IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

A Secure Cloud Computing based Framework for Big Data Information management of smart Grids

Vandesh Goyal[1], Rishika Movva[2], Alekya Kunadharaju[3]

Student, Computer Science and Engineering, SRM University, Chennai[1,2,3]

Abstract: A smart grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users It possesses demand response capacity to help balance electrical consumption with supply. It is pointed out that there are tenacious economic as well as environmental urgings for the refurbishment of the conventional power systems, and its replacement with a Smart Electrical Power Grid or simply Smart Grid. The main challenges of smart grids, however, are how to manage different types of front-end intelligent devices such as power assets and smart meters efficiently; and how to process a huge amount of data received from these devices. Smart grid is an electric grid which includes a variety of operational and energy measures including smart meters, smart appliances which are used to measure the power consumption of those devices, and it consists of renewable energy resources, and energy efficiency resources which can be used by those devices. In this paper, we propose a cloud computing based framework for big data information and 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, Big Data, Cloud Computing, Information Management, Smart Frame, Security.

I. INTRODUCTION

A. Big Data and Smart Grids

A smarter grid applies technologies, tools and techniques available now to bring knowledge to power and knowledge capable of making the grid work far more efficiently ensuring its reliability to degrees never before possible maintaining its affordability, reinforcing our global competitiveness, fully accommodating renewable and traditional energy sources, potentially reducing our carbon footprint, introducing advancements and efficiencies yet to be envisioned. When compared to normal electrical power grids, smart grids are proving to be the best solution for metering the electrical usage by the users. Smart Grid is a generic label for the application of computer intelligence and networking abilities to the existing dumb electricity distribution systems.

Smart Grids are being launched in many countries but they are often limited to smaller regions this is because of certain challenges that are being faced by Smart Grids to be launched on larger regions. The main challenge for the Smart Grid to be launched on a larger region is the information management that is related to information gathering, information storing, and information processing. Since there are a large number of front-end intelligent devices, managing a huge amount of information received from these devices is not an easy task.

As there are a large number of front end devices there are many chances for the information to be delayed when the user requests. So there should be a proper framework or a structure in which the information has to be handled well so that that the information will be easily accessible.

B. Cloud Computing based Framework

Cloud computing is the latest distributed computing paradigm and it offers tremendous opportunities to solve large-scale scientific problems. It has become popular recently due to several advantages over traditional computing models. It has been expected to be a dominant computing model in the future. By employing cloud computing in smart grids, we not only address the issue of large information management but also provide a high energy and cost saving platform. Cloud computing is naturally a good fit for storing and processing the big data.It is because the framework can scale very fast to deal with changes in the amount of processing information and also It can provide a high utilization of computing resources and also makes the resources available at low cost. This framework enables for easy access of the data whenever required.

C. Proposed Framework

We introduce a design of Smart-Frame, based on cloud computing technology. Our 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. The top cloud computing center takes responsibility of managing general devices and accumulation of data across the regional cloud computing centers which are placed in

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

the lower level in the hierarchy. The regional cloud computing centers are in turn in charge of managing intelligent devices, which have lower hierarchical level than the regional cloud computing centers in specific regions.
A Smart-Frame, a cloud computing based framework for data information management in application, which provides not only flexibility and scalability but also security features. We present a security solution for the proposed framework based on identity-based encryption and proxy re- encryption schemes, which provides secure communication services for the Smart-Frame. We further implement the prototype of our proposed solution to show its practicality.
1) The general architecture of the Smart-Frame.
2) Deals with its security issues and proposed a solution based on identity-based cryptography and proxy re-encryption techniques.

