International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 1 No: 3 March 2016

Smart Alert For EB Metering With Enhanced Security

Brindha.C[1], Murari Devakannan Kamalesh[2]
[1,2]Department of Computer Science Engineering, Faculty of Computing,
Sathyabama University, Chennai, India.
[1]brindhasbu@gmail.com, [2]kamal2gd@gmail.com

Abstract: Smart EB metering, which is a valuable means of data collection. There is a demand for identifying the consumption of electric power in industry to compute the amount of user's electric energy consumption. Monitoring both web and mobile communication is predicted by use of the GSM (Global system for mobile communication). This an advanced metering intrusion detection system used to give the most recent information consumption data, with the help of a smart meter. This model has the capability to detect energy stealing, more accurately. Also, it provide the information about consumption data. An accurate model is proposed here for detecting theft-related behavior.

Keywords: Smart meter, advanced metering, storage controller, consumption data, theft detection.

1.INTRODUCTION

In recent years, the "intelligent electricity system" has moved from conceptual to operational. The smart grid has undergone significant innovation, with the most important focus area being the response to demand [1] [2]. Minimizing the cost of electricity is to minimize the demand for peak load and moving peak hours for off peak hours. Shifting the use of electricity to allow the generated power to be used and reducing costs for consumers and utilities [3,4].

2. LITERATURE SURVEY

The advent of advanced communication infrastructure allows the electricity provider and the consumer to communicate. The utility company has been able to provide consumers with time - dependent electricity prices in both real - time and day - to - day fashion [5,6,7,8,9]. The user changes the corresponding load according to the fixed quantity. The advanced metering infrastructure [10] enabled the collection of data use and communication with other advanced metering infrastructure equipment. Users can calculate electricity consumption using the power management controller using advanced meter read data [6,11,27].

A programmable logic controller [12,13] is used to integrate the algorithm for response to demand. The programmable logic controller also provides modules for the processing of signals with special interface requirements [14]. Many companies have recently developed a home energy management system based on programmable commercial logic controllers [15, 16]. The research community on smart grids has studied the various problems of response to demand. In [17], the study is based on the problem of energy planning. The assumption here is based on the known energy consumption of all appliances. In [18], the energy schedule is carried out on the basis of the assumption that all appliances have known operating times. According to the statement of a known energy consumption for all appliances, both works consider a single user scenario in order to find the optimal start times of the appliances in a system with multiple users. In [19,21], the author uses a stochastic algorithm to solve a similar problem in a dispersed framework. In [11], the author proposes an energy schedule, in which the start time and the end time are first known and the energy consumption is constantly changing. The distributed optimization is sequential and all users in the system must transmit their schedules to all other users. It is also assumed that all appliances belong to the same class. In [22], the author proposed the two component each counterbalanceing a transmitor series volt injection, It connected with common dc-link. In[23], the author proposed the approach of wireless sensor network application to do the real-time data at the water supply sources to obtain the required parameters measuring to optimizing the water resource management.A smart algorithm for XML parsing and secured personalized access is discussed [24,25]. Detection of duplicates and threats is done by using string based algorithm[26]. The aim is to develop a model, where both web and mobile infrastructure calculate the bill amount. The server will provide the accurate bill to the user. Also to detect the EB theft by analyzing the transformer load. Now, users are building on the basis of electricity bills, waste of time, and a robust dynamic pay-per-use mechanism is not provided. Against this background, a distributed device scheduling algorithm for the home energy management system has been developed, such as electricity meter readings, water reading. The front end of the web infrastructure is the Node controller. The node controller's main functions are: Monitoring the availability of resources ; running instances ; and arbitration of resources. In the infrastructure, the cluster controller manages one or more nodes and is responsible for deploying web instances on the nodes. The intelligent metering module is used to monitor the use of infrastructure resources and monitor the use of resources.

3. ARCHITECTURE DIAGRAM

Fig,1 describes the user's information is sent to node controller to analysis the amount of units and then it is stored in the storage system.

4. SYSTEM MODELS

4.1 Node Controller & Analysis

In node controller, the node may be the single phase or the three phases. It consist of potential transmitter, load transmitter to transmit node from one end to another and the automatic reading machine which is used to display the amount of user's usage.

