SMART FRAME- AN EFFICIENT SECURITY FRAMEWORK FOR BIG DATA MANAGEMENT SCHEME ON CLOUD

***Mrs.J.Sarojini Premalatha, **Mr.C.GopalaKrishnan, **Mrs.D.C.JOY WINNIE WISE,**

** M.E. (CSE), M.E.,Ph.D,Francis Xavier Engineering College, Tirunelveli, India*

*** Assistant Professor CSE Department, Francis Xavier Engineering College, Tirunelveli, India*

ABSTRACT

The evolution of the Smart Grid heavily relies on the utilization and integration of modern information technologies. The main challenges of smart grids are how to manage and process huge amount of data received from smart meters. For managing and storing the huge amount of data received from these devices cloud servers are used because it has been used popularly for storing and managing the data. In this a Smart-Frame, secure information management framework is designed for smart grids based on cloud computing technology. The idea behind the scheme is at three hierarchical levels: top, regional, and end-user levels in which the first two levels consist of cloud computing centers that are responsible for managing general devices and data accumulation while the last level contains end-user smart devices. Sensitive data stored in the cloud must be protected from being read in the clear by a cloud provider that is honest but curious. Additionally, cloud-based data are increasingly being accessed by resource-constrained mobile devices for which the processing and communication cost must be minimized. So, in addition to this framework, an identity based advanced encryption schemes are also used for preventing the information leakage.

Keywords:- Smart Grid, Smart Meters, IDAES, attributes, encryption.

INTRODUCTION

A smart grid is a system which includes a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficiency resources. Electronic power conditioning and control of the production and distribution of electricity are important aspects of the smart grid [1], [4], [5]. The smart grid is a new technology that uses new and sophisticated techniques for electrical transmission and distribution in order to provide excellent electrical service to customers, and allow them to manage their electricity consumption in a two-way communication. This communication network will be constructed to enable new energy services, such as real-time pricing, load shedding, and consumption management. It also enables cost saving resulting from peak load reduction and energy efficiency, integration of plug-in hybrid electric vehicles for grid energy storage, and the integration of distributed generation including photovoltaic systems and wind turbines. The new network will be created using various communication paths including fiber optic cable, hybrid fiber coax, twisted pair, wireless technology, and broadband over power line. These types of communication networks are all currently operating in the electric grid but are not yet implemented to the extent required for enabling the smart grid. The smart grid incorporates many resources, applications, and enabled technologies. Resources are the devices that may affect supply, load, or grid conditions, including delivery infrastructure, information network, end-user systems, and related distributed energy resources. Applications are operational strategies that use resources to create benefits or values. Enabled technologies are essential crosscutting elements of the smart grid that facilitate many resources and applications. They include smart meters, standards, and protocols. Fig 1 shows the architecture of smart grid.

A smart meter is usually an electronic device that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing. Smart meters enable two-way communication between the meter and the central system. Unlike home energy monitors, smart meters can gather data for remote reporting. Such an advanced metering infrastructure (AMI) differs from traditional automatic meter reading (AMR) in that it enables two-way communications with the meter. The term Smart Meter often refers to an electricity meter, but it also may mean a device measuring natural gas or water consumption. Similar meters, usually referred to as interval or time-of-use meters, have existed for years, but "Smart Meters" usually involve real-time or near real-time sensors, power outage notification, and power quality monitoring. These additional features are more than simple automated meter reading (AMR). They are similar in many respects to Advanced Metering Infrastructure (AMI) meters. Interval and time-of-use meters historically have been installed to measure commercial and industrial customers, but may not have automatic reading.

