International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Security in Smart Meter using Iot

Somalina Chowdhury, Santanu Kumar Sen

Abstract: ***Today digitalization is key of our lifestyle not only in cities but also in rural areas. Nowadays, Internet of Things (IoT) is adding feathers to this globalization. In this research paper we will discuss about the safety and security of one of the most popular applications in IoT, i.e, Smart Meter in Smart Grid. Especially about Smart Meter in Smart Grid, which is fundamental part of it. Smart Meter unlike traditional metering system bidirectional in nature. Thus they have two streams one for power flow and second is data collection, analysis and processing i.e, communication, this is done by communication channel. Assured, strong, high-end security must be designed to the communication network so that data cannot be tampered, manipulated or interrupted by outer world. Here we will apply a unique technique of cryptography by which a secure communication channel method using Genetic Algorithm can be designed. By implementing this technique we can ensure a safe communication between customer and utility company. Thus, provide security to the data flow.***

Keywords: Smart Grid, Smart Meter, IoT, Cryptography, Genetic Algorithm

I.INTRODUCTION

Power grid is use to distribute generated electricity or power from utility company to the customer through Smart Meter as per demand. It includes generators, high voltage transmission lines, and data concentrator for carrying electricity and distribution lines that connects end customers. But these power grids has limitations like low reliability, low security, high rate electricity failure, high greenhouse gas effect and high carbon emission. These loopholes are overcome by Smart Meter in Smart Grid [1]. Smart Meter has unique ID and it helps in bidirectional communication between the utility companies and its customers. AMI in regular metering help to automate it to certain extent but Smart Meter along with IoT enhance the process. SG collects data from Smart Meter. Then analyse the data and compose it as per power supply and customers or utility wants. In SMART METER data are stored in cloud server. IoT based Smart Meter uses sensors, RFID, cloud, transmission lines etc., all of these must ensure safety and security. Any communications network that can be public, private, wired, and unwired all can have threats. Cyber security must be guaranteed availability, integrity, confidentiality and control system required to manage, operate and protect Smart Meter in Smart Grid infrastructure [2]. Delay of data arrival and packet loss degrades system performance.

II.RELATED WORK

IoT interact with living and non-living things. Thus it works in all three dimensions i.e, Physical, real and virtual world. It can collect data from Smart Meter and analyse is the data of the customer. These data can be personal data of them like how much electricity consume by them, when the power is having high usage or low etc. Thus can even predict when users are at home or not [3] or can theft electricity consumed data and manipulated it. Smart Meter must implement high encrypted security device or sensor. There can be many cyber or security attacks like Man in the Middle, Replay, Denial of service, Spoofy, tamper, fake user etc. These are overcome by many cryptographic techniques introduced like Rabin encryption for secure data [4] or RSA etc. Data is collected through Smart Meter and send through transmission line with the help of ZigBee, WiFi, 3G etc. Cyber security in SG that can occur in Smart meter deployment, is one of vital problem. We categorized the Smart meter security issues into three divisions which are attacks on network, attacks on physical hardware and attacks on data. Each division, a number of security issues and attacks that have been identified[5].Cyber-attack in Smart Meter can cause false billing, customers personal data like at what time of the day how much power consumed or their billing accounts details etc. and analyse them in adverse way. Secured communication must be our goal. In this paper we will apply encryption decryption algorithm with genetic algorithm proposed in one of my papers. So that we can strengthen our security process [6].It is an asymmetric key cryptographic algorithm where two kinds of key is used public and private. Public key for encryption and private for decryption. Data receive herein digital format. We will take out our algorithm on per 64 bit each time we encode. Here genetic algorithm is implemented so that the method get stronger.

III.METHODOLOGY

The algorithm given is capable of **giving** security to data communicate through a very strong process of data security. After securing the data during communication it must be storage in local database. Like these various Smart Meter stores their data. After interval of time, these data send to cloud. We can also designed web page that linked with smart meter to give information to customer and utility companies.

