Efficient And Secure Data Acquisition For Cloud-Supported Internet of Things In Smart Grid

Naveen N[1], Dr. Mary Cherian[2]
[1]Dept of Computer Science & Engineering
[2]Professor, Dept of Computer Science & Engineering
[1, 2] Dr. Ambedkar Institute of Technology, Bengaluru

Abstract- *Cloud-supported Internet of Things (Cloud-IoT) has been broadly deployed in smart grid systems. The IoT front-ends are responsible for data acquisition and status supervision, while the substantial amount of data is stored and managed in the cloud server. Achieving data security and system efficiency in the data acquisition and transmission process are of great significance and challenge, because the power grid-related data is sensitive and in huge amount. In this project, an efficient and secure data acquisition scheme based on CP-ABE (Cipher text Policy Attribute Based Encryption) has been presented. Data acquired from the terminals will be partitioned into blocks and encrypted with its corresponding access sub-tree in sequence, thereby the data encryption and data transmission can be processed in parallel. Furthermore, the framework protects the information about the access tree with threshold secret sharing method, which can preserve the data privacy and integrity from users with the unauthorized sets of attributes. The formal analysis demonstrates that the framework scheme can fulfill the security requirements of the cloud-supported IoT in smart grid. The numerical analysis and experimental results indicate that our scheme can effectively reduce the time cost compared with other popular approaches.*

Keywords- Cloud Computing, Homomorohic encryption, data sharing, Privacy-preserving, Smart Grid.

I. INTRODUCTION

There have been several instances when power grids across the globe risked catastrophic failure[1]. Often, power outages are caused by localized defects in the electricity networks. If a small defect is not dealt in a proper and timely manner, it could lead to a cascading failure of the power supply network. For example, a power outage on the east coast of the U.S. and Canada in 2003 was such a case. A power line was damaged by a tree in Cleveland, OH, USA. Making matters worse is that nearby lines became overloaded and overheated by rerouted power and sagged from the excessive heat. This eventually tripped circuit breakers after these lines contacted trees. Approximately 50 million people in the Northeast U.S. and part of Canada were left without power for several days. Power outages can also be caused by overloaded electrical circuits. Electricity consumption is higher during hotter summer days[2]. In some cases electrical demands may exceed power grid capacity. In such cases appliances should be turned off to conserve energy or additional resources should be added to grid to compensate demands. If left unaddressed, an overloaded power grid could fail, resulting in blackouts. It is thus crucial that we monitor power grid systems in real-time to ensure that abnormalities are dealt with promptly and effectively.

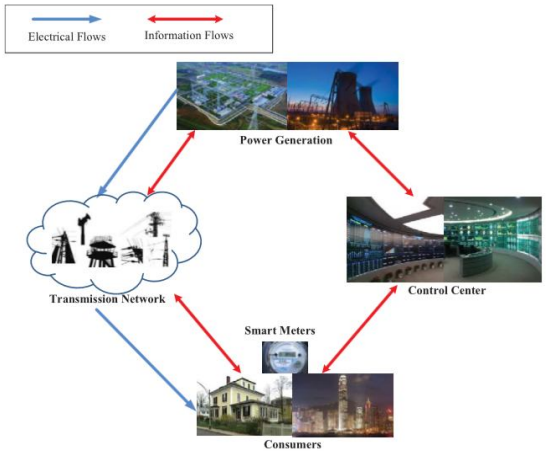

Figure 1: Communication Architecture for Smart Grid

Smart grids have recently been gaining popularity. They support real-time diagnosis and can react to avoid failures and blackouts. In the traditional power grid, there exists only one-way electrical flows, i.e., electricity utilities only deliver power to consumers. In contrast, smart grids allow for two-way information flow communications. As shown in Figure 1, the two-way information flows in the smart grid are almost parallel to that of the one way power flows. However, a control centre is also involved in information flows. A control centre collects data with which it can decide on how to alter a grid. With electricity consumption reports, a control center can analyze consumer's electricity consumption data and forecast electricity consumption, and adjust power generation accordingly over a given period. Regular electricity consumption reports are keys in smart grid efficacy.

To prevent the unauthorized entities from accessing the sensitive information, Associate in Nursing intuitional answer is to cypher information then transfer the encrypted information into the cloud. however, the standard public key encoding and identity based mostly encoding (IBE) can not be directly adopted. The reason is that they only ensure the encrypted data can be decrypted by a single known user, such that it will decrease the flexibility and scalability of data access control.

