A Secured Access Control Architecture Consideration For PLC based Smart Grids

Tshepiso Mooketsio[1],Bakhe Nleya and Mendon Dewa[2] , Andrew Mutsvangwa[3]

[1,2]*Department of Electronic Engineering, Steve Biko Campus, Durban University of Technology*

[1]thepisonicole@gmail.com, [2]andrew.mutsvangwa@nwu.ac.za

***Abstract*—Power supply, distribution and generation industry is now turning the existing electrical grids to smart grids, thus making them more efficient in both effective power management and reliability, reduced production costs, and more environmentally friendly energy generation. Despite its attractive features, Smart Grid technology remains vulnerable to security threats. This paper summaries some of these potential security issues by exploring a data access control mechanism that ensures privacy to customers. The proposed access control mechanism gives selective access to consumer data stored in data repositories and used by different smart grid users. An attribute-based encryption (ABE) is suggested. The entire grid network is subdivided into clusters each with its own remote terminal unit (RTU) as well as a gateway smart meter. User data in a given cluster is aggregated and sent to the local substation where it is monitored by the RTU. RTUs and users have attributes and cryptographic keys distributed by several key distribution centers (KDC). RTUs send data encrypted under a set of attributes. Users can decrypt information provided they have valid attributes. The access control scheme is quite resilient because of its being distributed in nature and does not rely on a single KDC to distribute keys. The encryption algorithm is based on Diffie-Hellman key establishment protocol and hash-based message authentication code, which allows smart meters at different clusters of the smart grid to mutually authenticate prior to data/information exchange and in the process maintaining low latency as well as relatively fewer authentication associated messages . Overall the control scheme is relatively collusion resistant.**

Keywords: Access control, clusters, decentralized, attribute-based encryption, homomorphic Encryption, Smart meters

I. Introduction

Smart grids are the new version native power system grids that adopt Information and Communication related technologies to enhance efficiency and reliability of power grid systems. Traditionally, most power generating systems have always relied on fossil fuels. However, because of the latter's fast depletion as well as environmental unfriendliness, there is a gradual attention towards renewable energy sources to replace them. Renewable energy sources such as wind and solar generate power intermittently, i.e. solar powered electric generating systems rely on the sun hence generate electricity during daylight times only. It is thus imperative that new generation power grid management system be developed to cope with associated challenges. Thus the smart grid is a promising solution towards the integrating and availing of renewable resources to the existing power grid and an ideal platform for power users to participate in the electricity enterprise. A typical smart grid has distinct components and functions in comparison with the traditional power grid in that it facilitates two way communication between users (meters) and the central controls.

Facilitating the two-way communication, was made possible by the deployment of an enabling advanced metering infrastructure (AMI) that contains a key component in the smart grid system called a smart meter. A smart meter usually has a processing chip and a non-volatile storage so that it can perform smart functions like being able to report periodic usage updates to end-users as well as the generation facilities at Power Supply Company and interact directly with "smart" appliances at home to control them [1].

The two-way communication assists is balancing demand versus supply. The main smart grid services summarily include:

- Automatic meter reading.
- Power grid monitoring: Key electrical parameters such as peak voltage, peak factor, and degree of synchronisation (with sources) as well as current levels in the power grid infrastructure are monitored in real time.
- Demand side management: it is comprised of two parts:
  - Load shifting/demand response.
  - Energy conservation, e.g., using energy efficient products [2].
- Home networking between electrical appliances for energy management.
- Vehicle to power grid technology: vehicles store power during non-peak hours and send it back to the power grid for the duration of on peak hours.
- Self healing: the power grid would be able to heal itself automatically. It can decide based on the collected data and react dynamically.
- Flexibility against attacks and disasters: this characteristic can be provided by increasing power grid robustness, protecting key assets from physical attacks and providing sufficient redundancy in the power grid [3].
- Equipment management and performance efficiency: the state of all equipment and operational efficiency can be monitored. An example would be cable performance as temperatures and other climatic conditions.
- New markets and operations: smart grid will integrate and open new businesses to the power grid. For instance, it integrates IT infrastructure to the power grid; smart devices need to be designed and communication infrastructure needs to be developed.

