International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 1 – JANUARY 2018.

# Privacy Preserved Data Acquisition Process for Smart Grid Applications Using Cloud Technology

Saqib Muhammad Ghulam[#1]

[#]*MSc Computer Science, Szabist, Dubai, United Arab Emirates.*

***Abstract*— The advancements made in the smart meters have enabled the automated process of the billing system of consumer electrical consumption. In order to automate the task of billing systems, cloud based billing model has been suggested. This sort of open source model can be easily traceable and tampered by the third party attackers. Hence, data security is the major concern during data acquisition and transmission process. This paper devises the ciphertext policy –Attribute Based Encryption (CP-ABE) for achieving efficient and secured data learning model for the smart grid systems. A collaborative key is generated for decrypting the data for the authorized user that enhances the security of the system. Initially, the obtained data is preserved with the access control policies. The data owner who possesses the collaborative key can access the sensitive data or else, the attribute revocation model restricts the data permission. By doing so, we can reluctantly solve the key escrow issues with lessened storage consumption in the cloud data sharing systems. Experimental analysis has shown the efficiency of the proposed CP-ABE in terms of time taken for key generation, encryption and decryption process. It depicts that the proposed CP-ABE performed better.**

***Index Terms*—Smart Meter, Energy, Power Consumption, Privacy, Cloud assisted systems and smart grid.**

## I. INTRODUCTION

Electricity is the energy of the future, which is growing day by day relative to that of gas, which is growing more modestly, and that of oil, which is clearly receding. This growth in electricity consumption is due to the development of new information and communication technologies and a climate imperative, i.e., reducing greenhouse gas emissions. The European Union (EU) is committed to reducing its energy consumption by 20% (compared to expected levels) by 2020. However, how can we control the electrical energy? The adaptation of Smart Grid is coming to answer this question. The Smart Grid is defined by the U.S. Department of Energy as an electrical system capable of intelligently integrating the actions of different users, consumers, and/or producers in order to maintain an efficient, sustainable, economical and secure electricity supply [1].

The traditional power grid worked very well from its inception in 1870 until 1970. Even though the consumers' demand for energy grew exponentially, it was still rather predictable. However, there has been a dramatic change in the nature of electrical energy consumption since 1970, as the load of electronic devices has become the fastest growing element of the total electricity demand and new sources of high electricity consumption have been developed, such as electric vehicles (EVs). The power grids endure a significant wastage of energy due to a number of factors, such as consumers' inefficient appliances and lack of smart technology, inefficient routing and dispensation of electrical energy, unreliable communication and monitoring, and most importantly, lack of a mechanism to store the generated electrical energy. Furthermore, power grids face some other challenges as well, including growing energy demand, reliability, security, emerging renewable energy sources and aging infrastructure problems to name a few [2].

In order to solve these challenges, the Smart Grid (SG) paradigm has appeared as a promising solution with a variety of information and communication technologies. Such technologies can improve the effectiveness, efficiency, reliability, security, sustainability, stability and scalability of the traditional power grid. SG solves the problem of electrical energy wastage by generating electrical energy which closely matches the demand. SG helps to make important decisions according to the demand of energy, such as real-time pricing, self-healing, power consumption scheduling and optimized electrical energy usage. Such decisions can significantly improve the power quality as well as the efficiency of the grid by maintaining a balance between power generation and its usage [3].

The paper is organized as follows: Section II presents the related work; Section III presents the proposed work; Section IV presents experimental analysis and results and finally, concludes in Section V.

## II. RELATED WORK

This section presents the prior work studied by other researchers. The author in [4] explained an approach to prove the schemes that can ensure anonymous authentication. In order to define the formal attack model and privacy, the author in [5] use a game on leaking individual meter's measurements. To prove the security model of ID-based multiservice provider authentication scheme, [6] uses security proofs of the work. In order to prove a privacy-preserving scheme is secure in the random oracle model which use a game played between a probabilistic polynomial time adversary A and a challenger C. The author in [7] uses

Zero-Knowledge Proof presented to prove the cryptographic building blocks. Based on strand space model, the author in [8] defines the protocol as a sequence of events for each role of the electric vehicle, local aggregator, and certification/registration authority. Therefore, the idea of sequences of games is used by the scheme in order to prove the semantic security, unforgeability, and batch verification security.

