Methodology for Data Security & Data Sharing in Cloud Computing

Kanak Hantodkar Dr. V. M. Thakre

***Abstract*:- CLOUD computing recognizes information technology that shares recourses and low-maintenance characteristics. CLOUD has became the next generation technology for enterprises, as it provides on-demand selfservice, ubiquitous network access, location independent, and less risk of transfer. These advantages bring new and challenging security threats toward users' data. So this paper have explained the papers that studied such as certificateless encryption technique, Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, Privacy-Preserving Public Auditing for Secure Cloud Storage. Hence this paper concluded a new methodology for data security and data sharing in cloud. It includes the two methods that have been discussed that are certificateless encryption and information flow control.**

***Keywords:*- Cloud computing, data sharing, data security, information flow control.**

I. INTRODUCTION

CLOUD computing has expanded to provide inexpensive, practical and on-demand access to computing resources. As the cloud does not know the keys used to encrypt the data, the confidentiality of the data from the cloud is assured. Major issue observed in cloud computing is data security. The idea of data storing by isolating the confidential data of different users in the application but such is not exposed to tenant applications. One of the important services given by cloud providers is data storage. A company allows staff of same group to store and share files in the cloud so that they could be able to access the same data. By utilizing the cloud, the staffs can be completely free from the local data storage and maintenance. It also posed a risk to the confidentiality of those stored files. Due to the high value of the sensitive information, the third party storage servers are the targets of various malicious behaviours which lead to expose of important data. The large size of the data and the user's resource capability, the tasks of auditing data correctness in cloud is expensive for the cloud users. This ensures the data integrity and save users' online burden which is critical to enable public auditing service for cloud. This helps users to resort the third-party auditor (TPA) to audit the data when needed. But the notion of public audit ability is being proposed in the context of ensuring remotely stored data integrity under different system and security models[1].

A traditional public key cryptosystem has a trusted Certificate Authority (CA) to issue digital certificates that binds user to their public keys. Because the CA has to generate its own signature on each user's public key and manage each user's certificate, the overall certificate management is very expensive and complex. CL-PRE (Certificateless Proxy Re-Encryption), which is a scheme for secure data sharing in public cloud environment. As the scheme is based on CL-PKC to solve the key estimation problem and certificate management, it depends on the pairing operations. In this paper, they address the shortcomings of previous approaches and propose a mediated Certificateless Public Key Encryption (mCLPKE) scheme that does not utilize pairing operations. This scheme reduces the computational overhead by using pairing-free approach [2]. The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally supports efficient user revocation and new user joining. The storage overhead and the encryption computation cost are constant. To protect data stored on a semi-trusted server, they adopted attribute based encryption (ABE) as the main encryption primitive. ABE can access policies which is based on the attributes of users or data that enables a user to share their data among few users by encrypting the file under a set of attributes. The complexities per encryption, key generation, and decryption are only linear with the number of attributes involved. To integrate ABE into a large-scale system, important issues are key management scalability, dynamic policy updates, and efficient on-demand revocation are nontrivial to solve, and remain largely open up-to-date[4].

Exploiting data encryption before outsourcing can be one way to mitigate the privacy concerned data auditing, but it can be over killed when employed for unencrypted/public cloud data. Encryption does not solve the problem of protecting data privacy against thirdparty auditing but reduces the complex key management. Unauthorized data leakage is still possible due to exposure of decryption keys. By using the HLA with random masking, this protocol guarantees that the TPA cannot learn any knowledge about the data content in the cloud server (CS) during the auditing process [1].

Also Information Flow Control (IFC) is having the potential to enhance cloud security. This gives a platform that supports the security policies to data. Firstly, developers coordinate with cloud provider and control the data flow in a cloud platform. Second, multi-tenancy, i.e. the practice of sharing services between cloud tenants, this becomes more secure as cloud platform can be checked to enforce security policies. Third, tracks the data flow across different services offered by the cloud provider to log sensitive operations, thus improving accountability[3].

