

Research Journal of Pharmaceutical, Biological and Chemical Sciences

A Smart-Frame for Information Management of Smart Grid in a Secure Cloud

Jaisri Kumanan^{1*}, Sivaranjini S¹ and Priya K².

¹U.G Scholar, Dept of IT, Sathyabama University, Chennai-119, Tamil Nadu, India.

²Assistant Professor, Dept of IT, Sathyabama University, Chennai-119, Tamil Nadu, India

ABSTRACT

Smart grid is a technological innovation in the Power Industry sector that improves reliability, efficiency, economics, and sustainability of electricity services. While this modern energy infrastructure plays a crucial role, it also has its own set of challenges. The key areas of focus are about efficiently managing their critical devices such as power assets and smart meters. It also includes the need to process the huge volume of data received from these devices. Cloud computing is a technology that gives computational resources on demand and at a very short lead time, is a good candidate for addressing these challenges. This technology complies with several good properties such as energy and cost saving, scalability, agility and flexibility. We introduce "Smart- Frame", a framework for information management in a secure cloud environment. The key function of this framework is to build 3 levels of hierarchical structure for data management, using cloud computing centers and end-user devices. This frame work will provide different types of computing services for information management and analysis. In addition to this framework, a homomorphic encryption based security solution is included to address critical security concerns of the proposed framework.

Keywords: Secure, Cloud Computing, Information Management, Smart Grid, Homomorphic Encryption.

**Corresponding author*

INTRODUCTION

Smart grid is the replacement of aging power system by intelligent power system incorporating ET & ICT. The growth and need of energy in various sectors, like automobile, software, manufacturing, production based industries, as well as urban and semi urban cities in all over world. Hence the scheduling and handling the energy requires huge manpower, which means the on the whole data handling and executive model increases. In order to share the excess amount energy to various part of the grid with the help of cloud based data system, which has huge amount of scalability. Due to the design it is a effective method to handle these data management.

Information management of Smart grid generally involves three basic jobs: gathering, processing and storing of information. It is a hierarchical structure which consists of centers of cloud computing to provide different kinds of computing services for information management analysis but it does not consider the security. Providing security for information of smart grids is very important since most of the information are sensitive in Smart Grid and needs to be highly protected. Leakage of information in smart grids can lead to attacks that affect individuals and the whole nation. This is because information that is leaked can be used to attack individuals and the whole smart grid. Due to their large-scale usage, smart grids are susceptible to several security vulnerabilities.

Cloud computing is more popular nowadays due to more advantages in conventional computing models. Those advantages are flexibility, scalability, liveness, energy efficient and cost reduction. Because of this it is estimated to be a leading computing model. Utilization of cloud based smart grids deals with the issue of large information organization and it also provides a high energy and cost saving platform. This is because 1) the framework can balance very quickly to contract with changes in the amount of information that need to be processed and 2) efforts have been dedicated to confirm that cloud computing can fulfill necessities of information management in these systems. Smart grid and cloud computing properties were examined to prove the connection involving them. Smart grid use cases were discussed to realize complete needs of information management, and properties of cloud computing were considered to show that they meet the needs. However, no one of this mechanism gives a solid design for information management in smart grids in addition to relatively abstract analyses.

A plan of Enhanced Smart-Frame is introduced, which is flexible and scalable. It provides a protected framework for information management based on cloud computing for smart grids. Basic scheme is to build a three level framework: they are top level, regional level, and end user level. Both the top and regional level have cloud computing centers and the third level consist of smart devices at the user end. The top level's task is to manage common devices and gathering of data across the local lower level cloud computing centers in the hierarchy. The local cloud computing centers are in charge of the management of the intellectual strategy, which are at hierarchical levels lower than the local cloud computing centers in the same regions (e.g., within a city), and dealing out data of these strategy. In this common framework, we suggest a solution for security for the framework based on Homomorphic encryption. Information safety for smart grids is very important since more of the information in smart grids is responsive and needs to be rigorously protected. In order to outflow in smart grids can show the way to vulnerabilities that involve individuals and also the entire people because leaked information can be used to initiate attacks. The major thought of our safety explanation for the Enhanced Smart-Frame is to permit all the concerned entities, i.e., top level and regional level cloud computing centers and end-users will be represented with their identities. This can be used as encryption keys. Identities of high-level entities can be used by the minor stage entities to encrypt their data for safe communication with the senior stage entities. For example, top cloud's entity can be used by the regional centers to encrypt their communication. By using an identity-based re encryption technique, the data storage, which are mechanism of regional clouds, the received secret data from the end-user strategy can be re-encrypted so that services provided by the end-users can decrypt and process the secret data without revealing the private keys of the data storages.

