International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

Hash Dynamic Data Allocate in Cloud Using Cloud Intrusion Detection Service

[1]Gongati Mahesh , [2]Borra Subba Reddy

[1]M.Tech Student , [2]Associate Professor

DEPARTMENT OF CSE

Dr.Samuel George Institute of Technology, Markapur, AP.

Abstract: : Cloud computing would be one of technologies which is going to play a vital role in the next generation of computer engineering field. Stored information and encryption keys are usually managed by the cloud provider. It is important to put cryptographically access control on the data we share through cloud. Identity based encryption builds a practical data sharing system. We propose a proxy re encryption technique which performs a two level encryption before storing the actual data into the cloud. We have used AES technique to encrypt data as well as decrypt data this paper also introduce the Cloud Intrusion Detection Service (CIDS) which detect the different attack and fire the alert to other cloud user. Identity Based Encryption (IBE) simplifies public key management and certificate management at Public Key Infrastructure (PKI) with help of Private Key Generator. To ensure the security of data we proposed a method by implementing RSA algorithm. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner). Finally we extend the proposed IBE scheme to present a CRA-aided authentication scheme with no period-limited privileges for managing a large number of various cloud services.

Index Terms: ID-PKS, Cryptography, CRA, Ciphertext, Encryption, Attribute-based signatures, Attribute-based encryption, proxy server, encryption, privacy,

1. INTRODUCTION

Cloud computing is a type of Internet-based computing. Most of the time data will be shared using cloud computing. Cloud is a big area to access any type of data and information. [1]. The Identity Based Encryption technique provides both the forward and backward security which was absent in the previous techniques that were implemented [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]. There is trusted third party called the Private Key Generator (PKG), who generates the corresponding private keys. For encryption and decryption operations, PKG first publishes a master public key, and then generate the corresponding master private key. Using this master public key, any user can generate a public key corresponding to the identity by combining the master public key with the identity value [9].

Fig. 1: Storage identity-based encryption

2. RELATED WORK

A Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which simplify key management in a certificate-based Public Key Infrastructure (PKI) with use of human-intelligible identities as a public keys. Franklin propose a fully functional identity-based encryption scheme (IBE). [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]. In this mechanism the private key has two components, the initially generated secret key is fixed and the time update key is updated frequently for non-revoked users. Thus the non-revoked users can directly decrypts the data stored in cloud while PKG stops issuing private keys for revoked users [15].

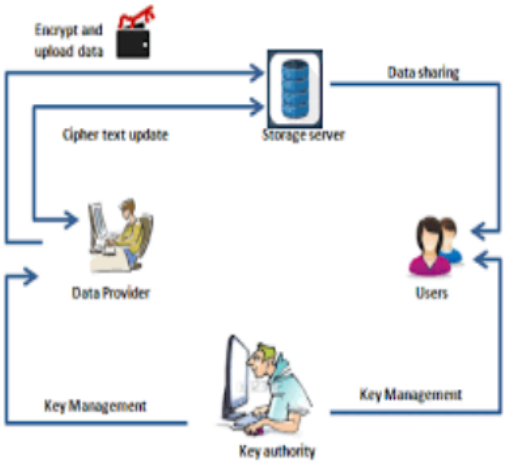

Fig.2. Data Sharing System Using RIBE

3. SYSTEM ARCHITECTURE

It is treated as a public cloud which will be run by another party to provide the capability of computing to PKG for regulating the network by using the services. The KU-CSP is given away from the users or the PKG, this PKG helps to reduce the storage cost and estimation of the users only by giving the flexibility and also the temporary extension to the user infrastructure [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 contains many informative details but here we only visualize it as a service provider, and concentrate on the way of designing it for the purpose of securing the users data with an unreliability KU-CSP. Further it consists of three requirements for such model the requirements.

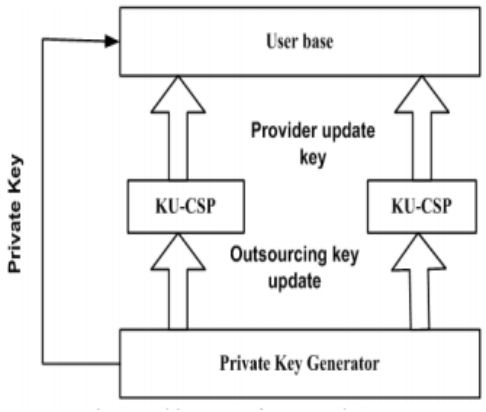

Figure-3: System Architecture

4. PROPOSED SYSTEM

A hash is a random-looking string of characters that individually identifies the data in question, just as it identifies your fingerprint. You can copy any data, either a file or just a string . Find the hash when you are running data using a hash generator. Whenever you have the same data, you will get the exact same hash value as a result [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]. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data [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].

