International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Determined and Accurate Access Method for Data Storage in Cloud Using Verification Algorithms

[1]Thumu Subba Reddy, [2]B.V Suresh Reddy
Assistant Professor, Department of CSE,
Tirumala Engineering College, JonnalagaddaVillage, Narasaraopet Mandal. Guntur District, Andhra Pradesh
subbareddy.thumu@gmail.com, boddu.lkv@gmail.com

Abstract: Big data is a collection of huge amount of large datasets and data volume but traditional management process cannot handle the big data storage. New high volume and velocity of big data is effective option to store big data in the cloud as the cloud is capabilities of storing big data and processing new volume of user access requests. It allows analyzing correctness, speed security qualities and computational effectiveness. Many techniques is proposed for achieving secure data access control in any cloud storage system, but policy updating is always a problem. The method is present the idea of quality with weight, being given to upgrade the statement of characteristic, which cannot just extend the expression from paired to discretionary state, additionally help the intricacy method. We propose new scheme that enabling efficient access control with dynamic policy updating for big data in the cloud. We focus to developing the outsourced policy updating method for ABE systems. It includes the data holder and eligible users who need to check the data user for accessing the data the user check content in the next user for accurate plain text recovery. Only the data owner is update the policy for his data in the cloud other than data owner cannot do this.

Index Terms: Cloud, Policy update, Signature generation, Data Protection, big data storage, removing escrow, weighted attribute, Cloud computing.

1. INTRODUCTION

Most existing approaches for securing the outsourced big data in clouds are based on either attributed-based encryption (ABE)or secret sharing to the best of our knowledge, policy update for outsourced big data storage in clouds has never been considered by the existing research [1].. We also update the access policy of the encrypted data in the cloud. Heavy communication overhead of the data retrieval can be eliminated and the computation cost on data owners can also be reduced [2]. The repeal joined work to our use conspire to check strategy be oppose likely assaults, for example, plot and cheating .the RSA cryptosystem, which is utilized for confirmation [3]. Most existing methodologies for securing the outsourced enormous information in mists upheld either ascribed based cryptography or mystery sharing. ABE based generally approaches offer the flexibleness [4]. Data under that policies such that only data users whose attributes that satisfies the access policy can able to decrypt the data [5]. Even though the huge advantages of cloud computing paradigms are exciting for IT companies, researchers and potential cloud users, the security issues in cloud computing will become a serious obstacle [6]. our technique can be utilized to express bigger quality space than any time in recent memory under a similar number of qualities [7].

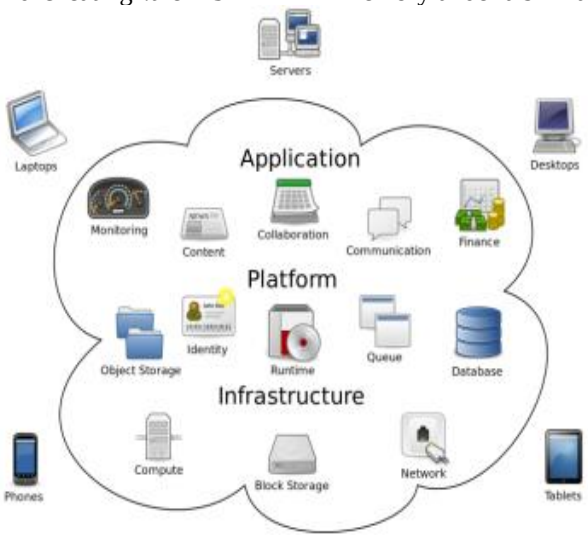

Fig1. Architecture of cloud computing

2. RELATED WORKS

The ABE is regarded as one of the most suitable technologies for data access control in cloud storage because it gives data owners more direct control on access policies [8]. To guarantee clients' certainty of the trustworthiness of their common information on cloud, various strategies have been proposed for information uprightness reviewing with centers around different useful highlights [9]. A fully secure attribute-based encryption scheme and a fully secure (attribute-hiding) predicate encryption (PE) scheme have been proposed [10]. On the other hand, cloud services are very dynamic, distributed and opaque, so establishing and managing trust between cloud service providers and consumers is an important challenge protecting information from cyber-attacks, malware, and internal cyber threats are a challenge [11]. A sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword is updated after the data sharing [12]. The major advantages of NTRU are quantum computing attack resistance and lighting fast computation capability to the best of our knowledge, policy update for outsourced big data storage in clouds has never been considered by the existing research [13].

3. SYSTEM ARCHITECTURE

Multiple users have access to upload the data in different formats and multiple structures with key. A key generator generates a encrypted key which use necessary actions to activate any resource in the cloud [14]. Considering the high volume of big data, it incurs a huge storage overhead even when only doubling the volume of big data. Fortunately, in ABAC, only one copy of cipher texts is generated for each data, which can reduce the storage overhead significantly [15]. Novel scheme was been proposed in this paper which enables for efficient with an access control. The analysis always shows that the policy update is correct and secure. This proposal does not evaluate competitive data ownership verification and flexible compensation for supporting copy and data access controlled for schema optimization [16].