To review, our contributions in this paper are twofold:

- *To introduce Enhanced Smart-Frame:* A HE based secure cloud computing framework for information management in smart grids which provides flexibility, scalability and also safety features.

- To additionally provide a safety solution for the enhanced framework which provides safe communication services for the Smart-Frame. It additionally implement the prototype of the proposed result to show the practicality of it.

Related Work

In this section, we are reviewing some cardinal working trends that are being used in modern cryptography and that have been executed to take into the account issue of privacy for Big Data Analytics in the cloud. The terms Big Data Analytics, as we observed is mostly concerned with two main targets-Data Analysis and security of the data on transmission over the open and unsecure Internet provided by some cloud provider or just some internet provider. Cryptography, a useful computational instrument in the hands spies and modern enterprise, is as old in application for security as human history. The modern introduction of digital computation through the applications of various cryptographic algorithms, has made information exchange fast, securely and simple. Nevertheless, maintaining confidentiality is a challenge in the systems. Most crypto algorithms rely on mathematical problems that are very difficult to solve especially in applying the algorithmic functionalities of heuristics models and number theories, and or abstract algebra as number theory is its child in the place of graph. Computer based algorithm i.e. geographic information system (GIR) [1], randomized algorithm [2], NBEA (Node Behavior Evaluation Algorithm) [3], NALM (Non-intrusive Appliance Load Monitoring) [4], coordinated scheduling algorithms [5], Multiple-forking algorithm [6], private-key generation algorithm [7], Cryptographic algorithm [8], Homomorphic encryption algorithm [9]. Similar researcher minded like ZORAN BOJKOVIC, BOJAN BAKMAZ proposed a two-way communication technology which is secure and computational intelligence in an integrated manner across the whole spectrum of the energy system from the generation process to the end processes of the electricity consumption [1]. The advantage of this system is analysis of requirements, which also includes the choice of appropriate technologies for each case study, and architecture for the resulting heterogeneous system. The disadvantage is that unlike the communications network, which routes information packets, the electric power grid routes the flow of power that are constrained by the laws of physics. Algorithm used in this paper is computer based algorithm i.e. geographic information system (GIR). X. Boyen proposed a fully secure IBE and IBKEM instantiations reducibility as the main design parameter [2]. The advantage of this system is we describe an efficient and fully secure IBE and IBKEM instantiations for each approach, with reducibility as the main design parameter. The disadvantage is pairings are powerful mathematical constructs that are defined over algebraic curves, and their recently discovered potential for creative cryptographic applications is not ceased to be an amazing source. A randomized algorithm is used in this paper. B.Padmini, N. Chandra Shekar Reddy, Ch. Mukunda Reddy proposal concentrates on the placement of the trust system in the border context which creates a new trust system that increases the flexibility and also expresses the trust system using TCP/IP router [3]. The advantage is that it summarizes the major threats that are against the SCADA systems. It discusses about the new trust system which implements a wider array of network enabled equipment. The disadvantage is that it is applied in wireless sensor network technique to this gateway mode. But as the node is vulture, to be attacked by eavesdropping etc. Algorithm used in this paper is NBEA (Node Behavior Evaluation Algorithm). Costas Efthymiou and Georgios Kalogridis proposed a method for anonymizing frequent electrical metering data sent by a smart meter securely [4]. The advantage is research in this area is going on and smart meter users need to be reassured the secureness their data. The disadvantage is that an aging infrastructure and to address new societal and environmental challenges. Algorithm used in this paper is NALM (Non-intrusive Appliance Load Monitoring). Zhong Fan, Parag Kulkarni's system focuses on some of the challenges of key communications for realizing interoperable and long term smart grid or metering networks, smart grid privacy and security, and how some of the networking technologies that exist can be used to apply to energy management [5]. The advantage is it discusses the coordinated standardization efforts in Europe to consolidate communications protocols and standards. The disadvantage is that once it is produced, it has to be used as storage of grid energy is very expensive. Algorithm used in this is coordinated scheduling algorithms. David Galindo and Flavio D. Garcia proposed the Schnorr like identity-based signature scheme is the most efficient scheme known till this date [6]. Algorithm used in this paper is Multiple-forking algorithm. Matthew Green and Giuseppe Ateniese proposed Identity-Based proxy re-encryption, where cipher texts are converted from one identity to another [7]. Algorithm used in this is private-key generation algorithm. N. Kuntze, C. Rudolph proposed the vision of an infrastructure for security for energy networks which is built on hardware security anchors [8].Cryptographic algorithm is used in this paper. Fengjun Li, Bo Luo and Peng Liu proposed a incremental distributed data aggregation approach, where data aggregation will be performed in all smart meters that are involved in data routing from the source meter to the collecting unit [9]. Homomorphic

encryption algorithm is used in this paper. Christian Schridde, Tim Dornemann proposed an identity based cryptographic approach that provides an independent setup of security domains that does not need a trust hierarchy when compared to the other identity-based cryptographic systems [10].