As mentioned earlier, smart meters manage, monitor and control power supply to the end users, and in some instances can also relay data to and from gateway smart meters [3]. The gateway smart meters, in turn, relay the collected data to control centres of utility companies to support the pricing and decision-making. In short, not all smart meters (nodes) can communicate with the collector directly. Intermediate smart meters cooperate in relaying data packets on behalf of one another until the data packets reach the gateway smart meter. This procedure is called data aggregation (figure 1). Typically we have home area networks (HANs), and building area networks (BANs). HANs collect information and send it via neighbour BANs. Ultimately all the information from smart meters is aggregated at a local substation, where a remote terminal unit (RTU) finally sends the aggregated data to a gateway smart meter. The gateway smart meters associated with each RTU finally send aggregated results to data centres, from which the information is distributed to users for maintenance, auditing, future predictions etc.

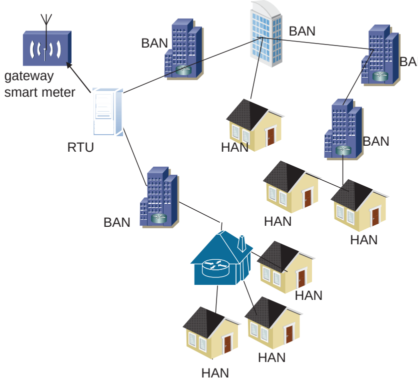

Figure 1

Data in transit becomes vulnerable in that, intermediate nodes can place the data at security risk without being detected by the core smart grid and thus it is important to secure the smart grid. As cited earlier, the information from RTUs at the substation is crucial for key management purposes such as power distribution, cost accounting, as well as future grid behaviour predictions.

Ideally, a security architecture that ensures privacy during both large scale data aggregation as well as access is desirable. Large scale data aggregation will require efficient data aggregation trees as well as reliable encryption key distribution for access control. A policy based encryption scheme for access control in smart grids was proposed in [4] with the assumption of the existence of a reliable and honest key distribution centre (KDC) that distributes keys and access policies to data senders and receivers, who in turn can only decipher information, if they have a valid set of attributes. For reasons of efficiency, reliability and security, multiple KDCs connected in a distributed fashion would be desirable (figure 2).

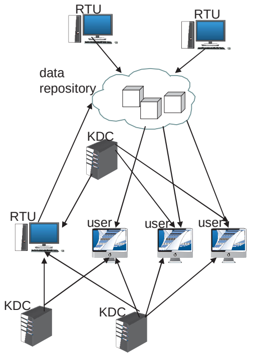

Figure 2

The paper is further organized as follows. We present an overview of related work on smart grid security issues in Section II. In Section III, we describe an access control scheme followed by its performance analysis in section IV and lastly conclusions in section V.

II. SMART GRID SECURITTY OVERVIEW

Desirable smart grids security requirements are summarised as follows [4]:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Identification & Authentication: Smart grid information system uniquely identifies and authenticates users and devices.

Authorization: Smart grid information system enforces assigned authorizations for controlling the flow of information within smart grid information system and between interconnected smart grid information systems in accordance with applicable policy.

Session management: Once a session is granted, its revocation should be guaranteed.

Boundary Protection: Defines the boundary of smart grid information system and monitoring and controlling communications at the external boundary of the system and at key internal boundaries within the system.

However, security requirements alone are insufficient to develop an optimized access control mechanism for the smart grid as it is a participating platform for many users, devices, and systems [3]. Therefore, in addition, access control mechanisms are required for management of the multiple many participants. Such access control mechanisms should ensure non-impeded interoperability among the participants as well as scalability provisioning for new participants.

Homomorphic encryption schemes which were originally designed for electronic voting are promising candidates applicable for smart grids data aggregation. The main idea for using homomorphic encryption is to carry out different operations on ciphertext and return results without reaching the semantics of the plaintext messages. Various homomorphism based encryption techniques have been proposed. Such examples include, multiplicative homomorphism (RSA), [5], additive homomorphism [6], and the recently proposed fully homomorphic scheme [6].

