RESEARCH ARTICLE OPEN ACCESS

Smart Grid of Big Data Information Management on Secure Cloud Computing Framework

[1]Sakthivel P., [2]Sajeevram.M.E.,
[1]PG Student, Department Of Computer Science and Engineering,
[2]AP, Department Of Computer Science and Engineering
School of Engineering, Vels University, Chennai, India.

Abstract:

Smart grid is a modern electrical grid technology that improves the efficiency and reliability. The main challenges of smart grids are how to manage different types of front-end intelligent devices such as smart meters and how to process a huge amount of data received from these devices. Cloud computing, a technology that provides computational resources on demands to address these challenges. It has several good properties such as energy saving, cost saving, scalability, and flexibility. The project has propose a secure cloud computing based framework for big data information management in smart grids, which called as "Smart-Frame" present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

Keywords — ***Smart Grid,*** **Smart Frame, Secure Cloud frame work, Encryption, Decryption**

I INTRODUCTION

An electric grid with the information and communications technology (ICT) is called a Smart Grid. To introduce a design of Smart-Frame, a flexible, scalable, and secure information management framework for smart grids based on cloud computing technology.

The basic idea is to build the framework at three hierarchical levels: top, regional, and end user levels in which the first two levels consist of cloud computing centers while the last level contains end-user smart devices. Providing information security for smart grids is very important since much of the information in smart grids is sensitive and needs to be strictly protected. Information leakage in smart grids can lead to vulnerabilities that affect not only individuals but also the whole nation because leaked information can be used to launch attacks to both individuals and the whole smart (power) grids.

II RELATED WORK

Review the related work about smart grid information management , smart grid security management, and finally the basics of identity- based encryption and proxy re-encryption schemes respectively.

III LITERATURE SURVEY

Janina POPEANGĂ

Increasing concern about energy consumption is leading to infrastructure that supports real-time, two-way communication between utilities and consumers, and allows software systems at both ends to control and manage power use. To manage communications to millions of endpoints in a secure, scalable and highly-available environment and to achieve these twin goals

of 'energy conservation' and 'demand response', utilities must extend the same communication network management processes and tools used in the data center to the field. This paper proposes that cloud computing technology, because of its low cost, flexible and redundant architecture and fast response time, has the functionality needed to provide the security, interoperability and performance required for large-scale smart grid applications.

2.2 Xi Fang, Satyajayant Misra, Guoliang Xue, Dejun Yang

Smart Grid (SG), regarded as the next generation electric grid, will use advanced power, communication, and information technologies to create an automated, intelligent, and widely distributed energy delivery network. In this article, we explore how Cloud Computing (CC), a next-generation computing paradigm, can be used for information management of the SG and present a novel SG information management paradigm, called Cloud Service based SG Information Management (CSSGIM). We analyze the benefits and opportunities from the perspectives of both the SG domain and the CC domain. We further propose a model for CSSGIM and present four motivating applications.

2.3 Reeshma K, Anjali S, Thota Subhashini

The financial resources are finite, but our computational needs are infinite. The demand for computational recourses keeps on increasing indefinitely, whatever the availability of resources, the need for „more „remains. Here the cloud plays its role, Cloud computing gets its name as a metaphor for the internet .Typically, the internet is represented in the network diagram as a cloud. The cloud icon represents "all that other stuff "that makes the network work. Many organizations are slowly shifting towards the use of Cloud computing, because Cloud computing promises to cut operational and capital cost and more importantly let IT departments focus on strategic projects instead of keeping the datacenter running. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers, but these providers may beuntrusted.To ensure the security and correctness of user‟s data in the cloud, this paper proposes a new paradigm for data Security in cloud computing.

2.4 Xi Fang, Dejun Yang and Guoliang Xue: Smart Grid (SG) is a power system with advanced communication and information technologies integrated and leveraged. In this paper, we study an optimization problem of leveraging the cloud domain to reduce the cost of information management in the SG. We propose a cloud-based SG information management model and present a cloud and network resource optimization framework to solve the cost reduction problem in cloud-based SG information storage and computation.

