International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 5 (2015) pp. 12643-12653

http://www.ripublication.com

Smart Alert for EB Metering with Enhanced Security

[a]Deepa.B, [b]Arthi Rathna.R, [c]Vigneshwari.S
[a,b,c]Department of Computer Science Engineering, Faculty of Computing, Sathyabama University, Chennai, India.
[a]thithikabalaji@gmail.com, [b]arthirathna93@gmail.com, [c]vikiraju@gmail.com

Abstract

Smart metering, which is an effective means of data collection. There is a demand for identifying the consumption of electric power in industry to calculate the amount of user's electric energy consumption. Monitoring both web and mobile communication is predicted using the GSM (Global system for mobile communication). This an advanced metering intrusion detection system used to give the latest information consumption data, with the help of a smart meter. This model has the capability to detect energy theft, more accurately. Also it gives 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.

Introduction

The "smart electricity system" has shifted from conceptual to operational type in the last few years. The smart gird has undergone significant innovation, with demand response[1], [2] being the important focus area. The minimization of electricity cost is to minimize the peak load and moving peak hours claim to the off peak hours.Shifting electric usage desired to allow for utilization of the generated power, and reduce the costs to both the consumers and utility companies[3,4].

Literature Survey

The advent of advanced communication infrastructure enables the power provider and consumer communicate between them. It has become feasible for the utility company to provide the consumers with time dependent price of electricity, for both real-time and the day-ahead fashion [5,6,7,8,9]. The user will change their corresponding load according to the fixed amount. The advanced metering infrastructure[10] has made

possible to collect the data usage and to communicate with other advanced metering infrastructure devices.

Using the advanced meter read data, users can schedule the consumption of electricity using the energy-management controller[6, 11,27]. A programmable logic controller[12,13] is used which helps to integrate the demand response algorithm. Programmable logic controller also provide modules to process signals that have special interfacing requirements[14].

Many companies developed commercial programmable logic controller based home energy management system recently[15, 16]. The smart grid research community has been studying the various demand response problems. In [17], the study is based on the energy scheduling problem.Here, the assumption is based on known energy consumption for all the appliances. In[18], the energy scheduling is done, under the assumption of known operating times for all the appliances. Both works consider a single user scenario in according to find the optimal start times of the appliances in a system with the multiple users, under the assumption of a known energy consumption for all the appliances.

In [19,21], the author solves the same problem in a distributed framework using a stochastic algorithm. In [11], the author propose an energy scheduling scheme, where the start time and the end time are known priorly, and the energy consumption is varied continuously. The distributed optimization is sequential and all users have to broadcast their schedules to all other users in the system. Also, all the appliances are assumed to 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 a days, users are build based on the electric bill, wastage of time and it does not provide for a robust dynamic pay-per-use mechanism. Against this background, a distributed algorithm of appliance scheduling for home energy management system like electricity meter readings, water reading, have been developed.

The present work about the architecture of the smart metering module; introduce the billing model used and the resulting pricing mechanism. The ***Node controller*** is the front end of the web infrastructure. The main functions of the node controller are: monitoring the resource availability; running instances; and resource arbitration. The cluster controller manages one or more nodes in the infrastructure and is responsible for deploying web instances on the nodes. Smart metering module is used for Monitoring resource utilization of the infrastructure and Monitoring resource utilization of the in 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.

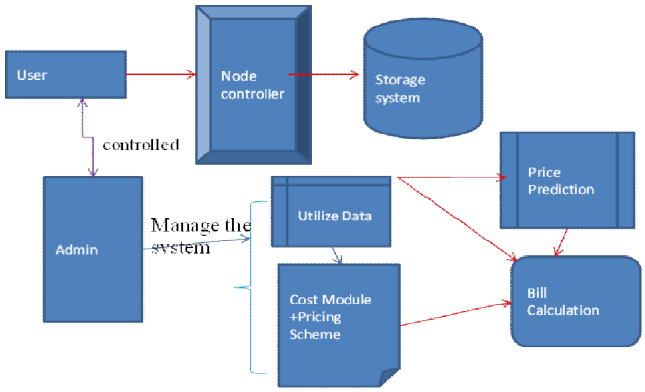

Figure 1: Architecture of the proposed system

System Models

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.

