Secure Electricity Bill Automation Using GPRS and Web Interface in Conjunction with Elliptic Curve Crypto-Stegano Scheme

Alok Kumar Vishwakarma and A. E. Narayanan, *Member,IACSIT*

***Abstract*—The significant improvement in the information and communication technology (ICT) increases various new needs. Electricity boards also has no exception but still there is only conventional way to measure the electricity bill i.e. assessing is done manually, which is an time consuming and expensive process and it requires lot of human effort. There are several methods were proposed for this but still there is problem with the security over the unsecure channel. In this paper we proposed the secure electricity bill automation model using GPRS and Web interface along with Elliptic Curve crypto-stegano scheme which provides the better security over the unsecure channel and solves the problem of manual billing system without replacing the existing energy meter. This project work can play a better role to make electricity bill measurement ICT enabled and also in delivering our vision of integrating technology towards a solution.**

***Index Terms*—GPRS, web interface, RF transmitter, elliptic curve crypto stegano-scheme.**

I. Introduction

As electricity is one of the four major utilities of human being and this is managed by the various electricity boards throughout the country. The measurement of electricity consumed by the particular user done manually and data sent manually to the electricity board where the amount is calculated based on the usage of electricity unit. But this method is a time consuming and unsecure process because the person who is checking the amount of electricity consumed by the user can change the reading which results in the financial loss to the electricity board and also the existing method is risky because you have to physically check the energy meter and there is chances of electric shock. Our proposed model and project work aims to make it ICT enabled i.e. measurement of electricity bill can be automated by the use of GPRS, Web interface. In this method we included a new approach for data security over the unsecure channel during the transmission of data. The encryption method named as Elliptic Curve Crypto-Stegano-Scheme which will give an improved security to data over the internet and protect from the intruders and hackers. This intended project work can make a great change in assessment of Electricity bill and can give benefit to Government by reducing manpower and time consumption which leads to cost reduction.

II. Benefits of Proposed Scheme

This proposed method provides several benefits and flexibility due to its enhanced security and user friendly features. Some of the major benefits include

1) *Reduced cost*- As this scheme greatly reduces the human effort and time by making this whole assessment process automated i.e. ICT Enabled without modifying the existing infrastructure which will results in cost reduction.
2) *Security and flexibility*- Since in our proposed scheme there is no need of physical contact with energy meter or any other electrical wiring or power line so it saves the accidents caused by electric shock. The use of Elliptic Curve Crypto Stegano Scheme increases the security over the unsecured channel and web interface provides the flexibility to get the print invoice and better user friendly environment.

III. Proposed Scheme

The proposed scheme of the EBA system is as shown in Fig. 1. In our proposed scheme there is four major components, power line, energy meter along with visible LED and PIN Photo diode and RF Transmitter, web server and control and billing unit.

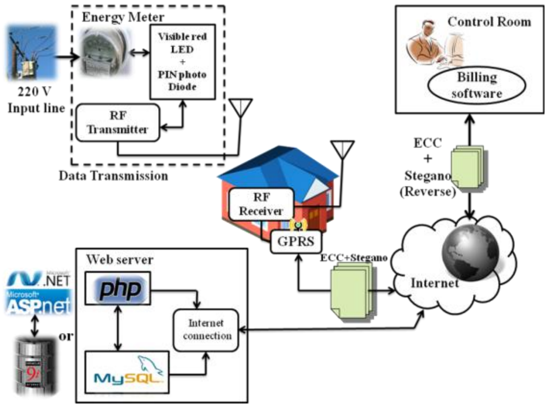

Fig. 1. Proposed model of the entire system.

The Elliptic Curve Crypto-stegano scheme is used as encryption method of data during the data transfer over the insecure channel.

IV. Description of Proposed Scheme

In our proposed scheme the input line of the power source is connected with the input of the energy meter. The energy

Manuscript received May 26, 2012; revised June 27, 2012.

Alok Kumar Vishwakarma is with the Information Technology at Periyar Maniammai University, Thanjavur, TamilNadu, India.