As earlier noted, the current world trend in scientific and commercial ventures is to go to the Cloud. Cloud computing now leverages a lot of computing difficulty including scientific data analysis, scientific computations and information storing platform[14].

Despite its seamless simple construct by definitions, the safe keeping platform, there are problems that inform security issues such as confidentiality, Integrity and privacy of the owners' data. Although encrypted data could be stored on the platform of the Cloud computing framework Rivest, this does not guarantee its safety[15].

Proposed Method (Enhanced Smart Frame)

Properties of Homomorphic Encryption

Gentry described the first fully homomorphic cryptosystem which supports both multiplication and addition. Gentry's proposed fully homomorphic encryption technique consists of several steps: Firstly, it develops a limited extent homomorphic scheme which allows working out of low-degree polynomials on the data that is encrypted. Next, it suppresses the decryption technique so that it will become a low-degree polynomial which the scheme supports, and finally, it uses a bootstrapping transformation to acquire a fully homomorphic scheme. The useful approach of this scheme is to derive and set up a process which can work out polynomials of high-enough degree by employing a decryption technique which can be used to express as a polynomial of low-enough degree. Once the degree of polynomials that can be worked out by the scheme goes beyond the limit of the degree of the decryption polynomial by a factor of two, the scheme is known as boots trappable and can then be converted into a fully homomorphism scheme.

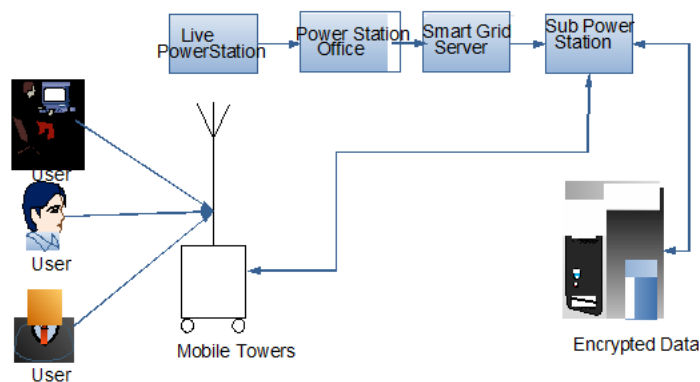
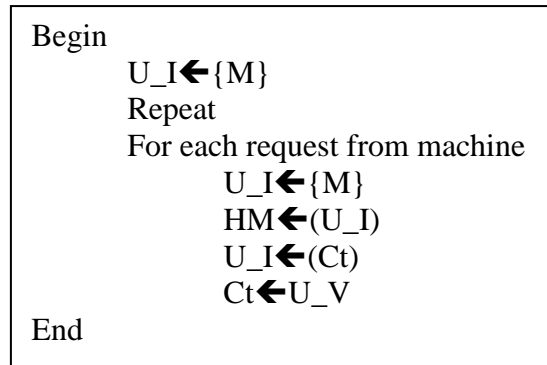


Figure 8: Proposed System architecture

Algorithm

- Accepting the Request from User to Store Register Information(Via) Machine M
- Obtain the information from the user => U_I
- Homomorphic Encryption HE => (H_Encryption, H_Decryption)
- Cipher Text => Ct
- User View => U_V



1. Accepting the Request from User to Store Register Information (Via) Machine
2. First Step will be repeated based on the user request.
3. The information will be stored in the variable U_I
4. The variables will be passed to the HM.
5. The encryption process will be performed.
6. The user information will be changed into cipher text.
7. Cipher text data are viewed to the user.

Modules

USER AND POWER STATION REGISTRATION

The process starts with User and Power station registration. Every user is registered with home user. Home user monitors the details of the each and every user regularly. By keeping those information, home user can calculate the necessary needs for every time and send these details to the substation. Those details will be collected and encrypted (due to security) and stored those details in database.

