International Journal For Technological Research In Engineering
Volume 5, Issue 4, December-2017 *ISSN (Online): 2347 - 4718*

CONFIDENTIAL PRESERVE ABE WITH ACCESS CONTROL IN SHARED CLOUDS

Gudivada Venkata Sudheer[1], Dr. Y .K. Sundara Krishna[2]
[1]Student of M.Tech (CSE), [2]Professor Department of Computer Science & Engineering,
Krishna University, Machilipatnam

Abstract: Cloud computing is a buzz express which means that accessing and storing of data and programs over the Internet in its position of your computer's hard drive. Protection and secrecy represent major concerns in the acceptance of cloud technologies for information storage. A insolent issue is how to crumble access control policies such that 2 layer encryption can be achieve. To overcome these problem proposed go a step further in the decentralization process in two layer broadcast encryption schema, by eliminate the group manager preliminaryunit of the set, with an advantage of the addition of supporting members to the coordination, does not want any central authorization. Our comprehensionformulate black-box operate of well-known primeval and can be considered as an enlargement to the subset-cover structure. It permits for efficient substance instantiations, with parameter extent that matches those of the subset-cover constructions;although at the same time achieving the maximum security level in the paradigmrepresentation.It utilize an resourceful scatter group key management scheme to facilitate communicative ACPs. Our coordination assures the confidentiality of the data and preserves the privacy of users from the cloud although delegating most of the access power enforcement to the cloud.Existing market inclination need Products to be developed at elevatedswiftness. To meet those requirements sometimes it requires collaboration between the organizations. Since of the proficient services that are being obtainable by the cloud service providers today, lots of business organizations started compelling advantage of cloud services. Specifically, Cloud computing enables a new form of service in that a service can be realized by components provided by different enterprises or entities in a collaborative manner. Contributing parties are commonly loosely connected and they are responsible for managing and protecting resources/data consign to them. Such situation demands advanced and modern mechanisms for better security and privacy protection of data shared among multiple participating parties. In this, we insinuateaccesses manipulate delegation approach that achieves federated security services and preserves autonomy and privacy sharing preferences of involved parties. An important feature of our mechanism is that each party will not need to reveal its own sensitive information when making a global decision with other collaborators, which will support an extensive range of collaboration and create extra business opportunities.

I. INTRODUCTION

Nowadays every organization perform access control polices (ACPs) means "which users can access which data or records"; these access control policies can be expressed in the terms of user property, called as identity attribute, using access control language. Such an approach, called as Attribute basis Access Control, maintain fine-grained access control which is indispensable for high-assurance data security and confidentiality The modern workforce is increasingly distributed, mobile and virtual. Thus there will be many hurdles for communication and effective collaboration within organizations. One of the greatest benefits of cloud computing has to do with improvements to organizations communication and collaboration, both internally and externally. Thus by switching to the cloud, corporate resources can be virtualized, enabling individuals to access the documents they need regardless of location or device. Several cloud's web-based tools are developed to reduce communication barriers by helping people connect to the organizations cloud and get relevant and timely responses with stake holders within every project so that everyone involved in their project is on the same page. Moreover, cloud service providers also collaborate among themselves in order to provide better services to their customers. For example, Apple Inc. collaborates with amazon's AWS and Microsoft's Azure to host its iCloud services. Oracle teams up with Amazon AWS to extend its services to customers. Oracle collaborated with Microsoft for providing Microsoft Azure customers with oracle software services. Cloud computing collaboration and communication suite of Sales force and Google Apps enables users of Sales force and Google Apps to collaborate more effectively using the 2 cloud. Hewlett-Packard (HP) team up with Sales imposecloud service provider. Sales impose thus runs a dedicated example of HP's coverage infrastructure on its cloud, providing a continuous service to HP's customers. From the above examples, cloud computing facilitate a new way of provision in that a provision can be realized by components provided by different enterprises or entities in a collaborative manner. Participating parties are usually loosely connected and they are responsible for managing and protecting resources/data entrusted to them. Such scenario demands advanced and innovative mechanisms for better security and privacy protection of data shared among multiple participating parties. In this paper, we propose an access control delegation approach that achieves federated security services and preserves autonomy and privacy sharing preferences of involved parties. We cast our solution in the context of the eXtensible Access Control Mark-upLanguage (XACML) [2] framework. XACML is a general purpose access control policylanguage which defines a

request/response language and framework to enforceauthorization decisions. We have chosen XACML because of its widespread adoption as3a language of choice for enforcing access control in traditional and distributedenvironments [7]. In a typical XACML framework, there is a policy enforcement point(PEP) and a policy decision point (PDP). The PEP is responsible for issuing requests andenforcing the access control decisions. The PDP receives requests from the PEP andevaluates policies applicable to the requests and sends a decision back to the PEP. Tosupport collaborative access control, we extend the XACML reference architecture byintroducing multiple PDP's that communicate with a centralized PEP through a requestdispatcher/decision coordinator. If the PDP's are at different hierarchical level, then thatPDP will have child PDP's. A global policy is thus decomposed into local policies foreach PDP according to availability/ sensitivity requirements of each party. Given arequest, the central PEP modifies the request and dispatches it to corresponding PDPs,and then combines the decisions.

