Shakti Arora et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 4, December 2016, pp. 66-70

# Enhanced Privacy Preserving Access Control in the Cloud

**Shakti Arora, Surjeet Dalal**

Dept. Computer Science and Engineering, SRM University, India

***Abstract:*** **Cloud computing is the widely used approach of computing utility, whereas users can store their data remotely and don't have any possession of their data. Once users have uploaded their data on the cloud they are not ware about their location and not responsible for maintenance of data. By outsourcing physically large and sensitive data on the outside location increases the threat of privacy and integrity of data. Cloud computing is a very challenging and potentially formidable task. So enabling public audit ability for cloud data storage is very critical and complicated task. In this paper, new adaptive scheme is proposed for privacy preservation of data on cloud. Extensive security and performance analysis shows that proposed schemes are provable and highly efficient.**

**Index Terms−Cloud computing, Access control, Privacy**

## I. INTRODUCTION

Cloud Computing has been envisioned as the next generation information technology architecture for enterprises. It has a number of advantages like : On demand self-service, ubiquitous network access, location independent resource pooling, rapid resources elasticity. Cloud computing has changed the way of business and usage of information technology. Cloud computing can be deployed into three different models:

1) Public model
2) Private model
3) Hybrid model

Private model:- It deals with managing , buying and organizing your own infrastructure. Hosting is done for specific types of clients , infrastructure required for hosting could be on – premises or third part y location. Security concerns are addressed through Virtual private network s or firewall. On premises approach is the better one for deploying private cloud .private models is the most secured and reliable model with limited access and network

**Public model:**

True cloud implementation is public cloud, where services and infrastructure are accessible to variety of clients. Services can be provided to different users either free of cost or pay per bases.
Google is a example of cloud computing. Best model for today's business. Instead of spending a lot on the capital, resources, man power and software we can purchase all of the service on rent ad can pay according to their usability.

**Hybrid d Model:-**

This model provides the advantages of both private and public cloud. This model is used for handling cloud bursting , which refers to a scenario where existing private cloud infrastructure is not able to handle load spikes and requires a fallback option to support the load. So cloud migrates the load between public and private hosting without any inconvenience to users.

## II. PRIVACY PRESERVATION

In real time environment. Thousand of clientcan are accessing the data at thesame time. So cloud service provider should provide astrong user verification mechanism , which is highly secured and reduces the computational overhead of cryptographic computation In the cncern of, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, but still having a large range of possibility of internal and external attacks that threaten the integrity of data.[3]-[7].it's also the possibility that CSP behaves unfaithfully towards the client repository which is outsourced .some unwanted data and rarely used data can be removed or leaked to external entities for financial benefits[8]-[10] in short we can predict that the outsourced data on the cloud is not offereing any guarnteeon data integrity and availability , and if the problem is not addressed , may impede the deployment of cloud architecture

Simply downloading of data everytime and checking the integrity of the data by applying integrity algorithm and then again saving the data on the cloud is very time consuming p and not feasible and practical approach. Overhead of using cloud services could be minimized. For easier management, cloud Server must inly be responsible for verification of the request from single party/ entity. That will reduce the burden over the cloud and increases the throughput. Introduction of third part or one more entity that can provides the assurance of the integrity of data and provides data .It eliminates the burden of users to periodically checking integrity of data. Auditing results provided



by TPA help the cloud service provider to increase the efficiency and usability of cloud resources. With this techniques dependencies of business industries increased and revenue of CSP and companies also increased.

Specifically, our contribution can be summarized as the following three aspects:

1) We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e.,our scheme enables an external auditor to audit user's outsourced data in the cloud without learning the data content.

2) To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

3) We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

## III. DESIGN GOALS

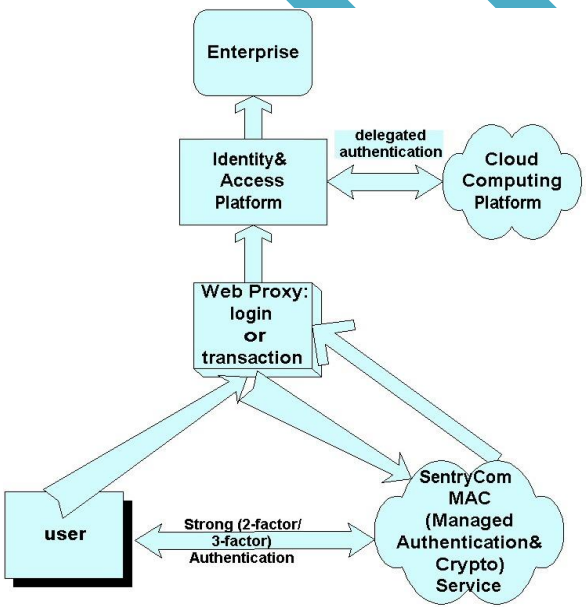
To design a privacy preserving public auditing for cloud data storage following security and performance issues should be considered :-

Public auditability: to allow third party to verify the correctness of cloud storage.