The author in [9] proposed an idea to solve the demand response problem with both spatially and temporally-coupled constraints in the smart distribution grid with a load-serving entity and multiple users. In addition, a recent work presented in [10], suggested an idea in order to guarantee simultaneously privacy, integrity, and availability in smart grid with the advanced metering infrastructure. Based on three main processes, including, 1) metering and querying process; 2) settlement process; and 3) revocation process, the scheme can preserve the customer privacy by ensuring the anonymity of fine-grained metering data. Similarly to the scheme in [11] suggested a pseudonym-based privacy-preserving scheme which is capable of detecting false data injection attacks in a smart-grid system which is equipped with advanced metering infrastructure (AMI). Besides, the scheme in [12] can reassure privacy, integrity, and authenticity. They also studied a scheme which considers three entities in a smart grid, including, (a) energy supplier as registration manager, (b) automation server as bidding manager, and (c) bidders. Specifically, the proposed scheme focuses on secure and private bidding for these three entities without relying on any trusted third party. Based on two main stages, namely, 1) winner announcement and 2) incentive claim, the scheme in [13] can provide anonymity, untraceability, non-linkability, no impersonation, unforgeability, non-repudiation, verifiability, and integrity.

Data aggregation techniques in wireless sensor networks have been proposed in many works [14]. The basic idea of these techniques is based on using an aggregator connected with users and a trusted authority. However, privacy of data aggregation demonstrates many research challenges in privacy protection for smart grids, as discussed by [15]. In order to preserve the privacy of residential users using data aggregation from the residential users to the control center in Smart Grid, [16] suggested protocol called Aggregation Protocol with Error Detection (APED). Specifically, DG-APED protocol uses three main phases, namely, 1) data encryption and reporting, 2) aggregation with error detection and 3) dynamic Join and leave. Using both data encryption and reporting phase, each user perturbs his/her sensed data with generated noise. In addition, DG-APED is not only providing error-detection and fault tolerance, but also is efficient in terms of communication and computation overhead compared to the schemes.

The author in [17] considered one aggregator and users (customers) equipped with an electricity smart meter. Based on two phases, namely 1) meter's reading report and 2) privacy-preserving aggregation. Another interesting work for privacy of data aggregation is studied. The PDA scheme is based on three phases, namely, 1) user report generation, 2) privacy-preserving report aggregation, and 3) secure report reading. PDA is efficient in terms of computation cost and communication overhead. In order to support both spatial and temporal aggregation of user electricity usages, the author in [18] suggested a scheme, called Privacy Preserving Data Aggregation scheme with Fault Tolerance (PDAFT), which is efficient in term of communication overhead compared to the scheme in [19], but lacks a study of computation cost. In the same context of PDAFT, the author in [20] suggested a scheme called DPAFT, which is a new differentially private data aggregation scheme with fault tolerance in order to provide fault tolerance for smart metering.

## III. PROPOSED METHODOLOGY

This section depicts the proposed methodology of our research study. In this work, we have improvised the Ciphertext Policy –Attribute Based Encryption (CP-ABE). The main intention of our study is to achieve the security parameters like confidentiality, integrity, and availability. The entities presented in our systems are discussed as follows:

a) Cloud Owner: It's about the concern of the data. It takes the responsibility of attributes to define the access policy.
b) Cloud User: It is an entity who desires to access the data of others. If the user satisfies the security parameters, then he/she can encrypt/ decrypt the data.
c) Cloud server: It assists to store the data. It also facilitates the sharing services, retrieval and revocation services.
d) Key Administration Center: It combines with the cloud server for generating and managing the keys between the entities for secure communication purpose.