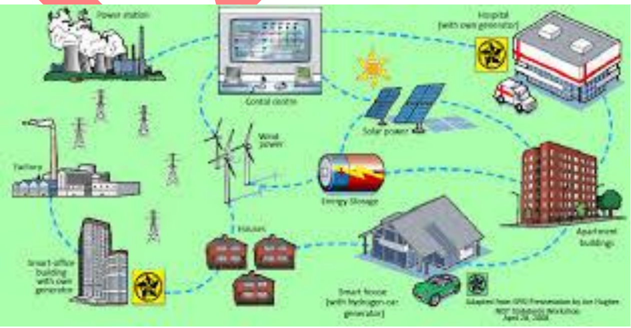


Fig 1 Smart Grid

RELATED WORKS

Mustafa Saed et al [1] have proposed attribute-based encryption are proposed to allow authorized users access to cloud data based on the satisfaction of required attributes such that the higher computational load from cryptographic operations is assigned to the cloud provider and the total communication cost is lowered for the mobile user. Furthermore, data re-encryption may be optionally performed by the cloud provider to reduce the expense of user revocation in a mobile user environment while preserving the privacy of user data stored in the cloud. Zhong Fan et al. [2] have discusses some of the challenges and opportunities of communications research in the areas of smart grid and smart metering. In particular, we focus on some of the key communications challenges for realizing interoperable and future proof smart grid/metering networks, smart grid security and privacy, and how some of the existing networking technologies can be applied to energy management. Hoon Wei Lim et al. [3] has presents a comprehensive investigation of the use of identity-based techniques to provide alternative grid security architecture. We propose a customised identity-based key agreement protocol which nicely with the Grid Security Infrastructure (GSI) and provides a more lightweight secure job submission environment for grid users. Boyen et al. [4] has surveys the practical benefits and drawbacks of several identity based encryption schemes based on bilinear pairings. After providing some background on identity-based cryptography, we classify the known constructions into a handful of general approaches. We then describe efficient and fully-secure IBE and IBKEM instantiations of each approach, with reducibility to practice as the main design parameter. Junbeom Hur [5] has proposed an attribute-based access control scheme using CP-ABE with efficient attribute and user revocation capability for data outsourcing systems. The proposed scheme has following advantages with regard to the security and scalability compared to the previous revocable CP-ABE schemes. First, enabling user access control enhances the backward/ forward secrecy of outsourced data on any membership changes in attribute groups compared to the attribute revocation schemes. Second, the user access control can be done on each attribute level rather than on system level, so that more fine-grained user access control can be possible.

SMARTFRAME

Smart-Frame, a flexible, scalable, and secure information management framework is introduced for smart grids based on cloud computing technology. The basic idea is to build the framework at three hierarchical levels: top, regional, and enduser 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 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 (e.g., within a city), and processing data of these devices. In addition to this general framework, a security solution for the framework based on identity-based advanced encryption scheme (IBAES) is proposed. 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 at the national level. The main idea of our security solution for the Smart-Frame is to allow all the involved entities, i.e., top and regional cloud computing centers and end-users to be represented by their identities which can be used as encryption keys. This framework consists of four main functional clusters namely Information storages, General user services, control and management services and distribution services. They are descibed as follows:

Information storages: These are main storages keeping all smart grid information received from front-end intelligent devices. These storages are designed to accept information from different transportation modes through both wired and wireless channels. For optimization purpose, statistics services are also located in this cluster.

General user services: This type of services consists of all services an electricity user needs to use. Typical examples are services that allow users to monitor, control or optimize the usage of their electric utilities. The majority of SaaS fall into this type of service. PaaS that provides libraries for user services also falls into this cluster.

Control and management services: This type of services includes all services needed for system management such as governance service, monitoring service, task scheduling service, and security service.