2.5 Berthold Bitzer

In the past power system is evolved through different restructuring and policy changes at different periods. From the early stage of state owned monopoly energy providing service to smart grid driven customer and third party aggregators' participation in order to cope up to the ever growing energy demand in terms of capacity as well as the dynamics of end user consumption, demand side management, different energy generation systems and demand response.

In this process information communication and computation systems are playing a major role in monitoring, controlling and improving the energy delivery system. In smart grid a vast amount of data is collected from every corner of the energy delivery network, from customer energy meters, energy generation units in the customer premises and third party players.

This bi-directional information flow needs appropriate communication ways and the collected vast amount of data has to be processed in a reliable, distributed, parallel and scalable computing resources. On the other hand the power system is lacking such computing capacity to address this requirement.

Researchers suggest that cloud computing may be used to address this problem. In this paper the application of cloud computing for power system application is analyzed. The feasibility study of the available cloud computing tools for smart grid is conducted.

IV METHODOLOGY

Methodologies are the process of analyzing the principles or procedure . The following are the five modules involved in the paper.

1. User Services

2. Integrating with cloud and Grid

3. Collect User Electricity Data

4. Store and manage Grid

5. Service Distribution

1. User Services:

Home user can get the services from the trusted person or society. They will provide an authentication for sending the data. New User can register details in power Station.

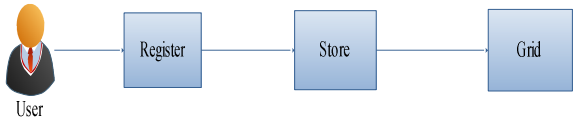

Fig.1 User Services

2. Integrating cloud with Grid:

A grid is a main role our project, it's deployed in a cloud storage. Because cloud is more secure and data manipulation is efficient.

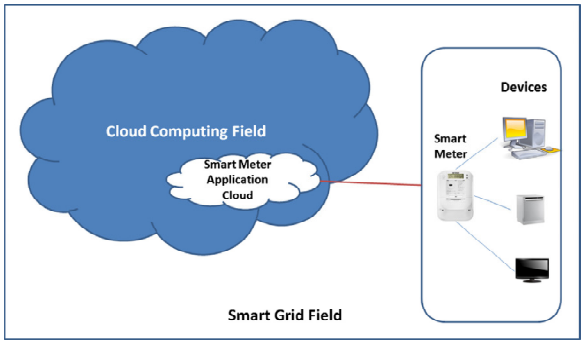

Fig2. Cloud Smart Meter Architecture

3. Collect User Electricity Data:

This module is used to collect the electricity readings from each user and store all information in grid. Each user's readings can be sending to grid via mobile towers.

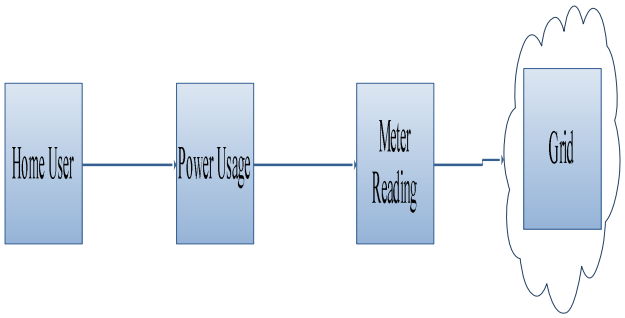

Fig.3 User data collection

4. Store and manage Grid:

The grid maintains overall power supply information and every user's power consumption readings. Grid stores the overall power supply details which is provided by power Live. Grid maintains each and every power station's power consumption records. Grid identifies the different power station's details by unique ID.

