I J C T A, 9(13) 2016, pp. 6143-6149

A Secured Smart Frame for Bigdata Information Management in Cloud

Kalaivani K.[1], Nagalakshmi Venugopal[2]

ABSTRACT

Smart Grid is an improved form of power grid which optimizes the loss of energy transmission. It also supports two way communications i.e., from home to meter and from meter to power station. Some challenges in smart grid are to manage and process huge amount of data received from the font-end devices such as smart meter, mobile phone, personal computer, laptops etc. Proposing a secured cloud based framework for big data information management in smart grids which is a smart frame. The idea is to build a hierarchical structure of cloud computing centers to provide services for information management and big data analysis. Also, consumer privacy is very important when collecting energy usage data with the deployment of smart grid technology. Thus providing security solution based on identity-based encryption, signature and proxy re-encryption for information management.

Keywords: smart frame; information security; cloud computing; secure;

I. INTRODUCTION

The increasing demands for energy and management of energy are the main reasons for making the consumers to seek for a smarter way of managing the electricity grid. The result is the introduction of Smart Grid which can bring smartness to the traditional power grid. According to the conceptual model of the National Institute of Standards and Technology (NIST), in which it has, complex infrastructure based on a set of seven chief domains: bulk generation, energy distribution, operational and control, market, power transmission, service providers and customers [1].

Smart Grid is an electric power network that utilizes two-way communication and control-technologies which integrate the behavior and actions of all users connected to it. This helps to ensure an economically efficient and sustainable power system with low loss percentage and high levels of quality, security of supply and safety.

The smart grid is a new innovative technology. It replaces the traditional power grids by provides several advantages such as efficiency, reliability, economics, and substantiality of electrical services. However,

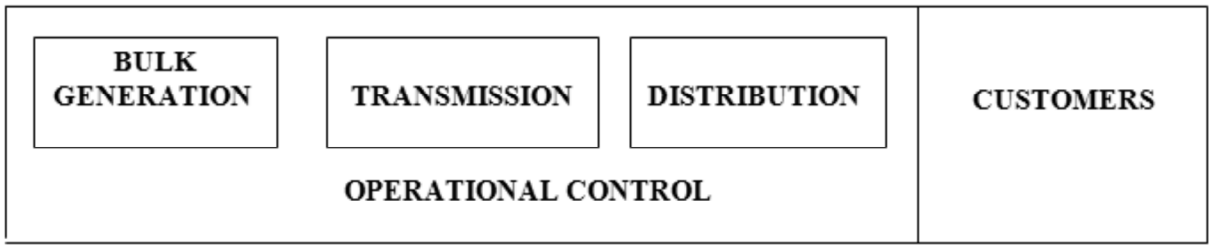

Figure 1: Architecture of Traditional Power Grid

[*] PG Scholar, Computer Science and Engineering, Dr. NGP Institute of Technology, Coimbatore,Tamilnadu, *E-mail: kalai.vani980@gmail.com*

[**] Associate Professor, Computer Science and Engineering, Dr. NGP Institute of Technology, Coimbatore, Tamilnadu, *E-mail: nagalakshmi.ngp@gmail.com*

it has several advantages; their deployment is often limited to small regions. This is due to information gathering, information storing, information processing and security in the Smart Frame. Since there are large number of front-end devices, managing a huge amount of data received from these devices is difficult task. Any delay may cause serious consequences in the whole system.

Additionally, smart metering is one of the key component for the smart grid [2]. This is because it is one of the major front end devices through which huge information arrives.

II. RELATED WORK

(A) Traditional Power Grid

Traditional power grid is a transmission system that transfers electricity from bulk generation systems to power distribution system and each system finally delivers electricity at a low voltage to their end users. The energy production and distribution are supervised by a centralized control system, known as Supervisory Control and Data Acquisition (SCADA) systems [3]. This system is in charge of mapping and visualizing any activities in the storage and demand power. It can also remotely and locally control the power transmission and distribution based on the demand and loads.

