International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 8
ISSN: 2454-4248
01 – 04

Securing the IOT Based Smart Meter Monitoring Using AES Algorithm

Mrs. Sapana Pradip Sonar
Research Scholar,
Shri JJT Univeristy
Rajastthan,India
Email:-sapnasonar@gmail.com

Dr. Anupama Deshpande
Department of Electrical Engineering
Shri JJT Univeristy
Rajastthan,India
Emailid:pankaj.vispute@rediffmail.com

Abstract-Smart meter is the upgradation of the existing meter in terms of cost, communication infrastructure, internet of things and reliable technologies. In the ambitious flagship programme of digital India-project an initiative of India, the potential fields of the missions are identified in the area are smart energy, smart meters, smart homes, and smart cities. More than 100 smart cities are planned for information and communication technology-driven solutions with big data analytics in India. The exponential growth in smart meter has given certain security risks, cyber threats and protection of stored data as Nation security. Smart meters, comprising of several communication, monitoring intelligent, metering and electrical equipment used in power meter, have a greater exposure to meter security and cyber-attacks which potentially disrupt distribution in a city. The paper proposed the energy meter with Advanced Encryption Standard (AES) algorithm enable with NodeMCU hardware. The data generated by the energy meter is stored in the cloud using AES algorithm to secure this data from intruders. This system ensures the AES can be employed in smart meter security and communication infrastructure.

Keywords- *Security, NodeMCU, AES algorithm, Cloud, energy meter*

*****

I. INTRODUCTION

A general definition, a wireless sensor network is composed of a set of nodes which communicate through a wireless medium in order to perform certain tasks. A couple of examples where WSNs can be deployed, as stated in [1], are fire extension detection, earthquake detection, environment surveillance for pollution tracking, intelligent building management, access restriction, detection of free spaces in parking lots and so on. Advantages brought by WSNs are enhanced flexibility and mobility, mainly because nodes are generally powered from an onboard battery and thus do not depend on their surroundings. This, however, is also their biggest weakness. The life expectancy of a node depends on its usage. The constraints mainly come from the limited energy source, as data processing and transmission can be energy intensive. A smart energy meter is an enhancement of a common electrical network, which delivers electrical energy from suppliers to consumers. It is expected to bring plenty of advantages and is widely promoted by many governments nowadays. It is supposed to provide customers with the advantages of the smart energy demand, a concept that is described as a base utility billing based upon accurate, time-of-use price signals. To illustrate this, users of smart energy meter s can decide to perform certain activities, for example washing clothes during the hours when the demand of electricity is lower, which reduces the prize and allows customers to carefully plan their energy consumption. Other benefits of the smart energy meter include improved reliability, efficiency, economy and protection of national security as the enhancement is easier to control and monitor. The smart energy meter is based upon an idea of using bi-directional digital communication in order to control appliances at consumers' households. Even though this concept is not totally new, the communication between the two sides was never carried out to such an extent as in the case of the smart energy meter. Embedded devices are expected to transform the landscape of networked services in many domains, among them smart homes and smart grid systems.

The reliable and optimized operation of smart grids is dependent on reliable data provided by end nodes (e.g. smart meters), and assurance of secure communication across networks. Understanding whether advanced security building blocks have a role to play in forthcoming infrastructures needs a basic understanding of each potential building block with respect to resource usage and impact on timing. Luan et al. (2015) state that "The data [from end nodes] offer utilities many opportunities to apply data analytics to potentially enhance their operational efficiency. For instance, smart meter data can be used for enhancing and estimating voltage and Volt-Ampere Reactive (VAR) optimization benefits, evaluating distribution line losses, identifying and quantifying energy thefts, and enabling improved load forecast, outage management, and distribution system analysis". These applications justify the need for the integrity of received data and reliable communication. Types of attacks on smart meters can be generally classified as physical (external tampering, neutral bypass, missing neutral etc.), electrical (over/under voltage, circuit probing, ESD etc.), and software and data (spy software insertion, cyber attacks). Except for physical tampering of the meter, the majority of these known vulnerabilities are associated with communication media and

 ISSN: 2454-4248
01 – 04

communication protocols as the grid becomes networked. Solutions for physical tampering include using magnetometer sensors (to detect powerful magnetic fields which affect meter readings in current transformer-based electricity meters), tilt sensors which detect removal or physical tampering of meters from authorized locations, usage of tampering algorithms as part of firmware that helps ensure billing is continued, and anti-tamper switches that can be placed on the casing of the meter to trigger a tamper when the casing is opened. The AMI includes software, hardware, communications, customer-associated systems, and meter data management (MDM) software. As meters become smart and networked, meter software must have adequate security against any unauthorized change in software configurations, reading of recorded data, change of calibration data, etc. Secure techniques need to be integrated with the solution to secure the communication channels and ensure the physical security of assets to make smart grids more secure and reliable.