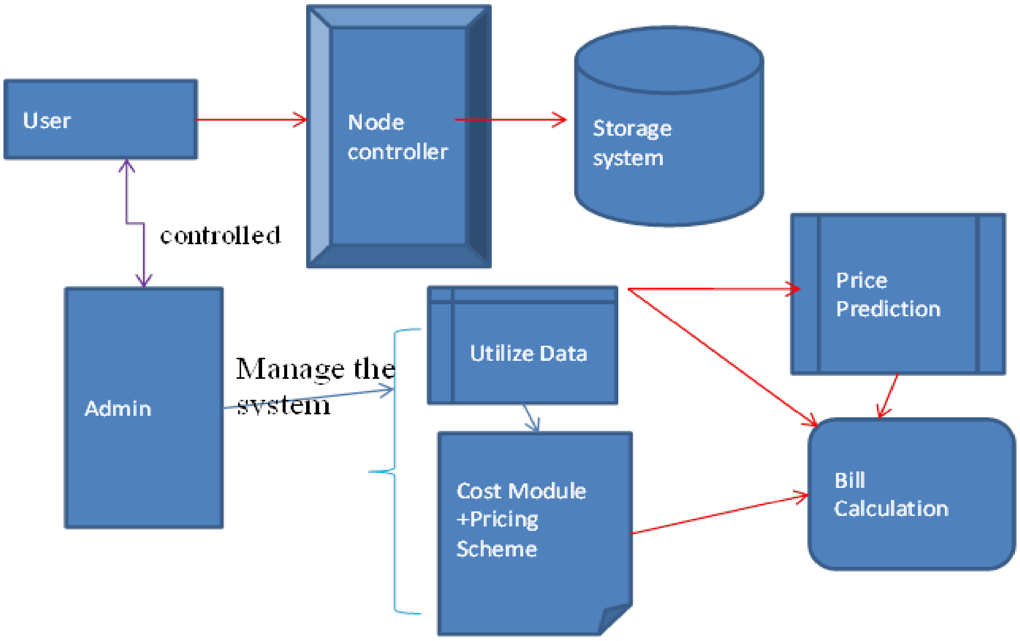


Figure 1. Architecture Of Proposed System

4.2 Storage Controller

The user's usage of load is stored in the storage controller. The storage controller which is used to store the data in automatic reading machine. The readings are sending through the GSM. It consists of capacitor, load transmitter and the potential transmitter.

4.3 Billing Model & Pricing Model

In this module, the user will get regular alerts on the amount of power consumed every day. The user will get the optimized amount of power consumption.

4.4 Theft Detection

This module provides an efficient way to detect and control external tempering when thefts occur and then apply a certain strategy to control this process. Energy meter is currently used for detection. If heavy load is introduced between the transformer and the energy meter, a large amount of energy will be consumed. Energy theft can be detected by recording it.

4.5 Both Web and Mobile Alerts

The reading of the Energy Meter was monitored using the Global System for Mobile Communication (GSM) module, which is interfaced with the Energy Meter so that the service provider knew the short messaging service (SMS) immediately. If any robbery is deducted between the transformer and the energy meter, the GSM module sends a message via GSM to the service provider. Mail services provide a web alert.

1. AES pseudo code

```
Cipher (byte in [16], byte out [16], and key_arrayround_key [n + 1])
Begin
Byte state [16];
State = in;
AddRoundKey (state, round_key[0]);
for i = 1 to n-1 stepsize 1 do
SubBytes (state);
ShiftRows (state);
MixColumns (state);
AddRoundKey (state, round_key[i]);
End for
SubBytes (state);
ShiftRows (state);
AddRoundKey (state, round_key[n]);
End
```

2. Advanced Encryption Standard Features

In AES algorithm, it performs to get the cipher text values. It consists of 10 round processes. In the first nine rounds all the four transformations will be taken place where as in the tenth round only three transformations will take place the mix column will not be taken into consideration. The matrix multiplication which is used to calculate the values in matrix form.