Assurance: To ensure there exist no cheating cloud server that can pass the TPA audit

Privacy preserving; to ensure that TPA cannot derives user content suring audit process.

Lightweight: To allow TPA to perform auditing with minimum communication and computation overhead.




The rest of the paper is organized as follows. Sect

## IV. RELATED WORK

Privacy-preserving cloud computing solutions have been developed from theoretical recommendations to concrete cryptographic proposals.

There are many works which deal with general security issues in cloud computing but only few works deal also with user privacy.

The authors [1] explore the cost of common cryptographic primitives (AES, MD5, SHA-1, RSA, DSA, and ECDSA) and their viability for cloudsecurity purposes. The authors deal with the encryption of cloud storage but do not mention privacy-preserving access to a cloud storage.

The work [2] employs a pairing based signature scheme BLS to make the privacy-preserving security audit of cloud storage data by the Third Party Auditor (TPA). The solution uses batch verification to reduce communication overhead from cloud server and computation cost on TPA side.Further, the paper [3] introduces the verification protocols that can accommodate dynamic data files. The paper explores the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing in a privacy-preserving way.These solutions [2] and [3] provide privacy-preserving public audit but do not offer the anonymous access of users to cloud services.

The work [4] establishes requirements for a secure and anonymous communication system that uses a cloud architecture (Tor and Freenet). Nevertheless, the author does not outline any cryptographic solution. Another non-cryptographic solution ensuring user privacy in cloud scenarios is presented in [5]. The authors propose a client-based privacy manager which reduces the risk of the leakage of user private information.In the paper [6], authors use a non-cryptographic approach to obtain the benefits of the public cloud storagewithout exposing the content of files. The approach is based on redundancy techniques including an information dispersal algorithm (IDA). Nevertheless, these solutions do not protect against the linkability of user sessions which can cause unauthorized user profiling.

Jensen et al. [7] propose an anonymous and accountable access method to cloud based on ring and group signatures. Nevertheless, their proposal uses a group signature scheme [8] which is inefficient because the signature size grows with the number of users.

The work [9] presents a security approach which uses zero-knowledge proofs providing user anonymous authentication. The main drawback of the proposal is a large communication overhead between a user and a cloud server due to the Fiat-Shamir identification scheme [10]. In the work [11], the author uses the CLsignature scheme [12] and zero-knowledge proofs of knowledge to achieve user's anonymous access to services like digital newspapers, digital libraries, music collections, etc.

The work [13] presents a cryptographic scheme to ensure anonymous user access to information and the confidentiality of sensitive documents in cloud storages. The work[14]deals with anonymity and unlinkability in cloud services by provided group signature schemes[15]. In the next section, we analyze the solutions [11], [13] and [14].

## V. PRIVACY PRESERVING ACCESS CONTROL IN THE CLOUD

We assume that the organizational data are grouped into documents. Each data item in a document is called a subdocument. CloudMask consists of the following entities: • Document Manager (DM) is usually an in-house entity that manages subscriptions and performs policy based encryption of documents. Some parts of the computations perfonned by the DM can be moved to a cloud infrastructure, such as Amazon EC2. However, we need to exercise care in doing so since we need to make sure that the actual keys are not exposed to the cloud. • Cloud Data Service (CDS) is a third party cloud service hosting the encrypted documents. The CDS may work under the SaaS or DaaS model. • Users (Usrs) are the employees of the organization. They register with the DM and retrieve documents from the CDS. • Identity Providers (IdPs) are independent entities that issue certified identity tokens, i.e., commitments 1 of identity attributes, to Usrs. Consider the following scenario. A hospital wants to move its EHRs [16] (documents) to a CDS. Usrs are the hospital employees playing different roles such as receptionist, cashier, doctor, nurse, pharmacist, system administrator, and nonemployees such as patients. A cashier, for example, need not have access to the data in EHRs except for the billing information (subdocument) in them, while a doctor or a nurse need not have access to billing information.

