Concealment safeguarding delegated access control in shared clouds

B Sunitha¹, Ch Sita Kameswari²

¹#1. M.Tech (CST) in Department of Computer Science Engineering, Baba Institute of Technology and Sciences, Visakhapatnam,
²#2. Assoc.Prof, Department of Computer Science and Engineering, Baba Institute of Technology and Sciences, Visakhapatnam. India.

ABSTRACT:
Cloud computing, as a developing computing standard. Cloud computing empowers clients to remotely store their information in a cloud furthermore profit by administrations on-interest. With fast improvement of Cloud computing, more undertakings will outsource their touchy information for partaking in a cloud. To keep up the mutual information secret against untrusted cloud service providers (CSPs), a characteristic path is to store just the scrambled information in a cloud. The significant issues of this methodology incorporate setting up Decomposing Access Control Policies, designated access control for the encoded information, evidence of proprietorship permit stockpiling server to check a client information possession in light of hash quality and the entrance rights from clients when they are no more approved to get to the scrambled information. In the proposed approach the security of clients is ensured while authorizing trait based ACPs and using the two layer of encryption diminish the overhead at Owner, restricted to unapproved access to information and to any information break amid sharing procedure, giving levels of access control confirmation. By utilization of methodologies of ordinary encryption, the security of the data against the cloud was guaranteed and is insufficient to hold up the entrance control approaches of fine grained authoritative implementation. Present day ways to deal with put into impact access control approaches on outsourced data by method for specific encryption oblige associations to regulate all keys and encryptions and transfer encoded information to block off capacity. We anticipated a two layer encryption based way to deal with determination this trouble by assigning however much of access control authorization undertakings as could be expected to Cloud while decreasing data presentation dangers because of plotting clients and additionally Cloud. Under the plan of two layer of encryption and can diminish the overhead of the proprietor and broad recreation results demonstrate that the methodology breaks down the entrance control arrangements. All through the starting encryption and ensuing reencryptions, plan of two layer of encryption was produced that reduces the overhead managed by the proprietor.

Keywords: - Access Control, Anonymous Data, Cloud Computing, Privacy preserving, Two layer encryption.

I. Introduction
Cloud computing is a developing innovation that cleared route for potential commoditization of processing assets. This innovation is on top of virtualization that makes the cloud offerings moderate. With the appearance of versatile and hand held gadgets and advancements with fundamental portable innovations and the omnipresent way of mobiles, Cloud computing extends to cell phones also. This prompted portable Cloud computing where cell phones are connected with Cloud computing and influence advantages of cloud. As individuals of all kinds of different backgrounds are utilizing cell phones, the portability highlight of the gadgets can have colossal effect on use of Cloud computing.
There is consistent development rate anticipated as for versatile Cloud computing in future. As cell phones are vitality and asset compelled, they are defenseless against different security dangers. Unless these dangers are tended to, portable Cloud computing can't be adjusted effortlessly. This paper tosses light into the versatile Cloud computing, its construction modeling, issues included and arrangements. The bits of knowledge got through audit of vital papers can offer in making some assistance with welling educated choices regarding versatile Cloud computing and its applications in this present reality. Cloud computing is the innovation that understands the fantasy of commoditizing figuring assets in comparative manner to power and water. Truth be told Cloud computing empowers clients to get to gigantic figuring assets. This new model of registering people groups and associations to get to processing assets in pay as you utilize style. Along these lines the model dodges the requirement for capital venture. It has got administration models like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Its organization models incorporate private cloud, open cloud, group cloud and half breed cloud. Portable Cloud Computing (MCC) is the Cloud computing where cell phones are included. In this paper our emphasis in on designating access control to open cloud. Towards this end we fabricated a model application that shows the evidence of idea. The assigned access control makes it a suitable model in broad daylight cloud where information proprietors can offer access to their information to various clients. The rest of this paper is organized as takes after.

