ISSN:0975-9646

Survey on Efficient Framework for Aggregate Key Management in Cloud.

Shrikant D. Jadhav#1, Jaising Jadhav#2, Vaishali Khaire#3, Pratiksha Giakwad#4 Sandeep Gore#5

#1234Student, 5Asst. Prof., Department of Computer Engineering, Savitribai Phule Pune University.
G.H.Raisoni College of Engineering and Management, Wagholi Pune, India.

***Abstract*— We suggest a decentralized and distributed access control mechanism which will generate and distribute keys to access data shared in public cloud with anonymous authentication with complex but efficient encryption and decryption of data on each access. As data needs to be transferred to and from the cloud on each access, AES and DES encryption scheme will not be used by our system which requires multiple passes to encrypt the data as it is inefficient for real time data transfer that why we use modified reverse circle cypher which exploits benefits of confusion and diffusion. The proposed idea is for public cloud which has multiple tenants which should be efficient in handling aggregate cryptosystem in cloud and should provide fast and efficient access to the shared data and eliminating cloud concerns like data loss or central server loss, data access, privacy and security from untrusted tenants/granter/hackers. Unique key generation, distribution for each transaction and allowed user should be able to access & modify the file based on the given hierarchy.**

***Keywords*— Decentralized, Multiple KDC, Circular character substitution, Cloud storage.**

I. Introduction

Nowadays cloud computing has received a lot of attention because of its advantages over other client-server and other systems. There is a lot of research still being done in academic and industrial work. Cloud computing is using network of remote servers hosted on the internet to store and process data, as opposed to a local server or personal computer. Cloud can provide several services which are put in these categories like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).The example of software as services is Drop box, Google drive, Microsoft One Drive these applications help us store and retrieve data while Google App Engine and Windows Azure which provide platform to developers to produce applications, some users need infrastructures for work which is provided by Google Compute Engine, Amazon's EC2 and Nimbus. As these services are provided by other it frees user for maintaining, upgrading their systems on site to meet any software or hardware demands. Cloud computing not only allows remote data management but also remote computing. An individual user or organization may not require purchasing large amount of data storage instead they can store their large amount of data to cloud to avoid information loss in case of their hardware/ software failures and which is maintained by the cloud providers thus further reducing maintenance and upgrade costs. Even though cloud has many advantages there are issues which need to be addressed.

Those are as follows.

1. Confidentiality -If you back up your data to the cloud, your Cloud Service Provider (CSP) shouldn't be able to see the data you store.
2. Integrity -to ensure that user's data is not modified or destroyed without his consent.
3. Availability- making sure data is available to user through reliable means only.

[2] says Cloud servers are prone to Byzantine failures, where storage server can fail in arbitrary ways. When a centralized cloud goes down in case of a disaster, we propose decentralized approach just as [1] so that the data can be recovered/accessed from other servers. There are some cloud concerns like where is my data or data loss, in case of data loss one can use hybrid cloud or decentralized cloud approach. But in hybrid cloud one has to still maintain his own private cloud which has its own advantages but many disadvantages which are overcome by decentralized approach and encryption of data.

II. Encryption and decryption

Secure data transaction in cloud can be achieved by suitable cryptography method. The data stored in cloud must be encrypted and decrypted when any authorized person or owner needs to access the file. Many methods like (DES & AES) use multiple passes over plaintext thus increasing the level of security [3]. As data is accessed by many users it needs to decrypt the data fast but many algorithm used nowadays are more and more unbreakable only a few algorithm focus on performance. The algorithm we are using is modified version of [4] which uses less time and memory but still retain satisfactory level of security. The algorithm uses circular character substitution for encryption.

III. Key generation and key assignment

The weakness of algorithm lies in the user selection of the key. Since key itself is stored in a file we recommend that the key to be a random set of sequence of alphabets and numbers to make it unique and unpredictable. We propose a unique key generation by selecting random characters from user's profile and time-date stamping it thus providing unpredictability.

A Cloud has large number of users so a single KDC(Key Distribution Center) cannot handle large set of users as well as it is a single point of failure. Therefore we emphasize on multiple KDCs in different locations in different servers. With keys there are a set off attributes only those users having matching set of attributes can decrypt the data stored in cloud.

IV. Literature survey

[1] Recommended decentralized access control scheme for secure storage in cloud with anonymous authentication. Only valid users are able to decrypt the stored data and the system is resistant to replay attacks. The system supports creation, modification and reading of data stored in cloud while providing user revocation. Authentication, communication, computation, storage and access control scheme is decentralized and robust unlike centralized approaches. Their system gained advantage over other system by using several KDCs as single KDC is a single point of failure. [1] Used ABS (Attribute Based Signature) scheme of [6] to provide authenticity, privacy and anonymity for the required user. But in their system cloud knew the access policy for each record stored; it even did not hide the attributes of the users. Their encryption/decryption scheme was not efficient.

[5] Had a distributed access control mechanism which avoided storing multiple encrypted copies of same data in cloud. They used an algorithm where one or more KDCs distributed keys to data owners and users. Owners encrypted data with attributes and users with matching set of attributes could retrieve this data from cloud. Attribute Based Encryption on bilinear parings on elliptic curves was used by them which was collusion secure. While their system did not provide authentication and their main drawback was that the users couldn't write the data, while write access was reserved for creator only. The access structure was not hidden from the cloud.