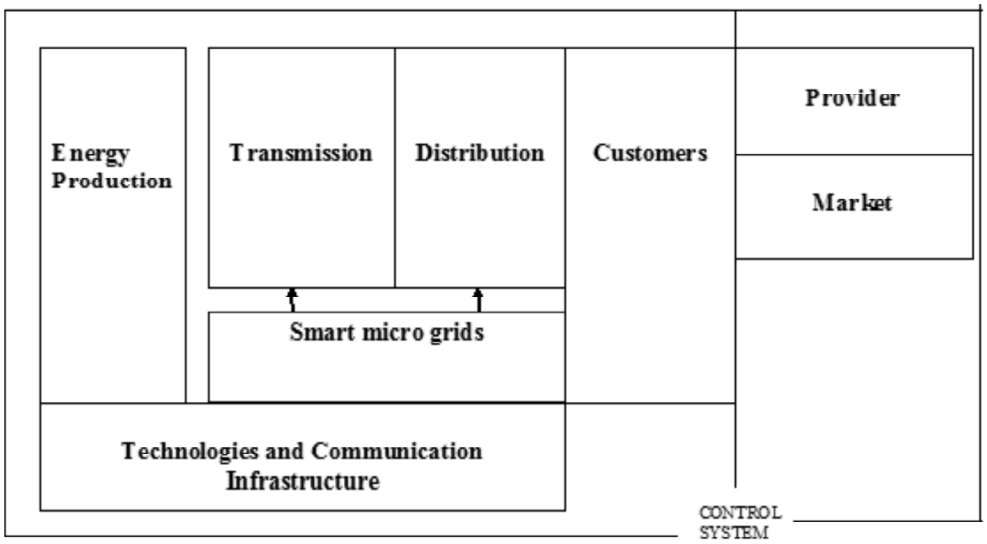

Figure 2: Architecture of a Smart Grid

(B) Smart Meter Communication

A smart metering communication system consists of the following components: smart meter which is a two-way communicating device that measures energy consuming at the appliances; Home Area Network (HAN) which is an information and communication network formed by appliances and devices within a home to support different distributed applications; Neighborhood Area Network (NAN) that collects data from multiple HANs and deliver the data to a data concentrator; Wide Area Network (WAN) which is the data transport network that carries metering data to central control centers; and Gateway which is the device that collects or measures energy usage information from the HAN members and transmits this data to interested parties[4].

Cloud computing provides access to the applications as utilities, over the internet. It allows users to create, configure, and customize the applications. It refers to manipulating, configuring, and accessing the applications online. It offers data storage, infrastructure and application. Thus it provides advantages such as flexibility, scalability etc. Employing cloud computing in smart grids, addressing issues of information management with high energy and cost saving [5].

III. FRAME WORK FOR THE PROPOSED SYSTEM

A framework should be more flexible, Scalable and secure. The idea is to build the three hierarchical levels. The first two levels are responsible for the system maintenance, Overall management of the devices. The last level is the end-users device.

The two levels are responsible to manage all devices and accumulation of data in regional level. The regional level is to manage and process data in these devices. A security solution is provided with the help of Identity Based Encryption and Signature and Identity Based proxy re-encryption. This is done to provide security to the information in smart grid. For the encryption keys or signature verification keys, the top, regional, and end user level are to be represented with their identities.

The entities in low level will use the identities in the higher level to encrypt the data. This is done to provide security.

