Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

The Conviction Keyword Search with Secure Authenticated Encryption in Cloud

Utchula Nissi komal
M.Tech Scholar and Department of Computer Science Engineering,

Dr. B.V.S. Varma
Professor, Department of Computer Science and Engineering, DNR College of Engineering and Technology,

Dr.G. Satyanarayana
Professor, HOD Department of computer Science and Engineering,
DNR college of Engineering and Technology, Bhimavaram, AP, India.

Abstract:
The Searchable Symmetric Encryption, as an important cloud security technique, allows users to retrieve the encrypted data from the cloud through keywords and verify the validity of the returned results. Dynamic update for cloud data is one of the most common and fundamental requirements for data owners in such schemes. Attracted by these appealing features, both individuals and enterprises are motivated to contract out their data to the cloud, instead of purchasing software and hardware to manage the data themselves. So far, most of the works have been proposed under different threat models to achieve various search functions, such as single keyword search, similarity search, multi- keyword Boolean search, ranked search, multi-keyword ranked search, etc. Among them, multikeyword ranked search achieves more attention for its practical applicability. propose a secure and ranked multikeyword search protocol in a multi-owner cloud model over encrypted cloud data,
***Keywords*: cloud security, privacy, utility computing, public auditing, third party agents and services.**

I.INTRODUCTION

Cloud Computing is the rising innovation where we can get stage as a service, programming as a service and framework as a service. With regards to storage as a service, data privacy and data use are the essential issues to be managed. To deal with the exchange of files to and from the cloud server, the files are scrambled before being redistributed to the business public cloud. The subject of cloud computing is picking up a great deal of consideration from both scholarly and modern universes. The fundamental thought is to make applications accessible on adaptable execution situations basically situated in the web. In cloud computing, clients can re-appropriate their calculation and storage to servers (additionally called clouds) utilizing Internet. Clouds can give a few kinds of services like applications (e.g., Google Apps, Microsoft on the web), frameworks (e.g., Amazon's EC2, Eucalyptus, Nimbus), and stages to enable designers to compose applications (e.g., Amazon's S3, Windows Azure). The storage holds appropriate data and data on capacity on how they will be executed.

Advancement on storage is based on how the storage office shielded from various assaults and accessibility of reinforcement. Cloud computing is constantly about consistency and accessibility of service which will normally require the storage to be accessible constantly. A great part of the data put away in clouds is exceptionally delicate, for instance, restorative records and informal communities. Security and privacy are therefore critical issues in cloud computing. In one hand, the client ought to verify itself before starting any exchange, and then again, it must be guaranteed that the cloud or different clients don't have the foggiest idea about the identity of the client. The cloud can consider the client responsible for the data it re-appropriates, and in like manner, the cloud itself responsible for the services it gives. The legitimacy of the client who stores the data is likewise checked. Aside from the specialized answers for guarantee security and privacy, there is likewise a requirement for law implementation. Cloud servers are inclined to Byzantine disappointment, where a storage server can bomb in discretionary ways. The cloud is additionally inclined to data alteration and server intriguing assaults. In server intriguing assault, the foe can bargain storage servers, so it can change

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

data files as long as they are inside reliable. To give secure data storage, the data should be encoded. Be that as it may, the data is frequently adjusted and this dynamic property should be considered while structuring effective secure storage procedures. Proficient hunt on encoded data is likewise a vital worry in clouds. The clouds ought not know the question but rather ought to have the capacity to restore the records that fulfill the inquiry. This is accomplished by methods for accessible encryption. Access control in clouds is picking up consideration since it is critical that just approved clients approach substantial service. A colossal measure of data is being put away in the cloud, and quite a bit of this is touchy data. Care ought to be taken to guarantee access control of this touchy data which can regularly identified with wellbeing, critical archives (as in Google Docs or Dropbox) or even close to home data (as in social networking).Access control is likewise picking up significance in online interpersonal interaction where clients (individuals) store their own data, pictures, recordings and offer them with chose gatherings of clients or networks they have a place with. It isn't sufficiently only to store the substance safely in the cloud however it may likewise be important to guarantee namelessness of the client. For instance, a client might want to store some delicate data yet does not have any desire to be perceived. The client should need to post a remark on an, yet does not need his/her identity to be uncovered. In any case, the client ought to have the capacity to demonstrate to alternate clients that he/she is a substantial client who put away the data without uncovering the identity.