II. SMART GRIDS

A. Smart Grid Information Management
A huge amount of data are received to a Smart Grid. That information is very complex, and the data processing over those data is inadequate. It is not an easy task to manage these set of data, which includes selection, monitoring, and analysis of smart grid data. So here we introduce a module which is the solution for the data management. There are many challenges while processing data in big data include analysis, capture, search, sharing, storage, transfer, visualization, and information privacy. In real time, information processing is very difficult and it is required by smart grid. Delay in information processing may cause serious sequences to the whole system. To make use of those data effectively and efficiently across the globe, we go for cloud computing technology where the information from those smart devices is maintained in cloud storage.
Smart Grid information management usually involves three basic tasks.
1) Information gathering
2) Information processing
3) Information storing

For information gathering, since smart grids have to collect information from heterogeneous devices at different locations, the main research challenge is to build efficient communication architecture. In order to make full use of computing resources, and to satisfy the need of smart grid for reliable storage and effective management of overall information, a construction method for information platform of smart grid based on cloud computing is proposed. In addition, based on the analysis of feasibility, advantages and problems of the new method, the architecture of information platform is given. Furthermore, considering the characteristics of condition monitoring of smart grid, the cloud computing platform based on Hadoop for condition monitoring of smart grid is proposed. To implement reliable storage and fast parallel processing of massive data, such crucial problems as virtualization, distributed storage and parallel programming model of MapReduce have further been researched. To process a large amount of data efficiently still remains as a big challenge. Cloud computing appears to meet this demand and also satisfy challenges of information storing. The architecture of smart grid using sensor networks is as below,

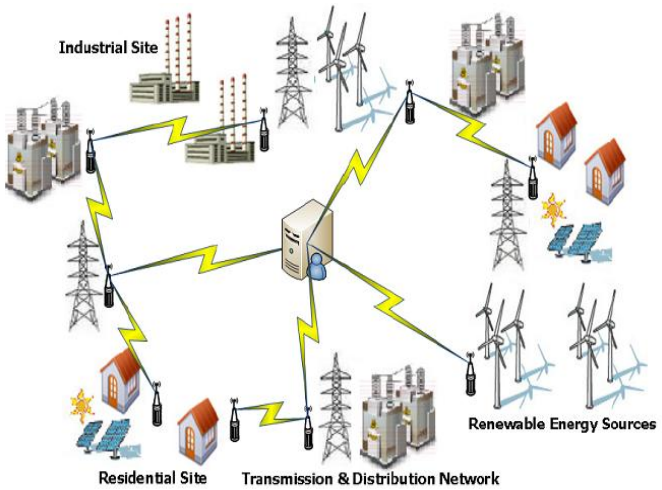

Fig. 1 Architecture of the Smart Grid

The difference between this optimized cloud model and the general cloud resource optimization is the following. First, our optimization framework is designed based on our novel cloud-based Smart Grid information management model,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

which takes into account the requirements of actors in the Smart Grid and resources provided by cloud providers and networking providers. Second, even from the perspective of general cloud resource optimization, our work is novel, since our cloud model is designed based on novel computation flow structures and aims to optimize the cost and information flow in multiple domains.

B. Various Security approaches applicable for Smart Grid
When large data is being handled by several clusters in a Smart Grid it has to be managed well for better access whenever needed and also has to be secured so that the unauthorised users will not have access to the data and misuse it. So security is an important aspect that has to be maintained on the information in the Smart Grid. There can be many ways by which the unauthorised users can access the data that is either through the data clouds or the information storages or the transmission networks/lines so, we need to provide security to the data in every way possible. The various security approaches that can be applicable on a Smart Grid are identity-based encryption, identity-based signature, and proxy re-encryption schemes.

1) Identity Based Encryption (IBE) : Identity-based encryption, is an important primitive of Identity-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user. One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. This can take place because this system assumes that, once issued, keys are always valid (as this basic system lacks a method of key revocation). The majority of derivatives of this system which have key revocation lose this advantage.