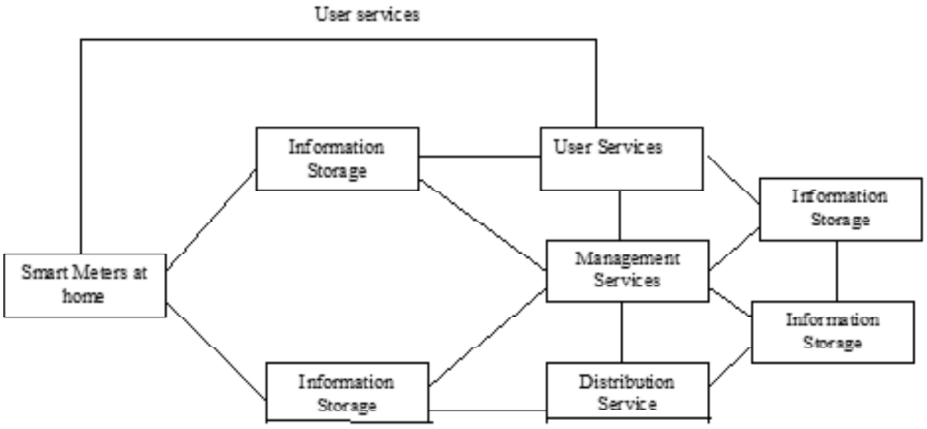

Figure 3: Fuction cloud computing centers

(A) Architecture

Information management should be done along with the security solution. To provide security, first is to build a hierarchical structure of cloud computing centers. The second step is to provide security with the help of identity-based encryption, signature and proxy re-encryption.

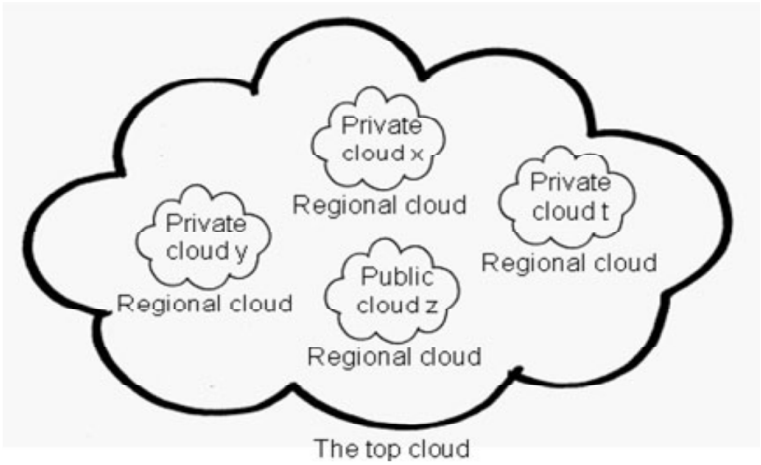

Figure 4: Architecture of Smart Frame

The services which are done by the smart frame in each level are as follows:

Information storages

They store all the information from smart grid which are received from front-end devices. It is designed in a way to accept all the information from different transportation modes.

General user services

This service will include all the electricity user needs to use. Most of Saas will come under this type of services.

Control and management services

This service includes all the system management services. Some of them are task scheduling, monitoring governance, security solution.

Electricity distribution services

All kinds of services which are related to electricity distribution will fall under these services. Some of them are, optimization, quality of service, distribution management.

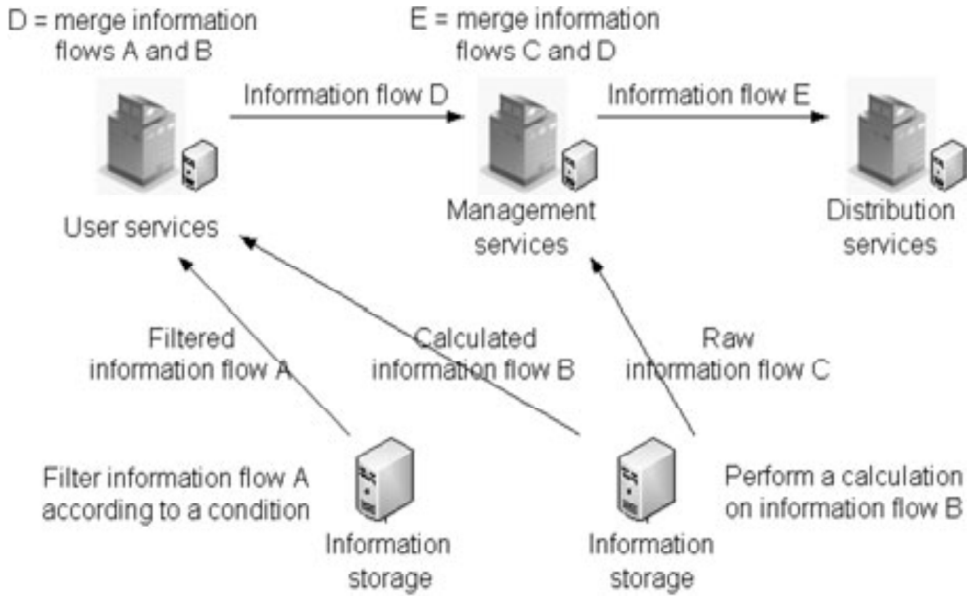

Figure 5: Information Flow

(B) Information flow

To manage huge amount of data in smart grid, it is necessary to manage information flows. In Smart-Frame, a centralized service is kept to manage all the information flows. It takes input of the information requested from service clusters and also from, general statistics from information storages. With the help of these inputs the service generates information flow schedule, which specifies source and destination of information flow.