[6] Proposed ABS (Attribute Based Signature) that allowed a user to sign a message with fine-grain control over his data. The signer possessed a set of attributes which can be used to sign a message with a predicate that can be satisfied by his attribute. The signature hides the attributes used to satisfy the predicate and any identifying information about the signer; this was used by [1] to achieve authenticity and privacy. This method wasn't resistive to replay attacks.

[7] Introduced a Multi-Authority Attribute Based Encryption, in which there was no need for global coordination other than the creation of initial parameters. The user used ABE by simply creating a public key and issuing private keys to different users that reflect their attributes. A user could encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Collusion resistance was achieved by generating user's private key randomly. In their system they assumed no coordination between different authorities. The system was secured by first converting the ciphertext and private keys to a semi-functional form and then arguing security. In their system decryption was done at user's end, so it was inefficient for users using mobile devices. The other drawback of ABE is that the size of the cipher text and the time required to decrypt it grows with complexity. To overcome the problems of [7], [8] suggested to outsource the decryption task to another server thus saving bandwidth and decryption time without increasing the number of transmissions. However the presence of one KDC and one proxy server makes it less robust than decentralized approach.[7] &[8] both had no way to authenticate user anonymously.

[9] Suggested ABS scheme for strong privacy and anonymous authentication but was centralized in nature. His recent paper [6] used improved ABS method with decentralized approach. [10] Combined uses of ABE & ABS scheme to provide access to thin clients with strong data confidentiality and fine grained access control. But [10] was centralized approach and single KDC was used to distribute keys and attributes.[11] was skeptical, as data is outsourced to untrusted cloud service providers security becomes a challenge. Existing systems either produced multiple copies of same data or required trusted cloud. Their Cipher text-Policy Attribute Based Encryption managed attributes and distributed keys in cloud system. They proposed Data Access Control for Multi- Authority cloud storage which provided secure data access control scheme with efficient decryption and revocation.[11] did not provide authentication to the users who wanted to remain anonymous.

[4] Concluded that many encryption techniques have been employed to ensure both personal data security and network security. But few use both. Most common personal security is done using DES & AES which run multiple passes over each block making them ineffective for real time data transfer. They suggest Reverse Circle Cipher which uses circular substitution and reversal transposition to confuse and diffuse. Their method uses variable key length which may be equal to the length of the plaintext. This method of encryption can be utilized for personal security or even for real time packet transfer for network security. Algorithm used by them effectively reduces both time and space complexities. But [4] Algorithm can only be used for text based system

V. Proposed methodology

We use decentralized and distributed access approach for storage and retrieval of data in public cloud instead of private and hybrid cloud. Private and hybrid cloud increase the maintenance and upgradation cost while public cloud is maintained and serviced by service provider and used on subscription basis by user. By using decentralized approach even if one server fails we can still access from other servers. In our experiment we combine the advantages of decentralized distribution as well as advantages of public cloud.

Random characters are selected from users profile string as key which is time and date stamped to create a unique key. Data from file are divided into blocks, block index is used as rotational size. Characters are rotated as clockwise or anti clockwise as per encryption or decryption. Then characters are replaced by special characters and blocks are again concatenated and keys are distributed and managed. These steps are illustrated in figure 1

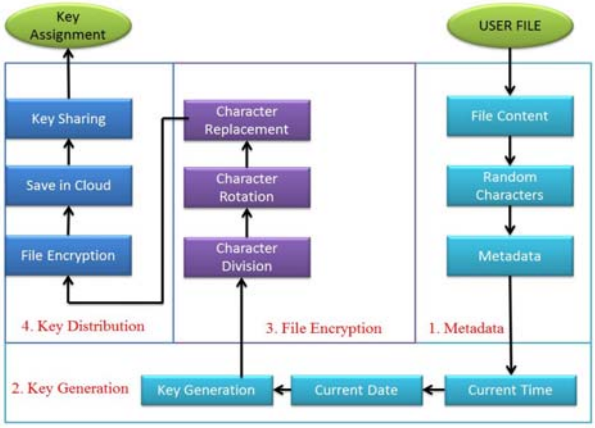

Figure 1: overview of our approach

VI. Discussions

In our experiment the algorithm is used to encrypt the data within our system. But we want to incorporate this to network. The size of the file should be limited as transferring large amounts of data will take more time while transferring small amounts of data will take less time. We assume that the keys will not be same as it will cause error. Cloud has a major disadvantage as it needs internet connection to work.

VII. Conclusion and future work

Reverse Circle Cypher techniques limits us for text based documents for image based files another efficient algorithm can be used. So the idea proposed in this paper is used to provide decentralized and distributed access with complex and efficient encryption/decryption using modified Reverse Circle Cipher and to manage and store keys while providing anonymity.

References

[1] Sushmita Ruj, Milos Stojimenovic, Amiya Nayak "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Trans. Parallel & Distributed Systems Vol 25 Feb 2014.

[2] C.Wang, Q.Wang, K.Ren, N.Cao and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Services Computing, Vol.5 no 2. Apr- June 2012.

[3] Matt Bishop, "Computer Security: Art & Science", Pearson Education, pp. 270-300, 2005.

[4] Ebeneser R.H.P Issac, Joseph H.R. Issac and J.Visumathi, "Reverse Circle Cipher for Personal and Network Security".

[5] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[6] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[7] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EURO-CRYPT), pp. 568-588, 2011.

[8] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp.,2011.

[9] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[10] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

[11] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012