II. PREVIOUS WORK DONE

Al-Riyami and Paterson introduced a new cryptosystem called Certificateless Public Key Cryptography

(CLPKC). Lei *et al* then proposed CL-PRE (Certificateless Proxy Re-Encryption) scheme for secure data sharing incloud. Its scheme is based on CL-PKC manages certificate by relying on pairing operations. But the computational costs required are still high compared to the costs of standard operations. Lu et al. proposed a secure provenance scheme, which is built upon group signatures and ciphertext-policy attribute-based encryption techniques. The user signs encrypted data with her group signature key for privacy preserving and traceability[2]. Narayan et al. proposed an attributebased infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE. Ibraimi et al. applied ciphertext policy ABE (CP-ABE) to manage the sharing of PHRs, and suggested the concept of social/professional domains. Ateniese et al. were the first to consider public auditability in their "provable data possession" (PDP) model for ensuring possession of data files on untrusted storage. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor. Denning proposed a model for secure information flow. The information flow model is a set of logical storage objects or information receptacles that has files, memory segments or program variables depending on the level of detail. Myers introduced the notion of security label to replace the security class of Denning's model. Clearance levels are examined as coarsegrained, permitting unnecessary access and have been replaced by the "need-to-know" principle, also known as Principle of Least Privilege.

III. EXISTING METHODOLOGY

mediated Certificateless Public Key Encryption (mCL-PKE) scheme that does not utilize pairing operations. This scheme reduces the computational overhead by using pairing-free approach. mCL-PKE scheme proves the definitions: The mediated certificateless public key encryption scheme is mCL-PKE=(SetUp , SetPrivateKey , SetPublicKey , SEM-KeyExtract , Encrypt,SEM-Decrypt , USER-Decrypt). They presented the formal security model and provided the security proof. Since mCL-PKE scheme does not depend on the pairing-based operation, it reduces the computational overhead[2].

Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud which is given name as MONA, which is designed for dynamic groups in the cloud. By observing group signature and dynamic broadcast encryption techniques, any cloud user could share data with other user. To achieve secure data sharing for dynamic groups in the cloud,user expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users [5]. Personal health record (PHR) is important patient-centric model for health information exchange, which is to be stored at a third party, such as cloud providers so that it could be easily accessible from any place and at any time. To achieve fine-grained and scalable data access control for PHRs attribute-based encryption (ABE) techniques are used to encrypt each patient's PHR file [4]. This scheme also helps in dynamic modification of access policies and supports in efficient on-demand user/attribute revocation. ABE and MA-ABE is used in the system and gives scalability building PHR systems. In workflow-based access control scenarios, the data access can be given for users' identities rather than their attributes, on the other hand ABE does not handle that efficiently. In those scenarios one may observe the use of attribute-based broadcast encryption (ABBE). The users should be able to use the cloud storage as it is a local without thinking about the need of verifying its integrity [4]. The auditing process is brought in and no new vulnerabilities are introduced towards the users' data privacy, and introduce no additional burden to user. The large size of the data and the user's resource capability, the tasks of auditing data correctness in cloud is expensive for the cloud users. This ensures the data integrity and save users' online burden which is critical to enable public auditing service for cloud. This helps users to resort the third-party auditor (TPA) to audit the data when needed. Encryption does not solve the problem of protecting data privacy against third-party auditing but reduces the complex key management. Unauthorized data leakage is still possible due to exposure of decryption keys. A public auditing scheme has four algorithms (KeyGen, SigGen, GenProof, VerifyProof). To achieve privacy-preserving public auditing proposes unique integrate the homomorphic linear authenticator with masking technique. In this protocol, the linear combination of sampled blocks in the server's response has marked randomly generated by the server. The correctness validation of the block-authenticator pair could be carried out in new way also with the presence of the randomness [1]. Information Flow Control (IFC) which can be explained as Mandatory Access Control Methodology. Earlier IFC models only targeted on security for centralized environment, hence it is observed that there is an opportunity for decentralized IFC for better cloud security. Major issue observed in cloud computing is data security. The idea of data storing by isolating the confidential data of different users in the application but such is not exposed to tenant applications. IFC is data centric, and is used for protection by giving security labels, tracks and limit data propagation. IFC security provides data protection policy that checks by comparing the label associated with the data. Some IFC schemes target custom hardware. When IFC is enforced by Operating Systems, IFC tracking is typically done at the process level. Library-level IFC systems track explicit flow of information within a web application by extending a given language with IFC related features[3].

