EFFICIENT SECURITY AND DATA DISTRIBUTE IN CLOUD USING CIPHER TEXT KEY GENERATION METHOD

K. Aruna kumari[1] , G. Pavani[2]
Assistant Professor in CSE Department ,Chalapathi institute of engineering and technology,Lam,Guntur,india

Abstract: Public key infrastructure (PKI) is a substitute other option to open key encryption whereas the Identity Based Encryption IBE is open key and confirmation organization. The issue of utilizing Internet of Things (IoT) in healthcare solutions relates to the problems of latency sensitivity, uneven data load diverse user expectations and heterogeneity of the applications. This paper also introduce the Cloud Intrusion Detection Service (CIDS) which detect the different attack and fire the alert to other cloud user. To prevent the untrusted servers from accessing sensitive data, traditional methods usually encrypt the data and only users holding valid keys can access the data. These methods require complicated key management schemes and the data owners have to stay online all the time to deliver keys to new users in the system. Consequently, the user which is removed cannot access the shared data anymore. Which is provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously Service Provider leaving just a dependable number of basic operations for PKG and clients to perform locally. We propose another progression which is provable secure under the beginning late formulized Refereed giving over of Computation model.

Index Terms: Cloud Computing, encrypting, decrypting, cipher text, security issues, Authentication, Signature, Cryptography, one time password.

1. INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization [1]. Sensitive data should be encrypted before uploading to cloud servers and a secure user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage [2]. . It provides the most modern security protocols. Conventionally, Cryptographic techniques provide protection for data and information transmitted over the network [3]. There are various algorithms available for the security services like authentication of user/data, confidentiality of data, data integrity [4]. The large utilization of sensors, mobility, and geographic distribution lead to issues of data volume, velocity, and variation, along with requirements for accuracy, security, Quality of Service (QoS) user expectations, and operational costs [5]. In this paper proposes encryption technique to providing extra-large security in cloud computing. Key is used to encrypt any type of data. Key function provide random key to data provider and number of user [6]. Data Provider is nothing but the server and data provider is responsible for the upload the data or files to storage sever. Number of user access the uploaded data of files or download the files using the key as well as opt code [7]. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures [8]. Cloud computing

is a hub of various server and many database to store data. The availability of these resources are very flexible in nature i.e. few are available to customers free of cost but some on a pay as use basis [9].

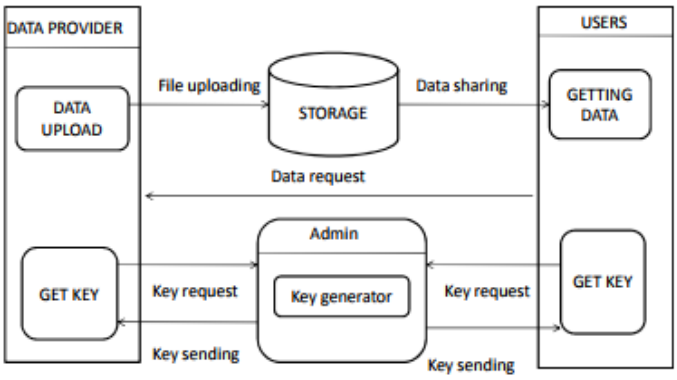

Figure 1: Subsequently data from the cloud server.

2. RELATED WORK

This paper allow the cloud to re-sign blocks on behalf of existing users during user revocation so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud [10]. The defense strategy should is flexible architecture to be applied to several cloud architecture and to Integrate both behavior and knowledge based techniques scheme propose the deployment of IDS on each layer of the Cloud to gather and correlate the alerts from different sensors [11]. Later proposed a authenticated key agreement scheme by applying chaotic map-based cryptography to solve these problems. This scheme realizes the protection of hospital data transmitted in the open channel and provides confidential protection during the remote diagnosing process allowing the patient to enjoy the secure and convenient healthcare through the TMIS [12]. The Health IoT enabled framework collects ECG data from smart phones and other sensors. Later send the collected to the cloud so that Doctors can access and assess the data seamlessly [13]. Cloud-based data analytics is used to detect the abnormality and error of the health data. Normally forward secrecy backward secrecy provided for security [14]. Forward secrecy is used for advanced security. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is used. Data providers upload the files into storage server using the encryption technique [15].