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.

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.

Theft Detection:
This Module provides efficient method for detecting and controlling external tempering, when thefts are happening and then apply certain strategy to control this process. Currently energy meter is used for detection. If heavy load is introduced in between transformer and energy meter, it will consume large amount of energy. By recording this, energy theft can be detected.

Both web and mobile Alerts
Energy Meter reading was monitored using Global System for Mobile communication (GSM)Module, which is interfaced with the Energy Meter so that service provider came to know immediately by Short Messaging Service(SMS). If any theft is deducted between transformer and energy meter, GSM Module at meter side sends message to the service provider through GSM. Web alert is provided by mail services.

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
```

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

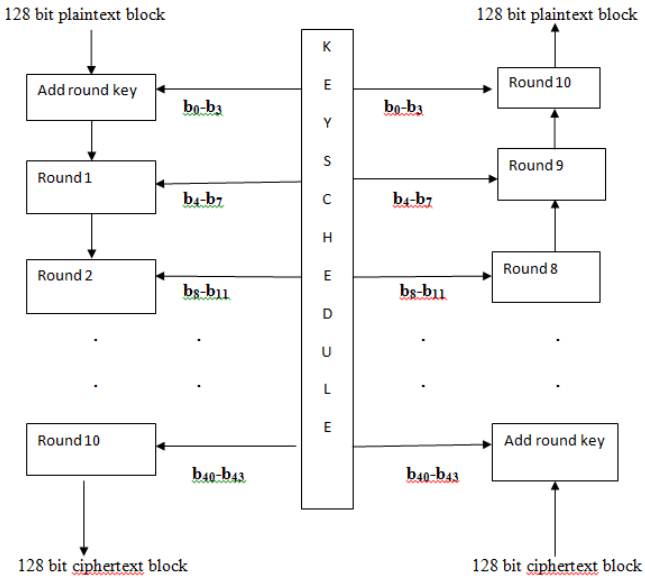

Figure 2: Transformation structure of AES

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

Sub Bytes:

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. $a'i = a\ (n+2) \bmod 8 \otimes a\ (n+5) \bmod 8 \otimes a\ (n+7) \bmod 8 \otimes c_i$ 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 rounds key. Each round of transformation step takes place in both encryption and decryption. The form of 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.

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

$n<Nb(Nr+1)$ (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.

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, $N \geq 64$ 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. 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
```

Length or bit strings is to the length K bit strings. It is defined using S-boxes on sub strings of input [21]. So, it is very efficient in hardware based S-box: π_s. The resulting substitution is

$$\sigma(w)=\pi_s(w_{(1)})||\pi_s(w_{(2)})||.....||\pi_s(w_{(m)}) \quad (2)$$

In permutation, when the domain is equal to co domain ρ is used. In expansion, when the domain is less than co domain domain<co domain , ξ is used. In contraction, when domain is greater than co domain domain>co domain, the symbol used is ,ĸ. The defined substitution σ from predefined S-box and the predefined permutation ρ. The round function is

$$g(w,K^i)=\rho o\sigma(w\oplus K^i) \quad (3)$$

Final round-no permutation + whitening.

$$h(w,k)=\sigma(w\oplus K^{Nr-1})\oplus K^{Nr} \quad (4)$$

Round function

Begin
$g(w,K^i) = w_R||w_L \oplus \rho(\sigma(\xi(w_R) \oplus K^i))$
Beginning and end slightly different
Apply "initial permutation" IP at start
Apply swap and at end (no key):
$h(w) = IP^{-1}(w_R||w_L)$
Initial XOR with first round key
Substitution σ = Sub Bytes at round-start
Permutation ρ = Shift Rows mid-round
Linear tarns' = Mix Columns near end
Round function:
$g(w^i, K^i) = \mu o \rho o \sigma(w^i) \oplus K^i$
σ and μ have natural interpretations as field theoretic functions viewing $P = F_{28}$.
First block y_0= rand. Initialization vector (IV)
Ciphers block formula:
$y_i = e_K(y_{i-1} \oplus x_i)$
Output feed back generates IV generates key-stream XOR'ed with plaintext
$z_i = e_K(z_{i-1})$
Cipher block formula is
$y_i = x_i \oplus z_i$
It is synchronous stream cipher
In Cipher Feed-Back, IV generates key-stream XOR'ed with plaintexts:
$z_i = e_K(z_{i-1})$
End

In sub bytes, the matrix transformation values will add the s-box values to get the cipher text. AES works in both the software and hardware. Here we are using the 128-bit key to process the 10 iterations of AES transformation.

