International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 3 1232 - 1236

Privacy and Security for Smart Metering System with Fault Controlling Technique

T. Gobinath
PG Student
Nandha Engineering College
Erode-52
E-mail:tgobinath92@gmail.com

Mrs. S. Brindha
Assistant Professor
Nandha Engineering College
Erode-52
E-mail:brindha.bliss@gmail.com

Abstract:- Smart Metering (SM) is an important and essential element of the upcoming energy network. The importance of smart metering is that it interconnects smart grid elements and functions among a two way communication network. The target is to support an economically efficient sustainable power system with high quality and security. To achieve this objective, advanced smart metering functions might include automated meter readings, distributed energy storage, distributed energy resource management, as well as further energy efficiency mechanisms such as real time optimizations for load shifting and scheduling. In existing system the information transmission security, privacy, meter reading observation between network and client then data transmission monitoring system which can be controlled through Wireless Area Network (WAN). However the information transmission observation system has not economical for fault dominant technique. In proposed system, whole system will be monitored, controlled, data have been secured and also effective load scheduling can be provided for this system too. EB line faults such as short circuit, over voltage and under voltage are monitored and controlled through WAN. It improves the protection and privacy of information transmission between network and client.

Keywords *– Privacy, Security, Risk Assessment, Smart Grid, Smart Metering.*

*****

I. INTRODUCTION

Smart metering may be defined as the communication system and associated information management system that permits process, collection, and distribution of information between customers, smart meter and utility companies. Risk analysis and impact assessment is a step toward securing in any system. The application of such a method is nontrivial in an SM network, considering its architectural complexity and interfacing with cyber physical SG functionalities, and therefore the scale of the potential damages caused by attacks. For example, protection against unauthorized access and repudiation could be a important demand for the AMR data to be trusted by both the utility suppliers and also the customers. This needs end to end communication security, tamper proof hardware, trusted software, and complicated access management.

In this project, we have a tendency to introduce a unified security and privacy protection (USaPP) framework that helps analyze basic issues of SM security and privacy, and search the solution space of security controls in a very organized and holistic manner. Instead, this paper provides a summary of user connected issues and solutions because the basis for suggesting a unified approaches. To this end, the main objective of this paper is to support the premise that the USaPP approach is important for vital for cyber-physical security and privacy management of SM systems, and, more generally, SG systems and similar complicated critical infrastructures. As an example application, we have a tendency to study the security and privacy of an electron volt dynamic charging use case and apply the USaPP methodology.

II. RELATED WORK

In this paper deals with however home energy resources is wont to shield the privacy of the collected information. Specifically we have a tendency to, a) introduce a power mixing algorithm to by selection shield a group of consumption events. b) develop a variety of various privacy protection metrics. c) analyze real smart metering information sampled twice a minute over a period of thirteen days and d) appraise the protection offered by completely different power mixture algorithms. Major factors that confirm the potency of the projected power mixture algorithms are known like battery capacity and power, and user preferences for privacy based mostly allocations of battery energy quotas[1]. During this paper, Onion routing is an infrastructure for personal communication over a public network. It provides anonymous connections that are powerfully immune to traffic analysis. Onion routing's anonymous connections square measure, close to real time, and may be used any place a socket association is used[2].

This paper deals with , Increasing complexness of power grids, growing demand for bigger reliableness, security and potency further as a jump in harnessing communication and information technologies[3].This paper deals with, Global electrical grids are verging on the most important technological transformation since the introduction of electricity into the house. The old infrastructure that delivers power to our homes and businesses is being replaced with a group of digital systems referred to as the smart grid. This grid is that the modernization of the existing electrical system that enhances customers and utilities ability to observe, control, and predict energy use[4].

There is nearly universal agreement that it is necessary to upgrade the electric grid to extend overall system potency and reliability. To upgrade the grid, and to operate an improved grid, would force important dependence on distributed intelligence and broadband communication capabilities. The access and communications capabilities need the most recent in established security technology for extremely giant, wide-area communications networks. This paper discusses key security technologies for a smart grid system, together with public key infrastructures and trusted computing[5].Plug-in Hybrid Electrical Vehicles (PHEVs) may be connected to the power grid. The power flow of this connection can be bidirectional, thus vehicles will charge and discharge. This vehicle-to-grid possibility will aid to improve grid efficiency and reliability. This paper shows that there might be a good combination with PHEVs as they will offer storage to take care of the excess of produced energy and use it for driving or release it into the grid at a later time. In that way, consumption and generation are additional expeditiously matched[6].