II. RELATED WORK

Fine-grained access control (FGAC) permits one to authorize particular access to the substance in view of expressive arrangement details. Research in FGAC can be classified into two scattering models: push-based and force based models. Our work concentrates on the draw based model. In the push-based methodologies [2], [3] subdocuments are scrambled with distinctive keys, which are given to clients at the enlistment stage. The scrambled subdocuments are then telecasted to all clients. Nonetheless, such methodologies require that all [4] or some [3] keys be dispersed ahead of time amid client enrollment stage. This necessity makes it hard to guarantee forward and in reverse key mystery when client gatherings are powerful. Further, the rekey procedure is not straightforward, along these lines moving the weight of procuring new keys on clients. Shang et al. [4] proposes way to deal with take care of such issue. It establishes the framework to make rekey straightforward to clients and ensure the security of the clients who get to the substance. In any case, it doesn't bolster expressive access control arrangements as in our methodology furthermore it is not straightforwardly appropriate to force based methodologies. Under the force based model, the substance distributer is required to be online with a specific end goal to give access to the substance. Late research endeavors [10], [12], [5], [13] have proposed ways to deal with build protection saving access control frameworks utilizing an outsider stockpiling administration. In such methodologies, the information proprietor needs to uphold the ACPs and the security of the clients from the substance distributer is not ensured. Further, in some methodologies, various encryptions of the same record are required which is wasteful. A noteworthy downside of all the above methodologies is that they don't consider the administration of scrambled information facilitated in a third get-together when clients are included or expelled from the framework or when the ACPs/subdocuments are upgraded. All the methodologies require the information proprietor to handle encryption. Di Vimercati et al. [7] first distinguishes this issue and proposes a beginning arrangement. While their answer enhances over existing arrangements, such arrangement does not bolster expressive property based approaches and does not ensure the security of the clients. The idea of characteristic based encryption (ABE) has been presented by Sahai and Waters [11]. The introductory ABE framework is constrained just to limit strategies in which there are in any event k out of n properties regular between the credits used to encode the plaintext and the characteristics clients have. Pirretti et al. [2] gave an execution of such a limit ABE framework utilizing a variation of the Sahai-Waters...
Large Universe development [6]. Since this introductory limit plot, a couple of variations have been acquainted with give more expressive ABE frameworks. Goyal et al. [8] presented the thought of key arrangement ABE (KP-ABE) frameworks and Bethencourt et al. [9] presented the thought of figure content strategy ABE (CP-ABE) frameworks. Despite the fact that these builds are expressive and provably secure, they are not suitable for gathering administration and particularly in supporting forward security when a client leaves the gathering (i.e. trait disavowal) and in giving in reverse security when another client joins the gathering. A percentage of the above plans recommend utilizing a lapse trait alongside different properties. Be that as it may, such an answer is not suitable for a dynamic gathering where joins and takeoffs are incessant.

III. CLOUD ACCESS CONTROL CHARACTERISTICS

The identification and definition of Cloud access control characteristics and requirements, namely the access control policy, greatly amplifies the design of a model and the implementation of a mechanism regarding access control. In order to appoint a series of characteristics regarding access control we use the conceptual categorization for Cloud systems proposed in (Gouglishis and Mavridis, 2010). Figure 1 depicts the four layers of the conceptual categorization. The entropy layer identifies requirements from the dispersion of the objects in a system and the assets layer from the type of shared objects within the boundaries of the entropy layer. The management layer defines requirements from policy management and the logic layer incorporates requirements that are not handled by the former layers. A set of core requirements for access control systems that are considered important for the Cloud environment, follows. The identification of the requirements incorporates also characteristics that are exposed by the three levels of the information security infrastructure in the Cloud viz. application level, host level, and network level, where applicable. These characteristics may vary depending on the use cases that need to be supported by a specific system.