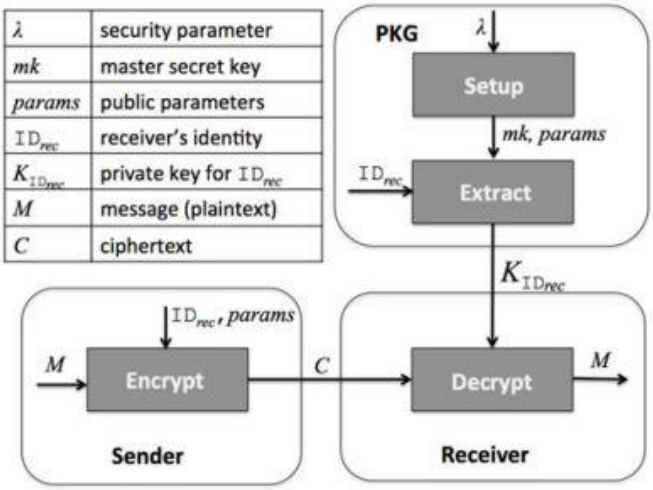

Fig. 2 Identity based Encryption Scheme

In an identity-based encryption scheme, the private key generator (PKG), a trusted party, first generates secret master key mk and public parameter params. Note that params, which is long-term, will be given to every party that is involved. Once a receiver submits his/her identity, denoted by IDrec, the PKG computes the private key KIDrec associated with IDrec by running the private key extraction algorithm Extract providing its master secret key mk as input. Here, the identity IDrec can be any string certificates issued in normal public key cryptography: Users such as an email address, a telephone number, etc. Note that the distribution of the private keys can be done in a similar way as digital would authenticate themselves to the PKG and obtain private keys associated with their identities. Secure channel may have to be established between the PKG and the users depending on the situation to prevent eavesdropping. Now any sender who is in the possession of IDrec, encrypts a plaintext message M into a cipher text C by running the Encrypt algorithm. Upon receiving C, the receiver decrypts it by running the Decrypt algorithm providing the private key KIDrec obtained from the PKG previously as input.

2) Identity Based Signature (IBS) : The first implementation of identity-based signatures and an email-address based public-key infrastructure (PKI) was developed by Adi Shamir in 1984, which allowed users to verify digital signatures using only public information such as the user's identifier. Under this scheme, a trusted third party would deliver the private key to the user after verification of the user's identity, with verification essentially the same as that

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

required for issuing a certificate in a typical PKI. 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.

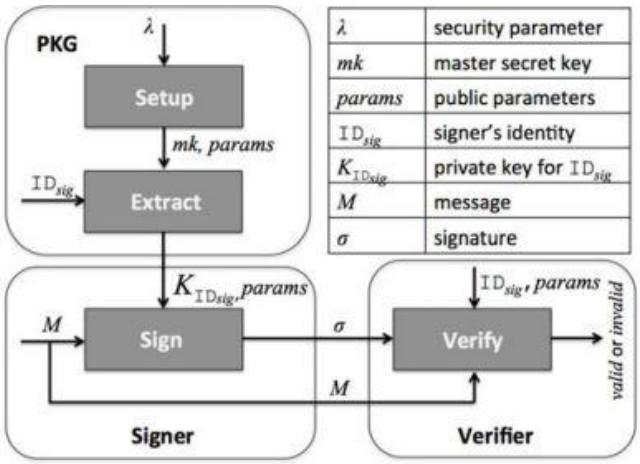

Fig. 3 Identity based Signature Scheme

When the signer submits his/her identity IDsig, the PKG computes the private key KIDsig associated with IDsig by running the Extract with the master secret mk. Using KIDsig, the signer can sign a message M to create a corresponding signature s by running the Sign algorithm. Providing the message M, the signer's identity IDsig, and the signature s, any party (verifier) can verify whether the signature s is valid one or not.

3) Identity Based Proxy Re-Encryption : Proxy re-encryption lets a proxy to transform a cipher text produced under Alice's public key in such a way that the transformed cipher text can be decrypted under another party Bob's private key. The concept of proxy re-encryption was first introduced by Mambo and Okamoto whose main goal was to achieve efficiency better than "decrypt and-encrypt" approaches. Identity based proxy re-encryption combine the two functionalities of IBE and proxy re-encryption without compromising the security.

III. SMART FRAME

A Smart Frame was the proposed framework for better performance in the cases of information management and the security solution for the information stored in the different levels of clouds and while transmitting the information between the end users and the clouds or between the main electricity distribution unit and the clouds, so, basically securing the information present in all the components of a smart grid.

