ENRICHED AND RELIABLE ATTRIBUTE BASED ACCESS CONTROL FOR MULTIAUTHORITY IN CLOUD COMPUTING

Lijin T V(lijint.v2018@vitstudent.ac.in), Anitta Balsalam Vasanthan(anitta.vasanthan2018@vitstudent.ac.in), Dr.Priya G (gpriya@vit.ac.in)

School of Computer Science and Engineering

Vellore Institute Of Technology, Vellore

ABSTRACT.

Cipher-Text Policy Attribute Based Encryption (CP-ABE) is a new approach that allows the owners of the data to place fine-grained and encryption-based access control over the data they share in the cloud. To build more secure and less expensive data access control for cloud storages, we propose a multi-authority CP-ABE scheme. It supports scalable user revocation and public cipher-text update. In our multi-authority CP-ABE scheme the system need no trusted central system and all attribute authorities generates secret keys for users independently. Also each the attribute authority can dynamically remove any unwanted user from its range such that those revoked users would not be able to access the data stored thereafter.

KEYWORDS: *Cloud Computing, Cloud Security, CP-ABE, Multi-authority*

I. INTRODUCTION.

Cloud computing is basically a type of computing which is purely based on internet and is used for processing of resources and data on demand by computing devices. It is a model that provides omnipresent, on-requesting resource to a collective group of configurable computing resources, which can be quickly provided and withdrawn with bear minimal management effort. In general, cloud computing and storage solutions provide users and businesses with the ability to store and process their data in third party data centers. It enables endeavors to get their software's fully operational quicker, with better manageability and less maintenance, and helps to swiftly fiddle .with resources to meet irregular and impulsive business demand. Cloud providers employ a "pay as you grow" form. This leads to unpredictably elevated charges if administrators could not familiarize themselves to the cloud pricing structure.

Cloud computing has turned into a profoundly requested administration or utility because of the upsides of high figuring force, modest expense of administrations, elite, adaptability, openness just as accessibility. Some of the few cloud vendors are witnessing expansion rates as high as 50% per annum, but still being in a phase of immaturity, it has difficulties that have to be rectified to mould it further dependable and user welcoming.

A) Cloud Computing Types

The four types of cloud computing are:

1)Private Cloud- Private cloud is basically a cloud model that runs for a solitary association, Which can be managed inside or through a peripheral third party and hosted either inside or outside.

2) Public Cloud: A cloud is called a "Public Cloud" when cloud services are presented over a public network that is open to public use. Public cloud services can be free. There is generally no significant difference between public and private cloud architectures, but there is less security for services provided by a cloud service provider that targets the public and when the transmission is over a network that cannot be trusted.

3) Hybrid Cloud: Hybrid cloud consists of two or more clouds that are linked together, thus providing the benefits of both. A hybrid cloud service cannot be placed as it crosses the boundaries of separation and provider in a single class of private, public, or community cloud service.

4) Community Cloud: It is a joint attempt to dispense infrastructure through a mix of organizations within a particular community with familiar concerns such as security, storage, jurisdiction, etc., whether managed within or through a peripheral third party and hosted within or outside it. The cloud is banned and worn by a set of organizations of common interest.

B) Benefits of having Cloud Computing

The major profit of cloud computing are:

1) Cloud service is highly scalable. Allotment and de-allocation of the resources are done dynamically and on demand.

2) It reduces the cost by decreasing the capital infrastructure.

3) It permits the users right to use the application free of their location and hardware configuration.

4) Storing information on the clouds is more dependable as it is not misplaced simply.

The need for key management in the cloud.

Key management points to anything that is done to a key excluding encoding and decoding .It primarily emphasize on the creation, deletion, activation, deactivation, transportation and storage of keys. Most Cloud service providers generally provide key encoding model for securing information or might abscond it to the user to encode their own information.

C) Secure Key Stores:

The key stores have to be protected from unauthorized users. If an unwanted user gains right entry to the keys, then all the data encoded with that key will be accessible to them. Hence the key stores must be protected themselves while they are being stored, transmitted and on a backup medium.

D) Access to Key Stores:

Right to use to the key stores should be assigned to the users that have privileges to access data. Severance of roles must be used to manage access by ensuring that unit that uses a specified key be supposed to be different from the one that stores the key.

E) Key backup And Recoverability:

The key used should be backed up and recovered securely. Loss of keys can help prevent data access, but it can overwhelm a trade and cloud providers need to ensure that keys are not lost by providing proper backup and recovery techniques.

F) Secure Data Sharing.

The system for data sharing includes the following system entities:

1) Key Generation Center: It is a key authority that creates the necessary public and secret parameters for Cipher-text Policy-Attribute Based Encryption. It issues, revokes, and updates the attribute keys for users. In it users are given different access rights based on their attributes. It is considered to be honest-but-curious. That is, it will carry out the tasks given to it honestly however, it would like to learn as much as possible about the encrypted content.

