© 2019 IJSRSET | Volume 6 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET196162

Security Preserved Data Acquisition Process for Keen Grid Applications Using Cloud Innovation

P. Raghavan, S. Edwin Raja

Assistant Professor, Department of Computer Science and Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi, Virudhunagar, Tamil Nadu, India

ABSTRACT

The progressions made in the savvy meters have empowered the mechanized procedure of the charging arrangement of purchaser electrical utilization. So as to mechanize the errand of charging frameworks, cloud based charging model has been recommended. This sort of open source model can be effortlessly recognizable and altered by the outsider assailants. Henceforth, information security is the major worry amid information procurement and transmission process. This paper devises the cipher text arrangement–Attribute Based Encryption(CP-ABE) for accomplishing productive and anchored information learning show for the shrewd matrix frameworks. A community oriented key is produced for unscrambling the information for the approved client that upgrades the security of the framework. At first, they got information is protected with the entrance control approaches. The information proprietor who has the synergistic key can get to the touchy information or disaster will be imminent, the trait repudiation show confines the information consent. Thus, we can reluctantly illuminate the key escrow issues with diminished capacity utilization in the cloud information sharing frameworks. Trial examination has demonstrated the productivity of the proposed CP-ABE as far as time taken for key age, encryption and unscrambling process. It delineates that the proposed CP-ABE performed better.

Keywords : Smart Meter, Energy, Power Consumption, Privacy, Cloud Assisted Systems And Smart Grid.

I. INTRODUCTION

Power is the vitality of things to come, which is developing step by step in respect to that of gas, which is developing more unobtrusively, and that of oil, which is obviously subsiding. This development in power utilization is because of the advancement of new data and correspondence advancements and a atmosphere basic, i.e., lessening ozone depleting substance discharges. The European Union (EU) is focused on decreasing its vitality utilization by 20% (contrasted with expected dimensions) by 2020. In any case, how might we control the electrical vitality? The adjustment of Smart Grid is coming to answer this question. The Smart Grid is characterized by the U.S. Office of Energy as an electrical framework able to do astutely incorporating the activities of various clients, purchasers, and additionally makers so as to keep up an effective, practical, conservative and secure power supply [1].

nature of electrical vitality utilization since 1970, as the heap of electronic gadgets has turned into the quickest developing component of the aggregate power request and new wellsprings of high power utilization have been created, for example, electric vehicles (EVs). The power matrices persevere through a huge wastage of vitality because of various components, for example, shoppers' wasteful machines and absence of savvy innovation, wasteful steering and agreement of electrical vitality, untrustworthy correspondence and checking, and most vitally, absence of a component to store the produced electrical vitality. Besides, control networks confront some other challenges too, including developing vitality request, dependability, security, rising sustainable power sources and maturing foundation issues to give some examples [2]. So as to tackle these difficulties, the Smart Grid (SG) worldview has showed up as a promising arrangement with an assortment of data and correspondence advances. Such advances can enhance the adequacy, productivity, unwavering quality, security, manageability, steadiness and adaptability of the conventional power network. SG tackles the issue of electrical vitality wastage by producing electrical vitality which nearly matches the interest. SG settles on imperative choices as indicated by the interest of vitality, for example, ongoing estimating, self-mending, control utilization planning and upgraded electrical vitality use. Such choices can essentially enhance the power quality and in addition the effectiveness of the lattice by keeping up a harmony between power age and its utilization [3]. The paper is sorted out as pursues: Section II shows the related work; Section III shows the proposed work; Section IV presents test investigation and results lastly, finishes up in Section V.

II. RELATEDWORK

This area exhibits the earlier work examined by other scientists. The creator in [4] disclosed a way to deal with demonstrate the plans that can guarantee mysterious confirmation. In request to characterize the formal assault model and protection, the creator in [5] utilize an amusement on releasing individual meter's estimations. To demonstrate the security model of ID-based multiservice supplier validation conspire, [6] utilizes security verifications of the work. So as to demonstrate a protection safeguarding conspire is secure in the irregular prophet demonstrate which utilize an amusement played between a probabilistic polynomial time foe an and a challenger C. The creator in [7] employments 2 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 semanticsecurity, 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, Un-traceability, non-linkability, no impersonation, un-forgeability, 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 perusing. PDA is productive as far as calculation cost and correspondence overhead. So as to help both spatial and transient accumulation of client power utilizations, the creator in [18] proposed a plan, called Privacy Preserving Data Conglomeration conspire with Fault Tolerance (PDAFT), which is effective in term of correspondence overhead contrasted with the plot in [19], however comes up short on an investigation of calculation cost. In the same setting of PDAFT, the creator in [20] proposed a conspire called DPAFT, which is another differentially private information accumulation plot with adaptation to internal failure so as to give adaptation to non-critical failure to shrewd metering.