Electricity distribution services: This type of services is directly related to electricity distribution. Examples are distribution management service, optimization service, and quality of service measurement. Fig 2 shows the system architecture of smart frame

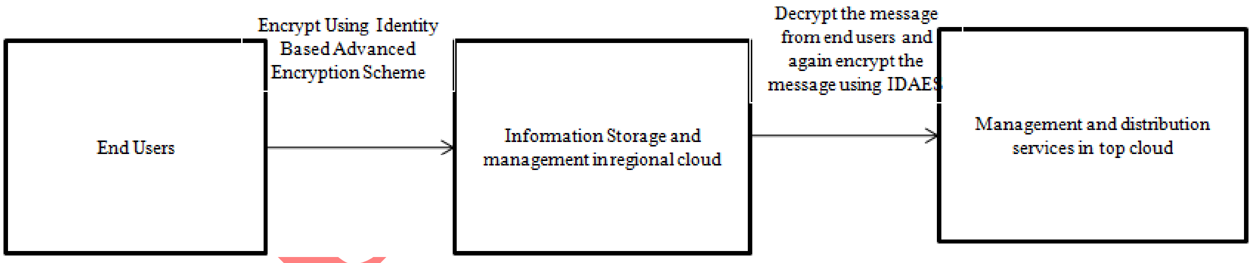

End Users
Encrypt Using Identity Based Advanced Encryption Scheme
Information Storage and management in regional cloud
Decrypt the message from end users and again encrypt the message using IDAES
Management and distribution services in top cloud

Fig 2 System Architecture

Since smart grids need to handle huge amount of data, it is extremely important to manage information flows efficiently. In the Smart-Frame, we suggest a centralized service to manage information flows. 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). Both information storages and services clusters need to follow this schedule for execution. Note that since information amount and requests in smart grid may change with time, each information flow schedule has an expiry time. After this time, a new schedule has to be generated and distributed again to all parties.

SECURITY SOLUTION FOR SMART-FRAME

A. Security of Smart-Frame Supported by Identity-Based Cryptography

Since security is a major concern in the smart grids, it is of great importance for our Smart-Frame to provide a solution to address that. As mentioned earlier, one of the huddles for widely deploying security solutions based on public key cryptography is the high cost for maintaining PKI. We envision that Identity-based cryptography can be a good solution (though it is not perfect) for resolving this problem since identity-based cryptography has the following advantages in regards to the Smart-Frame security.

1) Under traditional public key cryptography, each participating entity must locate and verify the public keys of the receivers. This is especially burdensome for end-user devices in our Smart-Frame, which are usually assumed as limited in power and networking capacity.

2) Although traditional public key cryptography is scalable in theory, a number of issues regarding user interfaces for maintaining public-key certificates (involving certificate revocation) have to be resolved. However, since any identifier strings can serve as encryption key or signature verification keys, identity- based cryptography could provide better scalability for the system. This is important in Smart- Frame in which numerous end-user devices can join and leave the system often.

3) For the convenience of the participating entities in the system, implementing key recovery is easy using identity- based cryptography. In contrast, in traditional public key cryptography, key recovery system is hard to implement requiring to keep secure database of private and public key pairs of the users. Due to the generic nature that private keys can be derived from the users' identities and master key of the private key generator, no secure database can be required for the system based on identity-based cryptography

4) In terms of encryption, traditional public key cryptography always require a setup phase to generate public-keys of the receiving parties. However, identity- based cryptography does not need such phase and users can encrypt their messages using the receiving parties' identities even before the receivers get the private keys form the PKG. This can be useful in the Smart-Frame where availability is an issues in the power grid. Availability will be assured by minimizing the time and frequencies for updating identities (public-keys).

5) Identities used as public keys in identity-based cryptography are flexible and versatile in format and description. They do not have to be restricted like the X.509 certificate format used in traditional public key cryptography. This versatility will be useful in our Smart-Frame in which identities can describe participating entities more flexibly.

B. Identity based Advanced Encryption Scheme

In realizing the security framework for the Smart-Frame, we make the following assumptions: There is a private key generator that can issue private keys for top and regional clouds, and end-users when they register. We assume that the PKG is a party that has responsibility and capacity of maintaining the Smart-Frame usually at the national level and its credential is fully trusted.