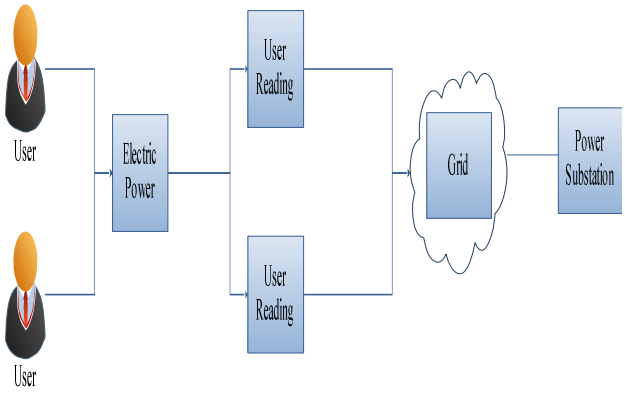

Fig.4 Grid Management

5. Service Distribution:

Finally the Grid can compare the overall supply which is given by power live and overall demand which is manipulated using user's readings. After the comparison the grid can generate a report for supply and demand then send the demand request report to power Live.

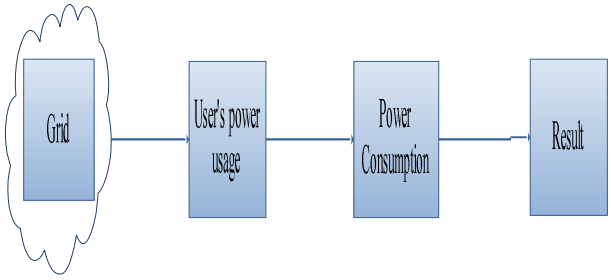

Fig.5 Service Distribution

V ARCHITECTURE DIAGRAM

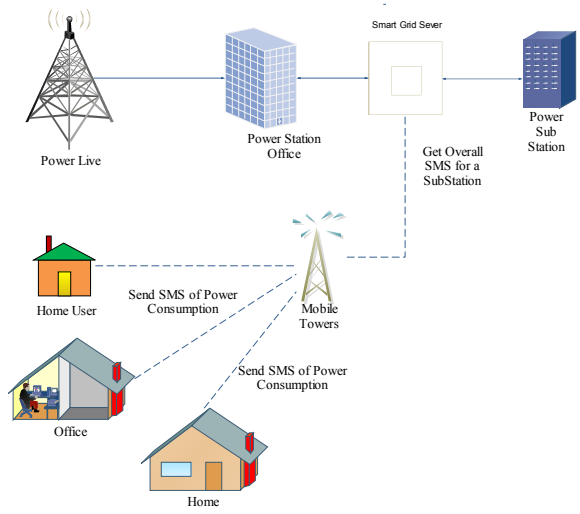

Fig.6 Architechture Diagram

Smart grid information management consist of three basic tasks such as information gathering, information processing, and information storing. For information gathering smart grids have to collect information from heterogeneous devices at different locations. The main research challenge is to build efficient communication architecture.

VI SYSTEM ARCHITECTURE:

The overall architecture of the Smart-Frame is shown in the figure. In this architecture, a smart grid can be divided into several regions each of which is managed by a cloud computing center that can be setup from either a public cloud or a private cloud. The role of a regional cloud computing center is to manage intelligent devices in the region as well as to provide an initial processing for information received from these devices. Besides regional cloud computing centers, there is a special cloud computing center at the top level, which is in charge of managing and processing data for the whole grid. In each of these cloud computing centers, the following cloud computing services could be deployed: Infrastructure-as-a-service (IaaS): This type of service forms the backbone of the system. Main tasks of information management in smart grids such as information gathering, information processing, and information storing, are all executed inside this layer of service. Software-as-a-service (SaaS): While IaaS is the backbone of the system, all smart grid services will be deployed as SaaS at the top of the system. Examples include services that allow customers to save or optimize their energy usage such as smart Meter. Platform-as-a-service (PaaS): PaaS provides tools and libraries to develop cloud computing applications and services. Salesforce is a typical PaaS example, which provides libraries to develop some specific types of applications in saleforce or fieldforce domains. In smart grid domain, since a number of applications could be required to follow special security requirements and have to allow lawful interceptions, it is useful to have a general PaaS that has already integrated these requirements to implement applications.
Data-as-a-service (DaaS): DaaS could be deployed to provide useful information for statistics purpose. Since smart grid data is often extremely large, it is useful to provide such statistics services for users. Statistics can be used for optimization purposes. Not only electricity users but also electricity providers at different levels.