The other issue which we are focusing in this thesis is, generally even if a singlepolicy in a global policy is modified or even if a single resource location has beenmodified, then the entire global policy will be re-evaluated which will incur with modified resource locations or modified policies instead ofevaluating whole global policy. Our Recommend guidelines decomposition approach crumbles a global policy that needs to be enforced among participating collaborators. After the decomposition, the access control rights will be delegated to corresponding parties based on information available at each local party. Given a request to access certain information, the request will be evaluated locally at respective participating parties. Then, the local decisions will be assembled to make the final decision.

II. TRADITIONAL ENCRYPTION APPROACH

In this section**,** the existing system is briefly discussed. Fig show Traditional Encryption Approach (TEA), whererecords or data items are combined together is based on access control policies and using different symmetric keyevery combined records or data items are encrypted after that key send only to authorize users for records or dataitem which users can have the authorization to access. Extensions to reduce the number of keys that need to bedistributed to the users have been proposed exploiting hierarchical and other relationships among data items. Suchapproaches have various limitations:

1. In TEA, Data Owner does not maintain a copy of the records or data, whenever user's dynamics changes, the Data Owner needs to:
a) Download and decrypt the data
b) Re-encrypt the data with new keys
c) Upload the encrypted data in the cloud.
This above step will apply to all encrypted records or data with same key but this process is inefficient when large data set to be encrypted.

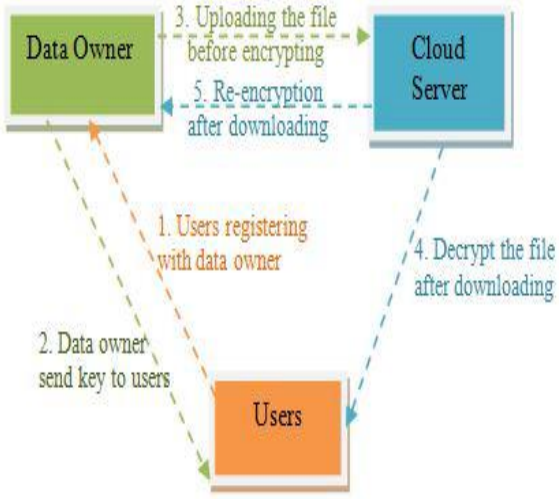

Fig. 1: Traditional Encryption Approach

2. Data owner needs to be establishing a private communication channels with the users for issuing new keys.
3. User's identity attributes confidentiality is not considered. So the cloud can learn user private information and their organization.
4. TEA does not support fine-grained ABAC policies.

TEA is based on broadcast key management scheme, addresses some of the above limitations, but it stillrequire data owner to enforce all ACPs by fine-grained encryption whenever user dynamics changes due to all theseencryption activities perform at Data Owner that needs high communication and computation expenditure. *For e.g.,*whenever user added or revoked in the system, the data owner need to download the affected data from the cloud,generate new encryption key, re-encrypt the downloaded data with new key, and then upload the re-encrypted datato the cloud server.

III. HYBRID ENCRYPTION APPROACH

In this section, the proposed system is briefly discussed. Hybrid Encryption Approach (HEA), by name itself says that there are two ways of encryption schemes, in the first way the Data Owner will encrypt all the records or data using symmetric key algorithm i.e. AES algorithm before uploading the encrypted records or data to the cloud sever in order to ensure the confidentiality of the records or data items from the cloud server and then second way carried out by cloud server, where cloud server performs the complete access control related encryption on the top of the data owner encrypted data or records. But challenging issue in this approach is how to decompose the ACPs so that it supports fine-grained ABAC policies while at same time the confidentiality of the identity attributes of users and records or data are assured [5]. However, performing two ways of encryption is new and provides a superior result than Traditional Encryption Approach. Fig. 2 show general ideas behind data under HEA, where initially data is encrypted by Data Owner and then again encrypted data is encrypted by Cloud server.

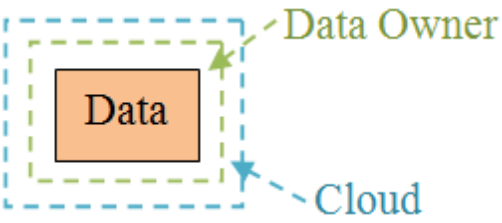

Fig. 2: Data under HEA

Consider the hospital example, where hospital acts as a Data Owner support access control on medical records and makes these records available to hospital employees acts as Users, and Users have different roles as an attribute such as receptionist (rec), cashier (cas), doctor (doc), nurse (nur), pharmacist (pha) and system administration (admin).