The proposed CP_ABE algorithm is explained as follows:

a) System Initialization: It describes about the security parameters of the system. The security parameter λ is generated for the registered sensitive attributes. It takes the input as, attributes set A arranged in an access structure manner. Thus, it outputs the public paramsParam$_{pub}$ and Public key Pub$_k$. It picks prime order p with random generator g of the group G. It also picks the hash function H:$Z_p$→ G which is defined as:

$$H(x) = g^{bx^2} \prod_{i=1}^{3} h_i^{\Delta i,3\,(x)}$$

Finally, the Params pub (g, e (g, g) $^{\alpha}$) and the secret key $s_k$= (g $^{\alpha}$, a, b, T).

b) Key Adminstration Center: When the KAC authenticates the user $u_{i,}$ the random integer is selected for generating secret key for the user. It takes the inputs of User Identity $U_{id}$, attribute A, and public key Pub$_k$. With these inputs, it generates the secret key $S_k$ for each identity ($U_{id}$). Based on the $U_{id}$, the access policy is defined. A unique path P € y is generated for the $U_{id}$ which helps to generate the secret key.

c) Attribute Lift Model (ALM): It describes the updation

of the key, in case of misbehavior of users. This model composes of lift list $Lift_l$ with a time period t and public key $Pub_k$. It outputs the update details to the KAC. Once the registered user is verified, then the collaborative key is generated for the lift list. Based on the time, the collaborative key is generated as:

$$(\{B^{\alpha_y t} H(t)^{r_{t,y}}, g^{r_{t,y}}\}_y \in ALM\ (lift_l, t))$$

Where $r_{t,y}$ are the random number generates for different users.

d) Encryption ($Param_{pub}$, Data D and time t): With the access policy, the $param_{pub}$, d and t, the ciphertext (D,). The ciphertext is generated for each user $U_{id}$ which is given as follows:

$$C = (C_D, C_s, (C_{i,j}) \quad 1 \le i \le l; 1 \le j \le A$$
$$C = (D, e(g,g)^{\alpha s}, g^s, (g^{D_{i,j}}) H(d)^s, H(t)^s$$

e) Decryption (C ($\Psi$)): If the attributes satisfies the access policy and the collaborative key $Collab_k$, then the data is decrypted. If the user is non-lifted, then the data is decrypted as follows:

$$\langle (L_{j,\bar{y}})_{1 \le j \le n_{max}}, (K_{x,\bar{y}})_{x \in S}, K_{\bar{y}}, D_{\bar{y}}, d_{\bar{y}} \rangle \text{ and } \langle E_{\bar{y}}, e_{\bar{y}} \rangle$$
$$e(C_s, K_{\bar{y}}) = e(g,g)^{\alpha s} e(g,g)^{at_{1,\bar{y}} s} e(g,g)^{t_{\bar{y}} bs}$$

Thus, we have successfully decrypted the data for the authorized users.

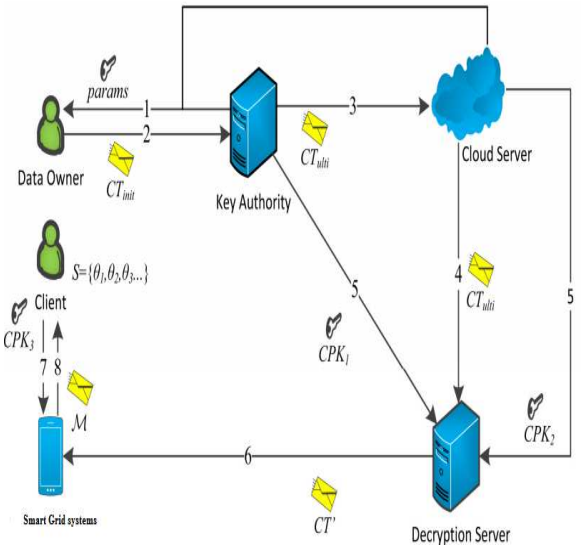


Fig.1. System Architecture

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section reveals the experimental analysis of the proposed systems. The uploaded data is then stored onto the access structure. Each outsourced data is the combination of binary tree with tree height=3 with 2h ciphertext classes. The service expected ratio r is derived from the ratio of present ciphertext c to the aggregate no.ofciphertext classes. The parameter settings for h=16 with variant service expected ratio r is shown in table 1.

| r | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 0.95 |
|---|---|---|---|---|---|---|---|---|---|---|
| Setup | 6.5 | | | | | | | | | |
| Extract | 2 | 4 | 7 | 7 | 12 | 9 | 11 | 13 | 15 | 15 |
| Decrypt | 4 | 6 | 9 | 12 | 14 | 15 | 16 | 18 | 20 | 20 |