IV. SECURITY SOLUTION FOR SMART FRAME

(A) Identity Based Encryption

Identity Based cryptosystem is used to eliminate the requirements of checking validity of certificates by using public key infrastructure. In a Identity Based Encryption Scheme, The private key generator (PKG),

a trusted party, generates secret master key (mk) and public parameters. Once a receiver submits his/her identity (IDrec), the PKG computes the private key (KIDrec).

Once a receiver submits his/her identity (IDrec), the PKG computes the private key (KIDrec). IDrec can be any string such as e-mail address, phone number etc. It is done by user. First the users will authenticate themselves to PKG and users to prevent eavesdropping. If any sender uses IDrec to encrypt a plain text message M into C by using Encrypt algorithm. Upon receiving C, the receiver will decrypt by using Decrypt algorithm, with the help of KID rec.

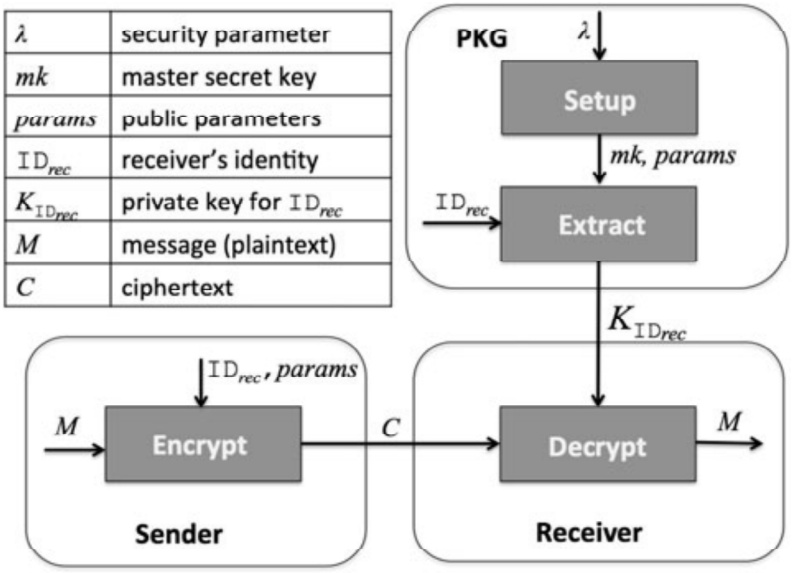

Figure 6: Identity based encryption

Identity Based cryptosystem is used to eliminate the requirements of checking validity of certificates by using public key infrastructure. In a Identity Based Encryption Scheme, The private key generator (PKG), a trusted party, generates secret master key (mk) and public parameters. Once a receiver submits his/her identity (IDrec), the PKG computes the private key (KIDrec).

Once a receiver submits his/her identity (IDrec), the PKG computes the private key (KIDrec). IDrec can be any string such as e-mail address, phone number etc. It is done by user. First the users will authenticate themselves to PKG and users to prevent eavesdropping. If any sender uses IDrec to encrypt a plain text message M into C by using Encrypt algorithm. Upon receiving C, the receiver will decrypt by using Decrypt algorithm, with the help of KID rec.

(B) Identity Based Signature

In identity-based signature [6] ,the signer has to submits his/her identity IDsig, the PKG then computes the private key KIDsig associated with IDsig using the Extract with master secret mk. Using KIDsig , the signer can sign a message M to create a signature s by running the Sign algorithm. When providing the message M, the signer's identity IDsig, and the signature s, any party can verify whether the signature s is valid one or not.