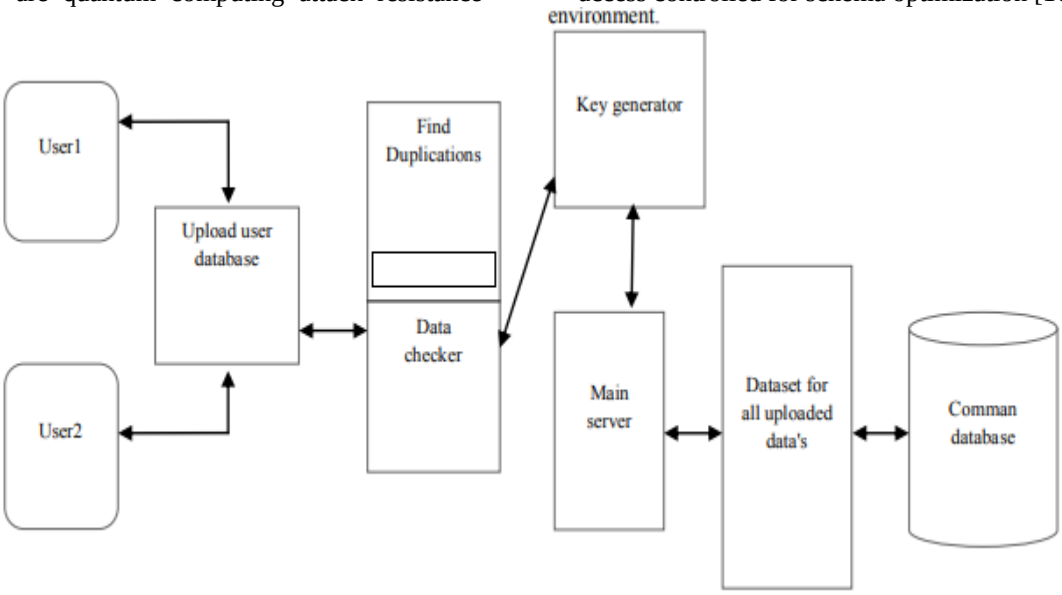

Fig2. The system module

4. PROPOSED SYSTEM

The proposed system focuses on solving the policy updating problem in ABE systems, and proposes a secure and verifiable policy update outsourcing method and let cloud server update the policies of encrypted data directly, which means that cloud server does not need to decrypt the data in the policy updating [17]. The authorities in this system are independent of any other authorities and who are responsible for giving or defining attributes among the different users of the system to user confidence assessment is not considered before withdrawal in the group [18]. In order tackle this TRSE (Two Round Searchable Encryption) scheme is proposed which achieved high data privacy through homomorphism encryption and search accuracy through vector space model.

Fig3. Proposed System Architecture

5. ALGORITHM

The encryption process uses a set of specially derived keys called round keys is applied with other operations, on an array of data that holds exactly one block of data the data to be encrypted.

A. Algorithm: AES

ABE based generally approaches offer the flexibleness for a data proprietor to predefine the arrangement of clients qualified for getting to the information anyway they experience the ill effects of the high many-sided quality of with effectiveness change the entrance strategy and cipher text [19].

Step1. Derive the set of round keys from the cipher key.

Step2. Initialize the new array with the block data

Step3. Add the starting round key to the starting state array.

Step4. Perform nine rounds of state manipulation.

Step5. Result the tenth and final round of new manipulation.

Step6. Copy the final new array out as the encrypted data

The reason new rounds have been listed as nine followed by a final tenth round is because the tenth round different slightly different manipulation from the others.

B. Signature Generation and Verification Algorithms

The specific file in the cloud and dynamic update policy new method has been implemented. So above are the some of the algorithms which are used to implement the dynamic access policy update in the cloud [20].

Step1: Generate File Select
File from local system f={f1,f2,f3,…fn}.

Step2: Encrypt File
Using Encryption for file (Cf),=(Ec,key,f).

Step3: Generate Access policy
Generate Access policy (Acc) for each file (f).

Step4: Upload Upload
Encrypt file (Cf) and Access policy (Acc) upload by data owner.

Step5: Update Access policy
Generate Update access policy (Accup)and Select File (Cf) from cloud Update access policy defends on file

Step6: Update and change access policy
Update Access policy (Accup, Cf)

Here Keys are generating for every unique files. At the time of user retrieving any file key is essential for access the file. In a linear scheme, the secret is viewed as an element of a finite field and the shares are obtained by applying a linear mapping to the secret and several independent random elements [21].

6. RESULTS AND DISCUSSION

We focus on solving the policy updating problem in ABE systems, and propose a secure and verifiable policy updating outsourcing method. Group Signature algorithm is used for user creation and user revocation. In proposed system only authorized user can update or change the access policy and for revoked user it is not possible to upload or download the file from cloud. y. It is based project to support encrypted data stored in the cloud at the equivalent time supports protected data access control. Propose an expressive and efficient data access control scheme for big data, which enables efficient dynamic policy updating.