**Audit log generation for regulatory compliance**

Due to various regulatory requirements, organizations need to maintain audit logs related to data access. For example, in USA, health care security and privacy regulations require organizations to keep audit logs that capture who did what to which health record, when, and on which system. In CloudMask, such logging could be easily implemented in different parts of the system. For example, during our OCBE protocol execution, the DM can keep the logs of user credentials that are used to get secrets to generate encryption keys for accessing subdocuments. Since user credentials are never revealed to the DM, we need a separate technique to keep track of user credentials. One possible solution is to use a conditional key escrow which reveals the credentials of a user only when a certain condition is met. Such an approach keeps the credentials of honest users secret from the DM while only revealing the credentials of misbehaving users. The logs kept by the DM could be used later on to identify who may have accessed any given subdocuments. One issue with keeping logs with the DM is that a user who executed the OCBE protocol later on may claim that even though she got the secrets to generate encryption keys, she never used keys to access data. To counter against such issues, another auditing layer could be added to the CDS. For example, each user may be provided pseudonyms and public keys signed by CloudMask. Using such signed pseudonyms and public keys, users can prove their identity to the CDS before retrieving any document. The CDS can easily store logs that are capturing the pseudonyms of the users who are downloading any given document. Given the logs kept by the CDS and DM, we can combine them to precisely learn users who downloaded documents and encryption keys together. We 177 leave the integration of such audit logs to our system as a future work. B. Improving the query efficiency There is a trade-off between the amount of security/privacy and query performance when the data is encrypted and stored in the cloud. Data encryption makes querying and retrieving selected files a challenging task. A naive solution is to let the Usrs download the complete encrypted data set, decrypt it and fi Iter the data they want to access based on the keywords or phrases. Such a solution is not acceptable since it requires high network bandwidth and the Usrs require high capacity storage and processing capabilities as they are required to decrypt all the documents to obtain the document(s) of interest to them. Ideally, the system should be able to let the Usrs download only those authorized encrypted documents they are interested in. One approach to address such issue is to support keyword based search. Since keywords can reveal sensitive information about Usrs, they should be encrypted as well. While traditional search over encrypted data techniques [30], [5], [17], [7] can be utilized to provide a basic keyword based querying capability, it is still an open problem to support authenticated querying beyond simple presence or absence of a set of keywords expressed as a Boolean formula. We plan to support authenticated querying in CloudMask. VI. RELATED WORK Searchable Encryption: Search in encrypted data is a privacypreserving technique used in the outsourced storage model where a user's data is stored on a third-party server and encrypted using the user's public key. The user can use a query in the form of an encrypted token to retrieve relevant data from the server, whereas the server does not learn any more information about the query other than whether the returned data matches the search criteria. There have been efforts to support simple keyword queries [30], [5], conjunctive keyword queries [17] and more recently complex ones involving conjunctive, subset and range queries [7]. The primary focus of such work is to protect the confidentiality of the published data from the third-party servers. Issues related to fine-grained access control (FGAC), such as key management, are not considered and the servers are trusted to preserve the privacy of the users who query the encrypted content. Further, these approaches are not able to support



general monotonic access control policies. There have been some recent attempts to provide keyword based searches in the cloud [31], [10], [21]. While these approaches provide different capabilities, such as fuzzy keyword search [21], ranked keyword search [31] and multi-keyword search [10], they do not provide authenticated search capabilities and do not address key management issues. Attribute Based Encryption: The concept of attribute-based encryption (ABE) has been introduced by Sahai and Waters [28]. ABE can be considered as a generalization of identity based encryption [6], [13] (IBE), where the encryption is based on some identity. Thus, ABE is more expressive than IBE. In an ABE system, the plaintext is encrypted with a set of attributes. The key generation server, which possesses the master key, issues different private keys to users after authenticating the attributes they possess. Thus, these private keys are associated with the set of attributes each user possesses. In its basic form, a user can decrypt a ciphertext if and only if there is a match between the attributes of the ciphertext and the user's key. The initial ABE system is limited only to threshold policies where there should be at least k out of n attributes common between the attributes used to encrypt the plaintext and the attributes users possess. Pirretti et al. [26] gave an implementation of such a threshold ABE system using a variant of the Sahai-Waters Large Universe construction [28]. Since the initial threshold scheme, a few variants have been introduced to provide more expressive ABE systems. Goyal et al. [18] introduced the idea of key-policy ABE (KP-ABE) systems and Bethencourt et al. [4] introduced the idea of ciphertext-policy ABE (CP-ABE) systems. Even though these constructs are expressive and provably secure, it is hard to support group management, especially to provide forward security when a user leaves the group (i.e. attribute revocation) and to provide backward security when a new user joins the group. Some of the above schemes suggest using an expiration attribute along with other attributes. However, such a solution is not suitable for a dynamic group where joins and departures are frequent. Fine-grained Access Control: Fine-grained access control (FGAC) allows one to enforce selective access to the content based on expressive policy specifications. Research in FGAC can be categorized into two dissemination models: pushbased and pull-based models. In a push-based system, content publishers push the content to users either by broadcasting or making the content available in a public location. In a pullbased system, every time users want to access some content, they login to the content provider and retrieve based on the access control policies. Our work focuses on the pull based model, but the techniques introduced can be used to construct push-based systems supporting FGAC. Under the push-based model, the database and security communities have carried out research concerning techniques for the selective dissemination of documents based on access control policies [3], [22]. In all such work, subdocuments are encrypted with different keys, which are provided to users at the registration phase, and broadcast the encrypted subdocuments to all users. However, such approaches require all [3] or some [22] keys be distributed in advance during user registration phase. This requirement makes it difficult to assure forward and backward key secrecy when user groups are dynamic with frequent join and leave operations. Further, the rekey process is not transparent, thus shifting the burden of acquiring new keys on existing users when others leave or join. In contrast, our approach makes rekey transparent to users by not distributing actual keys during the registration phase. Another distinction is that all these approaches focus on achieving confidentiality of the content and privacy of the users who access the content is not considered. In contrast, our goal is not only to provide confidentiality but also to preserve 178 the privacy of users who access the documents. Under the pull-based model, the content publisher is required to be online in order to access the content. There has been some recent research efforts [14], [8] to construct privacy preserving access control systems by combining oblivious transfer [9], [1] and anonymous credentials [2]. The goal of such work is similar to ours but we identify the following limitations. Each transfer protocol allows one to access only one record from the database, whereas our approach does not have any limitation on the the number of records that can be accessed at once since we separate the access control from the authorization. Another drawback is that the size of the encrypted database is not constant with respect to the original database size. Redundant encryption of the same record is required to support policies involving disjunctions. However, our approach encrypts each data item only once as we have made the encryption independent of the policies. Further, such approaches are not designed to support privacy preserving content based access control