A. E. Narayanan is with the in Fault Tolerant Systems at Periyar Maniammai University.

meter will have a rotational wheel with black band on it. By using a visible red LED and a PIN Photo Diode [1], [2], [3] this black band is detected and time is measured by counting each wheel rotation. Using RF Transmitter that information is sent to a matching RF receiver which is interfaced with a GPRS Module, mounted somewhere in the house. A microcontroller or a computer can keep track of time of each rotation and no of rotations. GPRS Module which acts as communication portal between the energy meter and internet. GPRS Module consists of a GPRS Device and a processor running software that controls the GPRS connection as well as tariffs, control signals and energy consumption data and the internet database. Through internet connection the web server is connected through the GPRS Module. The PHP interface in web server consists of PHP software which is hosted on the web server and acts as a dynamic portal to the internet database. Internet database consists of a MySQL database running on a MySQL web server. Optionally we can use Oracle database as backend and the software portal can design using ASP.NET. It will acts as the core of the whole system which is responsible for data handling, storing functionality and control related data. The control room consists of billing software with internet connectivity so that it can be connected through the web server. The billing software also has the capability of creating pdf document as invoice for the energy consumption. As the security of data is the major concern in this project work so in order to achieve that the encryption is done before sending the data to the web server using Elliptic Curve Crypto-Stegano Scheme so that we can ensure the data security over the unsecure channel. The reverse of this algorithm is applied at the control room side and data is decrypted and received successfully without any interruption by the hackers and intruders.

V. Elliptic Curve Crypto Stegano Scheme

The idea behind this scheme is very simple that is, it is the combination of two algorithms Elliptic Curve Cryptography and Steganography. Because of this it is called as Elliptic Curve Crypto-Stegano Scheme. [4], [5] As the security over the network is a big challenge, this method enables us to enhance the security. In this at first the ECC algorithm is applied on the data and it is encrypted and hidden in an image using steganography. After applying the steganography it's very difficult for the hackers to identify that the image which is sent over the network contains any information. If in case the hacker or intruder find out the information which we are sending after applying this scheme, then also he cannot understand the information hidden in the image because of ECC algorithm encryption. As this encryption technique is more secure and hard to crack due to difficulty of solving the Elliptic Curve Logarithm problem. So it will provide the enhanced security over the insecure channel. The use of WTLS protocol makes this much more secure and hard to hack the system. Elliptic Curve cryptography (ECC) is a Public key cryptography. In Public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key where as the public key is distributed to all users taking part in the communication. The mathematical operations of ECC is defined over the elliptic curve $y2 = x3 + ax + b$, where $4a3 + 27b2 \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

What makes ECC hard to crack-? The security of ECC relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), i.e. finding k, given P and $Q = KP$. The problem is computationally intractable for large values of k. Among other things, this makes it possible for two entities to agree on a shared secret across an insecure communication channel without revealing that secret to an eavesdropper. This secret can then be used as a key to encrypt/decrypt sensitive information.

VI. Steganography

Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganlysis is process to detect of presence of steganography. In this hiding information into a media requires following elements

1) The cover media(C) that will hold the hidden data
2) The secret message (M), may be plain text, cipher text or any type of data
3) The stego function (Fe) and its inverse (Fe-1)
4) An optional stego-key (K) or password may be used to hide and unhide the message

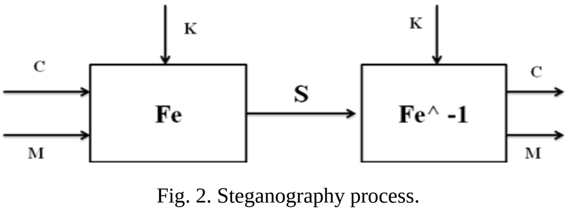

Fig. 2. Steganography process.

VII. Design and Implementation

The design and implementation is much simpler because we are making the automation of electricity bill without changing the existing infrastructure with the help of visible red LED and PIN Photo Diode and a RF Transmitter. The Design and implementation can be done in two parts.

