BIG DATA INFORMATION MANAGEMENT OF SMART GRID IN CLOUD COMPUTING

DIVYA.V¹ and GRACE PRAMILA.T²

Student, Information Technology, Panimalar Institute Of Technology, Chennai, India¹ ²

Abstract—The rise of cloud computing and cloud data stores has been a precursor and facilitator to the emergence of big data. Cloud computing is the commodification of computing time and data storage by means of standardized technologies. Smart Grid is the methodology that states how efficiently we manage and utilize the energy resources and it plays a crucial role in modern energy infrastructure. Smart Grid is used to increase the sustainability of electricity services and it also processes the huge amount of data received from the power assets. For processing such huge data, cloud computing is used. The key idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this Identity Based Encryption and Advanced Encryption Standards are used for protecting the data in cloud.

Index Terms—Big Data, Cloud Computing, Information Management, Secure, Smart Grid

I. INTRODUCTION

Smart grids are gradually replacing traditional power grids due to increased efficiency, reliability, economy, and substantiality of electricity services. Following the success of ENEL Telegestore which yielded an annual savings of 500 million Euros, other smart grid projects such as Hydro One project in Canada, the Evora InovGrid project in Portugal, and the Modellstadt Mannheim (Moma) project in Germany have followed suit. Due to constraints in receiving huge amount of information from a large number of front-end intelligent devices, smart grids could not be deployed at a very large scale (e.g., in the whole country). To quote an example, the amount of data required to process transactions of two million customers at a particular utility reached 22 gigabytes per day. Hence, the selection, deployment, monitoring and analysis of such enormous smart grid data is not an easy task. Further, real-time information processing is usually required in the smart grid. Any delay may cause a serious consequence in the whole system. To stride over these difficulties, cloud computing has been employed due to its flexibility, scalability, agility, energy efficiency, and cost saving properties.

1. SOFTWARE DEVELOPMENT

1.1 Authentication and Authorization Module

Authorization is the process by which a server determines if the client has permission to use a resource or access a file. Authorization is usually coupled with Authentication, so that the server has some concept of who the client is that is requesting access. Authorization and Authentication involves obtaining the details of the User of the application before accessing the data base to avoid unauthorized usage. The Registration involves getting the details of the users who wants to use this application

1.2 File Encryption and Data Storage in Cloud

In this module, the user uploads the files which he intends to share. Initially, the uploaded files are stored in the Local System and later uploaded to the real Cloud Storage. While uploading to the Cloud the file gets encrypted by using IES (Identity Based Encryption Standard) Algorithm and generates Private key. Again the Encrypted Data is re-encrypted using AES (Advance Encryption Standard) Algorithm. The data is then converted into Binary Data for security purposes and stored in Cloud.

1.3 Signature And 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. The first fully functioning proxy re-encryption scheme was proposed by Atieniese et al. Compared with the previous approaches, their proxy re-encryption scheme was unidirectional, so it does not require delegators to reveal their secret keys to anyone in order to allow proxy to re-encrypt their cipher texts. Since Atieniese et al.’s work, numerous proxy re-encryption schemes with various functionalities have been proposed. Among them, the identity-based proxy re-encryption scheme proposed by Green and Ateniese is closely related to our Smart-Frame. In an identity-based proxy re-encryption scheme, a delegator allows a proxy to transform an encryption under Alice’s identity into one encrypted under Bob’s identity. The proxy then uses re-encryption keys to conduct the transformation without being able to learn any information about the plaintext. Also, no information about the private keys of Alice and Bob would be deduced from the re-encryption keys. Note that identity based proxy re-encryption combine the two functionalities of IBE and proxy re-encryption without compromising the security. Note also that Green and Ateniese’s identity-based proxy re-encryption scheme.

1.4 Information Management And Big Data Analysis

The data uploaded by an average person is 15 times more than
the data uploaded three years ago, and according to IDC the amount of digital information in the world is more than doubling every two years. The practice of syncing data in batches has given way to more frequent updates, and real-time streaming of data. Cloud computing clusters require a new breed of data capture and analytics infrastructure that can handle the increasing volume and velocity of data. The best way to get big data flowing in real-time is with middleware that takes care of message queuing and delivery so publishing applications and sensors can send data without worrying about where it needs to go or how it needs to get there. This entails the establishment and management of topics and queues, dynamic routing rules, and intelligent handling of fault conditions (such as applications or network links being down or slow).

1.5 Sending Reports To End User By Email And SMS
In this module, reports are sent to the end user via E-Mail or SMS. The final electricity details are intimated to the end user through their mails and mobile numbers. Only authorized registered members are offered this service.

2.1. FEASIBILITY STUDY
The feasibility of the project is analyzed in this phase. A general plan for the project and cost estimates is arrived. During system analysis the feasibility study of the proposed system is carried out to ensure that the proposed system is not a burden to the Company. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key consideration involved in the feasibility analysis are
1. ECONOMIC FEASIBILITY.
2. TECHNICAL FEASIBILITY.
3. SOCIAL FEASIBILITY.

2.1.1. ECONOMIC FEASIBILITY
This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system is well within the budget. This was achieved because most of the technologies used are freely available and only the customized products had to be purchased.

2.1.2. TECHNICAL FEASIBILITY
This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources which will in turn lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

2.1.3. SOCIAL FEASIBILITY
The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

II. EXISTING SYSTEM

By 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. It can scale very fast to deal with changes in the amount of processing information and can provide a high utilization of computing resources. Actually, prior to our work, initial efforts have been devoted to prove that cloud computing can satisfy requirements of information management in these systems. In particular, properties of smart grid and cloud computing were analyzed to prove the relationship between them. Furthermore, cases of smart grids were discussed to understand detailed requirements of information management and cloud computing environment does not consider the power constraints. The Large Data centre can acquire as much electric power required for running a small town. The power consumption of data centres is totally dependent on the overall data processed by data centres. Data centres are not configured with energy and power source management.

III. PROPOSED SYSTEM

Cloud computing, a technology that provides computational resources on demands, is a good candidate to address these challenges since it has several good properties such as energy saving, cost saving, agility, scalability, and flexibility. Thus the Big Data Information Management of Smart Grid in Cloud Computing is implemented, which we call “Smart-Frame.” The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, a security solution based on identity-based encryption and proxy re-encryption to address critical security issues of the proposed framework is formulated.

ADVANTAGES OF PROPOSED SYSTEM

- It has a Hierarchical Structure of cloud computing.
- It provides High security based on Identity-based encryption and proxy re-encryption.
- It implements a simple prototype for the proposed framework. It processes a huge amount of data received from these devices.
IV. CONCLUSION

In this paper, we have introduced the Smart-Frame, a general framework for big data information management in smart grids based on cloud computing technology. Our 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, we have presented a solution based on identity-based cryptography and identity-based proxy re-encryption. As a result, our proposed framework achieves not only scalability and flexibility but also security features. We have implemented a proof-of-concept for our framework with a simple identity-based management for data confidentiality. Our immediate next step is to also support proxy re-encryption for the framework.

REFERENCES

[25] IEEE, P2030/D7.0 draft guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), and end-user applications and loads, P2030/D670, 2011.


Divya.V  
Student, Panimalar Institute Of Technology, B.Tech. Information Technology, Chennai

Grace Pramila.T  
Student, Panimalar Institute Of Technology, B.Tech. Information Technology, Chennai