II. RELATED WORK

ABE was proposed by Sahai and Waters [26]. In ABE, a client has an arrangement of attributes notwithstanding its one of a kind ID. There are two classes of ABEs. In Key-strategy ABE or KPABE (Goyal et al. [27]), the sender has an access approach to scramble data. An essayist whose attributes and keys have been renounced can't compose back stale data. The beneficiary gets attributes and mystery keys from the attribute specialist and can unscramble data on the off chance that it has coordinating attributes. In Cipher arrangement, CP-ABE ([28], [29]), the recipient has the access strategy as a tree, with attributes as leaves and monotonic access structure with AND, OR and other limit doors. Every one of the methodologies adopt a concentrated strategy and permit just a single KDC, which is a solitary purpose of disappointment. Pursue [30] proposed a multi-specialist ABE, in which there are a few KDC experts (facilitated by a confided in power) which disperse attributes and mystery keys to clients. Multi-expert ABE convention was examined in [31], [32], which required no confided in power which requires each client to have attributes from at all the KDCs. As of late, Lewko and Waters [35] proposed a completely decentralized ABE where clients could have at least zero attributes from every specialist and did not require a confided in server. In every one of these cases, decoding at client's end is calculation concentrated. Along these lines, this system may be wasteful when clients access utilizing their cell phones. To get over this issue, Green et al. [33] proposed to re-appropriate the unscrambling assignment to an intermediary server, so the client can process with least assets (for instance, hand held gadgets). Be that as it may, the nearness of one intermediary and one key conveyance focus makes it less vigorous than decentralized methodologies. Both these methodologies had no real way to confirm clients, secretly. Yang et al. [34] introduced a change of [33], confirm clients, who need to stay mysterious while accessing the cloud. To guarantee unknown client validation Attribute Based Signatures were presented by Maji et al. [23]. This was likewise a concentrated methodology. An ongoing plan by similar creators [24] adopts a decentralized strategy and gives verification without unveiling the identity of the clients. Be that as it may, as referenced prior in the past segment it is inclined to replay assault. Cryptography is one of the systems that are generally utilized in reality for anchoring applications. Notwithstanding, cryptography when connected to cloud data elements respect execution issues. Arrangement based substance scattering [9] is another methodology that appeared in 2010. Later access control arrangements appeared. In this paper additionally we attempted access control which is erased to public cloud. Designated access control is additionally examined in [10]. Anchoring spread of XML reports was investigated in [8]. While distributing data security of data utilizing cryptography is the concentration in [7]. Access control in cloud is additionally investigated in [6] and comparable sort of research was done in [5]. Communicate encryption component was investigated in [4] where encryption is connected to broadcasting. Unaware attribute endorsements idea was utilized in [3] for anchoring data. In comparable design attribute based security is given in [2] as far as gathering key administration. Stateful unknown certifications were investigated in [1]. In this paper our emphasis in on appointing access control to public cloud. Towards this end we assembled a model application that shows the confirmation of idea. The designated access control makes it an appropriate model in public cloud where data proprietors can offer access to their data to numerous clients.

III. PRIVACY PROTECTION METHODS

Various methods have been put forward to overcome this issue of privacy preserving. This work studies some of those approaches and provides a concise outline. It is important, that the privacy has to be preserved anytime and anywhere. The protection can be done by both provider and user at server side and client side.

Encryption Strategies

The data can be encrypted and decrypted before storing in the cloud. User can encrypt their data while uploading it on the cloud and decrypt while downloading it. In [3], review of various encryption schemes is provided.

Key Policy Attribute Based Encryption

A set of descriptive attributes is labeled by the encrypt or for each cipher text. An access structure is associated with Each private key that indicate which form of cipher-texts the key can decrypt. In the work of Jin sun [4], the key policy ABE is associated with the broadcast encryption to provide a dual system encryption. With this standard model, the scheme can achieve fixed-size public criterion, force no bound on attribute set size used for encryption.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

Cipher-text policy Attribute Based Encryption
Here attribute policies are associated with data and attributes are associated with keys. Decryption is possible only those keys which are collaborated with attributes satisfy the policy collaborated with the data. This encryption satisfies the security needs demanded by the customer.