2) Data-Storing Center: It is an entity that provides data sharing services. It has the duty to control the accesses to the stored data by outsiders and to provide appropriate content services. Another key authority generating custom user key with the Key Generation Center is the data storage center and issues and revokes group attribute keys for validation users for each attribute used to

implement a fine - grained user access control.

3) User: It refers to the entity that wants to access the data. If a user has a set of attributes that satisfy the access policy of the encrypted data and is not cancelled in any of the valid groups of attributes, then he will be able to decipher the encrypted text and get the original data.

4) Data Owner: It is a user who owns the data and wants to upload it to the data storage center for easy and efficient sharing. It is the responsibility of a data owner to define access policy and enforce it on their own data by encrypting data using the policy before it is distributed.

G) Attribute Based Encryption.

Attribute-based encryption is a kind of open key encryption where attributes require a client's mystery key and cipher-text. In this context, the scrambling of a figure content is conceivable only if the configuration of the client key attributes matches the attributes of the figure content.. A pivotal security part of Attribute-Based Encryption is plot obstruction: An enemy that holds various keys should possibly have the capacity to get to information if something like one individual key gifts get to. Attribute-based encryption can be utilized for log encryption. Rather than encoding each piece of a log with the keys all things considered, it is conceivable to scramble the log just with attributes which coordinate beneficiaries' attributes. This crude can likewise be utilized for communicate encryption so as to diminish the quantity of keys utilized.

H) Removing Escrow.

An escrow is an authoritative course of action in which an outsider obtains and distributes cash or archives for the essential executing parties, with payment subject to conditions agreed by the executing parties, or a record established by a representative for holding assets in the interest of the merchant's key or some other Person until the exchange has been completed or terminated ; or a trust account held in the name of the borrower for payment of liabilities, e.g. property expenses and protection fees. Key escrow is a course of action in which the keys expected to unscramble scrambled information are held in escrow so that, in specific situations, an approved outsider may access those keys. These outsiders may incorporate organizations, who may need access to representative’s private interchanges, or governments, who may wish to probably see the substance of scrambled correspondences.

The specialized issue is a generally basic one since access to ensured data must be given just to the expected beneficiary and no less than one outsider. The outsider ought to be allowed access just under cautiously controlled conditions, concerning occasion, a court request. Up to this point, no framework configuration has been appeared meet this prerequisite completely on a specialized premise alone. Every such linkage or controls have significant issues from a framework structure security point of view. Frameworks in which the key may not be changed effectively are rendered particularly helpless as the incidental arrival of the key will result in numerous gadgets winding up completely bargained, requiring a prompt key change or substitution of the framework.

II. LITERATURE SURVEY.

The scheme in [1] is the first of its kind to incorporate searchable attribute - based encryption with attribute - based proxy re - encryption that applies to many real-world applications. The system enjoys better computational efficiency in each metric except token generation. But we need a larger space to store our keyword search token compared to other systems and thus the corresponding computational cost is more. Although the new system enjoys its valuable advantages, it has three main interesting problems: how to reduce the size of search token, how to allow a secret key holder to generate search token individually, and how to provide more expressive keyword search.

In [2] the authors prove the security of the proposed Attribute Based Encryption scheme under a chosen-cipher text attack model without using random oracles. Note that the combination of binary state attributes is not an appropriate solution for construction of an arbitrary-state attribute. This is because that the system should predict and prepare all possible public parameters and values for these binary-state attributes in advance and meanwhile the system parameters will become very complex. In this scheme, the set of the possible contents of an arbitrary-state attribute can be defined until encryption, and it can be re-defined whenever encryption. It is unnecessary for the system to predefine the contents of the attributes to cover all possible use-cases. Hence, the combination of binary-state attributes will not achieve the goal that an arbitrary-state attribute can achieve.

The straightforward construction used in[3] is helpless against agreement assaults in which an alliance of clients figures out how to decode figure writings planned to none of them, gave that the association of the attribute vectors of the intriguing clients meets the entrance approach. This sort of assaults must be anticipated practically speaking. This issue can be tended to by randomizing the mystery keys allocated to every client, and, by utilizing the entrenched double encryption methods.

The new hybrid peer-to-peer system in [4] is composed of two parts: a center transit network and many stub networks, every one of which is connected to a hub in the center transit network. The basic thought behind the hybrid peer-to-peer system is that the t-network is used to give effective and precise service while the s-network is used to give estimated best-exertion service to oblige adaptability. Peers can join either t-network or s-network straightforwardly. A s-network is composed of peers that serve the information of some regular properties. A information query is restricted to a s-network if the questioned information has the normal properties served by the s-network. The query request is passed around the s-network through flooding or arbitrary walk. Flooding creates a ton of network traffic which is a noteworthy downside.