It consists of 4*4 matrix transformation

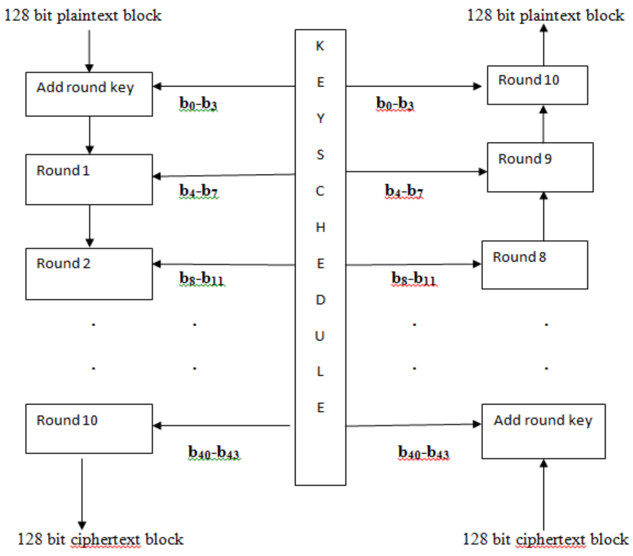


Figure 2. Transformation structure of AES

In the above fig.2 the plaintext undergo ten transformation techniques to get the cipher text.

5. SUBBYTES

Sub bytes defined as the byte-by-byte substitutions. Each input byte produces the substitution byte for using the matrix transformation. The size of the matrix transformation is 16 × 16. The input byte used to find the substitute; here, divide the two 4-bit patterns by input byte, each input byte requires the integer value from 0 to 15. The 16×16 matrix transformation requires the row and the column index. The row index tends to the first hex values and the column index tends to another hex values. a′i = a (n+2) mod 8 ⊗ a (n+5) mod 8 ⊗ a (n+7) mod 8 ⊗ c_i where c_i is the n^{th} bit element of the byte value c then the hex decimal value will be 0x05. At last, it regenerates the byte with the help of its multiplicative process. The S-box behavior will be the 16 × 16 matrix transformation which is same for all the byte values.

Shiftrows:

The shift rows consists of four steps.

1. Row one is fixed
2. Row two moves one byte left

3. Row three moves two byte left
4. Row four moves three byte left

The first four values are filled in the array of first column; the second four values are filled in the array of second column; simultaneously the third and fourth values follow

If the row is left unaltered; the row one is fixed, the row two moves one byte right, the row three moves two byte left, simultaneously, row four follows

Mix Columns:

The column of each byte replaces the function of all bytes in that same column. Then, the column in each byte replaces that byte by two times, then adds the next byte by three times, and adds the next bytes; add the other byte that follows. The state array of bytes in the first row can be stated as,

$r'0,m = (0x02 \times r0,m) \otimes (0x03 \times r1,m) \otimes r2,m \otimes r3,m$

The byte in row two is

$r'1, m = r0,m \otimes (0x02 \times r1,m) \otimes (0x03 \times r2,m) \otimes r3,m$

The byte in row three is

$r'2, m = r0,m \otimes r1,m \otimes (0x02 \times r2,m) \otimes (0x03 \times r3,m)$

The byte in row four is

$r'3, m = (0x03 \times r0, m) \otimes r1, m \otimes r2,m \otimes (0x02 \times r3,m)$

Addroundkey:

The 128-bit encryption key of each rounds have its own round key. Each round of the transformation step takes place in both encryption and decryption. The form of the state array is arranged in 128-bit input block, the aes algorithm of 4×4 array is arranged in the form of 16 bytes of encryption key. The 128-bit key of the round being in one-one correspondence. The key expansion, which is divorced conceptually from the round based input block.

3. Key Expansion:

```
Key (byte key [4*Nk], word z [Nb*(Nr+1)], Nk)
begin
word temp
n=0
While (n<Nk)
z[n]=word(key[4*n], key[4*n+1], key[4*n+2], key[4*n+3])
n=n+1
end while
n=Nk
while (n<Nb*(Nr+1))
temp=z[n-1]
if(n mod Nk=0)
temp=sword(Rword(temp))xorRcon[i/Nk]
else
if (Nk>6 and n mod Nk=4)
temp=sword(temp)
end if
z[n]=z[word]xor temp
n=n+1
end while
end
```

AES performs the 10 round to convert plain text into cipher text

$$n<Nb(Nr+1) \tag{1}$$

The sword which is function of four byte input word. The Rword which is to performs the permutation and the Rcon which contain the values xn-1 being the x powers.

6. ENCRYPTION

First, the original text that means empty text is changed into bytes and the AES algorithm performs the encryption, need to generate both the keys i.e. derived bytes and symmetric key.

Decryption:

In encrypted text, the cipher text also changed into bytes and also the encryption process generates the both keys i.e. derived bytes and symmetric key.