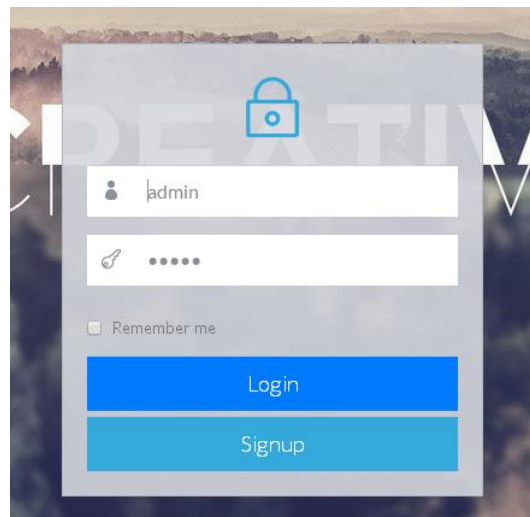


Figure 1: login page

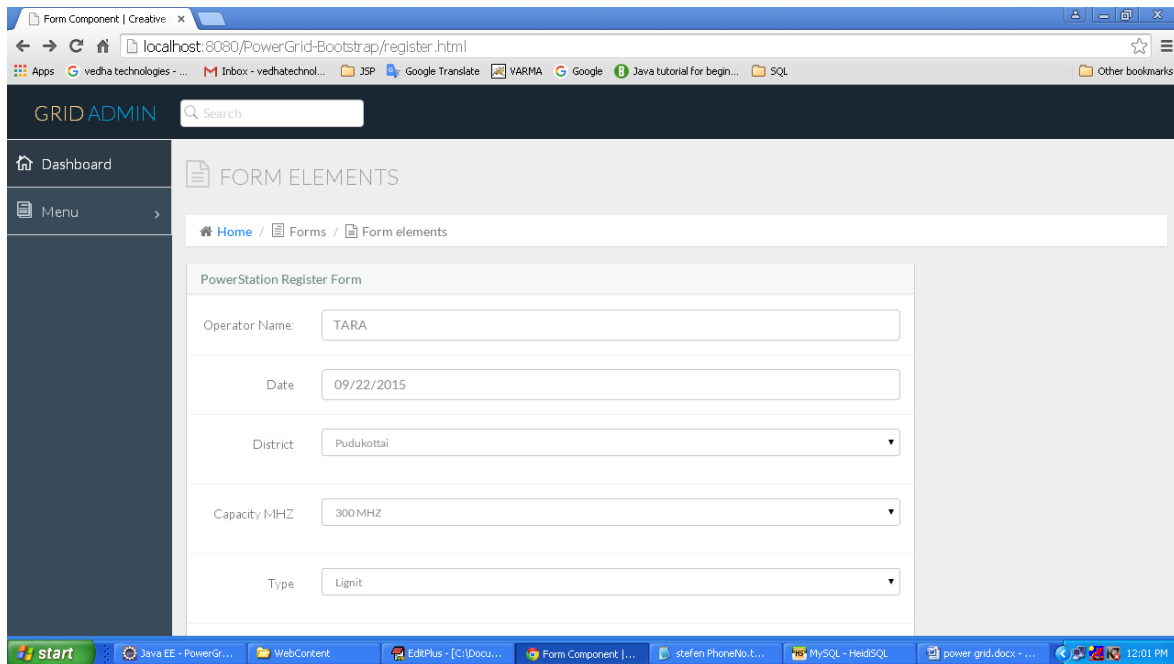


Figure 2: power station registration form

COLLECTING USER ELECTRICITY CONSUMPTION DATA

This module is used to collect the electricity readings from all the users and store all those information in grid. Each and every user's reading will be collected in grid via towers. The stored information will help in computing the shortage and excessive power information from all the stations. With this information we can allocate the excessive power to the station facing problems with insufficient power supply.