- The top cloud, regional clouds and end-users (e.g., smart meters at home) are identified by unique strings, which are to be used as encryption keys or signature verification keys.
- Each entity will obtain a private key associated with its identity, so it can decrypt the confidential data.
- Each entity will send confidential data to the entity which is only one-level higher. That is, the end-users send confidential data to the entities in the regional cloud only. Similarly entities in the regional cloud can send confidential data to the top cloud only.
- Each entity will authenticate data using the private key obtained from the PKG.

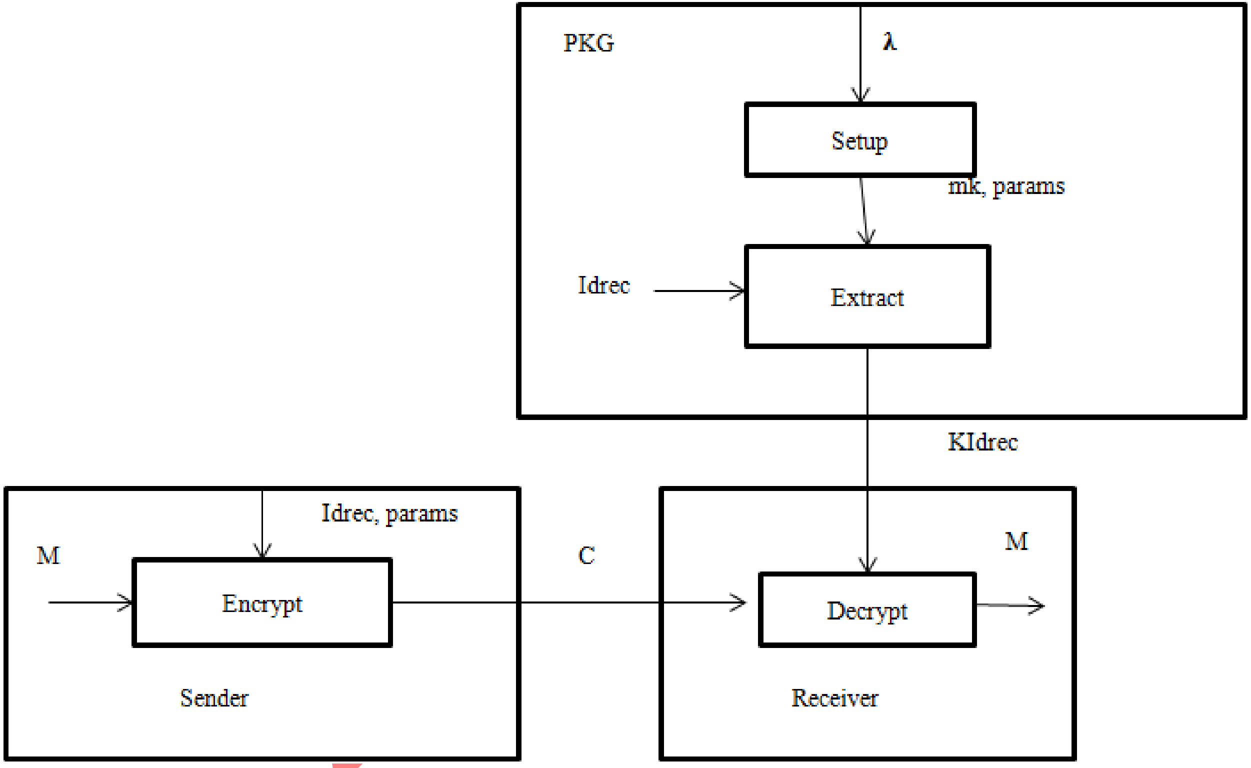
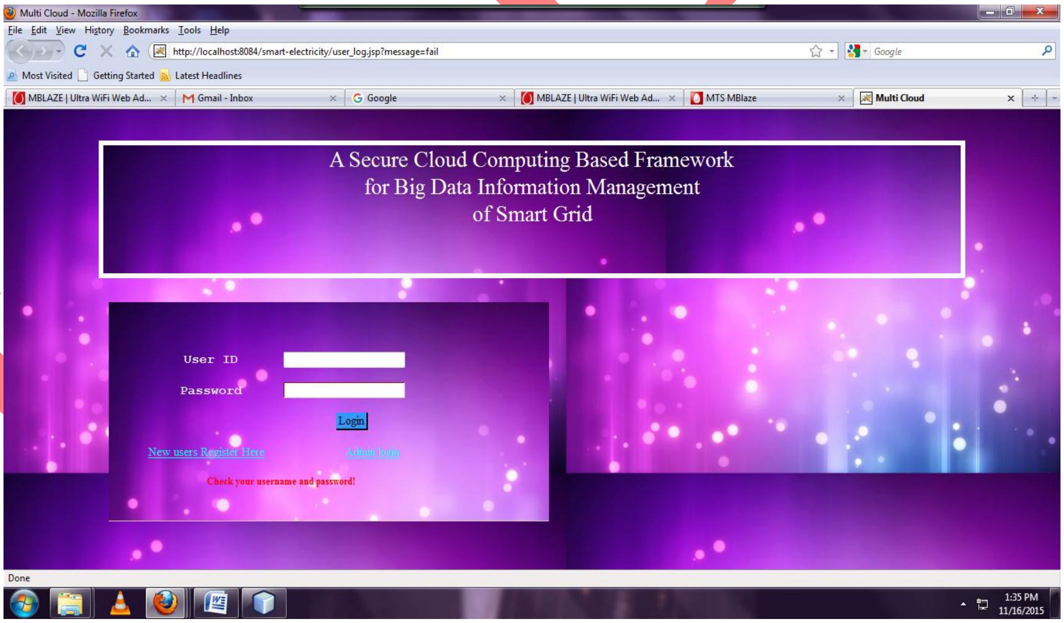