## VI. PROPOSED ARCHITECTURE

The Single KDC architecture with no anonymous authentication makes it more complicated and it also increases the storage overhead at the single KDC.

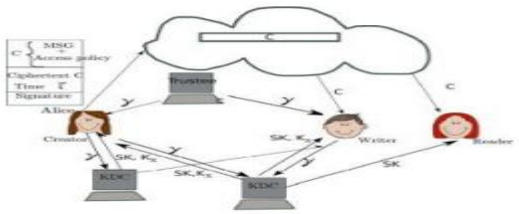


Fig. 2 Decentralized KDC architecture

The pictorial overview of the decentralized KDC is depicted in Fig. 2.The proposed decentralized architecture, also authenticate users, who want to



remain anonymous while accessing the cloud[1]. We proposed a distributed access control mechanism in clouds. In the preliminary version of this paper, we extend the previous work with added features which enables to authenticate the validity of the message without revealing the identity of user who has stored information in the cloud. In this paper, we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy[12]. Our scheme is resistant to replay attacks, in which user can replace fresh data with stale data from previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud[2]. The proposed architecture consists of the following modules. The decentralized Key Distribution Centre architecture here considers two KDC[4]. The pictorial representation of the overall flow of the proposed architecture is depicted in Fig. 2a.

## VII. CONCLUSION

All approaches not provided authentication and also not able to protect the user identity. Existing ids system are not detect HIDS and masquerade attack in efficient way and all takes large time to detect the attack. So there are need to overcome all this problem for that there are need a system to help the data owner achieve fine-grained access control on files stored and allow a multiple write on cloud by cloud servers but also authenticates users who store information in the cloud.

## REFERENCES


[1]. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public cloud,” in IEEE Transactions on Knowledge and Data Engineering, 2014.

[2]. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model” in IEEE International Conference on Information Reuse and Integration (IRI), 2012.

[3]. M. Nabeel and E. Bertino, “Privacy preserving policy based content sharing in public clouds,“In IEEE Transactions on Knowledge and Data Engineering, 2012.

[4]. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, “Towards privacy preserving access control in the cloud,” in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing, ser. Collaborate Com ’11, 2011, pp. 172–180.

[5]. M. Nabeel and E. Bertino, “Towards attribute based group key management,” in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

[6]. Nesrine Kaaniche, Maryline Laurent,” A Secure Client Side Deduplication Scheme in Cloud Storage Environments” 6th International Conference on new Technologies, Mobility and Security year 2014.

[7]. D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security And Privacy, 8(6):40–47, 2010.

[8]. A.Fiat and M. Naor, “Broadcast Encryption,” Proc. 13th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’93), pp. 480-491, 1994.

[9]. D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[10]. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attri-bute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007.

[11]. E. Bertino and E. Ferrari, “Secure and Selective Dissemination of XML Documents,” ACM Trans. Information and System Security, vol. 5, no. 3, pp. 290-321, 2002.

[12]. J. Camenisch, M. Dubovitskaya, and G. Neven, “Oblivious Trans-fer with Access Control,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS ’09), pp. 131-140, 2009.

[13]. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS ’06), PP 89-98, 2006.

[14]. J. Xu, E.-C. Chang, and J. Zhou. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS ’13, pages 195–206, New York, NY, USA, 2013. ACM.