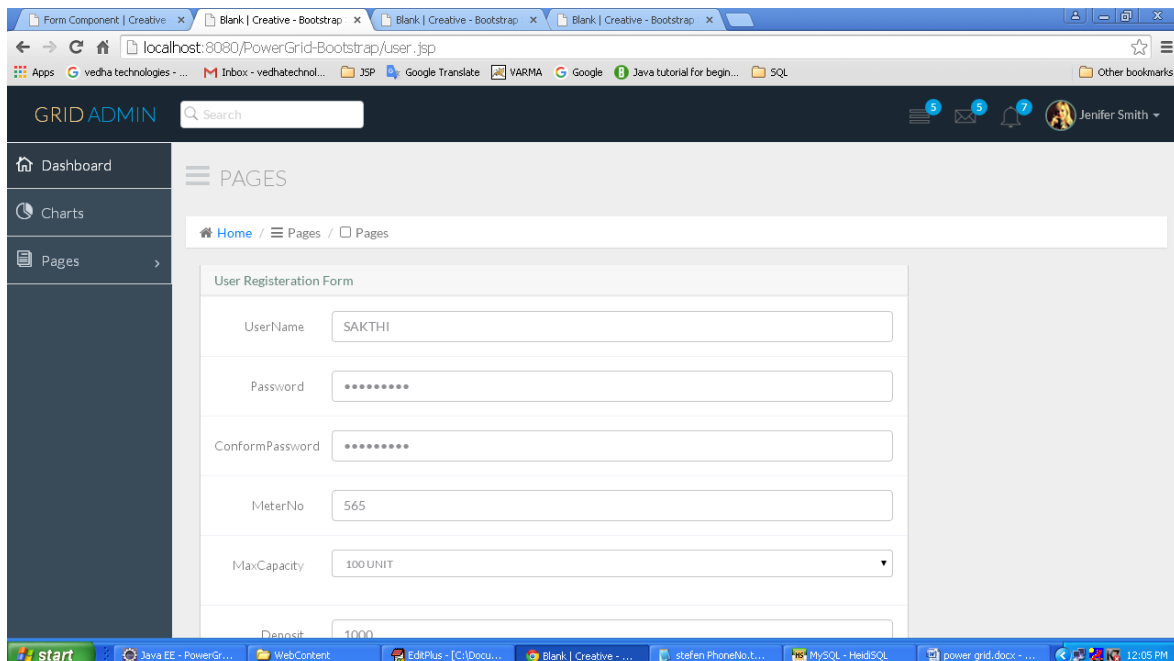


Figure 3: User registration form

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 Station. Grid maintains each and every power station’s power consumption records.