II. RELATED WORKS

Literature survey is mainly carried out in order to analyze the background of the current project which helps to find out flaws in the existing system & guides on which unsolved problems we can work out. So, the subsequent topics not solely illustrate the background of the project however additionally uncover the issues and flaws that driven to propose solutions and work on this project. a range of analysis has been done on power aware programing. Following section explores different references that discuss about several topics related to power aware scheduling.

The proposed framework is mainly related to "access control of outsourced data." In this section we will review some of these related works. Yu *et al.* [6] Proposed a secure, scalable, and fine-grained data access control system on the cloud server by using key policy attribute-based encryption, proxy re-encryption, and lazy re-encryption.Wang *et al.*[5] Proposed a searchable and privacy-preserving data access control system over outsourced cloud data by using searchable encryption. Shao et al. Recently Shao *et al.* [4] proposed a secure, scalable, searchable, and fine-grained data access control system in cloud computing for mobile devices by using cipher text-policy anonymous attribute-based encryption, proxy re-encryption, lazy re-encryption, and transformation key. However, none of the above systems supports evaluation on the cipher texts.

In the this paper[3], we study the privacy-preserving data sharing in smart grid. In the resultant framework, all the ECs encrypt their electricity consumption reports under the TA's public key. Sahai and Waters proposed the Attribute-Based Encryption (ABE) to realize fine-grained access control on encrypted data. In ABE, the encryption policy is associated with a set of attributes, and the data owner can be offline after data is encrypted. Vipul Goyal et al developed a new cryptosystem for fine-grained sharing of encrypted data based on Sahai's work, called Key-Policy Attribute-Based Encryption (KP-ABE). In their scheme, the ciphertext's encryption policy is associated with a set of attributes, but the attributes that organized into a tree structure (named access tree) are specified by data receivers. Bethencourt et al proposed the Ciphertext Policy Attribute Based Encryption (CPABE). While the proposed framework in this paper is a more generalized one, since it allows the ECs to encrypt their electricity consumption reports under public key as they want.

III. PROPOSED FRAMEWORK

First, we have a tendency to propose a unique data-sharing framework for sensible grid, wherever we have a tendency to mix the 2 fashionable infrastructures: a) the smart grid and b) cloud computing. In particular, we allow the electricity consumption reports generated in smart grid to be stored in the cloud. Distributed ERs can obtain the statistics and analysis results from the cloud computing. Hence, our proposed framework can take advantages of cloud computing for the smart grid. Second, our projected framework makes use of the homomorphic coding technique to facilitate the statistics and analysis on the encrypted electricity consumption reports, and the proxy re-encryption technique to keep the statistics and analysis results secret from the cloud. In this projected theme, any user will recover the outsourced information if and provided that this shopper holds comfortable attribute secret keys with reference to the access policy and authorization key in relevancy the outsourced information. additionally, the projected theme enjoys the properties of constant-size cipher text and tiny computation price. Besides supporting the attribute-level revocation, our projected theme permits Energy Resource to hold out the consumer-level revocation.

System Design

Design is a creative process; a good design is the key to effective system. The system "Design" is outlined as "The method of applying numerous techniques and principles for the aim of shaping a method or a system in enough detail to permit its physical realization". Various design features are followed to develop the system. The design specification describes the features of the system, the components or elements of the system and their appearance to end-users. A solid design is the fundamental for any good software. The design of the project is given in this section.

System Architecture

System design is that the abstract style that defines the structure and behavior of a system. AN style description may well be a proper description of a system, organized in a very method that supports reasoning regarding the structural properties of the system. It defines the system components or building blocks and provides an inspiration from that

merchandise square measure typically procured, and systems developed, which is able to work on to implement the final system.