Cipher-text policy Attribute Set Based Encryption
A recursive set-based structure is framed by organizing user attributes and allows users to demand dynamic constraints on how those attributes may be associated to satisfy a policy. By using this techniques encrypted data can be kept secret even if the storage server is not trustworthy; moreover, this method provide security against collusion attack. This methods are related to conventional access control methods such as Role-Based Access Control (RBAC).

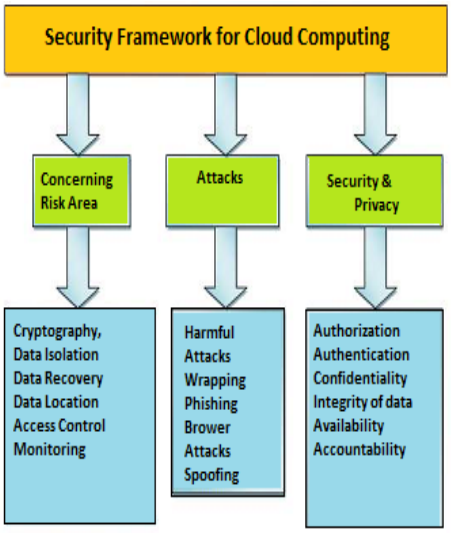

Fig 1: A framework for secure cloud computing.

Fuzzy Identity-Based Encryption
As measured by the overlap distance metric, the identities a and a' should be close to each other then only it is possible to decrypt a cipher-text encrypted with an identity a' with a private key for an identity a. In fuzzy, a biometric can also be used as attributes for the identities.

Identity Based Authentication
In [5], SSL Authentication Protocol is applied in cloud computing, will become so complicated that users will undergo a bulk point both in computation and communication. It based on the identity-based hierarchical model for cloud computing. In [6], the authors proposed a dynamic authentication protocol that can support dynamic operations in cloud. This enables only valid users to authenticate in cloud.

IV. ACCESS CONTROL SCHEME IN PUD

The PUD is characterized by a huge number of users, a lot of attributes owned by the user, complexity management, and indefinite users' identity. In view of the above characteristics, the user can only have the read access permission. Although the attribute-based encryption scheme (CP-ABE) can achieve access control, it cannot meet the needs of complex cloud environment. In traditional CP-ABE scheme, there is only one attribute authority responsible for the management of attributes and distribution of keys. The authority may be a university registrar's office, the company's HR department or government educational organizations and so on. The data owner defines access policies and encrypts the data files in accordance with this policy. Each user is distributed a key related to his attribute. As long as the user's attributes meet the access policy he can decrypt the file.
However, if there is only one authority in the system and all public and private keys are issued by the authority. Two problems will appear in the practical application:
1) In the practical cloud environment, there are a lot of authorities and each authority in their own field manages part of users' attributes. The attributes owned by the user are issued from different authorities. For example, a data owner may want to share his medical data with a user who owns the doctor attribute issued by medical institutions and the medical researcher attribute by the clinic practice man secret Othagement. Therefore, exploiting multi authority is more realistic in the practical scenarios.

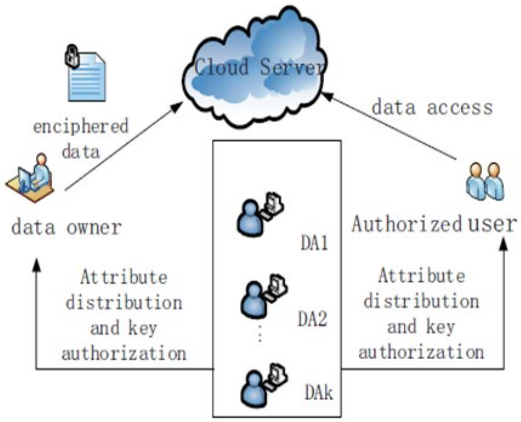

Fig 2. Access control framework of PUD

Therefore, multi authority ABE (MA-ABE) is used in this paper. To reduce the computation overhead of users in PUD, we propose an outsourcing decryption MA-ABE scheme. Firstly the data owner uploads the attribute-based encrypted data files to the cloud server. When a user requests the encrypted data from the cloud server, the cloud server will first check his transformation key. Only if the corresponding attributes satisfy the access structure, will the cloud server output a partially decrypted ciphertext and then sends it to the user. Finally, upon receiving the partially decrypted ciphertext, the user can use his private key to recover the message. The framework of this area is shown in Fig.2