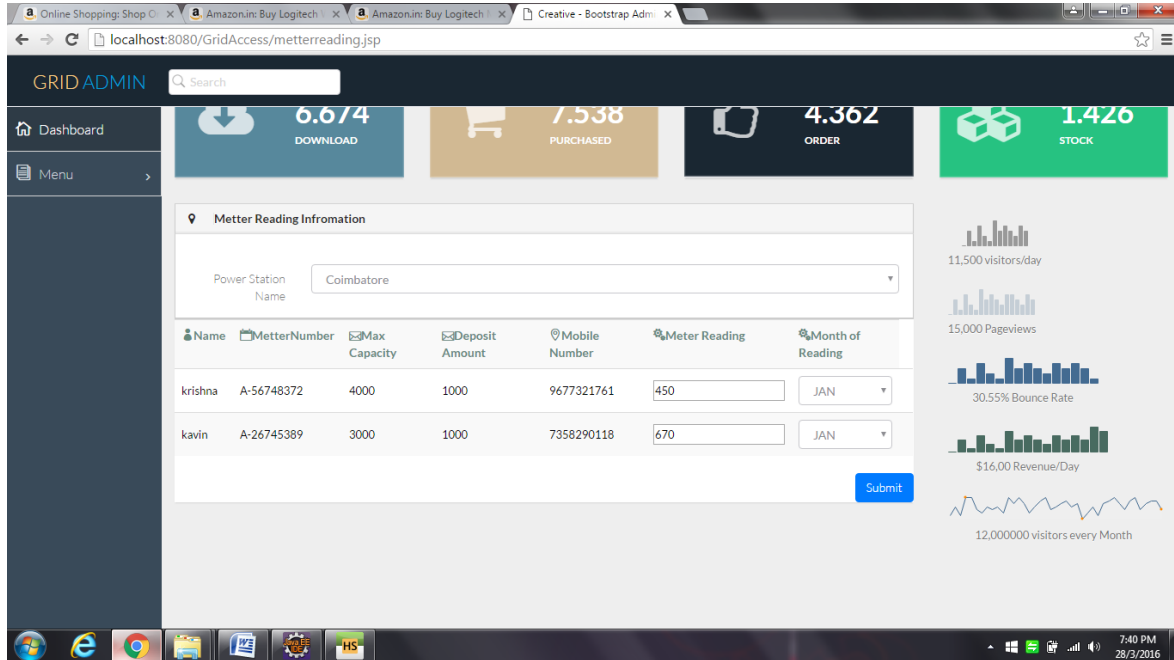


Figure 4: Input meter reading

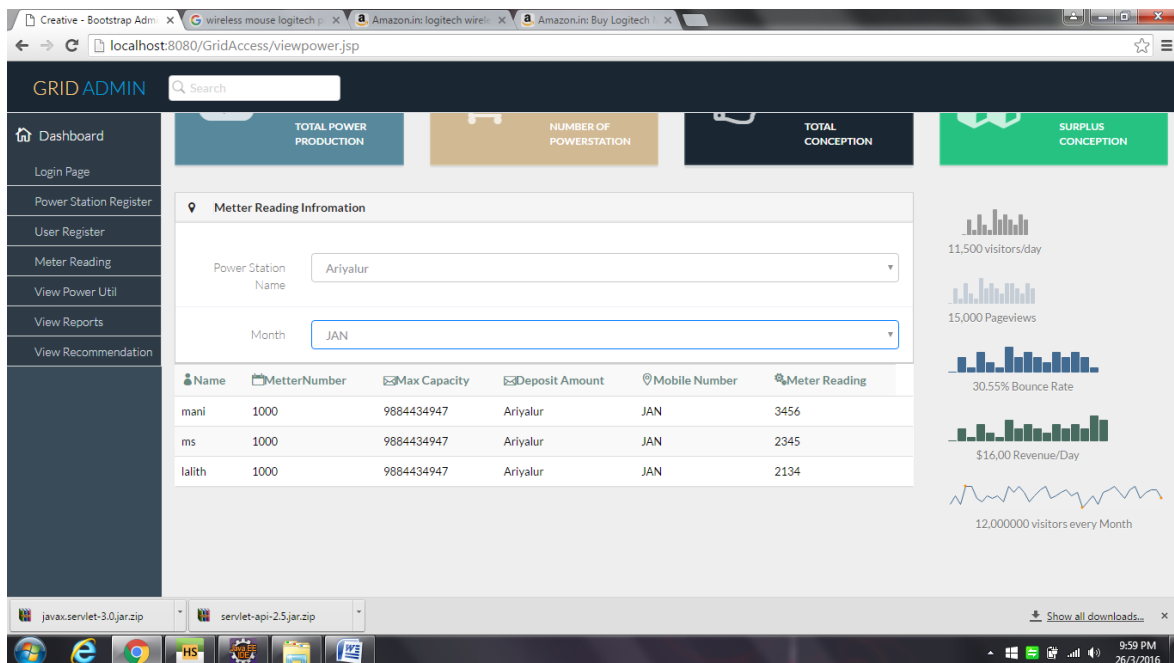
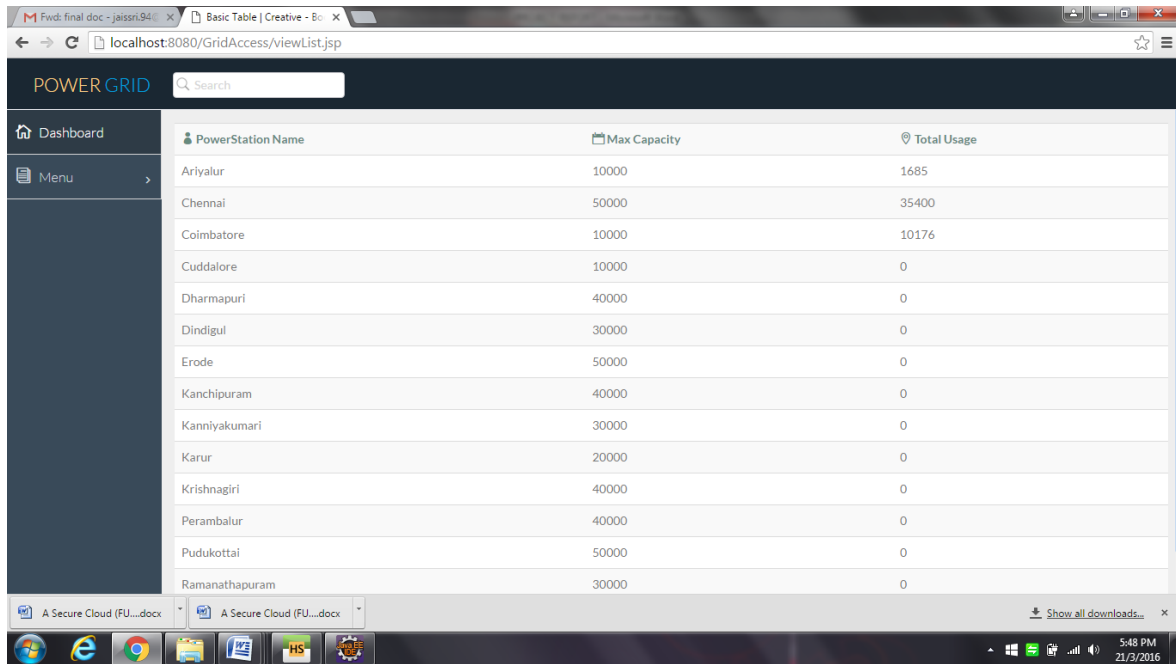