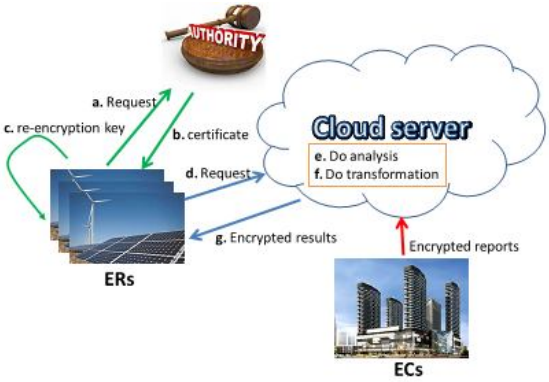

Figure 2 : System Architecture

In this paper, we only focus on how the electricity consumption reports are securely shared among the distributed generation resources. In explicit, we have a tendency to take blessings of the data-as-a-service (DaaS) model in cloud computing, wherever the system consists of the subsequent parties: the trustworthy authority (TA), many electricity customers (ECs), several ERs and therefore the cloud server as shown in Figure.2. The TA is responsible for generating the system parameters and the certificate for the public key of each ER. The ECs manufacture the electricity consumption reports that area unit outsourced to the cloud server to attain the confidentiality, the electricity consumption reports ought to be encrypted by victimisation the general public key of the corresponding ER wherever the consumed electricity comes from. In order to make a smart decision on the power generation, price and others, each ER would like to do analysis on the electricity consumption reports corresponding to itself or other ERs. Before doing the analysis, the ER should obtain the analysis rights from other ERs.

Sequence diagrams of system operation

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows however processes operate with each other and in what order. It's a construct of a Message sequence Chart. The sequence diagrams are shown below,

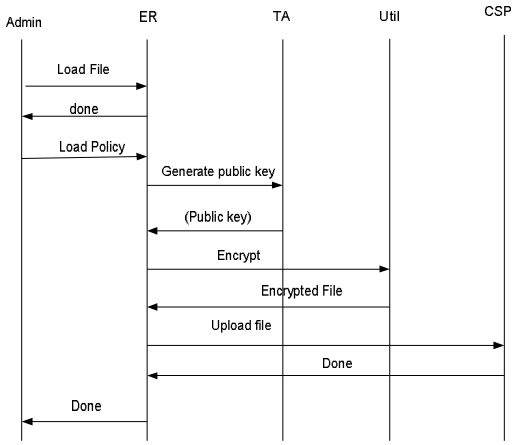

Figure 3: Sequence diagram for Upload Flow

The figure 3 shows the upload flow sequence diagram, where Admin, ER, TA, Util, CSP all are processes in above diagram. Admin loads file to ER, and receives acknowledgment from ER. Admin loads Policy to ER, ER receives the load Policy and asks TA to generate public Key. Util returns the Public Key to ER. ER asks Util to Encrypt the file and forwards the file to Util. Util returns the Encrypted file to ER. The ER uploads the file to CSP [cloud service provider]. CSP sends back the acknowledgement to the ER, that it's done. ER sends the acknowledgment to the Admin, that it's done.

The figure 4 shows the upload flow sequence diagram. where, Admin, EC, ER, TA, CSP, Util, all are processes in above diagram. Admin asks for the required file from the User. EC sends the request to the ER to give the Authorizing keys. The ER returns the authorizing key for the required File. EC requestd for the PrivateKey from the TA. TA returns the private key to the User.EC gets the Downloads File from CSP. EC sends the file to Util for Decrypting. Util returns the file's Decrypted form. EC collects the file from Util and send it to the admin.

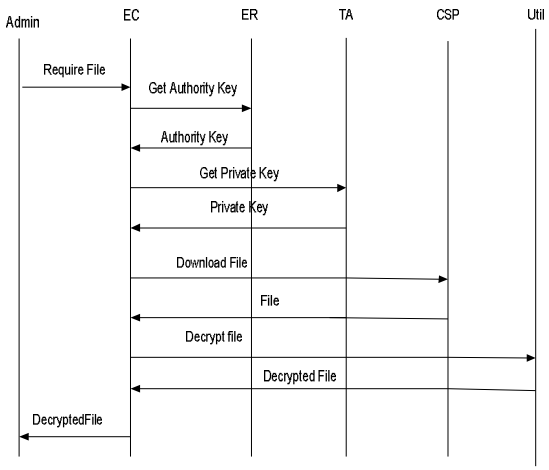

Figure 4: Sequence Diagram for Download Flow

CP-ABE Algorithm

• **Setup**. A irregular algorithmic rule Setup(k) takes in as input a security parameter and provides a collection of public parameters (PK) and therefore the passkey values (MK).

• **coding.** The algorithmic rule Enc(M, T , PK) may be a irregular algorithmic rule that takes as input the message to be encrypted (M), the access structure T that must be happy and therefore the public parameters (PK) to output the ciphertext CT. We can say, that the coding algorithmic rule embeds the access structure within the ciphertext specified solely those users with attributes satisfying T are going to be ready to decipher and retrieve the message M.