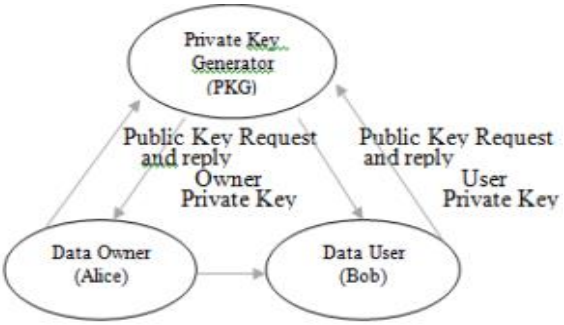

Figure 2: Identity based encryption

3. SYSTEM DESIGN

Data provider first decides the user (e.g Shamir and David) who can share the data. Then Shamir encrypt the data under the identities Shamir and David, and upload the cipher text of the shared data to the cloud server. When either Shamir or David wants to get the shared data, she or he can download and decrypt the corresponding cipher text [16]. If key will be match then user is authorized to download the data. Else it cannot the file. After matching of key again OTP will be send to user for extra security. User can write the OTP within time period Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety [17]. It is asserted that the plan can accomplish fine-grained access control and repudiated clients won't have the capacity to get to the sharing information again once they are revoked.

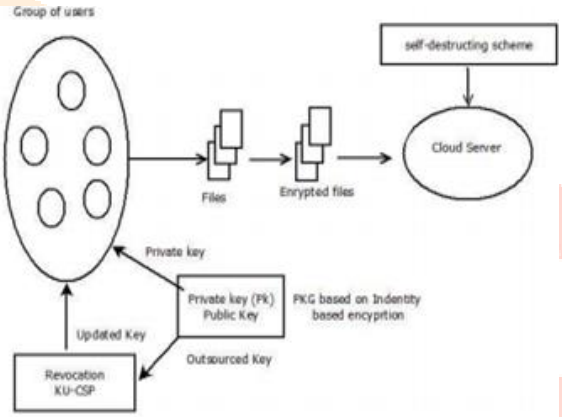

Figure-3: System Architecture

4. PROPOSED SYSTEM

Personality Based Encryption (IBE) which unwinds the general open key and articulation association at Public Key Infrastructure (PKI) is an essential other decision to open key encryption. Notwithstanding, one of the essential effectiveness disservices of IBE is the overhead calculation at Private Key Generator (PKG) amidst client foreswearing. Beneficial renouncement has been all around considered in conventional PKI setting, yet the unwieldy association of affirmations is absolutely the weight that IBE endeavors to reduce [18]. Network admin maintains the Privacy table which contains unique encryption key for all the patients. RSA is a block cipher in which every message is mapped to an integer [19]. Data provider getting key from key generator, using that key data provider will encrypt data and stored into database. Whenever getting the new request from the user that time re-encrypts the data using new key, also uploading in database [20]. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the entrusted cloud [21].

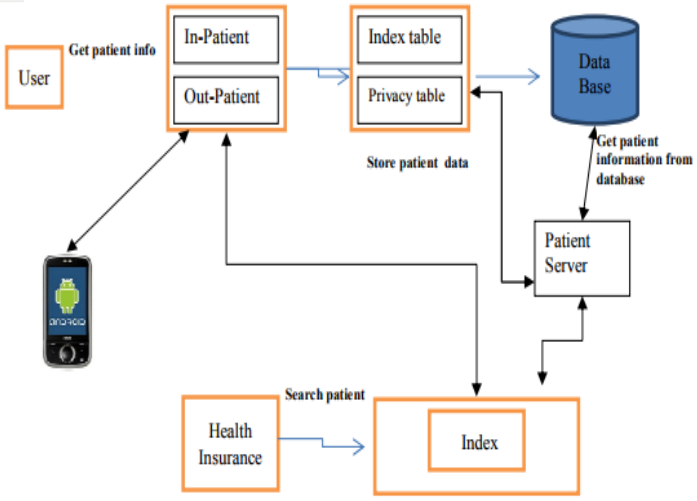

Fig. 4 User getting data based on time

A. **Cipher Text Policy based Key Generation Method**

The data owner will encrypt the stored data and stored into cloud storage the encryption process the data owner will choose stored file and retrieve the name of file. In the encryption process the key will be used as name of file. Before using the file name as key the data owner will encrypt that file name and use that cipher format data as key of the encryption process [22]. The implementation procedure of cipher text policy based key generation schema is as follows.