TABLE 1. PARAMETER SETTINGS

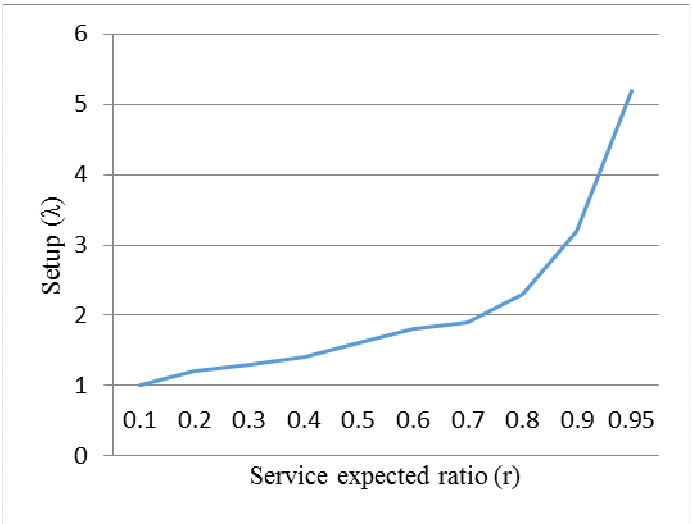


Fig.2. Service expected ratio (r) under tree-based approach

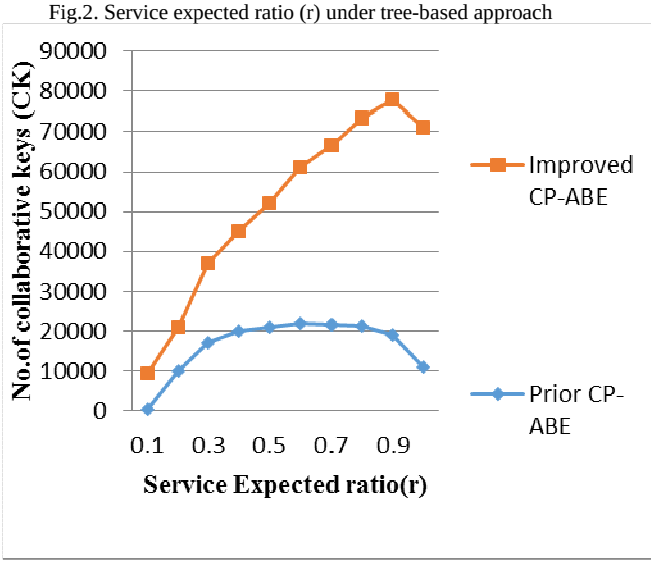


Fig.3. Formation of the collaborative keys for the authorized users

From the fig.2 and 3, our proposed approach, improved CP-ABE works efficiently in terms of service expected ratio and no. of collaborative keys.

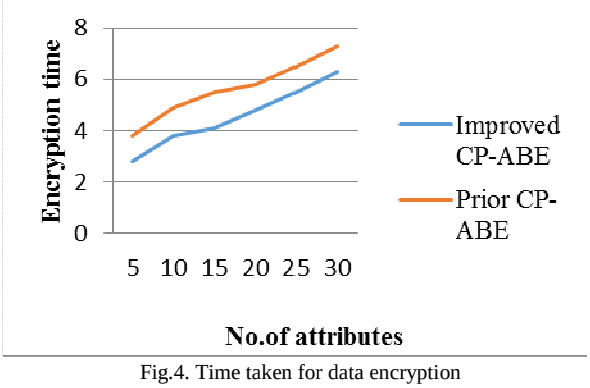


Fig.4. Time taken for data encryption

The fig.4 describes the time taken for the data encryption process. It is evident from the results that the proposed CP-ABE consumes lower time than the prior CP-ABE. Similarly, the time taken for decryption process is also quite lower for providing authenticity of the different users which is shown in fig.5.