IV. POSSIBLE SOLUTIONS FOR THE PRIVACY PROBLEMS BASED ON DIFFERENT METHODS

Cloud Computing is presently one of the hottest topics in information technology (IT). Since the outsourcing of all the essential data is available with a third party, there is always having a concern of cloud service provider’s trustworthiness. Due to data privacy, it is essential for users to encrypt their sensitive data before storing them into the cloud. Yet, there exist some shortcomings in the situation of traditional encryption. When a secret key owner wants to look for some data that are stored in the cloud storage, he may be needed to download all encrypted data from the cloud server, and then decrypts and searches them. If the encrypted data are huge or the client is a mobile user, then it will be very inefficient and is not convenient. Otherwise he must send his key to the cloud server which performs the decryption and search procedures. It causes a serious trouble that the cloud server obtains the secret key So many models were existed to ensure the integrity of data file. In “Provable Data Possession” (PDP) model [4] ensures the possession of data files on untrusted storages. It uses a RSA based homomorphic linear authenticator for auditing outsourced data, but this model leaks the data to external auditors and hence was not provably privacy preserving. Juels et.al [5] describes a “Proof of Retrievability” (PoR) model, where spot-checking and error correcting codes are used in order to ensure the possession and retrievability. But this approach works only with encrypted data. Improved versions of PoR protocols had been proposed which guarantees private auditability and one which make use of BLS signatures. But these approaches were not privacy-preserving. Then comes the TPA based approach to keep online storage honest. This scheme only works for encrypted files which requires the auditor to keep state, and suffers from bounded usage, which potentially brings in online burden to users when the keyed hashes are used up. Thus to provide secure cloud storage supporting privacy preserving many methodologies, frameworks and protocols have been proposed. This paper examines those existing methodologies that guarantee the privacy in cloud.
storage by categorizing it into four types by which the privacy in cloud storage is achieved and performs the analysis on the existing methodologies which best suits to deal with the privacy issue.

Encryption Methods

There are approaches that make use of encryption techniques to achieve privacy in cloud and the papers [6]-[10] state about it. RuWei et.al [6] proposed the design of privacy-preserving cloud storage framework to solve privacy security problem, this comprises the design of data organization structure, the generation and management of keys, the interaction between participants and the handling of change of user’s access right and also supports the dynamic operations of data. It uses an interactive protocol and an extirpation based key derivation algorithm. It ensures data confidentiality, solve ineffectiveness of key derivation, reduces the burden of encryption and decryption, can be able to manage numerous keys, saves owners storage space, reduce run-time overheads of the system, gives excellent privacy security and can apply to multiple users, data owners and service providers. But it needs to have techniques to reduce owner’s encryption burden and to work on ciphertext. A method for improving user privacy with secret key recovery in cloud storage that allows users’ to encrypt their files in the cloud storage has been proposed in [7]. A Secret sharing Algorithm to Key Recovery Mechanism is used. AES-128 to encrypt user’s file, the key length is set to 128 bits is used. Key Recovery scheme partially trusted because no one has the full information about the encryption key except the user himself. The compression algorithm used here is ZIP. The user’s privacy is protected and it decreases the risk of encryption key lose. But it puts a big computation burden for users. It has concerns about transforming speed. Renewing user’s key is a challenge here, users can’t search words and there is dispersal of information. RuWei et.al in [8] provides a privacy-preserving cloud storage framework supporting ciphertext retrieval, it is to solve the problems while operating on an encrypted data and to reduce the data owner’s workload on management of data and support data sharing. Interaction protocol, Key derivation Algorithm, combination of symmetric and asymmetric encryption and Bloom Filter is used here. It can operate on encrypted data; reduce data owner’s workload on managing the data and storage space, reduce communication, computation and storage overhead. It can manage numerous keys and is efficient, safe and economic. But it supports only owner-write-user-read and lacks in technique that support cipher text-based computing. The paper [9] is about controllable privacy preserving search functionalities which include revocable delegated search and un-decryptable delegated search that are based on symmetric predicate encryption in the cloud storage. Thus the Owner of cloud can easily control lifetime and search privileges of data which is suitable for delegation-based business applications. But it cannot support complex access control and search privileges. A method using discretion algorithm [10] for preserving privacy through data control in a cloud computing architecture, which provides security solution that requires more than user authentication and digital certificate are discussed. Here the SP can directly use data without any key and is more flexible and safe to protect individuals’ privacy. But the use of Encryption limits data usage and needs communication and compatibility with heterogeneous host. The main problem in using encryption based technique is that it limits the data usage and puts into an additional burden. The access control mechanisms are available which will overcome the burden of the above overheads.