In [5] the authors propose general structure for enormous information data the executives in smart grids based on cloud processing innovation. The basic idea is to set up cloud processing centers for monitoring data at three progressive levels: top, regional and end - user levels. While each local cloud focus is accountable for processing and overseeing territorial information, the best cloud level provides a worldwide perspective on the structure. The authors have implemented a proof-of-concept for the framework with a simple identity-based management for data confidentiality. The system does not support proxy re-encryption and hence comes with the inherent vulnerabilities associated with it. The authors provided an enhanced security data sharing scheme based on the classic CP - ABE in [6]. It solves the problem of key escrow by using a free key issue protocol where the key generation center and data storage center work together to generate secret user key. Consequently, the computational cost of generating the secret key of the user increases as the protocol requires interactive computation between the two parties. In [7] the authors proposed a novel framework for secure cloud - based sharing of PHR. We provided an overview of multiple access control mechanisms and analyzed the best for scenarios where data is stored or outsourced on a commercial PHR system to a data center for third parties. In these scenarios, most of the existing access control mechanisms and encryption techniques cannot be used. In cloud computing, fine - grained data access control can be effectively carried out by the CP - ABSC. It requires a full trusted authority to generate and issue users ' secret keys with its own master secret key as input. Therefore, the key escrow problem is inherent, so the authority has the "power" to decrypt cipher - texts for all system users. The scheme in [8] is the first of its type to achieve the adaptive Chosen Cipher-Text Attack security in the common model, but also to provide unlimited size input for access policy without degrading the functionality of proxy re-encryption. The dual encryption adapted in this system leads to increased computational cost and time. It also opens up a problem of how to convert the DFA based FPRE in the prime order bilinear group.

In [9] the authors proposed the notion of IND - CCA security for CP - ABPRE systems and proposed the first adaptive CCA - secure CP - ABPRE system without loss of Access policy expression through the integration of dual system encryption with selective proofing technique. In addition to computational complexity compared to other systems, it also creates a problem with how to convert our system into the bilinear group of prime order.

In[10] the authors proposed the TimePRE scheme to achieve fine - grained access control and scalable user revocation in a cloud environment. The scheme allows the access right of each user to be effective over a predetermined period of time, allowing the CSP to automatically re-encrypt cipher-texts based on their own time. The data owner can therefore be offline in the user revocation process. The main problem with the scheme is that for all attributes associated with a user it requires the effective time periods to be the same. While it may provide an improvement, more will be issued to users.

III. PROPOSED METHOD.

Cloud storage enables both individuals and businesses to share their data over the internet in cost-effectiveness. Provides in the proposed authorization solution safe and cost - effective attribute - based access control for cloud storage system. This scheme supports efficient user revocation and public cipher-text update for cloud storage systems. We provide safe and cost -

effective data access control for cloud storage systems. In particular, we are building a multi-authority Cipher-text Policy Attribute Based Encryption scheme that features: the system does not need a fully trusted central Authority and all attribute authorities independently issue secret user keys; Any attribute authority may dynamically remove any user from its domain so that the revoked users are unable to access data; cloud servers may update the encrypted data from the current time period so that the revoked users are unable to access the previously available data; secret key and cipher-text updates are made publicly available.

The advantages of the system are:

1) All attribute authorities issue secret user keys independently.
2) Each attribute authority can remove any user from their domain dynamically.
3) Users who have been revoked cannot access the data previously available.

A) SYSTEM SETUP

Initially, the third party and each authority set up the public parameter of the system by running the following algorithms. GlobalSetup: This algorithm, which accepts a security parameter as an input and, is executed by the third party. It outputs the global public parameter GP of the system, which is available for all Attribute Authorities and users in the system. AuthSetup: This algorithm, which takes as input the global public parameter, system time periods numbers in total, and the number of system users, is run by each attribute authority. It produces the local public parameter and the Master Secret Key of this authority. In addition, it creates a revocation list initialized as an empty set and the state information used to manage users's identifiers. We note that the two algorithms do not take the attribute universe as input, which implies that the public parameter of the system is independent of the attribute universe, and any string can be an attribute.