A. General Architecture of Cloud Based Information Management System of a Smart Frame
The overall architecture of the Smart-Frame is shown in the figure below,

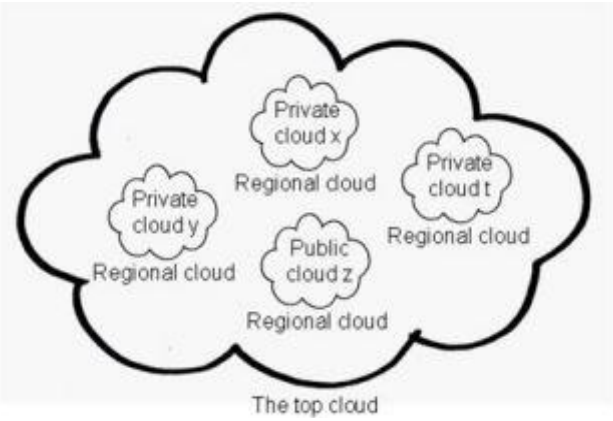

Fig. 4 Smart Frame Cloud Clusters

DOI10.17148/IJARCCE.2017.6610

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

In the architecture of the Smart-Frame there are several regions which are managed by the cloud computing center. The clouds in which the information is being stored can either be a public cloud or a private cloud and this is chosen in relevance to the data that is being stored and the authentication standards. 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. As the data is being stored in various clouds and is being assisted by cloud computing it provides the end users with several kinds of services such as Platform-as-a-service, Software-as-a-service, Data-as-a-service and Infrastructure-as-a-service.

As the data is being managed and shared between several clouds there should be a proper flow of the information in order to avoid the delay in providing the information or a condition where the users will be waiting for the data which will never be released unknowingly. So the Information flow has to be managed by a centralised service which takes care of the information flow in the entire smart grid for faster response times to the users and ease of access to the data. This service takes inputs as both information requests from service clusters and general statistics (e.g., the amount of information, time of arrival) from information storages. Using these inputs, the service generates an information flow schedule, which specifies sources and destinations of information flows as well as how they are processed (e.g., which specific operators are applied on information flows and where they are applied).

B. Security Approaches provided by the Smart-Frame

As we know there are three types of security approaches for the Smart-Frame that is Identity Based Cryptography under which we have Identity Based Encryption Scheme and Identity Based Signature Scheme, Identity Based Proxy Re-encryption Scheme. There is way by which we can provide security that is by involving a public key generator (PKG) which provides the users or the clouds with private or public keys to encrypt and decrypt the data.

1) Identity Based Cryptography: There is a problem by securing the data through PKG i.e., deploying security solutions based on public key cryptography is the high cost for maintaining PKG. So, we introduce Identity Based Cryptography as a solution for the security of the Smart Grid. Identity based scheme is the existing algorithm used for security purpose. The idea of this algorithm is that, the cloud centres and the end devices are to be represented by their identities which can be used as encryption keys. In an identity-based encryption scheme, the private key generator (PKG), a trusted party, first generates secret master key mk and public parameter params. Note that params, which is long-term, will be given to every party that is involved. Once a receiver submits their identity, denoted by IDrec, the PKG computes the private key KIDrec associated with IDrec by running the private key extraction algorithm Extract providing its master secret key mk as input. Here, the identity IDrec can be any string such as an email address, a telephone number, etc. The entire process is the same for the Identity Based Signature scheme in which the the signatures of the users are verified along with the identities and a certificate is given depending on the signature and identity. The certificate provided should be of the format similar to that of X.509 certificates with the help of which the authorisation of the user is checked. The architecture of the PKG which issues keys to the public and private clouds is as below,