1) Hardware design and interfacing
2) Software Design

Flow Diagram of system-

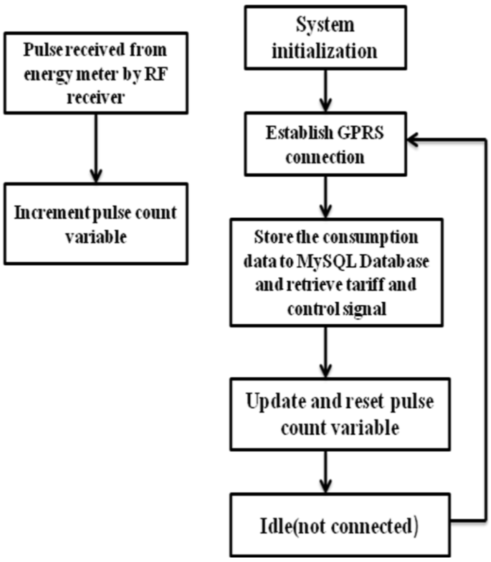
Pulse received from energy meter by RF receiver
Increment pulse count variable
System initialization
Establish GPRS connection
Store the consumption data to MySQL Database and retrieve tariff and control signal
Update and reset pulse count variable
Idle(not connected)

Fig. 3. Flow diagram of system.

The Fig. 3 shows the flow diagram of the events which is to be performed during the operation. A counter variable is incremented after receiving the pulse information sent by the RF Transmitter to RF receiver which is interfaced with the GPRS Module. Initially the system will remain in idle state and the GPRS connection is established. Once the connection is made with the web server the data received by the GPRS can be stored in the MySQL database. [6] After certain time duration the count variable is incremented and updated. By using a microcontroller or computer the time and no of rotation can be counted and base on this information the energy consumption can be calculated. In Hardware design and interfacing the visible LED is placed above the wheel which so that it can illuminate the black band and the photo diode is placed in such a way so that it can detect and measure the time for each rotation of wheel. The RF Transmitter interfaced along with GPRS [7] and placed anywhere in the house. It will receive the Data and send it to web server where the Data will be stored. From the control room the all information can be retrieved and result can be generated as pdf document which can be printed and sent to the individual users.The block diagram depicts the additional hardware components which are used to collect and transmit the information from the existing Analog energy meter.

The software design parts involves with the design of two softwares. First one needed for web server which can be made using php and can be hosted on the web server. As a backend

We can keep the MySQL Database where all the information will be stored. The php portal is structured as is the case with most dynamic web pages especially those used for the login page of a service. Most of the code is responsible for the structuring the static content on the page and remaining is

Considered with the input parameters, output parameters and the handling of both. Usually the input parameters are user name and password, but are the account no and pulse count in this case. Because of the modularity that this approach lends. other important data can easily be extracted from or entered to the MySQL database quite simple by modifying the php codes. The design of the Database needs to be concerned with not only all the information regarding the client data but also all the data logging of energy as well as the tariff in effect or the non essential load of users are to be switched on or off.

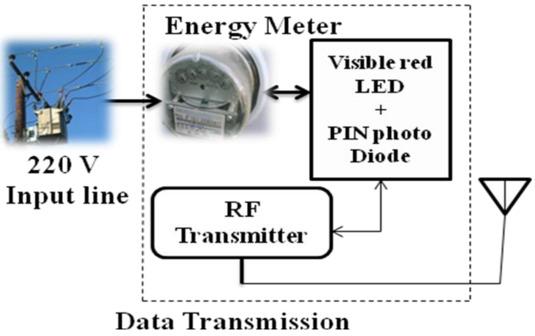

Fig. 4. Additional H/W components interfaced with existing energy meter.

The database was implementing three perspective tables, each linked by shared key and each distinguished by primary key. The separate table is made for client and billing information. The main function of this table is to record the logging data from the energy meter, including a time stamp and tariff effect that was in effect when meter started logging. There is a separate table has to be made which contains the current as well as previous tariff as well as a time stamp. The main function of this table is to provide the PHP portal with the latest tariff and control information. The secondary purpose of this table is to provide the billing software with the tariff that was in effect when a specific logging session started.