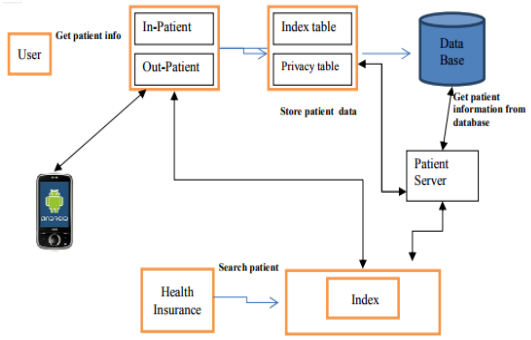

Fig. 4 Privacy preservation in Health care system

A. Homomorphism Scheme

Cryptographic techniques provide protection for data and information transmitted over the network. There are various algorithms available for the security services like authentication of user/data, confidentiality of data, data integrity. Modern cryptography includes the disciplines of mathematics as well as computer sciences and engineering [22]. A cryptosystem performs a pair of transformations called encrypting and decrypting. Encryption means encoding the data so that it cannot be intercepted by anyone except the one who is intended receiver after transforming back to plaintext [23].

1. Key Generation (λ)
   • **Input:** Security parameter λ
   • **Output:** A tuple (Si , Pi) consisting of the secret key Si and public key Pi .
2. Encryption (Pi , Pt)
   • **Input:** A public key Pi and a plaintext Pt
   • **Output:** cipher text Ct
3. Decryption (Si , Ct)
   • **Input:** a secret key Si and a cipher text Ct
   • **Output**: the corresponding plaintext Pi
4. Evaluation (Pi , C, Ct)
   • **Input:** a public key Pi a circuit C with x inputs and a set Pt of x ciphertext,Pt1,Pt2,Pt3,..,.Pt x
   • **Output:** a cipher text Ct

5. HEALTHCARE SOLUTION STRUCTURE

We discuss a general structure of the Cloud-based IoT-Healthcare solutions. Later a Fog-based IoT-Healthcare solution structure in proposed which can be interoperable with the Cloud-based solutions Cloud-based IoT-Healthcare usually comprised of several entities IoT sensors wearable devices [24]. In Healthcare solution, hand held or body connected devices for example; pulse dosimeter ECG monitor smart watches perceive health context of the users. Resource manager is responsible for coordinating the Cloud resources while dealing with IoT enabled Healthcare data [25]. In Cloud-based Healthcare system, two types of Servers are used predominantly Application Server and Database Server. In Application Server the backend applications web-services are hosted whereas Database Server solely handles the data repository and associate operations [26].

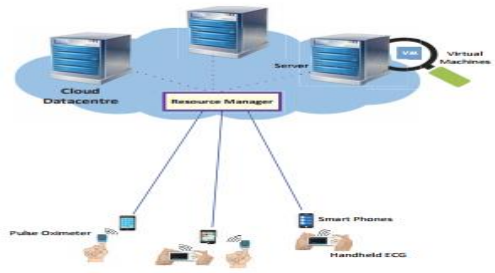

Figure 5: Cloud-based Healthcare System Architecture

A. RSA Algorithm:

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data [27]. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only [28].

The data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.

2. Compute n = a * b.

3. Compute Euler's toting function, Ø(n) = (a-1) * (b-1).

4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.

5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplication inverse of e mod Ø(n).

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).

7. The Public-Key consists of modulus n and the public exponent e (e, n).

8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret (d, n).

User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.

B. AES Algorithm

Algorithm finds the Proxy Re-Encryption: A PRE scheme is represented a topple of polynomial time algorithms (KG; RG; E; R; D). (KG; E; D) are the standard key generation, encryption, and decryption algorithms [29].

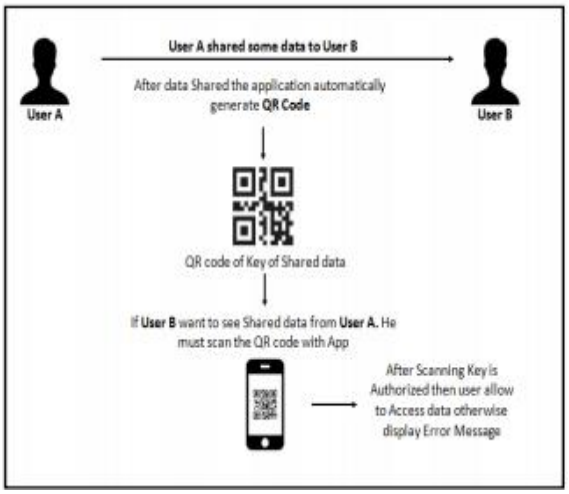

Fig. 6. Data transferring by using QR code scanning.