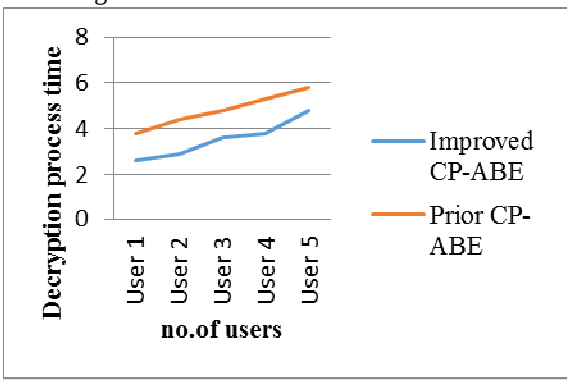


Fig.5 Time taken for decryption process

## V. CONCLUSION

This paper addresses the novel and significant issue of the cloud assisted smart grid applications. The data acquisitioned from the smart grid systems are assisted by the cloud technologies. Usually, Attribute Based Encryption (ABE) is an appropriate model supports practical possibilities of the cloud data information systems. The data collected from the smart grid systems has to be securely preserved at the storage end. In order to support the wide scope of storage services, a novel cloud storage system is adopted. The objective of the system is to securely store the collected data over the cloud environment. We have developed an improved Ciphertext policy- Attribute Based Encryption (CP-ABE) which encrypts and decrypts the data with access policy for an authorized user. The obtained data are stored in the access tree structure with the unique identifier. Based on the unique identifier at time t, the secret key is generated. In order to verify the user, the secret key is used which further helps to generate the collaborative key. With the submission of collaborative key, the encrypted data is decrypted by the authorized user. By doing so, we reluctantly achieved the lesser storage space for large no.of users. Experimental analysis have validated in terms of service expected ratio (key generation time), encryption time and decryption time. It is evident from the results that our proposed CP-ABE achieves better performance than the prior CP-ABE by facilitating the voluminous users.

## REFERENCES

[1] Zhitao Guan et al, “Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Smart Grid”, IEEE internet of things, 2016.
[2] J. Bethencourt, A. Sahai, and B.Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Secur. Privacy, 2007, pp. 321-334.
[3] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute-based encryption,” in Proc. Int. Conf. Pairing-Based Cryptography, 2009, pp. 248-265.
[4] B. Waters, “Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization,” in Proc. Public Key Cryptography, 2011, pp. 53-70.
[5] M. Green, S. Hohnberger, and B. Waters, “Outsourcing the decryption of ABE ciphertext,” in Proc. USENIX Secur. Symp., 2011, pp. 34.
[6] J. Lai, R. H. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Trans. Inf. Forens. Security, vol. 8, no. 8, pp. 1343-1354, 2013.
[7] S. Lin, R. Zhang, H. Ma, and M. Wang, “Revisiting attribute-based encryption with verifiable outsourced decryption,” IEEE Trans. Inf. Forens. Security, vol. 10, no. 10, pp. 2119-2130, 2015.
[8] M. Chase, and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. ACM CCS, 2009, 121-130.
[9] G. Zhang, L. Liu, and Y. Liu, “An attribute-based encryption scheme secure against malicious KGC,” in Proc. TRUSTCOM, 2012, pp. 1376-1380.
[10] J. Hur, “Improving security and efficiency in attribute-based data sharing,” IEEE Trans. Knowl. Data. Eng., vol. 25, no. 10, pp. 2271-2282, 2013.
[11] P. P. Chandar, D. Mutkurman, and M. Rathinrai, “Hierarchical attribute based proxy reencryption access control in cloud computing,” in Proc. ICCPCT, 2014, pp. 1565-1570.
[12] X. A. Wang, J. Ma, and F. Xhafa, “Outsourcing decryption of attribute based encryption with energy efficiency,” in Proc. 3PGCIC, 2015, pp. 444-448.
[13] L. Cheung, and C. Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM CCS, 2007, pp. 456-465.
[14] J. Hur, and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214-1221, 2011.
[15] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” in Proc. ACM CCS, 2006, pp. 99-112.
[16] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM CCS, 2008, pp. 417-426.
[17] A. Xiong, C. Xu, and Q. Gan, “A CP-ABE scheme with system attributes revocation in cloud storage,” in Proc. ICCWAMIP, 2014, pp. 331-335.
[18] Q. Wu, “A generic construction ofciphertext-policy attribute-based encryption supporting attribute revocation,” China Commun., vol. 11, no. 13, pp. 93-100, 2014.
[19] S. S. M. Chow, “Removing escrow from identity-based encryption,” in Proc. Int. Conf. Practice and Theory in Public Key Cryptography, 2009, pp. 256-276.
[20] M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan, and N. E. Othman, “Comparison between android and iOS operating system in terms of security,” in Proc. CITA, 2013, pp. 1-4.