Second is billing software design. The billing software can be implemented using a single (VLC) form which can be divided into panels. The panels represent the different aspects of interfacing with the MySQL Database. The main centre panel acts as a display, showing the contents of a query. For a query to be extracted, there need to be some parameters that define the query, such as account number and date parameters. The main right hand side panel is used to set these parameters for the query to be executed. When the “Create PDF” button is pressed, the software creates a .pdf document from the last query, if no queries have been executed yet, the software automatically creates a query from the parameters and creates the .pdf file based on that. Optionally we can create the web application in ASP.NET and instead of MySQL we can also use Oracle Database. [8]

VIII. Conclusions

Since from the above work, we can conclude that this proposed model can provide a secure and efficient way to make Electricity bill calculation ICT Enabled by using the GPRS and Web interface along with Elliptic Curve Crypto-Stegano Scheme. The use of visible red LED, PIN photo Diode and RF Transmitter enables to transmit the data remotely without changing the existing infrastructure. This method solves the problem of manual assessment of Electricity Bill and delivers our vision of integrating technology towards a solution. The area of information and communication technology is unlimited. As the technology evolves the new advancements will come in the area of information and communication technology which can give a better user experience to future generation.

ACKNOWLEDGEMENT

The Author is thankful to Mr.Dr.G.Jagajothi (HOD-IT) and Mr.A.E.Narayanan (Asst.Professor, Dept.of IT) who is a part of this work, and for their valuable suggestions to complete this paper.

REFERENCES

[1] Honeywell. [Online]. Available: http://content.honeywell.com/sensing/prodinfo/infrared/catalog/Pg_088.pdf

[2] Vishay. [Online]. Available: http://www.vishay.com/docs/81521/bpw34.pdf

[3] Google PIN Photo diode. [Online]. Available: http://www.google.co.in

[4] *Elliptic Curve Crypto Systems by Mugino Saeki*, School of Computer Science, McGill University, Montreal

[5] N. F. Johnson and S. C. Katzenbeisser, *A Survey of steganographic techniques*

[6] My SQL. [Online]. Available: http://www.mysql.com/

[7] General Packet Radio Service-Wikipedia. [Online]. Available: http://en.wikipedia.org/wiki/General_Packet_Radio_Service

[8] Oracle. [Online]. Available: http://www.oracle.com/us/products/database/index.html

Alok Kumar Vishwakarma born in Kasdaha, Ambedkar Nagar, Uttar Pradesh, India on August 28th 1989. He is pursuing his B.Tech. in Information Technology at Periyar Maniammai University, Thanjavur, TamilNadu, India. He awarded with the Best UG Student in the year 2008-2009 for his outstanding performance among all UG students and served as the Vice-Chairman of IEEE Student Branch of Periyar Maniammai University during the year 2010-2011. He undergone through various training programs in HCL and CMC Limited, Noida, NewDelhi, India. He published various International Conference proceedings and International Journals in the area of Cloud computing and Advanced Networks. His research area includes Distributed Computing, Cloud Computing and Computer Networks.He is a Student Member of IEEE, IACSIT (International Association of Computer Science and Information Technology) and IEEE Communication Society.

Mr. A. E. Narayanan born in Kanyakumari district TamilNadu, India on May 30th 1972 and currently working as an Asst. Professor at Department of Information Technology, Periyar Maniammai University, Thanjavur, TamilNadu, India. He pursued his B. E. in Electrical and Electronics Engineering from Govt.College of Technology, Coimbatore and M.Tech in Information Technology from Manonmaniam Sundarnarar University, Triunelveli. He is doing his PhD in Fault Tolerant Systems at Periyar Maniammai University. He organizes various National Conferences such as RITIDS in association with Ministry of Earth Sciences, Govt. of India New Delhi. He also conducted various National Level workshops in collaboration with IIT Bombay, ISTE and MHRD and guided various M.Tech students for their project and research work. His areas of research are Digital Image Processing and Fault Tolerant Systems. He is the Member of ISTE, CSI and IEI.