Step 1: Choose two distinct prime numbers p and q.

Step 2: Find n such that n = pq. n will be used as the modulus for both the public and private keys.

Step 3: Find the toting of n, ϕ(n) ϕ(n)=(p-1)(q-1).

Step 4: Choose an e such that 1 < e

In other words pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or ϕ(n). This is often computed using the Extended Euclidean Algorithm, since e and ϕ(n) are relatively prime and d is to be the modular multiplicative inverse of e. d is kept as the private key exponent Another research direction would be to give the data owner physical access control over the data [30]. Instead of accountability the data owner can create a set of access control rules on his data and send the data along with the access control policy.

6. PERFORMANCE ANALYSIS

We present the Module description, how it works, practical results and environment. Pseudonym Generation: We generate pseudonym for each user..In Triple Data Encryption algorithm, use 192 bits key size. The major challenge in cloud is security of data. So we concentrated mainly on data confidentiality,

forward and backward secrecy but this results in reducing computation costs and increasing complexity.

RSA uses 1024-bit keys but its not secure and it works only if it is correctly implemented and good key management is employed. Hackers will find it difficult to decrypt such encrypted data. Hence papillae cryptosystem is proved to be a stronger mechanism.

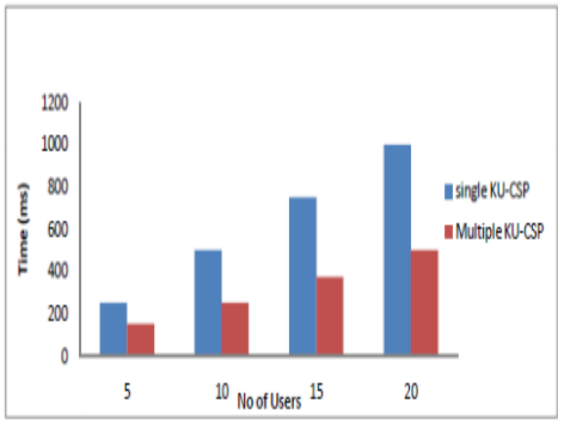

Figure 7: Comparing RSA, Elgamal and Paillier Encryption Time

7. CONCLUSIONS AND FUTURE WORK

Focusing on issue of identity revocation, we have introduced outsourcing computation into IBE and proposed a revocable scheme in which the revocation operations are delegated to CSP. Doctors are provided with highly secured and efficient storage of hospital data hence patient data are accessed securely. This method can solve the issue of protecting patient private information against unauthorized viewers and provide high level of protection. Cloud file sharing also was known as the cloud-based file sharing or online file sharing is a system in which user is allocated storage space on a file server which carries read and writes options on the file server. We have used RS-IBE and AES algorithm to revoke as well as encryption, re-encryption and decryption. We have given time period to users for downloading data. Certificate Authorities and secure communication channels. The increased need of allocating the data over the Internet is acquired by the Cloud. Cloud computing has brought vast comfort for the society and the individuals.

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] Wei, Jianghong, Wenfen Liu, and Xuexian Hu. "Secure Data Sharing in Cloud Computing Using Revocable-Storage IdentityBased Encryption."

[3] Huang, Jyun-Yao, I-En Liao, and Chen-Kang Chiang. "Efficient identity-based key management for configurable hierarchical cloud computing environment."Parallel and

Distributed Systems (ICPADS), 2011 IEEE 17th International Conference on. IEEE, 2011.

[4] Qiu, Shuo, et al. "Identity-Based Private Matching over Outsourced Encrypted Datasets."

[5] Tseng, Yuh-Min, et al. "Identity-Based Encryption with Cloud Revocation Authority and Its Applications."

[6] Wang, Cong, et al. "Secure ranked keyword search over encrypted cloud data." Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010.

[7] Wang, Cong, et al. "Privacy-assured outsourcing of image reconstruction service in cloud." Emerging Topics in Computing, IEEE Transactions on 1.1 (2013): 166-177.

[8] Li, Jingwei, et al. "Outsourcing encryption of attribute-based encryption with mapreduce." Information and Communications Security. Springer Berlin Heidelberg, 2012. 191-201

[9] Prof. Jagruti Dange,Sheetal Y.Gaykwad,Gauri K.Khule,Linakshi N.Ahire,Mansi S. Bodhai,"Advanced Secure Data Sharing In Cloud Computing using Revocable Storage Identity Based Encryption",Vol.4,ISSUE 4,APR-2017.