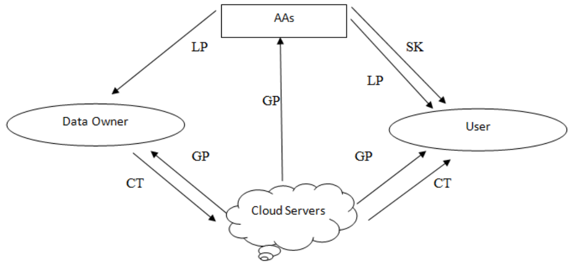

Fig.3.1 System Architecture

B) KEY DISTRIBUTION

For a user with a unique global identifier and an attribute set, where subset of attributes belonging to the authority δ, he/she would require a secret key component from each authority. Each attribute authority δ generates the corresponding secret key component for such a user by carrying out the following algorithm. Secret Key Generation: This algorithm intakes the public parameter, the master secret key, the user’s identifier, the corresponding attribute set Sδ, and the current state information as an input. The algorithm first checks the validity of the user’s identifier and attributes. If they pass through the verification, it generates a secret key component, for the user, and also outputs the updated state information. Then, the authority δ would send the secret key component to the user through a secure way. After getting all secret key components from all Attribute Authorities, the user structures his/her complete secret key.

C) DATA ENCRYPTION DECRYPTION KEY GENERATION

Before data owners upload their data to a cloud server, they first define access policies and implement them over these data by calling the following encryption algorithm.

Encrypt: This algorithm takes as input the system public parameter, an access policy, the data file to be encrypted, and a time period t. It outputs a cipher-text of file at the time period t. We shall presume that A and t are implicitly attached to the cipher-text. Update key generation: Each attribute authority periodically produces an update key such that the users which are not removed can utilize it to update the corresponding secret key component. Specifically, the following algorithm is used by the attribute authority to perform the above assignment. The algorithm produces an update key component, which is available to all users. However, it is only useful for non revoked users. The update key of the whole system at the time epoch t consists of all update key components generated by these Attribute Authorities.

D) CIPHER-TEXT UPDATE

The cloud server regularly refreshes the encoded data by using the public parameter. By calling the following algorithm, it completes this task. Cipher Text Update: This algorithm takes the public parameter, a cipher-text, and a new time frame t > t as an input. The original cipher-text is updated to the new time period and a new cipher-text is output, while the original cipher-text is erased.

E) USER REVOCATION

When a user’s permission authorized by an authority δ expires, the authority removes him/her from its domain. It achieves this by running the following algorithm. Revoke:

This algorithm takes as input the user’s identifier to be revoked, the current revocation list RLδ, and state information δ as well as are vocation time t. It propagates an updated list of revocations.

IV. CONCLUSION.

In this work we projected a safe and cost - effective multi - authority attribute - based access control scheme for data distribution in the cloud storage systems, a multi - authority Cipher - text Policy - Attribute Based Encryption scheme supports scalable user revocation and public cipher - text update. The proposed scheme achieves the intended safety properties of forward safety and backward safety, and can also withstand key exposure to decryption. The performance discussions and implementation experiments show that for practical applications our scheme is more desirable. It helps to ensure that the data stored in the cloud by the data owner is valid or not. Data storage security is still in its early years in Cloud Computing, a field complete of challenges and of supreme significance, and many research remains to be identified in the future.

REFERENCES

[1]Liang, K. and Susilo, W., 2015. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Transactions on Information Forensics and Security, 10(9), pp.19811992.

[2]Fan, C.I., Huang, V.S.M. and Ruan, H.M., 2014. Arbitrary-state attribute-based encryption with dynamic membership. IEEE Transactions on Computers, 63(8), pp.1951-1961.

[3]Liu, X., Ma, J., Xiong, J. and Liu, G., 2014. Ciphertext-Policy Hierarchical Attribute-based Encryption for Fine-Grained Access Control of Encryption Data. IJ Network Security, 16(6), pp.437-443.

[4]Yang, M. and Yang, Y., 2010. An efficient hybrid peer-to-peer system for distributed data sharing. IEEE Transactions on computers, 59(9), pp.1158-1171.

[5]Baek, J., Vu, Q.H., Liu, J.K., Huang, X. and Xiang, Y., 2015. A secure cloud computing based framework for big data information management of smart grid. IEEE transactions on cloud computing, 3(2), pp.233-244.

[6]Hur, J., 2013. Improving Security and Efficiency in Attribute-Based Data Sharing. IEEE Trans. Knowl. Data Eng., 25(10), pp.2271-2282.

[7]Liu, J., Huang, X. and Liu, J.K., 2015. Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. Future Generation Computer Systems, 52, pp.67-76.

[8]Liang, K., Au, M.H., Liu, J.K., Susilo, W., Wong, D.S., Yang, G., Phuong, T.V.X. and Xie, Q., 2014. A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, 9(10), pp.1667-1680.

[9]Liang, K., Au, M.H., Liu, J.K., Susilo, W., Wong, D.S., Yang, G., Yu, Y. and Yang, A., 2015. A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Future Generation Computer Systems, 52, pp.95-108.

[10]Liu, Q., Wang, G. and Wu, J., 2014. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information sciences, 258, pp.355-370.