(C) Identity Based Porxy Re-Encryption

In a proxy-encryption, a proxy is transformed to a cipher text produced by Alice public key and the same way it can be decrypted by Bob's private key. To achieve efficiency better than decrypt and encrypt algorithm. Proxy re-encryption is first introduced by Mambo and Okamoto [7]. Later, Green and Ateniese's [8] identity-based proxy re-encryption, is related to the smart frame. In this scheme, a delegator allowed a proxy to get

transformed under Alice's identity into alone encrypted under Bob's identity .Then proxy uses re-encryption keys to conduct transformation without the knowledge of the plain text.

Also, no information about the private key of Alice and Bob can be deduced from re-encryption key.

V. EXPERIMENTAL RESULT

In a real time environment managing the data at a single server is not much efficient when compared to cloud based storage. When implementing smart meter in the real time, the data which comes from them are huge when compared to normal meter data. Also, the data to be retrieved for the end users purpose takes much time for the data to reach the destination.

Thus, for the cloud computing centers in which three hierarchical levels are maintain to manage information. The data is stored under top, regional and bottom levels. Here, the top level is for management of data in regional and end user level. The regional level will maintain all the connection and disconnection process along with the user level. In user level, only the user data such as their personal information are saved.

Now comparing the both data retrieval rate of physical server and the cloud based storage of three hierarchical levels we achieving a fast retrieval rate. The below graph shows the comparison between the two servers retrieval rate.

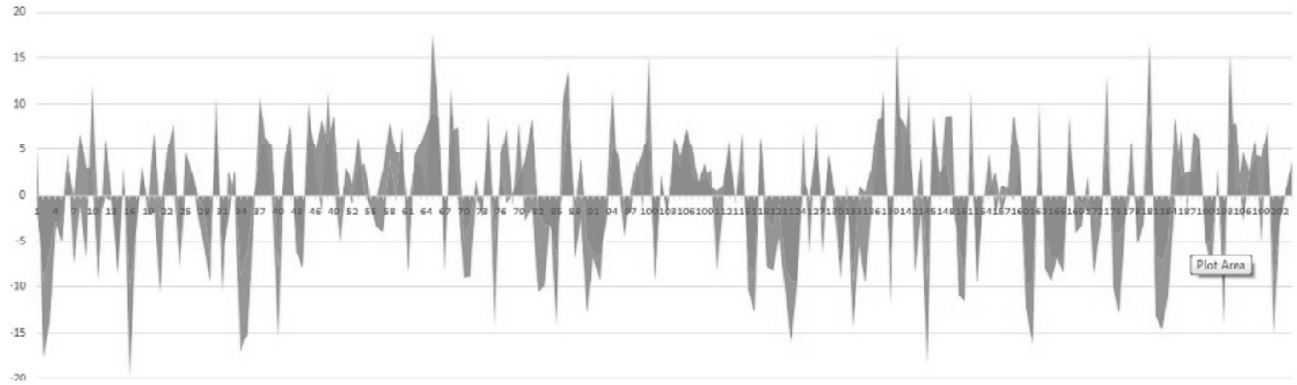

Figure 7: Comparition graph for the retrival of data

VI. CONCLUTION & FUTURE WORK

Thus the framework for big data information management is designed. The three levels of cloud computing centers are done i.e., top, regional and end-user level. The security for the information is provided with the help of identity based proxy encryption, identity based proxy re-encryption. In proposed, the bill amount will be calculated on particular date of recording the reading. To make comfort for the users and to avoid unnecessary problems, the idea is to predict the bill amount earlier according to the amount of energy they consumed for a month. Thus, future work is to make a big data analysis of the smart meter data and also to predict the bill previously. By providing an approximate amount prior the users will be benefited.

REFERENCES

[1] K. P. Birman, L. Ganesh, and R. V. Renesse, "Running smart grid control software on cloud

[2] computing architectures," in Proc. Workshop Comput. Needs Next Generation Electric Grid, 2011, pp. 1–33.

[3] H. Li, R. Mao, L. Lai, and R. Qiu, "Compressed meter reading for Delay-sensitive and secure load report in smart grid," in Proc. 1s Int. Conf. Smart Grid Commun., 2010, pp. 114–119.