III. FUNDAMENTAL SECURITY AND PRIVACY PROBLEMS

The SM system is also attacked from many alternative entry points. As an example, information integrity and authentication is also compromised through network attacks like man in the middle spoofing, impersonation, or denial of service (DoS) attacks. Similarly, information security is also compromised by sabotage/insider attacks like viruses and trojan horses. Hence, rigorous HW/SW security is needed to make sure the validity of various communicating parties such as head ends and smart meters. As an example, consider an attacker takes over the head-end and sends all meters a DDR management message to interrupt supply. The interruption will be created permanent by also commanding all meters to alter their crypto keys to some new value only known to the attacker[14]. The impact will be monumental scores of homes might be left while not power till they are regionally replaced or reflashed with authentic keys, people's support might be affected, health and safety might be jeopardized, and businesses may lose millions. SM security needs to perform the following:

1)prevent such attacks from happening

2)provide a recovery/survivability mechanism just in case of attack.

The notion of privacy is complicated and is perceived and outlined in several approach in different countries. Privacy is related to the notion of Personally Identifiable Information (PII) that will be contained in or linked with certain data. During this direction, we would like to use the notion privacy in the context of the subsequent two notions.

1)Anonymity could be a property of however sufficiently the identity of a user related to a message is hidden.

2)Undetectability is a property of however a selected item of interest related to a message is sufficiently distinguished by whether it exists or not.

The SM privacy problem stems from the potential of a smart meter to measure energy consumption in way more detail than a conventional meter. Smart meters are expected to provide accurate readings automatically at requested time intervals (e.g., each few minutes) to the utility company, electricity distribution network, or wider SG to facilitate optimizations like DSM and DR. Such elaborated energy usage are wont to deduce detailed information about appliance usage and way patterns and additionally teaches that obscure assurances of privacy are undesirable as they often result in restrictive capture and irrecoverable data misuse damages.

SYSTEM DESIGN

To improve the privacy and security, dividing this project into small modules, they are given as below.

- Data collection and controlling module
- Monitoring and GUI module.

The monitor is to access the home appliance parameters such as temperature, gas level condition, and power consumption through wireless area network (or monitored on the specific web page). It can be provided for monitoring and access the home appliance parameter world widely through internet. This system makes simple and flexible assessment to manage the home appliance parameter.

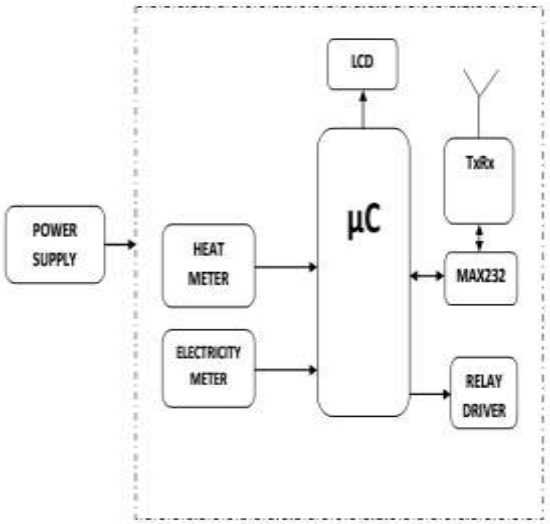

FIGURE1. Data collection and controlling module

In the data collection module, room temperature, LPG gas condition and power consumption are measured by the corresponding sensors. Here microcontroller is employed for information conversion (ADC) and data transmission. The Simple Object Access Protocol (SOAP) is used to select the sequence of the home appliance parameter and additionally send the information from physical layer to Network layer. MAX232 is a dual driver (or) receiver. It is used to convert the Recommended Standard 232 (RS232)

serial port signal to suitable signal in Transistor Transistor Logic (TTL) compatible digital logic circuits.

The data collection module will transmit the information so the information is received by controlling module using RF transceiver through WSN. Relays are provided with in the management unit which may be access through WAN. This type of relay is employed to protect the home appliances parameter from over and under voltage problem, short circuit problem and over consumption of electrical energy. If the problem occurs means the relay is off simultaneously. In monitoring and controlling module is used to receive the information by using RF receiver. This module works under the principle of Interface Meta Data Access Points (IFMAP).