Attribute based encryption (ABE) schemes have also been proposed. These allow users to encrypt and decrypt messages based on user attributes. The main idea is to distribute attributes to receivers and attributes to senders so that only receivers with matching attributes structure can access the data. Data is encrypted using attribute based keys, which are distributed by a central key distribution centre KDC. A special form of ABE called the identity based encryption (IBE) was proposed in [7], where senders each have a single unique attribute. In [8], a new key policy based ABE (KP-ABE) scheme which can handle any monotonic access structure was proposed.

In [9] a ciphertext-policy ABE (CP-ABE) is presented. With this scheme the ciphertext is encrypted using a set of attributes under a given access structure and thus a receiver will only be able to decrypt the information if it has a corresponding matching set of attributes.

All the above schemes generally rely on a central key and attribute distribution centre, which itself is prone to failures and thus rendering the schemes unreliable. Further, in [9] a multi-authority protocol scheme, where several KDCs generate and distribute keys and attributes is proposed. One of the KDCs is designated as a central trusted authority thus coordinates the rest of the KDCs. To completely do away with central authority, in [10] the authors propose a scheme where the authorities can coordinate amongst themselves on a peer-to-peer basis without the requirement of a central authority. Unfortunately, the scheme requires each user to have at least one attribute from each KDC.

Recently a multi-KDC CP-ABE scheme was proposed which does not require trusted authority or any coordination between the KDCs. It also allows any type of monotonic access structure.

III. CP-ABE BASED ACCESS CONTROL

In this section, for securing access control and targeted broadcast in smart grid, we illustrate how the CP-ABE technique [12] can be effectively applied. In this scheme, we will that all the smart grid users have some attributes. A sample tree-based access structure for the considered CP-ABE targeted broadcast for smart grid is depicted in Fig. 3. As illustrated, each non-leaf node represents a logic gate, and has a threshold. If its threshold equals one, it is an OR gate and alternatively if its threshold equals its children number, it is considered as an AND gate. On the other hand, each leaf node is considered as an attribute. All the nodes in the access tree are ordered by index numbers as demonstrated in the figure.

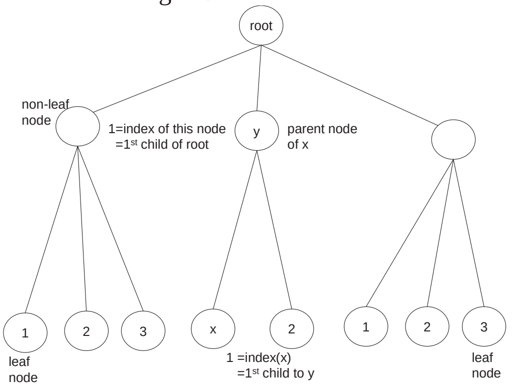
root
non-leaf node
1=index of this node =1st child of root
y
parent node of x
1
2
3
x
2
1
2
3
leaf node
1 =index(x) =1st child to y
leaf node

Figure 3. Tree based access control structure for CP-ABE.

We first define a set of attributes as, $N\ :1,...,\mathrm{n}$ for some natural integer n . Next we let I represent the set of attributes that are needed for decryption. The scheme considers access structures that comprise a single AND logic gate whose inputs are literals, represented by $\wedge_{i\in I}\underline{i}$, where $\underline{i}$ is a literal (i.e. i or $-i$).

SETUP

- Select bilinear groups G_1 and G_2 of prime order p with generator g_1 and g_2 respectively. A bilinear map $e : G_1 \times G_2 \rightarrow G_T$ is defined on them..
- Choose random exponents y , $t_1,...t_{2n}$

The published key is: $PK = \left(e, g_1, g_2, Y, T_1,..., T_{2n}\right)$;

where $Y = e\left(g_1, g_2\right)^y, \forall \in Z_{2n} : T_i = g_1^{t_i}$.

The master secret key is $MK = \left(y, t_{1,...,t_{2n}}\right)$.