IV. PERFORMANCE ANALYSIS

In this section first present experimental results concerning the policy decomposition algorithms. Then present an experimental comparison between the TLE and TLE Dynamic broadcast encryption approaches. Utilized the AB-GKM scheme with the subset cover optimization. Then used the complete subset algorithm introduced by Naor et. al. as the subset cover. Figure 2 shows the size of the attribute condition cover, that is, the number of attribute conditions the data owner enforces, for systems having 100 attribute conditions as the number of attribute conditions per policy is increased. In all experiments, the Dynamic Subset-Cover algorithm performs better than greedy search cover algorithm, as the number of attribute conditions per policy increases; the size of the attribute condition cover also increases.

V. RELATED WORK SEARCHABLE ENCRYPTION

Search in encrypted data is a privacy preserving 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.

VI. PROPOSED ARCHITECTURE

In this paper, we are using two-layer encryption for storage of data across multi-clouds rather than a single public cloud. This two layer enforcement helps one to reduce the load on the Owner and delegates access control enforcement over the cloud. Especially, it provides a better way for various updates, user locations, and modifications of the data. The system goes through one additional phase compared to the existing system. Also, it provides several functions based on the decomposition or splitting of data to store across various clouds, which are finally retrieved by the user with the help of keys.

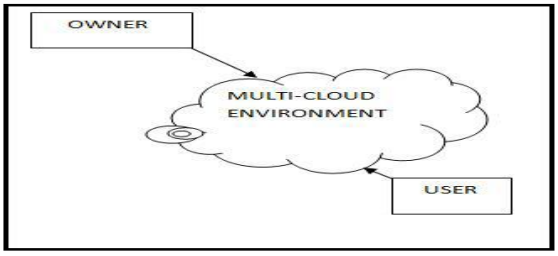

Fig : Multi-cloud storage

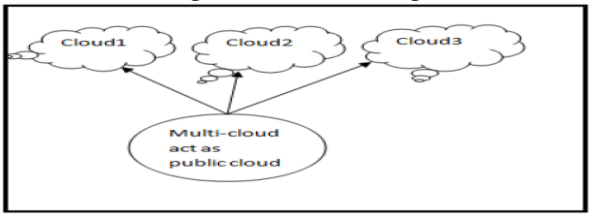

Fig : Multi-cloud splitting

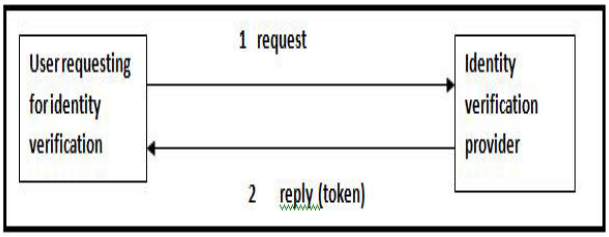

Fig : Two layer encryption in multi-cloud Environment

VII. 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 or organizational authorization policies/data change. In this paper, we proposed a two layer dynamic broadcast encryption based approach to solve this problem .The decentralized dynamic broadcast encryption and subgroup key exchange, a building block use in our construction that may be of independent interest 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. As future work, plan to investigate the alternative choices for the TLE approach further. It also plans to further reduce the computational cost by exploiting partial relationships among ACPs.

REFERENCE

[1] Bin Wu ,Yixin Jiang, Jiaxiao MengA Modified Hierarchical Attribute-based Encryption Access Control Method for Mobile Cloud Computing IEEE Transactions on Cloud Computing 2015

[2] M. Moniruzzaman, M.S. Ferdous and R. Hossain, "A study of privacy policy enforcement in access control models," In proceedings of 13th International Conference on Computer and Information Technology (ICCIT). Dhaka, Bangladesh, pp. 352 – 357, 2010. DOI:10.1109/ICCITECHN.2010.5723883.

[3] M. Jafari, P. W. L. Fong, R. Safavi-Naini, K. Barker, and N. P. Sheppard, "Towards Defining Semantic Foundations for Purpose- Based Privacy Policies," In proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, Taxas, USA, 213-224, 2011.

[4] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy-preserving approach to policy-based content dissemination," in ICDE '10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[5] 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.

[6] M.Nabeel, N.Shang, and E.Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Transactions on Knowledge and Data Engineering, 2012.

[7] Cecile Delerablee, Pascal Paillier, and David Point cheval. Fully collusion secure dynamic broadcast encryption with constant-size cipher texts or decryption keys. In T. Takagi et al., editor, Pairing 2007, volume 4575 of LNCS, pages 39-59. Springer, 2007.

AUTHORS:

GUDIVADA VENKATA SUDHEER is a student of KRISHNA UNIVERSITY, MACHILIPATNAM.Presently he is pursuing his M.Tech (CSE) from this college and he completed his B.Tech (CSE) from ANU in the year 2014.

Dr. Y .K. Sundara Krishna

M. Tech, Ph. D., MISTE, MASMS is a Professor in the Department of Computer Science and Engineering and working as a principal at KRISHNA UNIVERSITY , MACHILIPATNAM. His research interests are Mobile Computing, Service Oriented Architecture and Geographical Information Systems and Supervising five research scholars He has 26 years of teaching experience.