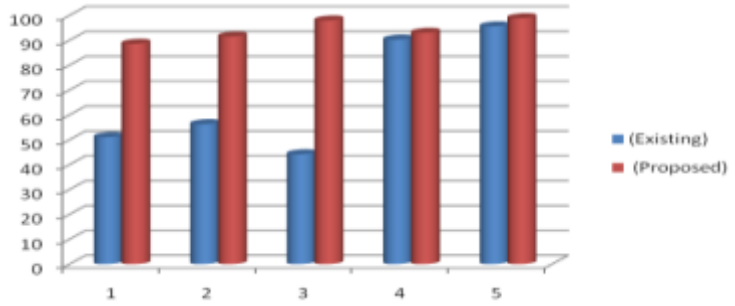

Fig4. Analysis of Graph

7. CONCLUSION AND FUTURE SCOPE

Our scheme allows the data owner to dynamically. Update the corresponding outsourced cipher text to enable efficiently. The proposed scheme guarantees that the actual data owner could pass the cloud server's authentication and legally update the cipher text corresponding to the owner's data, authentication and performance. The Administrator can revoke the users and he will become unauthorized user for the data and even he cannot download the data with the old access policy. Our plan additionally empowers dynamic alteration of get to approaches o underpins proficient on-request client/property denial and break-glass access under crisis situations there is lot of scope for research in improving data security, privacy and access control.

REFERENCES

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.
[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in S&P'07. IEEE, 2007, pp. 321–334.
[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in PKC'11. Springer, 2011,pp. 53–70.
[4] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in EUROCRYPT'10. Springer, 2010, pp. 62–91534–542.
[5] E. Damiani et al. 2010.New Paradigm for Access Control in Open Environment. Proceeding of 5th IEEE International Symposium on Signal Processing and Information.
[6] P. Bonatti and P. Samarati. 2012. A unified framework for regulating access and information release on the web. Journal of computer Security. 10(3): 241-272.
[7] L. Wang, D. Wijesekera and S. Jajodia. 2014. A logic based framework for attribute based access control. Proceeding of ACM workshop on formal methods in Security Engineering. pp. 45-55, ACM press
[8]X. Liu, T. Peng, and J. Wu, and Q. Lin, "Dynamic access policy in cloud based personal health record (PHR) systems", Information Sciences, Vol 379, pp. 62-81,2017.
[9]K. Liang, M.H. Au, K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient cipher text policy attribute based proxy re-encryption for cloud data sharing", Future generation Computer Systems, Vol. 52, pp. 95-108,2015.
[10]J. Weiyu, W. Zhan, L. Limin, and G. Neng, "Towards efficient update of access control policy for cryptographic cloud storage", In China Communications, Vol.12, No. 12,pp.43- 52,2015.
[11]S. R. Krishnan, A. Krishna, and P. Laxmi, "Efficient framework for verifiable access control based dynamic data updates in public cloud", In: Proc. of the International Conference ICDCIT, 2017.
[12]A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic crendentials and cipher text delegation for attribute based encryption", In: Proc. of the International Cryptol Conference, pp.199-217, 2012.
[13]K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud", IEEE Transactions on Parallel and Distributed Systems, Vol 26, No. 12, pp.3461-3470, 2015.
[14]Z. Liu, Z.L. Jiang, X. Wang, S.M. Yiu, C. Zhang, and X. Zhao, "Dynamic attribute based access contol in cloud storage systems", IEEE Trustom/BigDataSE/ISPA, pp.129-137, 2016.
[15] F. Corradini, F. Angelis, F. Ippoliti and F. Marcantoni, "A Survey of Trust Management Models for Cloud Computing", In 5th International Conference on Cloud Computing and Services Science, Pgs. 158-162, 2015.
[16] P. Mell, T.Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.

[17] JieXu, Qiaoyan Wen, Wenmin Li and ZhengpingJin,"Circuit Ciphertext-policy Attribute-based HybridEncryption with Verifiable Delegation in CloudComputing", IEEE TRANSACTIONS ON PARALLELAND DISTRIBUTED SYSTEMS ,2015

[18] Danwei Chen, Liangqing Wan, Chen Wang, Su Pan,YutingJi, "A Multi-authority Attribute-based EncryptionScheme with Pre-decryption", 2015 IEEE SeventhInternational Symposium on Parallel Architectures,Algorithms and Programming

[19] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attributebased encryption "in Proceedings of IEEE Symposium on Security andPrivacy, pp. 321V334, 2007.

[20] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A. Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method", IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 4, 2016.

[21] K. Liang, W. Susilo, and Joseph K. Liu, "PrivacyPreserving Ciphertext Multi-Sharing Control for Big Data Storage", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, 2015.