Fig 3 Identity Based Advanced Encryption Scheme

At the top of the hierarchy is the top cloud, which consists of power stations, distribution services or management services. Below the top cloud, there are regional clouds that consist of general user services and information storages. These regional clouds, in turn, have higher hierarchy than smart (intelligent) end-user devices (simply we call "end-users"), which are at the bottom of the hierarchy. Based on the principle of identity-based cryptography, the PKG will generate private keys for top cloud and any entities in regional clouds and end-users. Using their identifiers and private keys, each entity can utilize IBE schemes to secure information flow. In addition to IBE schemes, any parties can authenticate their data employing IBS schemes. Another important security issue that should be addressed is to make it possible for an information storage in the regional cloud to forward the received confidential data (ciphertexts) from the end-users to specific services in such a way that the services decrypt the ciphertexts correctly but the secrecy of the information storage's private key is never compromised. That is, the information storage performs heavy tasks of distributing confidential data to various services residing in the regional cloud while maintaining the security of cryptographic keys held by the information storage. We employ an identity-based proxy re-encryption scheme to achieve this. When an end-user wants a specific service to receive, use and process its data, the information storage generates a decryption key using its identity and the identity of the requested service. The information storage then uses the generated decryption key to decrypt the confidential data encrypted using the information storage's identity so that the target service can receive, decrypt, and process the data. Fig 3 shows the entire process of identity based advanced encryption scheme.