1. The sender enter plain format data contain character A-M will be transformed into plain text ascii code value pulse 45.
2. The character of plain text contains N- Z will be transposed into plain text ascii code value pulse 19.
3. The plain text range between a-m will be transposed into plain text ascii code value minus 19.
4. The plain text range between n-z will be transpose into plain text ascci code value minus 45.
5. In the second classification process the plain text character range between 0-4 the cipher text is equal to multiplied by 2 plus one.
6. The plain text character range in 5-9 the cipher text is equal to plain text multiplied by 2 minus 10.
7. In the third classification process of plain text character contains special character, the cipher text values is also same as the plain text character.
8. After completion of step 7 result will be taking and convert those characters values into ascii code.

The data owner will take those ascii values as key and perform the encryption process. In this paper we are using idea algorithm for encrypt the data and stored into cloud [23].

B. **One Time Password Generation**

The data consumer or user will perform the decryption process and get the original plain format file the data consumer again verified by system using the one time password verification process. The generation of one time password is as follows [24].

1. During the registration of user will enter password contains numbers from 1 to 9 and get that password.
2. By using that password the system will generate one time password.
3. Before generating one time password the system will generate 9 * 9 format grid contains data of a-z, A-Z, 0-9 and special characters
4. After generating grid the system will take password and retrieve each two value from that password.
5. Take two values and first value will be searching in the row and second value will be searching the column. Here we are maintaining grid position from column wise and row wise
6. So that take those values and repeat this process until the length of password is completed.
7. The result one time password will send to respect mobile number of the data consumer.
8. The data consumer will enter one time password and verify that passwords are equal then the decryption provision will be displayed.
9. If the passwords not equal it will not get decryption provision.

After completion of verification process the data consumer will retrieve the required file name and perform the cipher text policy based key generation schema [25]. By performing that process the data consumer will retrieve the cipher format key and using that it will decrypt the file. By performing the decryption process the data consumer will use idea decryption technique.

5. OTHER IDENTITY BASED ENCRYPTION SCHEMES

Taking after the Boneh-Franklin conspire, loads of other personality based encryption has been proposed. Some attempt to enhance the level of security; others attempt to adjust extraordinary sorts of open key cryptosystems to the setting of personality based encryption. In this segment we give a short review of some critical frameworks that have been created.

A. Hierarchical identity based encryption

The idea of various leveled character based encryption was initially presented in conventional open key infrastructures there is a root testament specialist, and conceivably a progression of other authentication experts. The root expert can issue authentications to experts on a lower level and the lower level endorsement specialists can issue testaments to clients. To diminish workload, a comparable setup could be valuable in the setting of character based encryption. In character based encryption the trusted party is the private key generator [26]. In various leveled personality based encryption framework in which the unscrambling time is the same at each chain of command profundity. It is particular ID secure without irregular prophets and in view of the BDHE issue.

B. Fuzzy identity based encryption

In Fuzzy identity based encryption framework. In Fuzzy identity based encryption, characters are seen as an arrangement of clear qualities, rather than a series of characters. The thought is that private keys can unscramble messages encoded with the general population key ϕ, additionally messages scrambled with people in general key ϕ' if d (ϕ, ϕ') < ϵ for a specific metric d and an adaptation to non-critical failure esteem ϵ. One significant use of fluffy character based encryption is the utilization of biometric personalities [27]. Since two estimations of the same biometric will never be precisely the same, a specific measure of blunder resilience is required when utilizing such estimations as keys. The security of the Sahai-Waters plot diminishes to the changed DBDH issue.

6. PERFORMANCE ANALYSIS

We discuss the performance of the proposed new scheme by comparing it with previous works in terms of communication and storage cost, time complexity and functionalities, these schemes all utilize binary data structure to achieve revocation. Furthermore, by delegating the generation of encryption key to the key authority, the cipher text size of this system also achieves constant. At this end, the key authority has to maintain a data table for each user to store the user's secret key for all time periods. The schema provides logarithmic storage of user's identity instead of linear storage for user identity storage. As the time complexity decreases the number of users involved increases with no effect in performance of the system.