[4] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Commun. Survey Tutorials, vol. 15, no. 1, pp. 21–38, Jan. 2012.

[5] B. Hayes, "Cloud computing," Commun. ACM, vol. 51, no. 7, pp. 9–11, 2008.

[6] M. Mambo and E. Okamoto, "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. E-80, no. 1, pp. 54–63, 1997.

[7] M. Mambo and E. Okamoto, "Proxy cryptosystems: Delegation of the power to decrypt ciphertexts," IEICE Trans. Fundam. Electron.

[8] A. Shamir "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO Adv. Cryptol., 1984, vol. 196, pp. 47–53.

[9] J. Baek, Q. Vu, A. Jones, S. Al-Mulla, and C. Yeun, "Smart-frame: A flexible, scalable, and secure information management framework for smart grids," in Proc. IEEE Int. Conf. Internet Technol. Secured Trans., 2012, pp. 668–673.

[10] H. Farhangi, "The path of the smart grid," IEEE Power Energy Mag., Jan./Feb. 2010, pp. 18–28.

[11] J. Duff, "Smart grid challenges," in Proc. Workshop High Perform. Trans. Syst.,2009, [Online]. Available: *http:// www.hpts.ws/ papers/2009/session4/duff.pdf*

[12] H. Farhangi, "The path of the smart grid," IEEE Power Energy Mag., Jan./Feb. 2010,pp. 18–28.

[13] D. Galindo and F. Garcia, "A Schnorr-like lightweight identitybased signature scheme," in Proc. 2nd Int. Conf. Cryptol. Africa,2009, pp. 135–148.

[14] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inf. Security: Adv. Cryptol., 2002, pp. 548–566.

[15] S. Rusitschka, K. Eger, and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in Proc. 1st Int. Conf. Smart Grid Commun., 2010, pp. 488.

[16] K. P. Birman, L. Ganesh, and R. V. Renesse, "Running smart grid control software on cloud computing architectures," in Proc. Workshop Comput. Needs Next Generation Electric Grid, 2011, pp. 1–33.

[17] Z. Bojkovic and B. Bakmaz, "Smart grid communications architecture: A survey and challenges," in Proc. 11th Int. Conf. Appl. Comput. Appl. Comput. Sci., 2012, pp. 83–89.

[18] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, vol. 2139, pp. 213–229.

[19] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "A trust system architecture for SCADA network security," IEEE Trans. Power Delivery, vol. 25, no. 1, pp. 158–169, Jan. 2010.

[20] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in Proc. 1st Int. Conf. Smart Grid Commun., 2010, pp. 238–243.

[21] H. Farhangi, "The path of the smart grid," IEEE Power Energy Mag., vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[22] D. Galindo and F. Garcia, "A Schnorr-like lightweight identitybased signature scheme," in Proc. 2nd Int. Conf. Cryptol. Africa, 2009, pp. 135–148.

[23] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. 5th Int. Conf. Appl. Cryptograph. Netw. Security, 2007, pp. 288–306.

[24] S. Zeadally, A. Pathan, C. Alcaraz, and M. Badra, "Towards Privacy Protection in Smart Grid", In Wireless Personal Communications, 2012,pp. 1-28.

[25] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," Comput. Netw., vol. 55, no. 15, pp. 3604–3629, 2011.

[26] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," IEEE Trans. Power Delivery, vol. 57, no. 5, pp. 1344– 1371, Apr. 2013.

[27] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in Proc. Eur. Conf. Innovative Smart Grid Technol., 2010, pp. 1–7.

[28] T. Zhang, W. Lin, Y. Wang, S. Deng, C. Shi, and L. Chen, "The design of information security protection framework to support smart grid," in Proc. Int. Conf. Power Syst. Technol., 2010, pp. 1–5.

[29] M. Shargal and D. Houseman, "The big picture of your coming smart grid," Smart Grid News, Mar. 2009. (Online). Available: *http://www.smartgridnews.com/artman/publish/commentary /The_Big_Picture_of_Your_Coming_Smart_Grid-529.html*

[30] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186, Jul.–Dec. 2013.