II. RELTAED WORK

An Intelligent Electronic Device (IED) is a technical term for a digital controlling device used in the electric power industry. An IED contains sensors delivering necessary data to issue control commands. A smart meter is an electronic device that uses two-way communication. It records consumption in intervals of an hour or less [1] and sends it regularly to the utility for monitoring and billing purposes. In other words, it is an enhanced home energy monitor able to gather data for remote reporting in short intervals. The most significant advantage is the ability of real-time monitoring including features such as power outage notification and power quality monitoring. The major technological problem regarding smart meters is communication. The fact that the device has to provide the measurements to the station controller in a secure and reliable way raises many problems. Another issue is the varying environments in which the meters operate. There are many solutions for communication including power line communication, Wi-Fi, WiMAX, satellite and cell networks technologies. However, we will consider only power line communication in this work due to its various benefits based on utilization of resources which are already in places such as the distribution network and maintenance tools. The problem of measuring the cost of encryption on wireless sensor node hardware has been addressed previously. In [5] Lee et al. analyze a range of symmetric-key algorithms and message authentication algorithms in the context of WSNs. They use the MicaZ and TelosB sensor nodes and measure the execution time and energy consumption of different algorithms. For AES they provide measurements for a hardware-assisted implementation and conclude that it is the cheapest when either time or energy is considered. They do not, however, study this implementation on different plaintext lengths and instead rely on data sheets to extend to lengths longer than one block. However, this conclusion is not backed by Zhang et al. in [6] which compares different AES implementations on the MicaZ nodes. They conclude that hardware-assisted encryption is faster, but also consumes more energy due to the external chip which handles the computation in hardware. Compared to their work, we study only AES-128 which is a well-known cipher also adopted by the National Institute of Standards and Technology (NIST) and which has been proposed as a viable alternative ([7]) to other less studied ciphers in WSN applications. This choice is also supported by the fact that multiple 802.15.4 transceivers offer a hardware accelerator for AES operations. We study the newer Sparrow v3.2 sensor nodes based on the ATmega128RFA1, which integrates the microcontroller with the radio transceiver and hardware encryption module, and show that AES-128 can be efficiently implemented reducing both execution time and energy consumption. We also provide hybrid implementations for modes of operation that are not natively supported by the hardware and show that they can still be efficiently implemented with the available primitives. In [7] Law et al. conduct a thorough survey of the costs of different block ciphers, when implemented on sensor node hardware. They conclude that Rijndael (AES) is the second most efficient cipher, being surpassed only by Skipjack. However, their analysis is based on older hardware and does not consider any hardware accelerated implementations. In [8] de Meulenaer et al. study the problem of key exchange and measure the cost of two key agreement protocols: Kerberos and Elliptic Curve Diffie-Hellman. They measure the energy consumption of the two protocols on MicaZ and TelosB sensor nodes and conclude that the listening mode is the principal factor in the energy efficiency of key exchange protocols, with Kerberos being the more efficient protocol. Compared to their work, we concentrate on encryption algorithms, and more specifically on AES, with key distribution left for future work.

III. ALGORITHM USED

AES is a block cipher encryption algorithm that uses symmetrical keys for encrypting a block of plaintext and decrypting a block of ciphertext [9]. The algorithm uses a series of rounds consisting of one or more of the following operations: byte-level substitution, permutation, arithmetical operations on a finite field and XOR-ing with a given or calculated key. As a general rule, the operations are handled bytewise. AES receives as input a plaintext of 16 bytes and the encryption key, which has a variable dimension of 16, 24 or 32 bytes. The input text is processed into the output text (ciphertext) by using the given key and applying a number of transformations. Encryption and decryption are similar, except for the fact that decryption needs an extra step it first runs a full encryption in order to obtain the modified key needed for decrypting data. In symmetrical encryption algorithms HAS two basic categories: block ciphers and stream ciphers. A

 ISSN: 2454-4248
01 – 04

block cipher encrypts a block of plaintext producing a block of encrypted data, whilst a stream cipher can encrypt plaintexts of varying sizes. This makes block ciphers prone to security issues if used to encrypt plaintexts longer than the block size, in a na¨ıve way, mainly because patterns in the plaintext can appear in the ciphertext. A more secure way to encrypt data with a block cipher can be achieved by combining the encryption algorithm with a few basic operations, in a mode of operation. It is worth mentioning that the operations are not directly securing data. This is the responsibility of the block cipher. Still, they should not compromise the security provided by the cipher.

AES is an iterative rather than Feistel cipher. It is based on 'substitution-permutation network'. It comprises a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

1.Byte Substitution (SubBytes): The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2.Shiftrows: Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of the row. The shift is carried out as follows −

- The first row is not shifted.
- The second row is shifted one (byte) position to the left.
- The third row is shifted two positions to the left.
- The fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3.MixColumns:

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4.Addroundkey:

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

5.Decryption Process:

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in a reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

IV. SYSTEM ARCHITECURE

The proposed system is divided into three parts,

1. Customer Premises: The Energy Meter (EM) block shown in Figure.1 consists of an energy meter, LED and NodeMCU (ESP8266). This part of the system resides on the consumer side. LED is attached to detect the status of the energy meter. The NodeMCU present on the customer side is configured with internet connectivity.