Access Control Mechanisms

The access control mechanisms that provide privacy has been discussed in papers [11] and [9]. A privacy preserving access authenticated access control scheme for securing data in clouds that verifies the authenticity of the user without knowing the user’s identity before storing information has introduced in [11]. Here only valid users are able to decrypt the stored information. It prevents reply attack, achieves authenticity and privacy. It is decentralized and robust which allow multiple read and write, distributed access control and the identity of user is protected. But in [9] the access policy for each record
stored in the cloud should be known and should be based on assumption that cloud administrator is honest but it does not support complex access control.

**Query Integrity/Keyword Searches**

There are approaches that make use of queries and keyword search scheme to check the privacy in cloud and papers [12]- [13] discusses those schemes. Qin Liuy et.al [12] proposed an efficient privacy preserving keyword search scheme in cloud computing that allows a service provider to participate in partial decipherment and enables them to search the keywords on encrypted files. It makes use of an efficient privacy preserving keyword search scheme (EPPKS). It provides protection of user data privacy, queries privacy and support keyword search on encrypted data. It is found efficient, practical and provably and semantically secure. But the computation on encrypted data was a challenge. A privacy preserving approach for data outsourcing in cloud environment which make use of Fragmentation and heuristic algorithm is used by Sayi et.al [13]. It proves to be efficient and effective but confidentiality is not achieved.

**V. Proposed Scheme**

In this paper the proposed scheme architecture is divided into three main parts: (1) Owner, (2) Cloud and (3) User. Cloud is further divided into three sub parts; Encrypted Storage (ES), Decryption Center (DC) and Key Generation Center (KGC).

The basic method is Double Encryption of the documents means there is two-layer encryption of the data or information. I extend the previous mCL-PKE scheme but in my system there is certification of the users. My simple scheme is owner will encrypt the contents two times using the KGC generated key and stores the documents to the Encrypted Storage, when user request any document the decryption center fetches the requested document and decrypts the outer layer of encryption and gives to the user, now user fully decrypts the document. In this paper the RSA algorithm is proposed which supports asymmetric key approach, RSA algorithm is very easy to implement and enhances the security of the data, and In RSA algorithm malicious users cannot learn the keys.

**Modules:**
The system is proposed to have the following modules along with functional requirements.

1) Identity token issuance
2) Identity token registration
3) Data encryption and uploading
4) Data downloading and decryption
5) Encryption evolution management

**Identity token issuance**
IdPs are trusted third parties that issue identity tokens to Users based on their identity attributes. It should be noted that IdPs need not be online after they issue identity tokens.

**Identity token registration**
Users register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users register their tokens related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues them two sets of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. The Owner keeps one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data.

**Data encryption and uploading**
The Owner first encrypts the data based on the Owner’s sub ACPs in order to hide the content from
the Cloud and then uploads them along with the public information generated by the AB-GKM: KeyGen algorithm and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the data based on the keys generated using its own AB-GKM: KeyGen algorithm. Note that the AB-GKM: KeyGen at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys.

Data downloading and Decryption

Users download encrypted data from the Cloud and decrypt twice to access the data. First, the Cloud generated public information tuple is used to derive the OLE key and then the Owner generated public information tuple is used to derive the ILE key using the AB-GKM::KeyDer algorithm. These two keys allow a User to decrypt a data item only if the User satisfies the original ACP applied to the data item.

Encryption Evolution Management

Over time, either ACPs or user credentials may change. Further, already encrypted data may go through frequent updates. In such situations, data already encrypted must be re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re-encrypts the affected data without the intervention of the Owner.