• **Key-Generation.** The KeyGen(MK, PK, A) algorithmic rule takes as input the passkey values (MK), the general public parameters (PK) and therefore the attribute set of the user (A), and outputs for the user a collection of secret writing keys SK that confirms the users possession of all the attributes during a and no different external attribute.

• **secret writing**. The secret writing algorithmic rule Dec(CT, SK, PK) takes as input the ciphertext CT, the user secret keys SK and therefore the public parameters PK, and it outputs the encrypted message (M) if and on condition that the attributes A embedded in SK satisfy the access structure T that was used whereas encrypting the ciphertext CT. i.e If T (A) = one then message M is output else, it outputs ⊥.

Result Analysis

In the proposed framework, the reports are encrypted by the homomorphic encryption. Hence, only if the underlying homomorphic encryption scheme is secure, the consumer's privacy in the reports can be guaranteed. On the other hand, the statistics and analysis results are encrypted by the proxy re-encryption. Hence, only if the underlying proxy reencryption scheme is secure, the confidentiality of the results can be guaranteed.In our framework, the TA only needs to generate a certificate for each ER, and the communication cost is only related to this type of data. The cloud server needs to verify the certificate, and run algorithms HE.Eva and PRE.ReEnc for every query from the ER, and the communication cost is related to these three types of data. As for the consumer side, the computation cost and communication cost is quite simple, and it is only related to HE.Enc. Regarding the ER side, the computation cost is mainly related to PRE.ReEnc and PRE.Dec. As shown in figure 5, the performance of our proposed framework is mainly up to the underlying homomorphic encryption scheme and proxy re-encryption scheme. While the proposed framework itself is quite simple and easy to analyze.

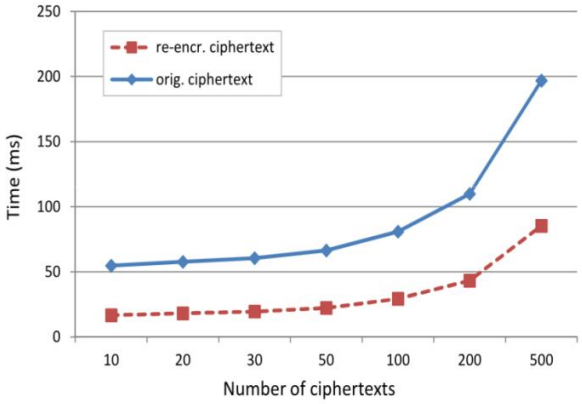

Fig. 5. Experimental results of algorithm HE.Eva

IV. CONCLUSION

In this paper, we have proposed a data-sharing framework for smart grid and also provided facility to access, edit and upload an energy consumption report. The proposed framework mainly studies how to keep smart grid still smart in the sense that electricity consumption reports can be analyzed by distributed ERs, while the consumer privacy in the reports can still be protected. We also presented a concrete scheme (supporting multiplication homomorphism) falling into the proposed framework. Extensive analysis shows that the concrete theme is secure and economical.

In addition work, we plan to design a concrete scheme supporting our requirements for the proposed framework and full homomorphism.. In addition, the proposed scheme provides the user-level revocation for ER in attribute-based data access control systems.

REFERENCES

[1] M. Jacobs, "13 of the largest power outages in history and what they tell us about the 2003 northeast blackout," 2013. [Online]. Available: http://blog.ucsusa.org/mike-jacobs/2003-northeastblackout-and-13-of-the-largest-power-outages-in-history-199

[2] D. Bobkoff, "10 years after the blackout, how has the power grid changed?" 2013. [Online]. Available: http://www.npr.org/2013/08/14/ 210620446/10-years-after-the-blackout-how-has-the-power-grid-change

[3] K. Alharbi, X. Lin, and J. Shao, "A framework for privacy-preserving data sharing in the smart grid," in Proc. IEEE ICCC, Shanghai, China, 2014, pp. 214–219.

[4] J. Shao, R. Lu, and X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for

mobile devices," in Proc. INFOCOM, Toronto, ON, Canada, 2014, pp. 244–252.

[5] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in Proc. INFOCOM, Orlando, FL, USA, 2012, pp. 451–459.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. INFOCOM, San Diego, CA, USA, 2010, pp. 1–9.