Security Solution for the Smart Grid in Cloud framework:

Security is the major challenges in the smart grid in cloud computing system due to its nature of outsourced computing. Mainly, confidentiality, integrity and authentication are the primary pain areas. Identity-Based encryption and proxy re-encryption standards are the good solution to address the security issues in the smart grid in Cloud framework.

Identity-Based Encryption (IBE) provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number. The corresponding private key can only be generated by a Private Key Generator (PKG) who has knowledge of a master secret. Using this construct, anyone can encrypt messages or verify signatures without prior key distribution beyond the dissemination of public parameters and the public key "strings." This is useful where the deployment of a traditional certificate authority-based PKI is inconvenient or infeasible, as IBE-based systems do not require certificate management, eliminating the need for certificate lookups and complex certificate revocation schemes. A central operational consideration of Identity-Based Cryptography is that private keys must be obtained from the PKG. It obtains this private key is essential to the security of the supported system. For example, how the PKG decides who should be given the private key associated with an email address

is crucial to maintaining the integrity of the system. Another consideration is cost: key generation can be computationally expensive. To ease the computation burdens of PKG operation, hierarchical IBE (HIBE) can be used to reduce the overload of a root PKG by replicating private key generation to slave PKGs.

In 1984, Shamir introduced the concept of identity-based cryptography to ease the certificate management in traditional public key system. A user's public key in an IBE scheme is the identity information of the user 1This paper is a revised and extended vision of conference proceedings submitted (e.g., email address). Hence the public key is implicit authenticated and the certificate management is simplified. However, the practical IBE scheme was only proposed 17 years after its concept was proposed. However, one part of the private key in all these IBE schemes is of the form: y=f (msk) where msk is the master key and y is an element in the underlying bilinear group G. The proxy re-encryption(PRE) has been proposed by Blaze et al. in 1998, which allows a semi-trusted proxy, with some information (a.k.a., the re-encryption key), to translate a cipher text under the delegator's public key into another cipher text can be decrypted by the delegatee's secret key. However, the proxy cannot access the plaintext. According to the direction of transformation, PRE schemes can be classified into bidirectional schemes and unidirectional schemes. Also according to the times the transformation can apply on the cipher text, PRE schemes can be classified into single-hop schemes and multi-hop schemes. Proposed a few unidirectional PRE schemes and discussed its several potential applications such as distributed secure systems. Later, many unidirectional PRE schemes with properties have been proposed Due to the simpler certificate management in IBE , extended PRE to the IBE setting, i.e. identity based proxy re-encryption (IBPRE). They also discussed its several interesting applications such as bridging IBE and PKE . Since then, several IBPRE schemes have been proposed, but none of them except can achieve master secret secure: the corrupted proxy and delegate cannot derive the delegator's private key. However, IBPRE schemes in are generic constructions relying on CCA-secure 2-level hierarchical ID-based threshold cryptosystem, IBPRE schemes in rely on conditional proxy broadcast re-encryption, only achieve secure against replayable chosen cipher text attacks (RCCA).

Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID.

As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must

obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt (or sign) messages without authorization. Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow. A number of variant systems have been proposed which remove the escrow including certificate-based encryption, secure key issuing cryptography and certificate less cryptography.