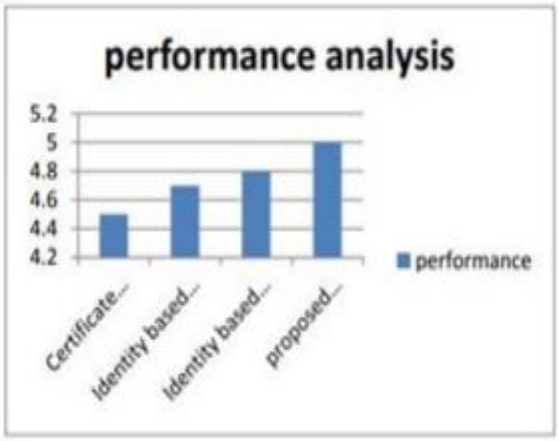

Fig 2: New Identity based encryption

7. CONCLUSIONS AND FUTURE WORK

Cloud computing has brought vast comfort for the society and the individuals. The increased need of allocating the data over the Internet is acquired by the Cloud. This method can solve the issue of protecting patient private information against unauthorized viewers and provide high level of protection. With the inclusion of modern techniques like the Internet of Things (IoT) these Cloud-based solutions become more dynamic and user oriented. The main security issue can be how to control the unauthorized data access in cloud. In this paper we proposed an efficient data access control scheme with improved security. Our

scheme not only restricts the unauthorized. We have given time period to users for downloading data. Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. In the addition, a actual building of RS-IBE is created. This proposal has advantage requisites of functionality and competence, and thus is possible for a realistic and producing good result with effective cost benefit.

8. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008

[2]. Kan Yang and Xiaohua Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[3]. A. Shamir, ―Identity-based cryptosystems and signature schemes,‖ in Proceedings of the 4st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'84. Springer, (1984), pp. 47–53.

[4] D. Boneh and M. K. Franklin, ―Identity-based encryption from the weil pairing,‖ in Proceedings of the 21st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'01. Springer, (2001), pp. 213–229.

[5]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attributebased encryption for fine-grained access control of encrypted data,‖ in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06). ACM, (2006), pp. 89– 98.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[7] International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518

[8]. P.Kalpana, "Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[9]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[10] Jansen W., Karygiannis, T. 1999, ―Mobile agents and security‖. Special Publication 800-19, NIST.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control of encrypted data,‖ in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[12] C. Doukas and I. Maglogiannis. 2012. Bringing IoT and Cloud Computing towards Pervasive Healthcare. In In Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 922–926.

[13] Dubey, Harishchandra and Yang, Jing and Constant, Nick and Amiri, Amir Mohammad and Yang, Qing and Makodiya, Kunal. 2015. Fog Data: ACM, New York, NY, USA, Article 14, 6 pages.

[14] C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT‟06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[15] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC‟08), 2008, pp. 197–206.

[16] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe in the standard model," in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.

[17] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010,vol. 6110, pp. 523–552

[18] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in Advances in Cryptology (ASIACRYPT‟05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.

[19] Rongxing Lu, Xiaohui Liang, Xu Li, XiaodongLin andXuemin (Sherman) Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications",IEEE Transactions on parallel and distributed systems Volume: 23, Issue: 9, Sept. 2012.

[20] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed paper on "Privacy Preserving Delegated Access Control in Public Clouds".

[21] Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong" proposed a paper on "A DFABased Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing".

[22] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identitybased encryption," in Topics in Cryptology (CT-RSA‟09),M. Fischlin, Ed. Berlin, Germany: Springer, 2009, vol. 5473, pp. 1–15.

[23] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS"10), 2010, pp. 261–270.

[24] D. Chaum and T. P. Pedersen, "Wallet databases with observers," in Proc. 12th Annu. Int. Cryptology Conf. Adv. Cryptology (CRYPTO"92), 1993, pp. 89–105.

[25] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," in Trends in Software Engineering, M. V. Zelkowitz, Ed. New York, NY, USA: Elsevier, 2002,vol. 54, pp. 215–272

[26] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

-[27] S. Micali, "Efficient certificate revocation," Tech. Rep., 199