Revised Manuscript Received on April 25, 2020.
* Correspondence Author
Somalina Chowdhury*, Assistant Professor,Dept. of Computer Application, GNIT
Prof. (Dr) Santanu Kumar Sen, Principal, GNIT

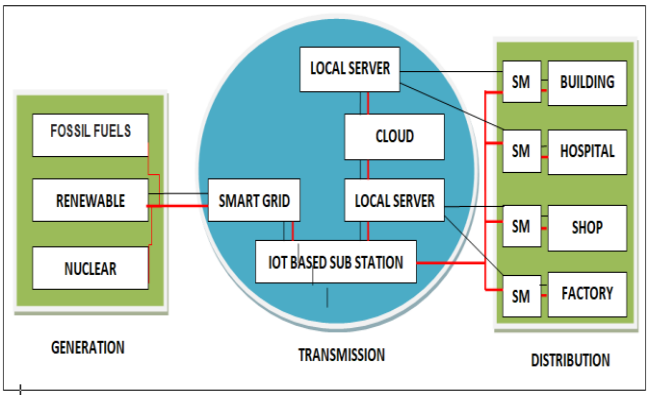


Fig: Block Diagram Of Smart Meter In Relation To Smart GRID (Here red line for power distribution and black for data distribution)

A. Smart Grid

In recent decades Smart Grid will be one of the most vibrant sector for researchers. The system will totally automated and free of human error. It is a technology by which power grid combines with sensor and IoT devises to interact between the utility and its customers. Smart Grid will consist of controls, sensors, IoT and many other digitally communicable devises. But the only problem is security issue which will be somehow overcome in this paper. There are many benefits of Smart Grids:

- Great transmission of power
- Less power faults
- Reduced peak time, thus reduce bill
- Vast range of renewable energy used
- Excellent customer and utility relationship

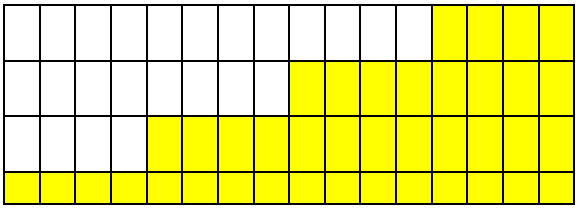
B. Smart Meter

Smart meters are next gen technology which provides less human effort with proper power consumption record of user, gives reduced billing facility and also gives important information to utility companies. They are designed so that have unique id and bidirectional communicational channel. They consists of Ardino, LCD, network connectivity, IoT device etc. It reads the power consumed automatically after fixed interval of times.

C. Algorithm

This algorithm is applied to make the data more secure during communication [6]. It is applied to this cryptography method while the data going from Smart Meter to the Utility through IoT. These algorithm will be configure in the IoT device in Smart grid specially Smart Meter. Thus by this way we can ensure high security in the system.

1. Break the message into 64 bits block each and encrypt each block.
2. Now, these 64 bits break into 4 x 16 block.
3. 4 bit shifting per row in a round format as marked in yellow:



4. Now again break into 2 block (32 bits per block). Left portion (LP) and Right portion (RP).
5. Perform Expansion permutation with RP to make it 48 bit block from 32 bit block.
6. Design key of 48 bit (described later).
7. XOR applied with 48 bit key and 48 bit RP to get new RP of 48 bit.
8. Now with the result apply genetic algorithm operations like selection, crossover and mutation. Fitness Function: From new 48 bit RP make 4 x 12 table.
9. Apply XOR to LP of step 4 and the result of step 8 i.e, current RP.
10. While RP of step 8 is taken as LP.
11. This time take LP of step10 and RP of step 9 to get in 16 x 4 table.
12. 4 bit shifting per column in a round form.
13. Thus we get our cipher text

D. Key Generation Method

In this system the **information** encrypted by using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. Below given private key generation technique. Public key is just reverse of it.

1. Randomly 64 bit are taken to organise them in 8 x 8 table form
2. Eliminate the 8th column of the table, the result is 56 bit key.
3. Organise 56 bit into table of 8 x 7 format. And eliminate mid or 4th row.
4. Thus key of 48 bit is ready to use. In 4 x 12 format.

IV.RESULT AND DISCUSSION

In this paper the algorithm that we have used is public-key cryptography or asymmetric cryptography along with the flavour of genetic algorithm where keys are generated randomly. As a result retrieving the information is difficult for third party. This algorithm has covered all the security aspects. Resultant data is having total security in all dimensions like, Confidentiality is maintained as the private key is kept with only by the person who will receive the information. Data integrity maintained as no other person can retrieve the message other than receiver. Authentication and Non-reputability are maintained by applying digital signature process. Thus this system assured strong security in all aspects.