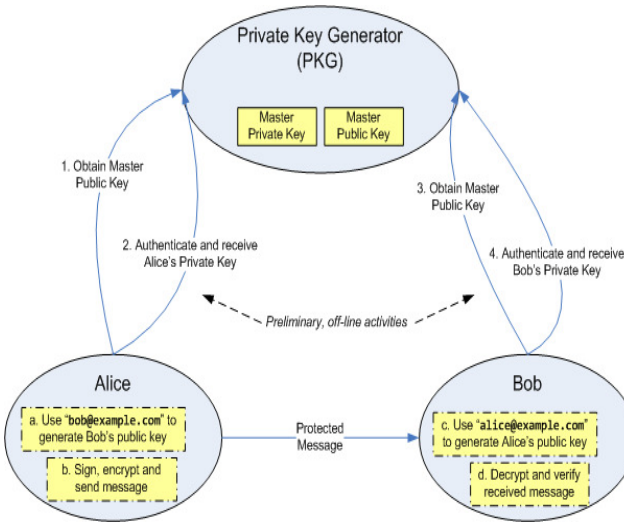

Fig.7 Identity based encryption

Setup: This algorithm is run by the PKG one time for creating the whole IBE environment. The master key is kept secret and used to derive users' private keys, while the system parameters are made public.

The proposed proxy re-encryption scheme consists of five algorithms, namely KeyGen, ReKeyGen, Enc, ReEnc and Dec.

KeyGen. On input the security parameter, outputs the public keyof each group and the corresponding private keyfor each member.

ReKeyGen. On input two private keyand, outputs a unidirectional re-encryption key.
Enc. On input message and a public key, outputs a cipher text.
ReEnc. On input cipher text and the re-encryption key, outputs a cipher text or an error symbol.
Dec. On input cipher text and a private key, outputs the corresponding message.

VI I CONCLUSION

This project introduced the Smart-Frame, a general framework for big data information management in smart grids based on cloud computing technology. The basic idea is to set up cloud computing centers at three hierarchical levels to manage information: top, regional, and end-user levels. While each regional cloud center is in charge of processing and managing regional data, the top cloud level provides a global view of the framework. Additionally, in order to support security for the framework, presented a solution based on identity-based cryptography and identity-based proxy re-encryption. As a result, The proposed framework achieves not only scalability and flexibility but also security features.

RESULT AND DISCUSSION

In our future enhancement will show the peak hour and Normal Hours charges. It will help us to save the huge amount of electricity. Normal Hour is nothing but in our home we do not use most electrical appliances in mornings. So the cost will be less as if we compared to the peak hour. In peak hours it is nothing but at night time were all users or people use many electrical appliances such as Air Conditioners , Fans,

etc. So the charges will be a huge amount as if we compare to the Normal Hours. The power Supply will be high at Night Times. And Other Enhancements are The power are given to the Districts. If any particular Districts uses more than the given supply. It will give a suggestion that if any district has unused Power it will display to the district who has exceeded the power supply. Further future enhancements are Smart card implementation to the smart meters and meter reading automations over the internet.

REFERENCES

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Security, vol. 9, no. 1, pp. 1–30, 2006.

[2] 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.

[3] A. Bartoli, J. Hernandez-Serrano, M. Soriano, and M. Dohler, "Secure lossless aggregation for smart grid M2M networks," in Proc. IEEE Conf. Smart Grid Commun., 2010, pp. 333–338.

[4] 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. Fig. 8. Basic processes for encryption and description in the Smart-Frame. 242 IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 2, APRIL/JUNE 2015

[5] 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.

[6] 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.

[7] IEC 61850: Communication Networks and Systems in Substations, IEC 61850. Dec. 2013.

[8] C.-K. Chu, J. K. Liu, J. W. Wong, Y. Zhao, and J. Zhou, "Privacypreserving smart metering with regional statistics and personal enquiry services," in Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Soc., 2013, pp. 369–380.

[9] X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," Int. J. Appl. Cryptograph., vol. 1, no. 1, pp. 3–21, 2008.

[10] 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.

[11] R. Davies, "Hydro one's smart meter initiative paves way for defining the smart grid of the future," in Proc. Power Energy Soc. Gen. Meeting, 2009.

[12] S. Rogai, "ENEL Telegestore Project," Economic Commission for Europe, Committee on Sustainable Energy, Steering Committee of the Energy Efficiency 21, Ad Hoc Group of Experts on Energy Efficiency, Investments for Climate Change Mitigation, Eighth meeting, Geneva, 31 May 2006. [Online]. Available at

http://ww.unece.org/fileadmin/DAM/ie/se/pp/adhoc/adhoc8May06/2_Rogai.pdf.

[13] 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.