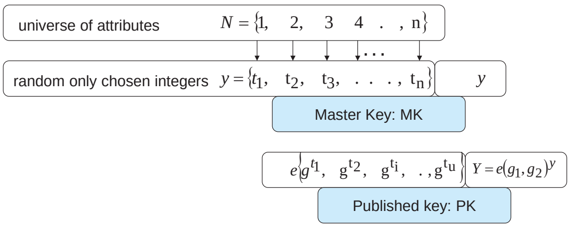
universe of attributes
$N = \{1, \ 2, \ 3 \ 4 \ . \ , \mathrm{n}\}$
...
random only chosen integers
$y = \{t_1, \ t_2, \ t_3, \ . \ . \ . \ , t_n\}$
y
Master Key: MK
$e\{g^{t_1}, \ g^{t_2}, \ g^{t_i}, \ . \ , g^{t_u}\}$
$Y = e(g_1, g_2)^y$
Published key: PK

Figure 4.a. Master key and Published key generation.

ENCRYPTION

Given a message $M \in G_T$ and an AND gate $W = \wedge_{i\in}\underline{i}$, the cyphertext is generated as $CT = \left(\vec{C}, \overline{C}\left\{C_{i,0}, C_{i,1} \middle| i \in N\right\}\right)$, where $\vec{C} = M.Y^S$, $\overline{C} = g^S$ and S is a random number in Z_p . Summarily for each $i \in I$, $C_{i,0}$ and $C_{i,1}$ are calculated as follows:

- If $\underline{i} = i$, $C_{i,0} = T_i^S$, $C_{i,1} = T_{n+i}^x$
- If $\underline{i} = -i$, $C_{i,0} = T_i^x$, $C_{i,1} = T_{n+i}^S$

In both cases x is a random number in Z_p and for each $i \notin I$, $C_{i,0} = T_i^S$ *,and* $C_{i,1} = T_{n+i}^S$.

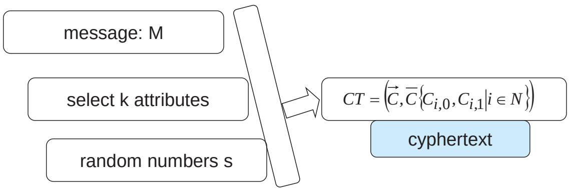
message: M
select k attributes
random numbers s
$CT = \left(\vec{C}, \overline{C}\left\{C_{i,0}, C_{i,1} \middle| i \in N\right\}\right)$
cyphertext

Figure 4.b. message enryption.

KEY GENERATION

In order to generate the decryption key we let S denote the input attribute set. For that, we every $i \notin S$ to be a negative attribute. Therefore the secret key is defined as $SK = \left(\vec{D}, \left\{D_i \middle| i \in N\right\}\right)$, where $\vec{D} = g_2^{y-r}$, $r = \sum_{i=1}^{n} r_i$, r_i is a random selected from Z_p . For each $i \in N$, $D_i = g_2^{\frac{r_i}{t_i}}$ if $i \in S$; otherwise

$$D_i = g_2^{\frac{r_i}{t_n + i}} . \tag{1}$$

.

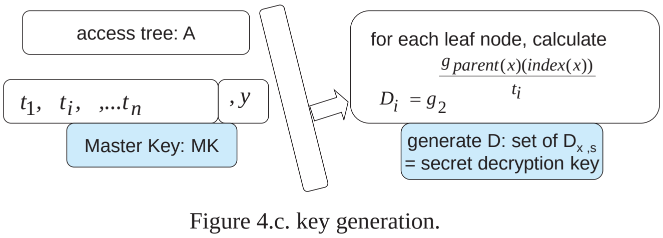
access tree: A
$t_1, \ t_i, \ ,...t_n$
$, y$
Master Key: MK
for each leaf node, calculate
$D_i = g_2^{\frac{g_{parent(x)(index(x))}}{t_i}}$
generate D: set of $D_{x,s}$ = secret decryption key

Figure 4.c. key generation.