Screenshots

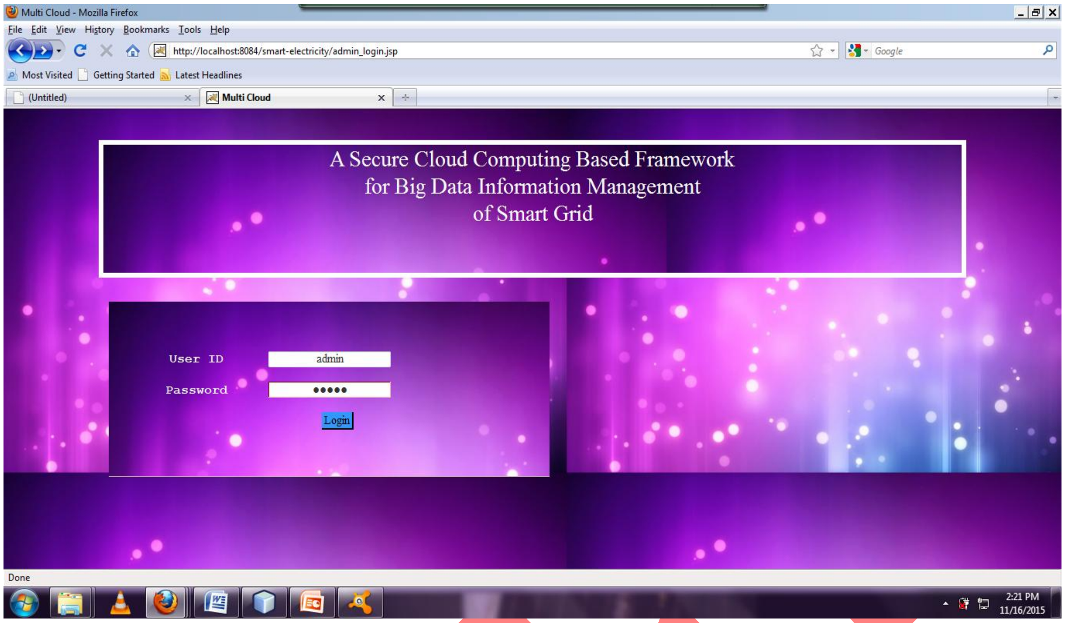


http://localhost:8084/smart-electricity/user_log.jsp?message=fail

A Secure Cloud Computing Based Framework
for Big Data Information Management
of Smart Grid

Check your username and password!

Fig 4 Home page



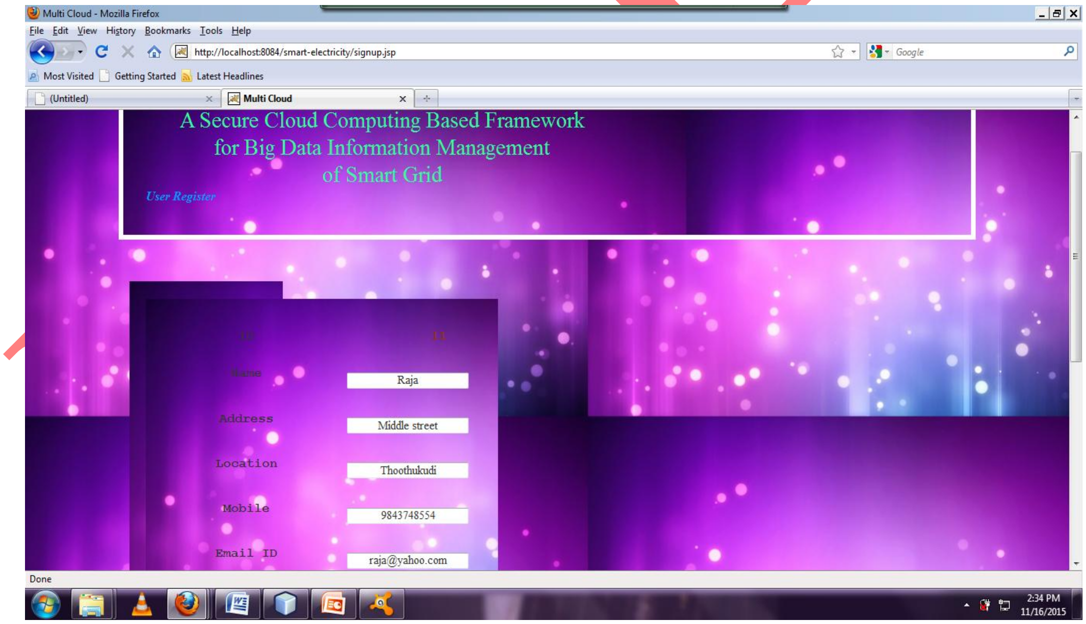
A Secure Cloud Computing Based Framework
for Big Data Information Management
of Smart Grid