The plain text space is denoted by $P = C = Z^n$, Typically, N ≥64 bytes. In round structure, apply some functions on intermediate cipher texts repeatedly N_r times. Use different round key K^n defined from k during nth term. Decryption should be same as encryption.

```
Begin
INPUT: plaintext x, key K
OUTPUT: cipher text y = $e_k(x)$ .
        Assumed the round function g, last round h, key
        Scheduling  procedure giving $K^n$.
$z^0=x$
for n=1 t0 $N_r$-1
$z^n=g(z^{n-1}, K^n)$
$y=g(z^{Nr-1},K^{Nr-1})$
      End for
End
```

This module provides an efficient way to detect and control external tempering when thefts occur and then apply some strategy to control this process. Energy meter is currently used for detection. If heavy load is introduced between the transformer and the energy meter, a large amount of energy will be consumed. Energy theft can be detected by recording it.

Both web and mobile Alerts

The reading of the Energy Meter was monitored using the Global System for Mobile Communication (GSM) module, which is interfaced with the Energy Meter so that the service provider knew the short messaging service (SMS) immediately. If any theft between the transformer and the energy meter is deducted, the GSM module on the meter side sends a message via GSM to the service provider. Mail services provide a web alert.

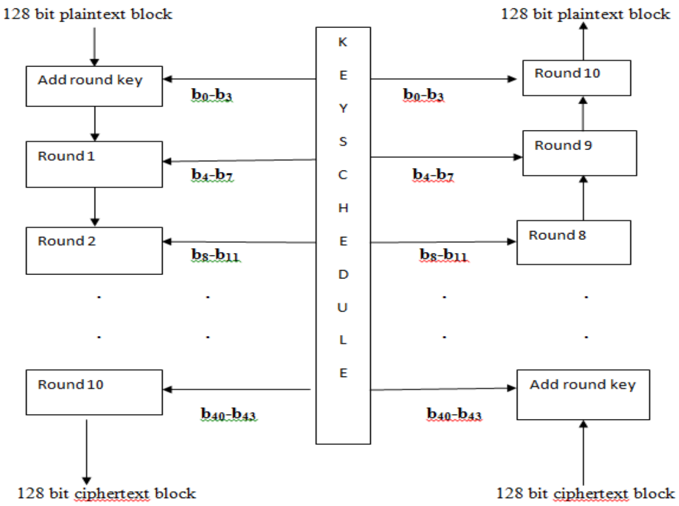
AES pseudo code

```
Cipher (byte in [16], byte out [16], and key_arrayround_key [n + 1])
Begin
Byte state [16];
State = in;
AddRoundKey (state, round_key[0]);
for i = 1 to n-1 stepsize 1 do
SubBytes (state);
ShiftRows (state);
MixColumns (state);
AddRoundKey (state, round_key[i]);
End for
SubBytes (state);
ShiftRows (state);
AddRoundKey (state, round_key[n]);
End
```

4. Advanced Encryption Standard Features:

In AES algorithm, it performs to get the cipher text values. It consists of 10 round processes. In the first nine rounds all the four transformations will be taken place where as in the tenth round only three transformations will take place the mix column will not be taken into consideration. The matrix multiplication, which is used to calculate the values in matrix form.

It consists of 4*4 matrix transformation



The encryption, need to generate both the keys i.e. derived bytes and symmetric key. In encrypted text, the cipher text also changed into bytes and also the encryption process generates the both keys i.e. derived bytes and symmetric key.

The plain text space is denoted by $P = C = Z^n$, Typically, N ≥ 64 bytes. In round structure, apply some functions on intermediate cipher texts repeatedly N_r times. Use different round key K^n defined from k during n^{th} term.

REFERENCES

[1] C. Chen, S.Kishore, and L. V. Snyder, "An innovative RTP-based residential power scheduling scheme for smart grids," in Proc. ICASSP, Prague, Czech Republic, May 2011, pp. 5956–5959.

[2] R. Hartway, S. Price, and C. K. Woo, "Smart meter, customer choice and profitable time-of-use rate option," Energy, vol. 24, pp. 895–903, 1999.

[3] E.Çelebi and J. D. Fuller, “A model for efficient consumer pricing schemes in electricity markets,” IEEE Trans. Power Syst., vol. 22, no. 1, pp. 60–67, 2007.