Figure 5: Each user’s power consumption for each month

SERVICE DISTRIBUTION

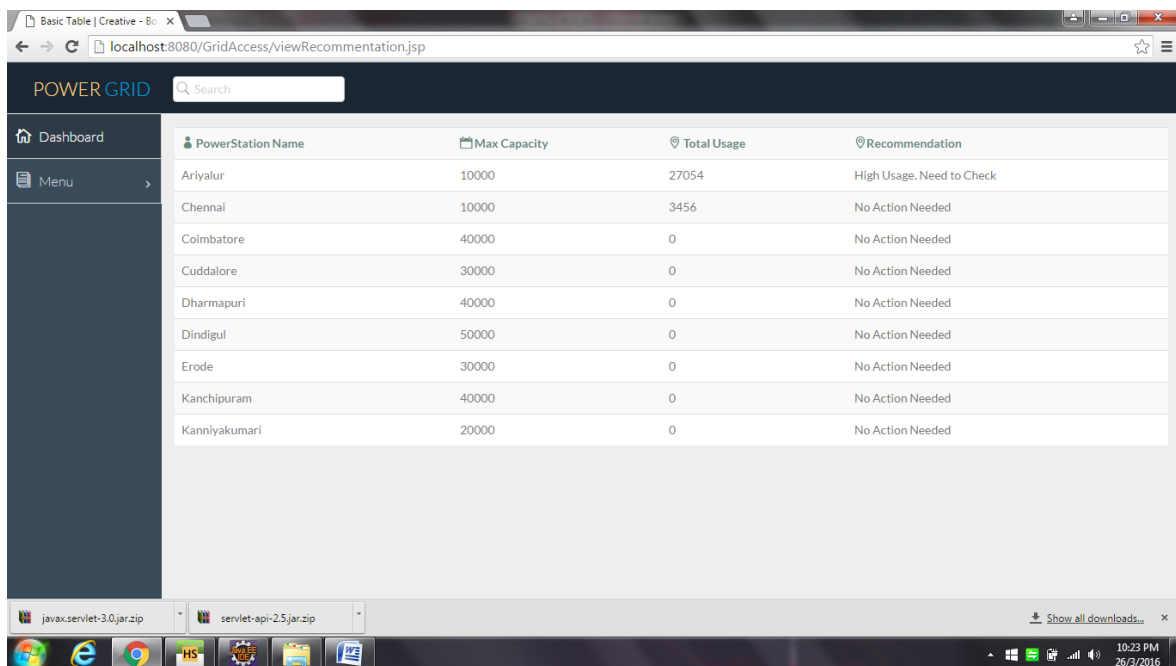
Finally the Grid can compare the overall supply which is given by power station and overall demand which is manipulated using user’s readings. After the comparison the grid would generate a report for supply

and demand and send the demand request report to power station. Along with the report, a recommendation report is also generated. This report is generated based on some criteria and it produces recommendations such as no action needed, need to alert the user or informing the power station to check the reason for over usage.



PowerStation Name	Max Capacity	Total Usage
Ariyalur	10000	1685
Chennai	50000	35400
Coimbatore	10000	10176
Cuddalore	10000	0
Dharmapuri	40000	0
Dindigul	30000	0
Erode	50000	0
Kanchipuram	40000	0
Kanniyakumari	30000	0
Karur	20000	0
Krishnagiri	40000	0
Perambalur	40000	0
Pudukottai	50000	0
Ramanathapuram	30000	0

Figure 6: Report showing demand for electricity



PowerStation Name	Max Capacity	Total Usage	Recommendation
Ariyalur	10000	27054	High Usage. Need to Check
Chennai	10000	3456	No Action Needed
Coimbatore	40000	0	No Action Needed
Cuddalore	30000	0	No Action Needed
Dharmapuri	40000	0	No Action Needed
Dindigul	50000	0	No Action Needed
Erode	30000	0	No Action Needed
Kanchipuram	40000	0	No Action Needed
Kanniyakumari	20000	0	No Action Needed

Figure 7: Recommendation report



Techniques:

- Identity-based encryption
- Signature and proxy re-encryption

Notations

Let (M, o) , the message be a finite (semi-)group, and let σ be the parameter for security. A homomorphic encryption technique (or homomorphic cryptosystem) applied on M is a quadruple (K, E, D, A) of probabilistic, expected polynomial time algorithms, fulfilling the following functionalities:

In-formally speaking, a homomorphic cryptosystem is an efficient algorithm to work out an encryption of the product or the sum, of two messages with the encrypted messages and the public key but not the messages themselves.