IV. ANALYSIS AND DISCUSSION

The improved approach performed on certificateless encryption technique a single encryption of each data item and reduces the overall overhead at the data owner. Hence, we can build for multiple users satisfying the same access control policies.

Some methods can be used on MONA to reduce the cost of the encryption computation. We can enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. The credentials from different organizations

may be considered equally effective, for that distributed ABE schemes will be needed. We designate these issues as future works [5]. Extensive analysis proved that schemes are provably secure and highly efficient. Its preliminary experiment was conducted on Amazon EC2 in future it can be demonstrated on the fast performance of the design on both, the cloud and the auditor side. DIFC can be integrated into a PaaS cloud model which can be tested by using existing open source technology as VMware Cloud- Foundry9 and Red Hat Open Shift.

V. PROPOSED METHODOLOGY

Hence it propose a new technique for data security and data sharing in cloud computing by combining the two earlier discussed approaches such as certificateless encryption and information flow control. The certificateless encryption provides the security to the data and maintains its confidentiality. The information flow control provides the data sharing concept in cloud and secure data sharing is done with the help of it. It proposes that data must be encrypted by using certificateless encryption technique and should be shored and transmitted by using information flow control technique. This will help in increasing the security level of data in the cloud and less possibility of data leakage and data accessed by unauthorized person.

VI. POSSIBLE OUTCOME AND RESULT

Data stored an transmitted through this proposed method, data will be secured n easy transfer will be seen. But there might be one drawback that the data that is being encrypted will be isolated in the need of providing confidentiality and it would be difficult to choose whether the data is arranged properly or not. The time required to perform the encryption operation in the mCL-PKE scheme for different message sizes. Since our scheme does not use pairing operations, it performs encryption efficiently. Taint-tracking systems can be seen as the simplest form of runtime IFC. More general runtime IFC methods will manage many different, and possibly orthogonal, notions of data security in their label metadata. For both taint and more general label tracking at runtime, the program statements that an application executes, as well as their execution order, are known. These include statements generated dynamically, e.g. when fetching code at runtime from remote locations. Data isolation is a prerequisite for effective data flow tracking. It prevents the application from exchanging data using mechanisms that are not explicitly controlled or monitored by the runtime IFC system.

VII. CONCLUSION

Security concerns are a major disincentive for use of the cloud, particularly for companies responsible for sensitive data. This paper have proposed the firstly mCL-PKE scheme without pairing operations and provided its formal security. mCL-PKE solves the key escrow problem and revocation problem. Secondly, believe that augmenting existing approaches to cloud security with IFC is a promising way forward. IFC has been used to protect user data integrity and secrecy. Thus, using these both technologies we can protect our data that is stored at cloud and is being shared by other users.

VIII. FUTURE SCOPE

We can further add more new techniques for providing security level to the data. We can also increase the level of encryption to the data to increase its secrecy.

REFERENCES

[1]. Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE. IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.

[2]. An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds Seung-Hyun Seo, *Member, IEEE,* Mohamed Nabeel, *Member, IEEE,* Xiaoyu Ding, *Student Member, IEEE,* and Elisa Bertino, *Fellow, IEEE.* IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 9, SEPTEMBER 2014.

[3]. Information Flow Control for Secure Cloud Computing Jean Bacon, Fellow, IEEE, David Eyers, Member, IEEE, Thomas F. J.-M. Pasquier, Member, IEEE, Jatinder Singh, Ioannis Papagiannis, Peter Pietzuch Member, IEEE. IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT.

[4]. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013.

[5]. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.