[4] P. Yang, G. Tang, and A. Nehorai, “Optimal time-of-use electricity pricing using game theory,” in Proc. Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Kyoto, Japan, Mar. 2012.

[5] S. Karnouskos, O. Terzidis, and P. Karnouskos, “An advanced metering infrastructure for future energy networks,” in Proc. NTMS 2007 Conf., Paris, France, May 2007.

[6] A.-H. Mohsenian-Rad, V. Wong, J. Jatskevich, and R. Schober, “Optimal and autonomous incentive-based energy consumption scheduling algorithm for smart grid,” in Proc. Innov. Smart Grid Technol. (ISGT) 2010, Vancouver, BC, Canada, Jan. 2010.

[7] M. A. Piette, O. Sezgen, D. Watson, N. Motegi, C. Shockman, and L. t. Hope, “Development and evaluation of fully automated demand response in large facilities,” Lawrence Berkeley National Laboratory, Tech. Rep., 2004 [Online]. Available: http://escholarship.org/uc/item/4r45b9zt

[8] S. Elpelt, F. Ersch, T. Gruenewald, and G. Lo, “PLC function block for automated demand response integration,” International Classification G05B 15/02 Patent, Jan. 2012 [Online]. Available:
http://www.google. com/patents/EP2402828A2?cl=en

[9] C. T. Jones, Programmable Logic Controllers: The Complete Guide to the Technology. New York: Patrick-Turner, 1996.

[10] Scheneider Electric: Modicon M168 PLC, Online Product Catalog [Online].
Available: http://products.schneider-electric.us/products-services/ products/plcs-pac-and-distributed-io/industrial-process-machines- and-oems/modicon-m168-hvac-controller/

[11] Keyence America: KV series PLC, Online Product Catalog [Online]. Available:
http://www.keyence.com/products/plc/plc/plc.php

[12] A.Mohsenian-Rad and A. Leon-Garcia, “Optimal residential load control with price prediction in real-time electricity pricing environments,” IEEE Trans. Smart Grid, vol. 1, no. 2, pp. 120–133, 2010.

[13] M. Pedrasa, T. Spooner, and I. MacGill, “Coordinated scheduling of residential distributed energy resources to optimize smart home energy services,” IEEE Trans. Smart Grid, vol. 1, no. 2, pp. 134–143, 2010.

[14] S. Caron and G. Kesidis, “Incentive-based energy consumption scheduling algorithms for the smart grid,” in Proc. IEEE Smart Grid Commun., 2010, pp. 391–396.

[15] J. Lee, G.-L. Park, S.-W. Kim, H.-J. Kim, and C. O. Sung, “Power consumption scheduling for peak load reduction in smart grid homes,” in Proc. ACM Symp. Appl. Comput., 2011, pp. 584–588.

[16] Prof. Zeph Grunschlag, Modern cipher, http://www.cs.columbia.edu/~zeph/4261/lectures/block-ciphers.pdf

[17] T.Ruban Deva Prakash, Dr. N. Kesavan Nair, “Voltage Sag Mitigation in Multi-line Transmission System Using Generalised Unified Power Flow Controller”, in Intelligent Electronic System, Vol.1, No.1,Page no. 72-78, November 2007.

[18] Ravi Kumar T., Raghava Rao K., A Sensor Web Model And Service For Drinking Water Distribution Management, in Information Sciences & Computing, Vol.7 No.1 January 2013, Page no.31-34.

[19] S.Vigneshwari and Dr. M. Aramudhan, An Approach for Ontology Integration for Personalization with the Support of XML, International Journal of Engineering and Technology , volume 5 , Issue 6, 2013 pp : 4556-4571

[20] S.Vigneshwari and Dr. M. Aramudhan, A Technique to User Profiling Ontology Mining And Relationship Ranking, Journal of Theoretical and Applied Information Technology(2014), Vol. 58. No. 3, pp:635-640

[21] Kavitha Esther Rajakumari, T.Jebarajan, Importance of string based techniques in clone detection, International Journal on Recent trends in engineering and technology, vol 5, No. 1, March 2011, pp: 137-142.

[22] Phani Chavali , Peng Yang, Arye Nehorai, A Distributed Algorithm of Appliance Scheduling for Home Energy Management system, IEEE transactions on smart grid, vol. 5, no. 1, January 2014,pp:282-290