If M is an additive (semi-)group, then the scheme is known as additively homomorphic and the algorithm is called Add. Otherwise, the technique is known as multiplicatively homomorphic and the algorithm is called Mult.

Encryption Process

If encryption is being done, the default encryption mode that MongoDB Enterprise uses is the AES256-CBC (or 256-bit Advanced Encryption Standard in Cipher Block Chaining mode) via OpenSSL. AES-256 uses a symmetric key; i.e. the same key for the encryption and decryption of the text. MongoDB Enterprise also allows authenticated encryption AES256-GCM (or 256-bit Advanced Encryption Standard in Galois/Counter Mode). FIPS mode encryption is also made available.

The data encryption includes:

- Generating a system key.
- Generating keys for each of the database.
- Encrypting data with the database keys.
- Encrypting the database keys with the system key.

The encryption occurs transparently in the storage layer; i.e. all data files are fully encrypted from a file system perspective, and data only exists in an unencrypted state in memory and during transmission.

Key Management:

The keys of the database are internal to the server and are only paged to disk in an encrypted format. Mongo-DB never pages the system key to the disk under any circumstances.

Only the system key is external to the server (i.e. kept separate from the data and the database keys), and requires external management. To manage the system key, Mongo-DB's encrypted storage engine allows two key management options:

- Integration with a third party key management appliance via the Key Management Interoperability Protocol (KMIP).
- Local key management via a keyfile.

Encryption and Replication

Encryption is not a part of replication:

- System keys and database keys are not replicated, and

- Data is not natively encrypted over the wire.

Eventhough you could use the same key for the nodes, MongoDB recommends the use of individual keys for each node and the use of transport encryption.

CONCLUSION

This paper has intentionally set out to give instruction to the application of the Fully Homomorphic Encryption scheme that could be applied to enhance the security of the Big Data Analytics. Ideally, certain modeling and simulation should have complemented the work, but for time constraints. This paper has adopted Homomorphic encryption algorithm to strengthen the cloud computing with big data for smart grid process. The strength of cloud computing is the ability to manage risks in some particular security issues. In the future, we will try to make advancement to our research by applying crypt mechanism to real time data implementations and producing results to justify our concepts of security for cloud computing using fuzzy logic.

REFERENCES

- [1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. ACM Trans. Inf. Syst. Security 2006;9(1): 1–30.
- [2] J. Baek, Q. Vu, A. Jones, S. Al-Mulla, and C. Yeun. Proc. IEEE Int. Conf. Internet Technol. Secured Trans 2012;668–673.
- [3] A. Bartoli, J. Hernandez-Serrano, M. Soriano, and M. Dohler. Proc. IEEE Conf. Smart Grid Communication 2010; 333–338.
- [4] K. P. Birman, L. Ganesh, and R. V. Renesse. Proc. Workshop Comput. Needs Next Generation Electric Grid 2011;1–33.
- [5] Z. Bojkovic and B. Bakmaz. Proc. 11th Int. Conf. Appl. Comput. Appl. Comput. Sci 2012;83–89.
- [6] D. Boneh and M. K. Franklin. Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol 2001;2139:213–229.
- [7] X. Boyen. International Journal of Applied Cryptograph 2008;1(1):3–21.
- [8] C.-K. Chu, J. K. Liu, J. W. Wong, Y. Zhao, and J. Zhou. Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Soc 2013; 369–380.
- [9] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski. IEEE Trans. Power Delivery, 2010; 25(1):158–169.
- [10] R. Davies. Proc. Power Energy Soc. Gen. Meeting, 2009.
- [11] C. Efthymiou and G. Kalogridis. Proc. 1st Int. Conf. Smart Grid Commun 2010;238–243.
- [12] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin. IEEE Commun. Survey Tutorials 2011;15(1):21–38.
- [13] C. Schridde, T. D_ornemann, E. Juhnke, B. Freisleben, and M. Smith. Proc IEEE Wireless Commun., Netw. Inf. Security 2010;644–649.
- [14] Priya.K and Gunavathi.I. International Conference on Communications and Signal Processing (ICCS) 2015; 1468 – 1472.
- [15] P. Ajitha, Dr. G. Gunasekaran. Journal of Theoretical and Applied Information Technology, Little Lion Scientific 2014;68(1): 20-26.