2. Server and control: This part of Figure 1 acts as the brain of the system. It has three different servers for storage, control and communication purposes. These servers ensure the proper functioning of the system. cloud service is used to store the data from different meters. The received data is stored in the specified variable in a table format. The Main server processes the received data. It controls all the other functioning of the system. Hosting site server acts as a communication bridge between the customers and the main server by providing messaging services.

3. User Interface: User can view the readings on the website. The user can fire queries to which the hosting server will respond.

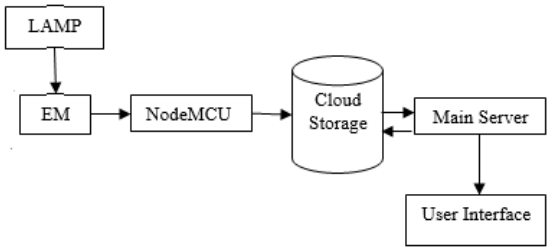

Fig1. Architecture of the Proposed System

As shown in fig 1, the electric meter is monitoring the usage of the Lamp and the readings will be stored in the cloud database as explained in the working of the system. The main server is monitoring all the processes in the system.

V. CONCLUSION

Smart Energy Meter which is a part of Smart Grid is being deployed in many countries towards automatically

capturing the energy values from Smart Meter of homes and industries by the Utility provider. These smart meter as it possesses wireless communication capabilities are vulnerable to a lot of security attacks which needs to be addressed. Some amount of research been carried out towards securing energy meter using Power line communication and so. The wireless networks use AES 128 bit security protocol. The smart Meter which possesses wireless communication needs to be validated for proper and good security protocol against energy theft attack. So the security protocols i.e AES has been validated and in real time using NodeMCU for varying meter data in terms of Key Generation and Execution time.

In addition to securing the meter data, there is also a need to securely transmit the meter data via the Gateway to the utility provider against DoS attack which is been addressed in this research So to prevent this type which is strong against DoS attack been modified with AES against DoS attack in terms of packet delivery ratio, throughput. AES is strong against DoS attack compared to other security algorithms in terms of packet dropped, packet delivery ratio and throughput which proves the Smart meter network reliable and secure.

VI. REFERENCES

[1]. Landi, C.; Dipt. di Ing. dell"Inf., Seconda Univ. di Napoli, Aversa, Italy ; Merola, P. ; Ianniello, G, "ARM-based energy management system using smart meter and Web server", IEEE Instrumentation and Measurement Technology ConferenceBinjiang, pp. 1 – 5, May 2011

[2]. K. Li, J. Liu, C. Yue and M. Zhang, "Remote power management and meter-reading system based on ARM microprocessor", IEEE Precision Electromagnetic Measurements Digest CPEM, pp. 216-217, June, 2008

[3]. Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, February 2014

[4]. ESP8266 802.11bgn Smart Device/Expressifsystems/October 2013

[5]. G. L. Prashanti and K .V.Prasad, Wireless power meter monitoring with power theft detection and intimation system using GSM and Zigbee networks, Proc of IOSR-JECE, Vol 9, Issue 6, Ves.I (Nov-Dec, 2014), PP 04-08

[6]. YujunBao and Xiaoyan Jiang, "Design of electric Energy Meter for long-distance data information transfers which based upon GPRS", ISA2009. International Workshop on Intelligent Systems and Applications, 2009

[7]. Vivek Kumar Sehgal,Nitesh Panda, NipunRaiHanda, "Electronic Energy Meter with instant billing",UKSim Fourth European

[8]. MstShahnajParvin and SM LutfulKabir. A framework of a smart system for prepaid electric metering scheme. In Informatics, Electronics Vision (ICIEV),2015 International Conference on, pages 15. IEEE, 2015.

[9]. Nayan Gupta and Deepali Shukla. Design of embedded based automated meter reading system for real time processing. In Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students Conference on, pages 16. IEEE, 2016.

[10]. Hao Zhang, Qijun Chen College of Electronics and Information, Tongji University, Shanghai, P.R.ChinaChunchiGu, "Design and Implementation of Energy Data Collection System UsingWireless Fidelity (Wi-Fi) Module and Current Transformer," in ,2014 IEEE Internrnational Conference on System Science and Engineering(JCSSE), Shanghai,China, July 11-13 2014.

[11]. MdMasudurRahman, MohdOhidul Islam, MdSerazusSalakin, et al. Arduinoandgsm based smart energy meter for advanced metering and billing system. InElec-trical Engineering and Information Communication Technology (ICEEICT), 2015International Conference on, pages 16. IEEE, 2015.

[12]. Ravi Ramakrishnan and Loveleen Gaur. Smart electricity distribution in residential areas: Internet of things (iot) based advanced metering infrastructure and cloud analytics. In Internet of Things and Applications (IOTA), International Conference on, pages 4651. IEEE, 2016.

[13]. RohitBhilare and Shital Mali. IoT based smart home with real time e-metering using e-controller. In2015 Annual IEEE India Conference (INDICON), pages 16. IEEE,2015.