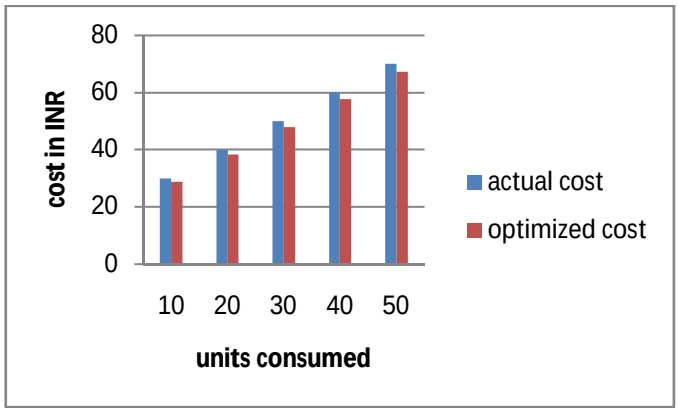

Figure 3: Per day consumption

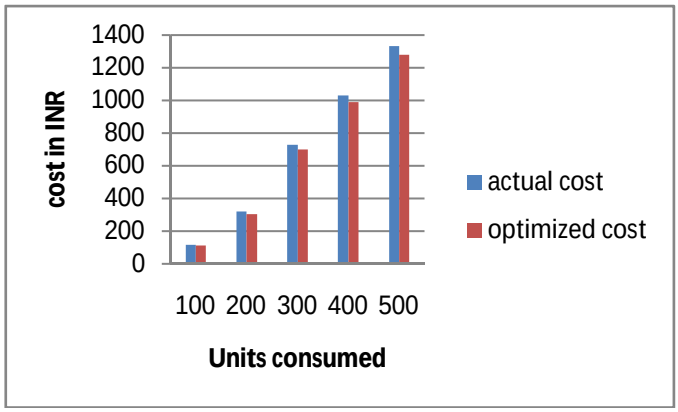

Figure 4: Per month consumption

Fig.3 shows, the per day consumption rate of electricity is reduced after optimization. Fig 4 shows the per month consumption rate of electricity is reduced after optimization. Here we are using three techniques 1) cipher block,2)output feedback,3)cipher feedback. It generates,4)key-stream XOR with the plaintext.

Conclusion

In this paper, we propose a smart metering to control power consumption in commercial buildings. This paper presents the advanced encryption standard algorithm protect to get the optimized values.

References

[1]. C.W. Gellings, "The concept of demand-side management for electric utilities," Proc.IEEE, vol.73, pp.1468-1470, 1985

[2]. "Benefits of demand response in electricity markets and recommendations for achieving them," U.S. Department of Energy, Tech. Rep, 2006 [Online]. Available: http://eetd.lbl.gov/ea/emp/reports/congress-1252d.pdf.

[3]. K. Spees and L. Lave, "Impacts of responsive load in pjm: Load shifting and real time pricing," *Energy J.*, vol. 29, no. 2, pp. 101–122, 2008.

[4]. P. Cappers, C. Goldman, and D. Kathan, "Demand response in U.S. electricity markets: Empirical evidence," Lawrence Berkeley National Lab, Tech. Rep. LBNL-2124E, 2009.

[5]. P. Samadi, A.-H. Mohsenian-Rad, R. Schober, V. W. Wong, and J. Jatskevich, "Optimal real-time pricing algorithm based on utility maximization for smart grid," in *Proc. Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, Oct. 2010, pp. 415–420.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

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

[11]. 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.

[12]. 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

[13]. 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

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

[15]. 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/

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

[17]. 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.

[18]. 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.

[19]. 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.

[20]. 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.

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

[22]. 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.

[23]. 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.

[24]. 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

[25]. 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

[26]. 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.

[27]. 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