IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

GSM BASED SMART ENERGY METER BILLING WITH LOAD MANAGEMENT

ANNA PEACHI.V[1], KAVIPRAKASH.S.T[2] ,NIYAS AHAMED.S[3], PRAVEEN.M[4]

1Assistant Professor 2,3,4 UG Students,

Electrical and Electronics Engineering,

M.Kumarasamy College of Engineering, Karur, Tamilnadu

ABSTRACT

Automated and smart meters are devices that are able to monitor the energy consumption of electricity consumers in real-time. They are considered key technological enablers of the smart grid, as the real-time consumption data that they can collect and enable new sophisticated billing schemes. It could facilitate more efficient power distribution system operation and could give rise to a variety of value-added services. At the same time, the energy consumption data that the meters collect are sensitive consumer information. Thus privacy is a key concern and is a major inhibitor of real-time data collection in practice. In this article, we review the different uses of metering data in the smart grid and the related privacy legislation. This system will alert the user through the user regarding the payment. If the user doesn't pay the bill, the system will automatically trip the system.

Keywords : Meter Billing & Sensor

1.1 INTRODUCTION

The internet of thing allows object to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer based systems, and resulting in improved efficiency, accuracy and economic benefit. The increasing generation needs empowered gadgets by wireless technology which includes Bluetooth, Radio Frequency Identification, Embedded sensors and many more. In that IOT technology has grown from its beginning and now presently widely using it. The electricity plays an important role in our life. Now-a-days as the consumers are increasing rapidly it became very hard to handle the electricity requirements. Without electricity it's impossible to survive and also it is important to save the electricity loss. As the generation is increases the consumer's requirements also increasing so in accordance with it the technology improvement is needed. So we developed the system with faster and improved technology i.e. IOT. The electricity also contains some issues like power theft. Power theft is a measure crime and it also directly affects the economy of our country. Transmission, generation and distribution of electricity include the loss of electricity. To avoid the losses we need to monitor the power consumption and losses, so that we can efficiently utilize the generated power. Meter tempering is part of power theft and also illegal crime which we can minimize. Billing is a process in general the human operator goes to every consumer's home then providing bill it will take lot of time. To resolve these issues we developed system on the base of IOT energy meter reading. IOT based energy meter reading consists of three parts: Controller, Theft detection and WIFI part. Controller part plays a major role in the system. Where all the information can send through this controller to the other part of the system and it also stores the information in it. WIFI part performs IOT operation in accordance with the Arduino controller. The energy meter connected with theft detection part if any temper happens it will send the information to the company as well as it will take automatic action by making power off.

2 LITERATURE SURVEY

2.1. A Holistic View of Security and Privacy Issues in Smart Grids
Muhammad RizwanAsghar and Daniele Miorandi

The energy system is undergoing a radical transformation. The coupling of the energy system with advanced information and communication technologies is making it possible to monitor and control in real-time generation, transport, distribution and consumption of energy. In this context, a key enabler is represented by smart meters, devices able to monitor in near real-time the consumption of energy by consumers. If, on one hand, smart meters automate the process of information flow from endpoints to energy suppliers, on the other hand, they may leak sensitive information about consumers. In this paper, we review the issues at stake and the research challenges that characterize smart grids from a privacy and security standpoint.

2.2 Estimating the lost real-time measurements under communication failure for distribution system state estimation
G N Anandin, Ishan Gupta

This paper introduces a new technique to estimate the lost measurements due to communication failure by taking advantage of the correlation between real-time measurements. The proposed technique was tested on a 95 bus UKGDS test system which highlights the impact of real-time measurements and communication failure on the performance of the distribution system state estimator. The results showcase the validity of the proposed method in increasing the accuracy of the state estimator under the loss of real-time measurements. The measurements from these meters reach the control center through various communication links like telephonic lines, optical fibers, satellites, microwaves, etc. Despite using advanced communication technologies, the data may be lost or delayed due to unintentional or intentional communication failures Unintentional communication failures may be due to human errors, natural calamities like floods, storms and others, causing failure of the equipment, aging of the equipment, manufacturing errors, etc. On the other hand, intentional communication failures are mainly due to intruders manipulating the grid through cyber-attacks.

2.3.Differentially Private State Estimation in Distribution Networks with Smart Meters
Henrik Sandberg, Gyorgy D ¨ an, and RagnarThobaben

State estimation is routinely being performed in high-voltage power transmission grids in order to assist in operation and to detect faulty equipment. In low- and medium voltage power distribution grids, on the other hand, few real time measurements are traditionally available, and operation is often conducted based on predicted and historical data. Today, in many parts of the world, smart meters have been deployed at many customers, and their measurements could in principle be shared with the operators in real time to enable improved state estimation. However, customers may feel reluctance in doing so due to privacy concerns. We therefore propose state estimation schemes for a distribution grid model, which ensure differential privacy to the customers. In particular, the state estimation schemes optimize different performance criteria, and a trade-off between a lower bound on the estimation performance versus the customers' differential privacy is derived. The proposed framework is general enough to be applicable also to other distribution networks, such as water networks.