DECRYPTION

We next show how decryption is accomplished. For that we assume that the input text is in the form; $CT = \left(\vec{C}, \overline{C}\left\{C_{i,0}, C_{i,1} \middle| i \in N\right\}\right)$ and we let $SK = \left(\vec{D}, \left\{D_i \middle| i \in N\right\}\right)$. For each $i \in N$, if the user's attributes is positive, then;

$$F_i = e\left(C_{i,0}, D_i\right) = e\left(g_1^{t_1,s}, g_2^{\frac{r_i}{t_i}} = \left(g_1, g_2\right)^{r_i \cdot s} \right) \tag{2}$$

However if the user’s attributes are negative, then

$$F_i = e\left(C_{i,1}, D_i\right) = e\left(g_1^{t_{n+i} \cdot S}, g_2^{\frac{r_i}{t_{n+i}}} = \left(g_1, g_2\right)^{r_i \cdot s} \right) \tag{3}$$

Finally decryption is accomplished as follows:

$$M = \frac{\vec{C}}{Y^S} = \frac{\vec{C}}{e\left(g_1, g_2\right)^{y.S}}, \tag{4}$$

where

$$e\left(g_1, g_2\right)^{y.S} = e\left(g_1, g_2^{y-r}\right)^{r-S} .e\left(g_1, g_2\right)^{r.S} = e\left(\vec{C}, \vec{D}\right)\prod_{i=1}^{n} F_i \tag{5}$$

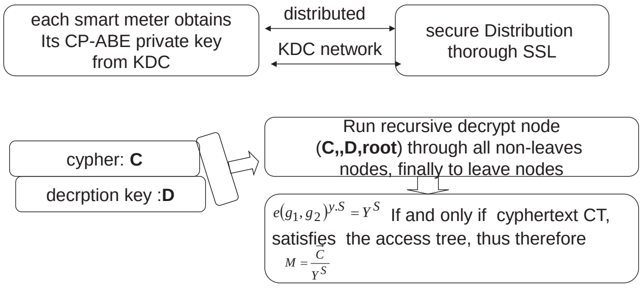
each smart meter obtains
Its CP-ABE private key
from KDC
distributed
KDC network
secure Distribution
thorough SSL
cypher: **C**
decrption key :**D**
Run recursive decrypt node
(**C,,D,root**) through all non-leaves
nodes, finally to leave nodes
$e(g_1, g_2)^{y.S} = Y^S$ If and only if cyphertext CT,
satisfies the access tree, thus therefore
$M = \frac{\vec{C}}{Y^S}$

Figure 4.d. Key distribution and decryption in smart meters

The last three equations, demonstrate how an intended user can decipher the cyphertext. If the user is not the intended recipient, there is at least one attribute for which the user gets F_i with the form $e(g_1,g_2)^{r_i.x}$ such that he/she cannot compute $e(g_1,g_2)^{y_i.x}$.

IV. PERFORMANCE

In this section we briefly analyse the security of the scheme in terms of its preciseness or rather correctness and degree of fulfilment of the desirable security goals previously discussed. The preciseness is fulfilled if a user can correctly decrypt M provided he/she has access or to all the intended attributes in the data access structure. Secondly, except for the authority, it should be impossible for unauthorised parties to generate a valid secret key component D_i for attribute $at_i x_i$ even in cases where they already know secret key components of other attributes. Overall, the scheme as outlined in section III ensures data confidentiality i.e., only intended users are able to decrypt the message M . Further more in the event of collusion, the unintended users cannot decrypt the message since each user’s SK is blinded by a blind factor r which is unique to each user. To ensure Confidentiality of Access Structure, i.e. to ensure that the ciphertext eavesdroppers are not able to derive the access structure information, the intended attributes are secretly marked with a random number $t_j \in Z_p$, $j \in Z_n$. We assume $C_{i,0}$ and $C_{i,1}$ of attribute i have the following form [13]:

$$C_{i,0} = g^{ko} h_{i,0}^{s_i + t_i} \tag{6}$$

$$C_{i,0} = g^{k1} h_{i,1}^{s_i} \tag{7}$$

In the two previous equations, $h_{i,0}$ and $h_{i,1}$ are not publicly known, thus effectively make $C_{i,0}$ and $C_{i,1}$ appear respectively as $C_{i,0} = g^{ko} g^{a_i(s_i+t_i)}$ and $C_{i,0} = g^{k1} g^{b_i}$ from an eavesdropper’s point of view. Since a_i and b_i are randomly and independently chosen for any attribute i , $C_{i,0}$ and $C_{i,1}$ indeed will appear to be independent and random to eavesdroppers. Thus it would be quite impossible for them to identify the marked ones and the magnitudes of attributes actually used in the access structure. Next, in order to totally protect and conceal the access structure information from intended recipients, the scheme thrives to ensure that the user does not know if he/she is the targeted recipient until after he/she has aggregated the secret key components of all his/her attributes and decrypted the ciphertext.. Since her attributes take effort only when they are aggregated, the user cannot tell which attributes grant or decline her access to the message M , nor how many attributes contribute to the access grant or declination. Thus, all users, no matter authorized or unauthorized, are completely unable to tell, which or how many attributes are actually used in the access structure. Collusion does not help reveal this information because of the unique blind factor r in each user’s SK .

For *backward secrecy*, the scheme has to ensure that new users cannot decrypt messages sent prior to their joining the group.

Finally we carry out the performance of the scheme based on the following:

- Computation Load on the Authority.
- Computation Load for Users.
- Communication Load.
- Storage Load for Users.

Computation Load on the Authority is mainly contributed to by the execution of three algorithms:

- *Setup p*erforms $2n$ operations, i.e. in the calculations of $h_{i,0}$ and $h_{i,1}$.
- *KeyGen*, performs $n+3$ operations, centred around he calculation of $\left\{ D_i = h^{r}_{i,\overrightarrow{X_i}} \right\}_{\forall i \in Z_n}$, as well as three other secret key components. .

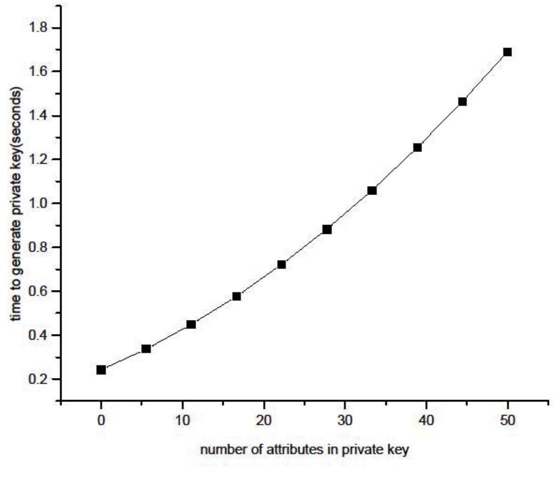

Figure 5. Private Key generation time

- *Encryption* performs $3(1+n)$ operations in the calculation of items in $\left\{C_i = \left(g^{s_i}, C_{i,0}, C_{i,1}\right)\right\}_{\forall i \in Z_n}$

Communication load for users is mainly contributed to by decryption operations, and this averages about $2n+3$ operations. *Communication load* involves $3n+3$ calculations *Storage Load for users* is for the secret key SK and involves about $(n+3)G_o$ group elements in total.