III. PROPOSED METHODOLOGY

This area delineates the proposed system of our look into study. In this work, we have ad libbed the Cipher text Policy – Attribute Based Encryption (CP-ABE). The primary expectation of our investigation is to accomplish the security parameters like privacy, uprightness, and accessibility. The substances introduced in our frameworks are examined as pursues:

a) Cloud Owner: It's about the worry of the information. It assumes the liability of ascribes to characterize the get to strategy.

b) Cloud User: It is a substance who wants to get to the information of others. In the event that the client fulfills the security parameters, at that point he/she can scramble/decode the information.

c) Cloud server: It helps to store the information. It too encourages the sharing administrations, recovery and denial administrations.

d) Key Administration Center: It joins with the cloud server for producing and dealing with the keys between the substances for secure correspondence reason.

The proposed CP_ABE calculation is clarified as pursues:

a) System Initialization: It depicts about the security parameters of the framework. The security parameter λ is produced for the enlisted touchy properties. It accepts the contribution as, properties set an organized in a get to structure way. Along these lines, it yields general society

paramsParampub and Public key Pubk. It picks prime arrange p with irregular generator g of the gathering G. It additionally picks the hash work H:Zp G which is characterized as:

At last, the Params bar (g, e (g, g) α) and the mystery key sk= (g α, a, b, T).

b) Key Adminstration Center: When the KAC confirms the client ui, the arbitrary whole number is chosen for producing mystery key for the client. It takes the contributions of User Identity Uid, property an, and open key Pubk. With these sources of info, it creates the mystery key Sk for every character (U id). In light of the Uid, the entrance strategy is characterized. A one of a kind way P € y is
produced for the Uid which creates the
mystery key.

c) Attribute Lift Model (ALM): It depicts the updation of the key, in the event of bad conduct of clients. This demonstrates makes out of lift list Lift 1 with a day and age t what's more, open key Pub k. It yields the refresh subtleties to the KAC. When the enlisted client is checked, at that point the synergistic key is produced for the lift list.

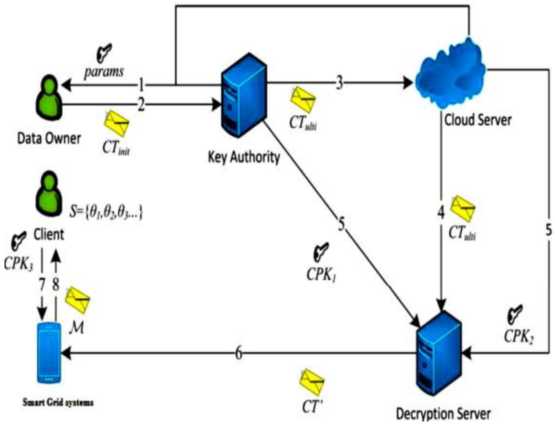

Fig.1. System Architecture

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This segment uncovers the exploratory investigation of the proposed frameworks. The transferred information is then put away onto the get to structure. Each redistributed information is the blend of paired tree with tree height=3 with 2h cipher text classes. The benefit expected proportion r is gotten from the proportion of present cipher text c to the total no.of cipher text classes. The parameter settings for h=16 with variation benefit anticipated proportion r is appeared table 1.

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 Cipher text 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.

VI. 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 attributebased 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 of ciphertext-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.

Cite this article as :

P. Raghavan, S. Edwin Raja, "Security Preserved Data Acquisition Process for Keen Grid Applications Using Cloud Innovation", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), ISSN : 2456-3307, Volume 6 Issue 1, pp. 298-302, January-February 2019. Available at doi : https://doi.org/10.32628/IJSRSET196162
Journal URL : http://ijsrset.com/IJSRSET196162