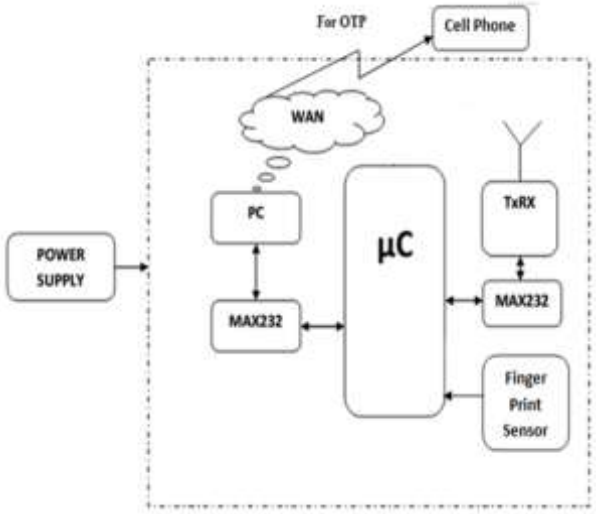

FIGURE2. Monitoring and GUI module

This protocol is employed to receive the data through the wireless area network with proper encoding and decoding technique for secures the transmission of data. This protocol used to send the data from network layer to Application layer. Finger print sensor unit and OTP (One Time Password) system are provided for privacy and security purpose. Finger print sensor used to detect the family member's access. OTP is provided for guest access like as familiar to family member. This sensor is used instead for user name and password system.

Finally the data is sent to pc through RS232 (or) USB port. The data are used to monitor and control the Graphical User Interface (GUI) is also called as Devices Profile for Web Services (DPWS). The data bus is used to interface data collection module, monitoring and controlling module and GUI module.

IV. SOFTWARE DESCRIPTION

To simulate this style in hardware varied software package tools in established required for this method. Network machine could be a distinct event network machine. It's fashionable in tutorial for its extensibility and plentiful on-line documentation. Network simulator is popularly utilized in ad-hoc network analysis. Network simulator support associative array of fashionable network protocols, providing simulation results for wired and wireless networks alike. It is additionally used as restricted functionality network imitator. Network simulator square measure licensed to be used beneath version a pair of the General Public License. This is often provided for observation and access the commercial knowledge worldwide through web. This method makes straight forward and versatile assessment of household appliance knowledge. Simulation working module as describe below.

Sensor Initialization

When you put in the device on network, you want to use the setup command to initialize it in order that will communicate with it over the network. With the setup command, tack basic device settings, together with the hostname, information processing interfaces, access management lists, and time settings.

Virtual Host Creation

On the web, virtual hosting is that the provision of net server hosting services in order that a corporation does not ought to purchase and maintain its own net server and connections to the web.

Verification of Network

During this section, knowledge is transmitted or received from or to network code is verified for network security.

IAA Initiation

IAA initiation is that the continuous observation of a proprietary network for uncommon events or extra ordinary trends.

Network Attack Initiation

A network attack is outlined as any methodology, process, or suggests that won't to maliciously arrange to compromise network security. There square measure variety of reasons that a personal would need to attack company networks. The people activity network attacks square measure unremarkably remarked as network attackers, hackers, or cookie.

V. FRAMEWORK ELEMENTS

In this technique, we have a tendency to propose a USaPP framework with a stress on home solutions. However, we have a tendency to conjointly think about that the projected framework is adopted to be used at intervals the scope of the broader SM/SG security system, like the heat unit charging. We have a tendency to organize smart metering USaPP within the following three categories.

1) Communication security. This category involves two distinct communication system: a) in home HAN, HEMS,HBES and b)WAN/NAN, as well as WMN/WSN.

2) Secure computing. This category involves the HW and compass point security systems integrated in several smart metering elements that operate smart metering system function like energy and cyber system management as well as communications.

3) System management. This category involves the

smart metering functions and therefore the variable (rules,decision making algorithms,policies,user input) that drive computing or communication USaPP operations. This category is liable for deciding what security services area unit required totally different for various functions and where different information area unit protected and communicated. That is, this category is liable for configuring home smart metering operations and resolution conflicting needs(privacy versus SG overrides versus energy savings versus user overrides). Each one of the same three categories integrates each security and privacy protection measures and contains three subclasses.

