generates a key which is unique and is provided to sender only, then the computer which receives it may decrypt the message using another key provided to it to decrypt it and use it.

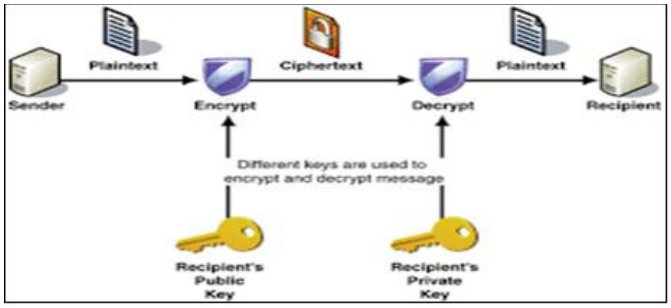

Fig: Symmetric Key Cryptography [12]

3. Cryptography in smart grid

Smart grid being a device which helps to generate a two way communication between the user and utility generally becomes an easy target for the cyber attacks. And to be safe from them cryptography is used as a technology to create a secured network. Using this new smart grid users can also generates their own electricity and check their bills and power consumption. And in this process what happens is the power generated is sent to user and then the user consumes it and sends the data back to utility which makes it a two-way communication and hence gives a better option instead of the previous or the traditional power grid. From the utility bill is generated which can be checked by the user also

whether it came according to the power consumed or not. And like this the user can generate their own energy according to their needs and their resources available.

And in this process the data is secured by the techniques of cryptography. Using the concept of encryption and decryption the data is secured between the sender and the receiver only. Using the high definition security of cryptographic algorithms and other techniques the smart grid security is ensured. Cryptography ensures that the moment of power signals is done right and with right security measures between the sender and the receiver.

3. Conclusion

Smart grid technology has a great potential to be an amazing power supply technology. Even the previous traditional grids and the latest smart grids have been revolutionary change in the world of communication networks. Although, the more vast and new the technology is the more prone it gets to the cyber attacks and thus creats a tension among the masses of protecting it or securing it from the cyber attacks. But the new method of securing it using the cryptography technology gave a turn to the technology and ensures the security of the data transferred in the network. Smart grid technology can be widely used for various other plans to complete like getting your own electricity using the renewable resources and thus getting an account of your own bills all by yourself. Also, smart grid helps to do all the communication in a more secure and safe way which can't be done by any other technology so efficiently. Also, cryptography provides a better way of using the smart grids efficiently and safely. Smart grid if worked and planned more in future can turn out to be a good technology which can benefit us in future.

4. References

[1]. Joonsang Baek, Quang Hieu Vu, Joseph K. Liu, Xinyi Huang, and Yang Xiang, A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid, IEEE VOL. 3, NO. 2, APRIL/JUNE 2015.

[2]. Security in the smart grid, ABB white Paper.

[3]. Wenye Wanga,_, Zhuo Lua, Cyber Security in the Smart Grid: Survey and Challenges, aDepartment of Electrical and Computer Engineering, North Carolina State University, Raleigh NC 27606, US.

[4]. Fadi Aloula, A. R. Al-Alia , Rami Al-Dalkya, Mamoun Al-Mardinia, Wassim El-Hajjb, Smart Grid Security: Threats, Vulnerabilities and Solutions

[5]. Department of Computer Science & Engineering, American University of Sharjah, United Arab Emirates (UAE), Department of Computer Science, American University of Beirut, Lebanon, International Journal of Smart Grid and Clean Energy, Manuscript received June 15, 2012; revised August 15, 2012.

[6]. Mickael Avril, Laurie Basta, Laurent Bouillet, Identity Based Cryptography for Smart-grid Protection.

[7]. Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli, Cyber–Physical Security of a Smart Grid Infrastructure, 2011 IEEE.

[8]. Dr. Sajjad Hussain, Raja Omman Zafar Department of E.E, Muhammad Ali Jinnah University Islamabad, Pakistan, Key Management Scheme and Cryptography in Smart Grid Elements, Volume 5, Issue 8, August 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[9]. Special section on Smart Grid Cyber-Physical Security, Call for Papers – IEEE Transactions on Smart Grid.

[10]. https://www.powerelectronicsnews.com

[11]. https://www.smartgrid.gov/the_smart_grid/smart_grid.html

[12]. http://ehindistudy.com/2015/10/01/symmetric-and-asymmetric-key-cryptography- in-hindi/

[13]. https://commons.wikimedia.org/wiki/File:COXqbcXUwAACzHg.png

[14]. https://www.hindawi.com/journals/ijdmb/2011/372020/

[15]. http://www.timreview.ca/article/702

[16]. https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

[17]. http://chinacrypt2012.ustc.edu.cn/archive/IT8.pdf

[18]. https://www.elprocus.com/overview-smart-grid-technology-operation- application-existing-power-system/