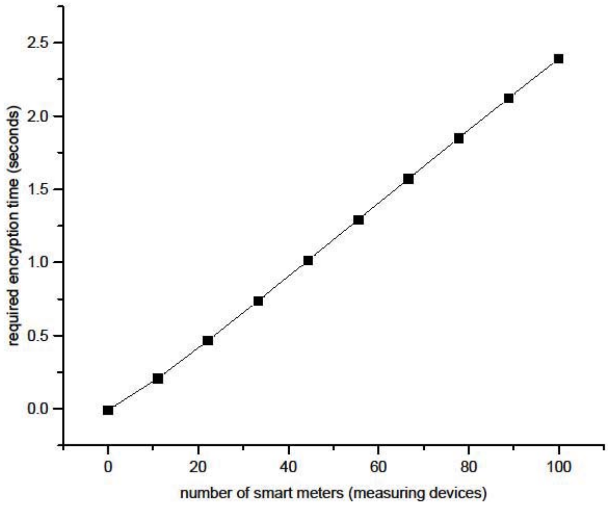

Figure 6. Message encryption time

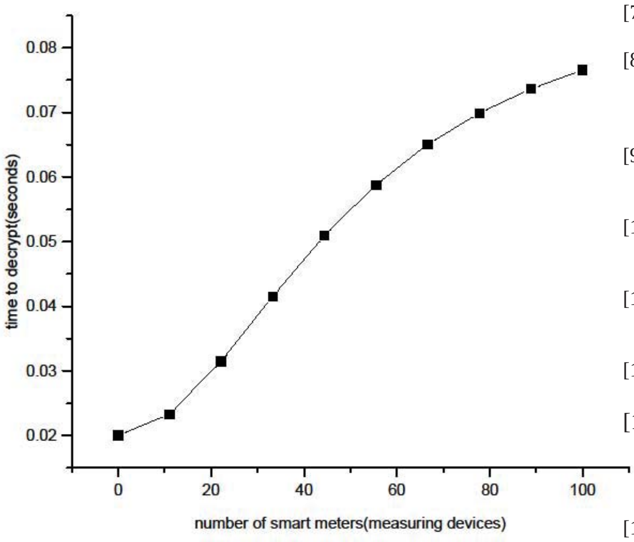

Figure 7. Message decryption time

A careful analysis of figures 5, 6 and 7 plotted from numerical and experimental results, shows that the scheme exhibits a moderate to acceptable computational loads. However, the loads would surge upwards if the number of attributes were increased.

V. CONCLUSION

In this paper, we addressed an important problem of access control. We presented privacy enhanced CP-ABE scheme in which data access structures are well protected. The scheme is suitable for large-scale applications since its complexity is just linear to the number of attributes rather than the number of users.

REFERENCES

[1] W. Wang and Y. Xu and M. Khanna, “A survey on the communication architectures in smart grid”, ComputerNetworks, (2011) July, pp. 3604-3629.

[2] V. C. Gungor, D. Sahin, T. Kocak and S. Ergut, “Smart Grid Technologies; Communication Technologies and Standards”, IEEE Transaction Industrial Information, vol. 7, no. 4, (2011), pp. 529-539.

[3] Xinxin Fan and Guang Gong. Security Challenges in Smart-Grid Metering and Control Systems. Technology Innovation Management Review, July, 2013.

[4] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovi. A Security Architecture for Data Aggregation and Access Control in Smart Grids. arXiv:1111.2619v1,[cs.NI],10 Nov 2011.

[5] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems (reprint),” Commun. ACM, vol. 26, no. 1, pp. 96–99, 1983.

[6] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in STOC, M. Mitzenmacher, Ed. ACM, 2009, pp. 169–178.

[7] A. Shamir, “Identity-based cryptosystems and signature schemes,” in CRYPTO, 1984, pp. 47–53.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, A. Juels, R. N. Wright, and S. D. C. di Vimercati, Eds. ACM, 2006, pp. 89–98.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2007, pp. 321–334.

[10] M. Chase, “Multi-authority attribute based encryption,” in TCC, ser. Lecture Notes in Computer Science, S. P. Vadhan, Ed., vol. 4392. Springer, 2007, pp. 515–534.

[11] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in ACM Conference on Computer and Communications Security, ACM, 2009, pp. 121–130.

[12] L. Cheung and C. Newport. Provably Secure Ciphertext Policy ABE. In Proceedings of CCS’07, New York, NY, USA, 2007.

[13] Depeng Li, Zeyar Aung, John R. Williams and Abel Sanchezc. No peeking: privacy-preserving demand response system in smart grids. International Journal of Parallel, Emergent and Distributed Systems, 2013.

[14] S. Yu. Attribute based data sharing with attribute revocation. Proceeding ASIACCS '10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Pages 261-270.