A FRAMEWORK FOR BIG DATA INFORMATION ORGANIZATION IN SMART GRIDS BASED ON SECURE CLOUD COMPUTING

Ms. Nandhini S [1], Mrs. Shanmuga Priya P [2], Mrs. Ramya K [3], Ms. Anusuya G [4]

[14]*Student, Dept. of Comp. Sci., Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India*

[23]*Assistant Professor, Dept. of Comp.Sci.,Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India*

---***---

Abstract - *To provide Security for the Big Data information management usually involves three basic tasks: information gathering, information processing, and information storing. In order to provide different types of computing services for information management and big data analysis. Information security for smart grids is very important since much of the information in smart grids is sensitive and needs to be strictly protected. Confidential data is not prevent from eavesdropping. In this work proposed idea is Smart Frame, 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. In this work private key Generator is used to provide master key for the above given hierarchical level. 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. In addition to this general framework, a security solution is provided which is based on identity-based encryption (IBE), signature and identity-based proxy re-encryption. So our present Smart grids, which provides not only flexibility and scalability but also security features. Our proposed work is concentrated for storage. The top cloud stored data for cloud storage server on LZ compression technique which is used to compressed the data after stored. So we can reduce the cloud space.*

Key Words: *Cloud Computing, Big Data, secure, information management, Cloud space.*

1. INTRODUCTION

Smart grid information management usually involves three basic tasks: information gathering, information processing, and 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. 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. Motivated by the previous work, in addition to this project, 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. 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 encryption (IBE) and signature and identity-based proxy re-encryption .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 is to provide a 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 or signature verification keys. The entities in the lower level can use the identities of higher-level entities to encrypt their data for secure communication with the entities in the higher level. For example, the regional centers use the top cloud's entity to encrypt their messages. By employing an identity-based re encryption scheme, the information storages, which are components of regional clouds, can re-encrypt the received confidential data from the end-user devices so that services requested by the end-users decrypt and process the confidential data without compromising the information storages' private keys. One of the obvious benefits gain from applying identity-based cryptography to the Smart-Frame is that through using identities rather than digital certificates which depend on traditional public key infrastructure (PKI), it can save significant amount of resources for computation and communications and resolve scalability issues. The saving gained from the elimination of digital certificate in the big data environment is especially momentous.

Since smart grids need to handle huge amount of data, it is extremely important to manage information flows effic iently. In the Smart-Frame, a centralized service to mana ge information flows. This service takes inputs as both in formation requests from service clusters and general sta tistics (e.g., the amount of information, time of arrival) fr om 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 ar e applied on information flows and where they are appli ed). Both information storages and services clusters nee d to follow this schedule for execution. So our present S mart grids, which provides not only flexibility and scalab ility but also security features. Our proposed work is con centrated for storage. The top cloud stored data for cloud storage server on LZ compression technique which is us ed to compressed the data after stored. So we can reduce the cloud space.

2. SYSTEM MODEL

In this section we consider the existing system design an d the proposed system.

2.1 Existing System

Smart grid information management usually involves three basic tasks: information gathering, information processing, and information storing. A hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. But it does not consider the security. 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. Due to their large-scale deployment, smart grids suffer from several security vulnerabilities. Since any security breach in smart grids may lead to a big loss, there are initiatives to address security challenges in this type of systems.

Problem Identified:

- Smart grids, which provide only flexibility and Scalability not fully, consider security features.
- Not for a secure communication.
- Confidential data is not prevent from eavesdropping.
- It does not consider the storage management as well as the cloud space.

2.2 Proposed System

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. In addition to this general framework, a security solution is provided for the framework based on identity-based encryption (IBE) and signature and identity-based proxy re-encryption. 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. 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. The top cloud stored data for cloud storage server on LZ compression technique which is used to compressed the data after stored. So we can reduce the cloud space.

Benefits:

- Smart grids, which provides not only flexibility and scalability but also security features.
- Provides Very secure communication services for the Smart-Frame.
- Identity-based cryptography could provide better scalability for the system.
- User confidential data from prevent eavesdropping.
- Simple identity-based management for data confidentiality.
- The top cloud stored data for cloud storage server on LZ compression technique which is used to compressed the data after stored. So we can reduce the cloud space.

3. DESIGN CONSTRUCTION

This Section consists of the following module design to fo rm the smart frame and their system architecture. These are to be explained in this section.

3.1 Identity Validation

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. The top cloud, regional cloud and end user for send identity for Private Key generator. Validation for all the identity on PKG.If it finished validation process generate the master key and parameter for individual in three levels. This parameter for send top cloud, regional cloud and end user.

3.2 Private Key Generation for an each entity

The Master key, parameter and identity for combined generate the Private Key for Top cloud, regional cloud and End user. Also generate the private key for information storage service for regional cloud. The extract the private key for using private key extraction algorithm.

3.3 Encryption to Regional cloud

Each end-user can encrypt a message M into a cipher text CIS by running the Identity Based Encryption algorithm Encrypt with parameter and the identity of the Regional cloud. Each regional cloud can decrypt a received cipher text C to message M by running the Identity Based decryption algorithm Decrypt with the private key KIS associated with the regional cloud identity and parameter.