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

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. Cloud Mask 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 Cloud Mask, 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 Cloud Mask. Using such signed pseudonyms and public keys, users can prove their identity to the CDS before retrieving any document.

VI. PROPOSED ARCHITECTURE

This proposed architecture is enhanced security model for cloud services like data storage. It consist of CSP i.e. Cloud Service Provider and user's. • Cloud Service Provider: - CSP generates a pair of keys i.e. secret key and public key by using cryptography algorithm RSA. CSP stores its own private key generated RSA algorithm and public key is shared by all. • User's:- User's must physically register on CSP. CSP check user's id. If user is already registered then there are some messages exchanged between users and CSP for establishing secure communication between them. User's generated a random request and encrypts this random request with the RSA public key of CSP and sends this request message to the server. Now server verifies this request if it is verified then server decrypt this message by using RSA secret key of CSP and generate a random key K_sym. Now with the help of this random key server generates a response by applying the X-OR operation to random and K_sym. Server send this response to user's. User's use this random key for file uploading and downloading and attain secure communication.

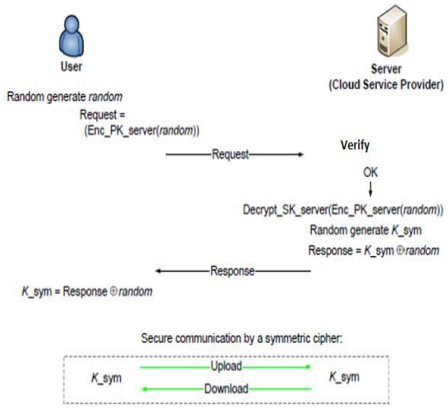

Fig 3. Proposed Architecture diagram

VI. CONCLUSIONS AND FUTURE WORK

We have presented a privacy preserving access control technique which is decentralized. The cloud authenticates the user by verifying the credential's even without knowing the original identity of the user. We also address user revocation and our scheme prevents replay attacks. Key distribution is done in a decentralized way. The individual user's access policy is been concealed and known only to each particular user. This paper can overcome the top threats in clouds which are identified recently. The threats that can be overcome are data loss, insecure APIs, Denial of Service, abuse of cloud services, shared technology issues. The proposed work also has options for file recovery. Using this file recovery options make our privacy system an efficient system. This project can overcome the top threats identified in clouds which are identified recently. The threats that can be overcome are data loss, insecure APIs, Denial of Service, abuse of cloud services, shared technology issues.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,"IEEE Transactions on Parallel and Distributed Systems, pp. 1045-9219, 2013.

[2] S. Ruj, M. Stojmenovic and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds”, IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.

[3] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing”, IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in IEEE INFOCOM. , pp. 441–445, 2010.

[5] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[6] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[7] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[8] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Tokenbased cloud computing,” in TRUST, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.

[9] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, “Trustcloud: A framework for accountability and trust in cloud computing,” HP Technical Report HPL-2011-38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[10] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” in ACM ASIACCS, pp. 282– 292, 2010.

UTCHULA NISSI KOMAL holds a B.Tech Degree in Computer Science & Engineering from West Godavari Institute of Science and Engineering, Prakasaraopalem, West Godavari District, Andhra Pradesh. She is presently Pursuing M.Tech in Department of Computer Science and Engineering from DNR College of Engineering and Technology, Bhimavaram.

Dr. B.V.S. VARMA, M. Tech., Ph.D., is working as a Professor and Vice Principal in the Department of Computer Science and Engineering, DNR College of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India

Dr. G. Satyanarayana, M. Tech., Ph.D., is working as a Professor and HOD in the Department of Computer Science and Engineering, DNR College of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India.