User ID: admin

Password: •••••

Multi Cloud - Mozilla Firefox
http://localhost:8084/smart-electricity/admin_login.jsp
Login
Done

Fig 5 Admin Login page



A Secure Cloud Computing Based Framework
for Big Data Information Management
of Smart Grid

User Register

ID: 11

Name: Raja

Address: Middle street

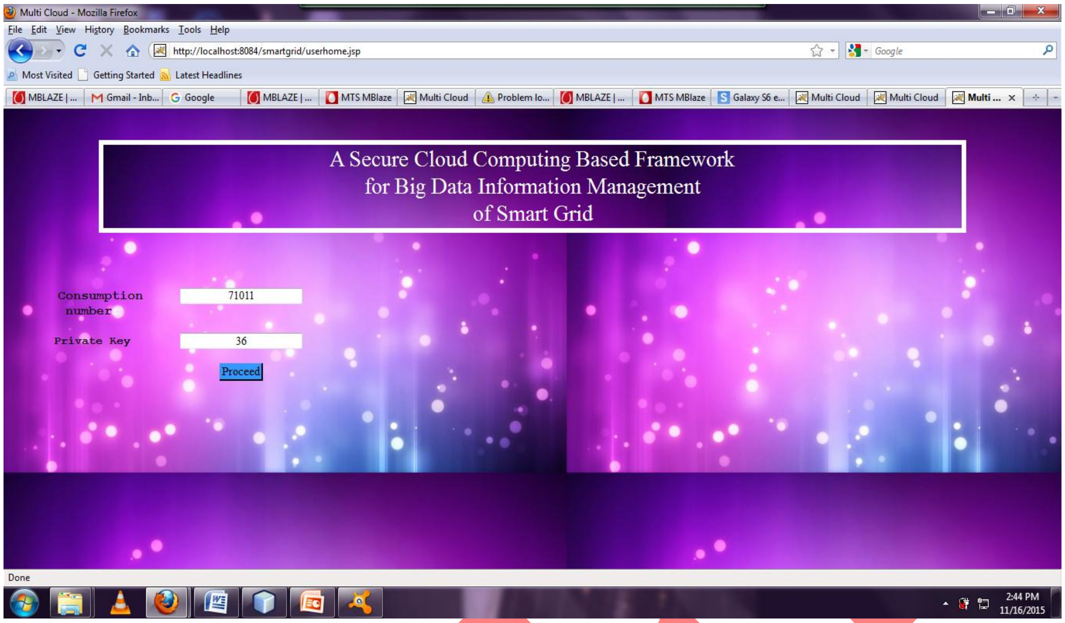
Location: Thoothukudi

Mobile: 9843748554

Email ID: raja@yahoo.com

Multi Cloud - Mozilla Firefox
http://localhost:8084/smart-electricity/signup.jsp
Done

Fig 6 Registration Page


Multi Cloud - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8084/smartgrid/userhome.jsp
Done