3.4 Re-Encryption to Information Storage

The regional cloud information storage is maintained at the several services. The example for ServiceA, ServiceB, Etc., The end user encrypted message for storage in different services. Before store the encrypted message for re-encrypted. First it has generated the individual private key for all the services. Example of providing its own private key ServiceA, its identity of regional cloud and the server A's identity as input, the information storage in the regional cloud generates a re-encryption key RKIS->SerA.

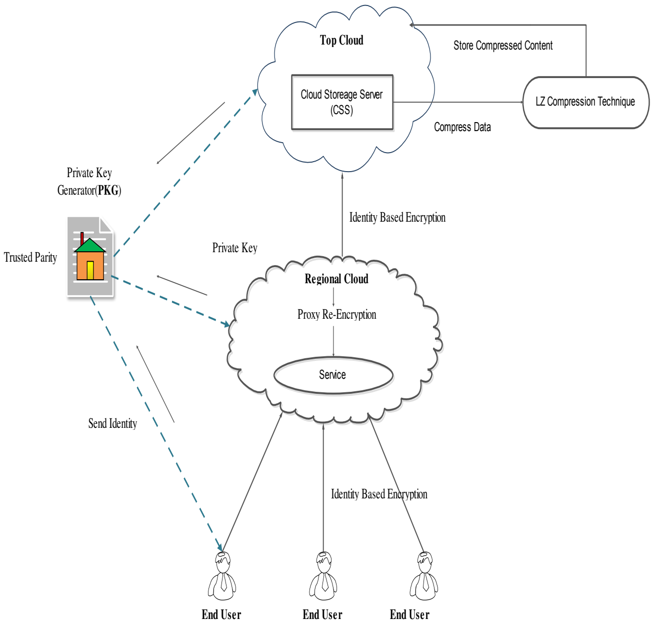
- **Reencrypt:** The information storage in the regional cloud re-encrypts the cipher text CIS Using the re-encryption key RKIS->SerA, Identity of regional cloud and SerA identity obtains a cipher text CSerA.
- **Decrypt Service:** The serviceA decrypts CSerA using its private key KSerA.

3.5 Encryption to Top Cloud

Each information storage in the regional cloud can encrypt a message M into a cipher text CTC by running the Identity Based Encryption algorithm Encrypt with parameter and the top cloud's identity. The top cloud can decrypt a received cipher text C to message M by running the Identity Based Decryption algorithm Decrypt with the private key KTC associated with the top cloud's identity and parameter.

3.6 System Architecture

System design is the process of defining the architecture, components, modules, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. If the broader topic of product development blends the perspective of marketing, design, and manufacturing into a single approach to product development, then design is the act of taking the marketing information and creating the design of the product to be manufactured. System design is therefore the process of defining and developing systems to satisfy specified requirements of the user.



4. PERFORMANCE EVALUATION

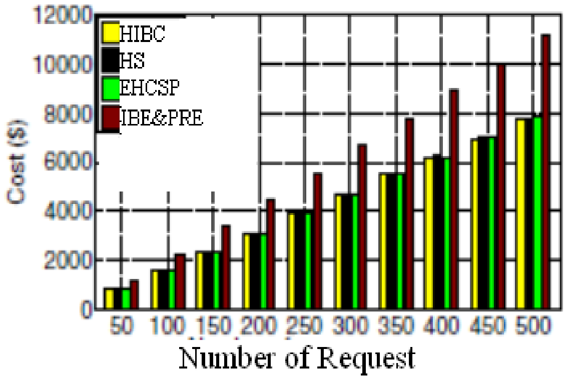


Chart 1- Information Storage

5. CONCLUSION

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, a security solution based on identity-based cryptography and identity-based proxy re-encryption. As a result, the framework achieves not only scalability and flexibility but also security features. A proof-of-concept for this framework with a simple identity-based management for data confidentiality. Also support proxy re-encryption for this framework. Our proposed work is concentrate for storage. The top cloud stored data for cloud storage server on LZ compression technique used compressed the data and after stored. So can reduce the cloud space.

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.

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

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

[9] 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.

[10] 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.

[11] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. 5th Int. Conf. Appl. Cryptograph. Netw. Security, 2007, vol. 4521, pp. 288–306.

[12] 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.

[13] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1, pp. 81–85, Jan./ Feb. 2010.

[14] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in Proc. 1st Int. Conf. Cloud Comput., 2009, vol. 5931, pp. 157–166.

[15] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smartgrids using homomorphic encryption," in Proc. IEEE Conf. Smart Grid Commun., 2010, pp. 327–332.

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

[17] H. Lim and K. G. Paterson, "Identity-based cryptography for grid security," Int. J. Inf. Security, vol. 10, no. 1, pp. 15–32, 2011.

[18] 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.

[19] A. Metke and R. Ekl, "Smart grid security technology," in Proc. Eur. Conf. Innovative Smart Grid Technol., 2010, pp. 1–7.

[20] K. Rogers, R. Klump, H. Khurana, A. Aquino-Lugo, and T. Overbye, “An authenticated control framework for distributed voltage support on the smart grid,” IEEE Trans. Smart Grid, vol. 1, no. 1, pp. 40–47, Jun. 2010.
[21] 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. 483–488.
[22] 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.

BIOGRAPHIES

Ms. Nandhini S received the B.E-CSE degree from Sri venkateswara college of engineering and technology, tiruvallur in 2014.She is currently doing her M.E-CSE degree in Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India.