[10] Shashikumar,Puneeth Hegade,Siddarth Gopinath, Zabiulla, Mrs.Sridevi K N,"Secur data sharing in Cloud Computing Using Revocable Data Using CP-ABE Techniques",Issue 05,Vol.4,2017.

[11] Prof. Hitesh Patel, Prof. Parin Patel, Prof Kiran Patel," Achieving Data Integrity in Cloud Storage Using BLAKE Hash Function", IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939,2014.

[12] Sheena Sathyan, Shaji R S Professor", a hybrid approach for the secure transmission of h.264/avc video streams",Vol.4,2015

[13]. Girishma, V., & Satyanarayana, K. V. V. (2016). Securing data stored in clouds using multi keys and proxy injection schemes. Journal of Theoretical and Applied Information Technology, 88(3), 553-557. Retrieved from www.scopus.com.

[14]. Paruchuri, V. L., Anantha, N. L., Konagala, V. L., & Bhattacharyya, D. (2016). Ciphertext-policy attribute-based encryption for access control of data in cloud. International Journal of Software Engineering and its Applications, 10(8), 13-22. doi:10.14257/ijseia.2016.10.8.02.

[15]. Ramya, K. R., Malleswari, D. N., Rani, C. R., Bhattacharyya, D., & Kim, H. -. (2016). Key aggregate based homomorphic encryption for efficient authentication for secure cloud storage. International Journal of Database Theory and

Application, 9(11), 137-148. doi:10.14257/ijdta.2016.9.11.13.

[16]. Vurukonda, N., & Thirumala Rao, B. (2017). Secure sharing of outsourced data in cloud computing with comparison of different attribute based encryption schemes: A review. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 14), 680-698. Retrieved from

[17] R Canetti, B Riva, & GN Rothblum. (2011). Two 1-round protocols for delegation of computation. Cryptology ePrint Archive, Report 2011/518.

[18] U Feige, & J Kilian. (1997). Making games short. Proceedings of the 29th annual ACM Symp. on Theory of Computing. New York: ACM. pp. 506–516.

[19] S Hohenberger, & A Lysyanskaya. (2005). How to securely outsource cryptographic computations. Proceedings of the 2nd Inter. Conf. on Theory of Cryptography. Berlin: SpringerVerlag. pp. 264–282.

[20] R Canetti, B Riva, & G Rothblum. (2012). Two protocols for delegation of computation. Information Theoretic Security (LNCS). Berlin: Springer. Vol. 7412, pp. 37–61.

[21] X Chen, J Li, J Ma, Q Tang, & W Lou. (2012). New and secure outsourcing algorithms of modular exponentiations. 17th European Symp. on Research in Computer Security, 2012.

[22] MJ Atallah, & KB Frikken. (). Securely outsourcing linear algebra computations. Proceedings of the 5th ACM Symp. on Information, Computer and Communications Security. New York: ACM. pp. 48–59

[23] Secure Data Sharing in Cloud Computing Using Revocable -Storage Identity-Based Encryption Jianghong Wei, Wenfen Liu, Xuexian Hu IJSDR1706010 International Journal Of Scientific Development and Research(IJSDR)

[24] Advance Secure Data Sharing in Cloud computing using Revocable Storage Identity-Based Encryption, International Journal for Research in Emerging Science and Technology, VOLUME-4, ISSUE-4, APR-2017 EISSN: 2349-7610.

[25] Survey: Identity-Based Encryption in Cloud Computing, International Journal of Science and Research(IJSR) ISSN(Online):2319-7064 Index Copernicus Value (2013) :6.14|Impact Factor(2014): 5.611

[26] Identity Based Encryption and Data Self Destruction in Cloud Computing International Journal on Recent and Innovation Trend in computing and Communication, volume 4 Issue: 7 ISSN: 2321-8169156-60.

[27] Authentic Data Sharing by Using Revocable-Storage Identity Based Encryption in Cloud Computing International Journal of Cloud computing International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) vol.4 special. issue 24 August. 2017.

[28] Data sharing in cloud computing using (RS-IBE) Revocable Storage Identity based encryption method IJARIIE-ISSN (O)-2395-4396 vol-2 Issue-5, 2017.

[29] Secure data sharing in cloud computing using Revocable Storage identity-based encryption. IEEE Transactions cloud computing (Volume:4, Issue 99 March 2016)

[30] Securing Cloud Services Using Revocable Identity Based Encryption JETIR (ISSN-2349-5162) March 2017, Volume 4, Issue 03.

AUTHORS DETAILS

Gongati Mahesh , Dr.Samuel George Institute of Technology, Markapur,AP

Mail id:maheshgongati@gmail.com

Borra Subba Reddy, Associate Professor in CSE , Dr.Samuel George Institute of Technology, Markapur, AP.

Mail id:bvsr79@gmail.com