2.4. The Economics of Privacy
Alessandro Acquisti∗ Curtis Taylor† LiadWagman

This article summarizes and draws connections among diverse streams of empirical and theoretical research on the economics of privacy. Our focus is on the economic value and consequences of privacy and of personal information, and on consumers' understanding of and decisions about the costs and benefits associated with data protection and data sharing. We highlight how the economic analysis of privacy evolved through the decades, as, together with progress in information technology, more nuanced issues associated with the protection and sharing of personal information arose. We use three themes to connect insights from the literature. First, there are theoretical and empirical situations where the protection of privacy can both enhance and detract from economic surplus and allocative efficiency. Second, consumers' ability to make informed decisions about their privacy is severely hindered, because most of the time they are in a position of imperfect

information regarding when their data is collected, with what purposes, and with what consequences. Third, specific heuristics can profoundly influence privacy decision-making. We conclude by highlighting some of the ongoing issues in the privacy debate.

2.5. Wiretap Codes for Secure Multi-Party Computation
RagnarThobaben, Gy ¨orgy D´an, and Henrik Sandberg

In this paper, we propose a new secret sharing scheme for secure multi-party computation. We present a general framework that allows us to construct efficient secret sharing schemes from channel coding techniques for the wiretap channel. The resulting schemes can be employed to securely calculate linear functions of data that are distributed in a network without leaking any information on the data except the desired result. For the examples considered in this paper, our schemes minimize the communication overhead while keeping the data perfectly secure. Compared to conventional schemes, for which the communication overhead grows quadratic ally in the number of clients in the considered scenarios, the communication overhead for our approach grows only linearly with the number of clients. This property is maintained even if our secret sharing scheme is set up to introduce redundancy in order to compensate for losses of secret shares. While we only consider the case of passive eavesdroppers and implementations based on nested Reed- Solomon codes in this paper, the proposed framework can also be applied in other cases (e.g., when clients tamper with the data) by taking into account the effects of attacks in the design of the underlying wiretap code.

3. WORKING OF PROPOSED SYSTEM

The energy meter will measure the energy used by the user and sends the usage of energy to the controller.The controller will monitor the usage of energy 24/7 and update the measured usage value in the IOT and also GSM.The user or the official can view the usage in the specific IOT website. This system will alert the user through the user regarding the payment. If the user doesn't pay the bill, the system will automatically trip the system.A LCD display is used to display the measured value.

3.1 ARDUINO

Arduino is an open-source prototyping platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board.To do so you use the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing.

3.2 CURRENT SENSOR

A current sensor is a device that detects electric current (AC or DC) in a wire, and generates a signal proportional to it. The generated signal could be analog voltage or current or even digital output. It can be then utilized to display the measured current in an ammeter or can be stored for further analysis in a data acquisition system or can be utilized for control purpose.

3.3 RELAY

A relay is an electrical switch that opens and closes under the control of another electrical circuit. In the original form, the switch is operated by an electromagnet to open or close one or many sets of contacts

3.4 GSM NETWORK

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation

GSM SERVICES:

- Tele-services
- Bearer or Data Services
- Supplementary services

4. CONCLUSION

We are concluded that automated and smart meters are devices that are able to monitor the energy consumption of electricity consumers in real- time. Focusing on the three uses of smart meter data, and its privacy aspects, we have reviewed cryptographic solutions for ensuring privacy-preserving management of smart meter data under the trusted operator model, and privacy- preserving solutions for data processing under the non-trusted operator model.

5. REFERENCE

[1] M. R. Asghar and D. Miorandi, "A holistic view of security and privacy issues in smart grids," in Smart Grid Security. Springer, 2013, pp. 58–71.
[2] Executive Office of the President of the US, "A policy framework for the 21st century grid: Enabling our secure energy future," http://www.whitehouse.gov/sites/default/files/microsites/ ostp/nstc-smart-grid- june2011.pdf, National Science and Technology Council, June 2011, last accessed: June 11, 2016.
[3] X. Han, S. You, F. Thordarson, D. V. Tackie, S. M. stberg, O. M. Pedersen, H. W. Bindner, and N. C. Nordentoft, "Real-time measurements and their effects o..336n state estimation of distribution power system," in Proc. of IEEE PES Innovative Smart Grid Technologies (ISGT) Europe, Oct. 2013, pp. 1–5.
[4] G. Wood and M. Newborough, "Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design," Energy and Buildings, vol. 35, no. 8, pp. 821–841, 2003.
[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security and Privacy Mag., vol. 7, no. 3, pp. 75–77, 2009.
[6] E. Quinn, "Privacy and the new energy infrastructure," Available at SSRN http:// ssrn.com/ abstract=1370731, 2009.
[7] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in Proc. of ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building (BuildSys), 2010, pp. 61–66.
[8] G. Kalogridis, R. Cepeda, S. Denic, T. Lewis, and C. Efthymiou, "Elecprivacy: Evaluating the privacy protection of electricity management algorithms," IEEE Trans. on Smart Grid, vol. 2, no. 4, pp. 750– 758, Dec 2011.
[9] C. Cuijpers and B.-J.Koops, "Smart metering and privacy in Europe: Lessons from the Dutch case," in European Data Protection: Coming of Age, S. Gutwirth, R. Leenes, P. de Hert, and Y. Poullet, Eds. Springer, 2013, pp. 269–293.
[10] A. Lee and T. Brewer, "Smart grid cyber security: Strategy and requirements," https://www.smartgrid.gov/sites/default/files/doc/files/ NISTIR
7628 Draft 1 Smart Grid Cyber Security Strategy Requi 200902.pdf, NIST, Sep.
2009, last accessed: June 11, 2016.