VI. EXPERIMENTAL RESULTS

The Overall system's results are discussed in this section. Hardware result's done ASP.NET ETHERNET API IMPLEMENTATION. ASP.Net may be a net development platform that provides a programming model, a comprehensive software system infrastructure and various services needed to create up strong net application for PC, additionally as mobile devices. Ethernet may be a family of computer networking technologies for local area (LAN) and bigger networks. The Ethernet standards comprise many wiring and signaling variants of the OSI physical layer in use with local area network.

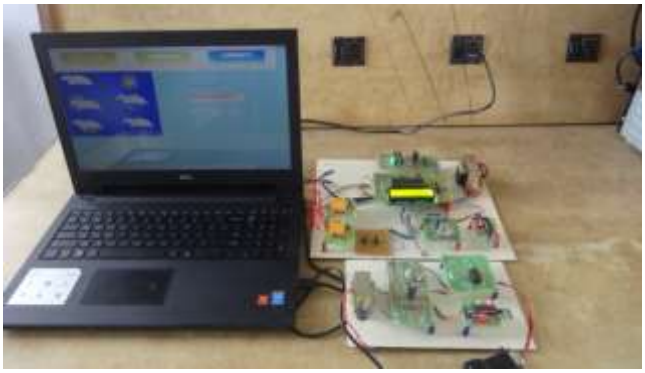

FIGURE3. Hardware snap shot module

In this project to measure the home appliance parameter are often entered in ASP.NET Ethernet through WAN and so monitoring and controlling action are often viewed in PC.

Simulation is completed by Network Simulator. During this section used SOAP and IFMAP protocol (Monitoring, Processing collected data and taking necessary action based on the limits given for individual sensors).The below figure shows the simulation result of information transfer. It describes the information list are sent to DHP.

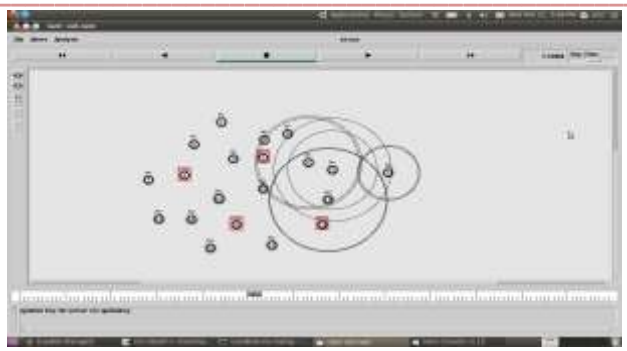

FIGURE4. Simulation result of data transfer

CONCLUSION

In this project, the case for a unified approach makes an attempt to handle home SM security and privacy necessities by fusing different solutions and mapping them to a variety of tightly interrelated system elements are made. The interrelated system component classify into three ways like as communications, computing, and system management. The projected system framework helps address SM network security and privacy problem, occurring in several cyber-physical elements of the system, for various use cases, in a systematic and holistic manner. Future work could also be motivated by several of the technical issues and solutions embedded in several areas of the framework.

REFERENCES

[1]. G. Kalogridis, R. Cepeda, S. Z. Denic, T. Lewis, and C. Efthymiou, "Elecprivacy: Evaluating the privacy protection of electricity manage-ment algorithms," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 750–758, Dec. 2011.

[2]. M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous con-nections and onion routing," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 482–494, May 1998.

[3]. K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 57–64, Jun. 2010.

[4]. P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Sec. Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[5]. A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[6]. K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of vehicle-to-grid on the distribution grid," *Elect. Power Syst. Res.*, vol. 81, no. 1, pp. 185–192, Jan. 2011.

[7]. J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surv. Tuts.*, vol. 14, no. 4, pp. 981–997, 2012.

[8]. NIST. (2010, August). Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, Gaithersburg, MD, USA, NISTIR 7628.

[9]. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th ACM DAC*, 2010, pp. 731–736.

[10]. A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proc. 10th Annu. ACM WPES*, 2011, pp. 49–60.

[11]. T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Waltham, MA, USA: Syngress, 2010.

[12]. NIST. (2010, Aug.). Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, Gaithersburg, MD, USA, NISTIR 7628. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[13]. C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. SmartGridComm*, Gaithersburg, MD, USA, October 2010, pp. 238–243.

[14]. R. Anderson and S. Fuloria, "Who controls the off switch?" in *Proc. 1st IEEE Int. Conf. SmartGridComm*, Gaithersburg, MD, USA, Oct. 2010,pp. 96–101.