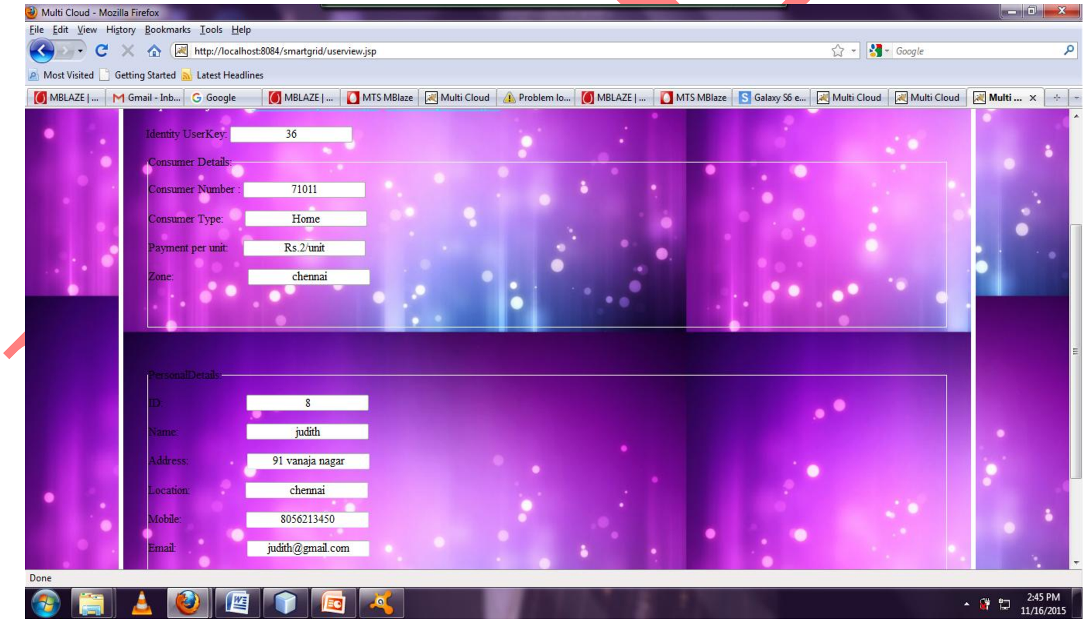
A Secure Cloud Computing Based Framework
for Big Data Information Management
of Smart Grid

Consumption number: 71011

Private Key: 36

Proceed

Fig 7 User's Private Key Page


Multi Cloud - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8084/smartgrid/userview.jsp
Done

Identity UserKey: 36

Consumer Details:

Consumer Number : 71011

Consumer Type: Home

Payment per unit: Rs.2/unit

Zone: chennai

PersonalDetails

ID: 8

Name: judith

Address: 91 vanaja nagar

Location: chennai

Mobile: 8056213450

Email: judith@gmail.com

Fig 8 Consumption Report Page

CONCLUSION

In the project the Smart-Frame, a general framework for big data information management in smart grids based on cloud computing technology is introduced. 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, a solution based on identity-based advanced encryption scheme is presented. As a result, our proposed framework achieves not only scalability and flexibility but also security features. In future proxy re-encryption scheme is applied instead of identity based advanced encryption scheme.

REFERENCES

1. Mustafa Saed, Kevin Daimi, Nizar Al-Holou Piotr K. Tysowski and M. Anwarul Hasan, (2013) “Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds” IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 1, NO. 2.

2. Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin (2013) Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1.

3. Hoon Wei Lim and Kenneth G. Paterson (2009) “Identity-Based Cryptography for Grid Security”, The Internet Engineering Task Force (IETF), RFC 3275.

4. X. Boyen (2009) A Tapestry of Identity-Based Encryption: Practical Frameworks Compared” ai.stanford.edu/~xb/ijact08/practicalIBE.pdf

5. Junbeom Hur and Dong Kun Noh, Member, IEEE “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 7, JULY 2011

6. Wenye Wanga,Zhuo Lua (2012) Cyber Security in the Smart Grid: Survey and Challenge, Elsevier

7. Kenneth P. Birman, Lakshmi Ganesh, and Robbert van Renesse1 (2009) “Running Smart Grid Control Software on Cloud Computing Architectures”, Department of Computer Science, Cornell University, Ithaca NY 14853

8. D. Galindo and F. Garcia, “A Schnorr-like lightweight identity based signature scheme,” in Proc. 2nd Int. Conf. Cryptol. Africa, 2009, pp. 135–148.

9. C. Gentry and A. Silverberg, “Hierarchical ID-based cryptography,” in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inf. Security: Adv. Crypto., 2002, pp. 548–566.

10. 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.