VI. CONCLUSION

Current approaches to enforce ACPs on outsourced data using selective encryption require organizations to manage all keys and encryptions and upload the encrypted data to the remote storage. Such approaches incur high communication and computation cost to manage keys and encryptions whenever user credentials change. In this paper, we proposed a two layer encryption based approach to solve this problem by delegating as much of the access control enforcement responsibilities as possible to the Cloud while minimizing the information exposure risks due to colluding Users and Cloud. A key problem in this regard is how to decompose ACPs so that the Owner has to handle a minimum number of attribute conditions while hiding the content from the Cloud. We showed that the policy decomposition problem is NPComplete and provided approximation algorithms. Based on the decomposed ACPs, we proposed a novel approach to privacy preserving fine-grained delegated access control to data in public clouds. Our approach is based on a privacy preserving attribute based key management scheme that protects the privacy of users while enforcing attribute based ACPs. As the experimental results show, decomposing the ACPs and utilizing the two layer of encryption reduce the overhead at the Owner. As future work, we plan to investigate the alternative choices for the TLE approach further. We also plan to further reduce the computational cost by exploiting partial relationships among ACPs.

REFERENCES


Authors:

B. SUNITHA  
Holds a B.Tech certificate in Information Technology (Raghu Institute of Technology) from the Andhra University. She presently Pursuing M.Tech (CST) department of computer science engineering from Baba Institute of Technology and Sciences, Visakhapatnam.

Ch. Sita Kameswari, M.C.A, M.Tech., M.B.A (Ph.D) is M.Tech (co-ordinator) BABA Institute of Technology & Science, A Lady of true vision towards modern professional education and deep rooted values. Mrs. Ch. Sita kameswari has come in association with BITS in the capacity of Professor, Dept. of CSE and PG Coordinator. She pursued her MCA in the year 1997 and M.Tech (CSE) with specialization in Artificial Intelligence and Robotics from Andhra University in the year 2008. Her quest for knowledge led her to attain the MBA degree from IGNOU. Currently, she is at the verge of submission of her thesis with GITAM University for the award of Ph.D. She has a reckonable and meritorious experience of 15 years in the teaching field since 1997. During this period she served for various professional colleges like J.A. Karia College, Jamnagar, Gujarat; Boston college for professional studies, Gwalior; ANITS, Visakhapatnam etc. in the capacity of Asst Professor, Associate Professor and also discharged the additional responsibilities as HOD of MCA and CSE. She was ratified for the post Associate Professor by AU, Visakhapatnam and RGPV, Bhopal. She has vast experience in the administration of departments, facilitating internships, project guidance and counseling of students on the progressive path. She played an active role as management representative for ISO 9001 certification during her tenure at Boston College Gwalior. She had Organized a joint International Conference on Swarm, Evolutionary and Memetic Computing (SEMCCO) and Fuzzy and Neural Computing Conference (FANCCO) at ANITS, Visakhapatnam Successfully in the position of organizing secretary in the month of Dec 2011 she organized ICSI AP student convention at ANITS, in coordination with CSI successfully as co-convener she organized various National level student Fests such as TECHNOCOM 2K6, AADYOTA-08, AADYOTA-09 in the institutions she worked with and earned the appreciation of one and all. She had published her research papers in 2 International Journals, 2 proceedings of International Conference and 2 National Conferences. She also presented papers in International and National Conferences. A few more papers of her are under processing for publication. She actively participated in about 20 workshops organized by Indian Science Congress and other Professional bodies at various organizations. Her areas of interest are Artificial Intelligence, Computer Graphics, Object Oriented Software Engineering, Operating Systems, System Programming, Machine Learning, and Neural Networks. Her hobbies include Listening to old and new melodies, reading books and playing shuttle badminton. She believes in the wording of swami Vivekananda “Arise, Awake and Stop not till the Goal is Reached”.

www.ijrcct.org  Page 1165