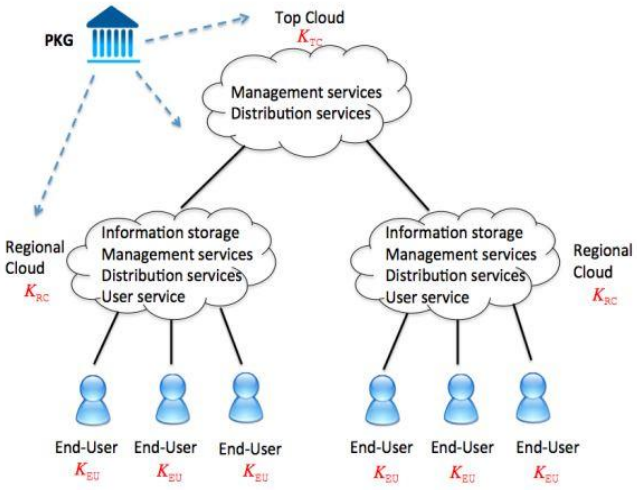

Fig. 5 Hierarchical Structure

2) Proxy Re-Encryption Scheme : The information stored in cloud can generate a signature for a message using the private key associated with its identity. The sender uses their identity as a key to encrypt the data before sending data

into the network. The receiver will decrypt the sender's private key. In Proxy re-encryption, the encrypted data is converted as binary data for data security and stored in cloud. When an end-user wants a specific service to receive, use and process its data, the information storage generates a re-encryption key using its identity and the identity of the requested service. The information storage then uses the generated re-encryption key to re-encrypt the confidential data encrypted using the information storage's identity so that the target service can receive, decrypt, and process the data. Note that the information storage takes care of heavy load of re-encryption but the services in the regional cloud cannot break the confidentiality of the data which they not entitled to process.

IV. CONCLUSION AND FUTURE ENHANCEMENTS

We have introduced a hierarchical structure framework called as a Smart-Frame for the information management and it also provides us with the security approaches to secure the data being stored in this vast network. We focussed on the Identity Based Cryptography and the Identity Based Proxy Re-Encryption schemes for providing the security to the Smart Grid. From this proposal we identified the few limitations while increasing the number of user. If top level data centre handled all the device information & user data, the performance will be weaken. So we built the regional and zone level data centre for maintaining the data. The top cloud level provides a global view of the framework and other will provide the information to parent cloud. From the above 3DES algorithm, we provided a solution based on "identity-based cryptography and identity-based proxy re-encryption" which provides secure communication services with the Smart-Frame. This will achieve not only scalability and flexibility but also security features.

ACKNOWLEDGEMENT

We have taken efforts in the research. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.
We are highly indebted to the professors of our university for their guidance and constant supervision as well as for providing necessary information regarding the project and also for their support in completion of the research.
We would like to express our gratitude towards our parents for their kind co-operation and encouragement which help me in completion of this research.

REFERENCES

[1] Joonsang Baek, Quang Hieu Vu, Joseph K. Liu, Xinyi Huang, and Yang Xiang,Wahida Banu, Harish, Nethra S, Vennela "A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 2, APR/JUN-15.
[2] Zhenhua Jiang, Fangxing Li, Wei Qiao, Hongbin Sun, Hui Wan, ianhui Wang, Yan Xia, Zhao Xu, Pei Zhang, "A Vision of Smart Transmission Grids " in IEEE Explore on OCTOBER 2009.
[3] C. Deepika, Dr. P.Mayilvahanan,"Smart Frame: Secure Cloud Computing Based Framework for Big Data Analysis of Smart Grid", in IJIRSET in Vol. 5, Issue 2, FEBRUARY 2016
[4] P Naveen1, Wong Kiing Ing1, Michael Kobina Danquah, Amandeep S Sidhu, and Ahmed Abu-Siada,"Cloud computing for energy management in smart grid – an application survey" in IOP Conf. Series: Materials Science and Engineering.(2016)
[5] K.M. Ravi Eswar,"Smart Grid-Future for Electrical System" in International Journal of Electrical and Electronics ResearchVol.3, Issue 2,April - June 2015, Available at: www.researchpublish.com
[6] Wahida Banu S, Harish, Nethra S N, Vennela N, "A Secure Cloud Computing Based Framework for Data Information Management System" in International Journal of Research In Science & Engineering Vol 1 Special Issue: 2 .