V.CONCLUSION

In upcoming days Smart Meter will be one of the high priority research area. In this paper it is discussed that how wan secure the data in Smart Meter in Smart Grid. And a way to securely communicate and preserved the data. The algorithm shown here is really a good approach to build a high security communication with maintaining the privacy of customers and utility companies. As discussed above this algorithm apply asymmetric key cryptographic method to design a secure method of data transmission so that any kind of attacker cannot break the security. Thus we can use Smart meter with advancement.

REFERANCES

1. Alireza Ghasempour, "Inter of Things in Smart Grid: Architecture, Applications, Services, Key Technologies and challenges", by MDPI
2. Zhao, Z., Chen, G," An Overview of Cyber Security for Smart Grid". In Proceedings of the 2018 IEEE 27th International Symposium on Industrial Electronics, Cairns, Australia, 13–15 June 2018; pp. 1127–1131
3. Mrs.Geetha.R, MR. Abhishek.D, Ms.Rajalakshmi.G,Mr.sabari murugan.G, Mr.Sureeender.V,"Smart Energy Meter Using IoT", in IJRTER and CELICS' 18, Special Isuue
4. Fariha Khan, Aruna Gawade, "Secure Data Management in Smart Meter as an Application of IoT", in IJSR
5. Milanpreet Kaur, Dr. Lini Mathew, Alokdeep and AjayKumar, "Implimentation of Smart Meter basedon Internet of Things", in ICCS-2017 and IOP conf:MSE331-2018
6. SomalinaChowdhury, Sisir Kumar Das, Annapurna Das, “Application of Genetic Algorithm in Communication Network Security", in IJIRCCE. Vol. 3, Issue 1, January 2015

AUTHORS PROFILE

Somalina Chowdhury, More than 8 years of experience in the field of Computer Application. Pursuing PhD in Computer Science and Engg. (CSE)/Information Technology (IT) from Maulana Abul Kalam Azad University of Technology (MAKAUT), West Bengal since Dec 2018. Completed MCA and BCA from MAKAUT in 2008 &2011 respectively. Member of Institution of Engineers (India).ReceivedBelievers Award from National Programme on Technology Enhanced Learning (NPTEL) for completion of four courses in a single semester. One patent is filed. Presently working as Assistant Professor in Guru Nanak Institute of Technology (GNIT), Kolkata since 2011. Awarded for organizing Smart India Hackathon, 2019. Areas of working interest are IoT, Cloud Computing, Big Data, and Genetic algorithm, Network Security, Cryptography and Wireless Sensor Network.

Prof. (Dr.) Santanu Kumar Sen, Around 25 years of experience (8 years in Industry and 17 years in Engineering Academia including Abroad). PhD (Engg.), MBA, M.Tech, B.E, Chartered Engineering. Professional Engineer, FIET (in process), UK Fellow: FIETE, FIE, SMIEEE, USA Senior Member- (SMCSI), India Life Member LMISTE, India Senior Member- MACM, USA. Awarded the 1st Professional Engineer Degree under Computer Science Division from IE in 2019. Expert Member of International Professional Engineering under CS from IE in 2019 Board Member of WBJEEB since 2015Advisor, National Cyber Security Cell, New Delhi. Technical Expert and Co-Chairman of WBSSC 2016, 2017. Rashtriya Shiksha Gourav Puroskar from Centre for Education Growth and Research,New Delhi in 2016. “Academic Excellence Award” – Special Leadership Award from JIS Group in 2017. “Indira Gandhi Sadbhavna Award” from Global Achievers Foundation, New Delhi in 2014. “Bharat Bibhushan Samman Puraskar” from EHRDA, New Delhi in 2013. Research Contributor of the year 2008, from Guru Nanak Institute of Technology (GNIT) PhD Recipient Award in 2008, GNIT Faculty Summit in 2008 National Scholarship in 1990 from Nationalized Indian Bank. Research Paper Publications: 70+ Patents filed and Published: 6 Work Experience: Presently working as Principal of Guru Nanak Institute of Technology Guru (An Autonomous Degree Engineering College) since 2012.