Implementation of Double encryption algorithm using two party Key provision Protocol for attribute primarily based information sharing theme on cloud

Ramya M L[1], KumaraSwamy S[2], Dr. Kavitha K S[3], Dr. Kavitha C[4]

[1]PG Student, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India
[2]Associate Professor, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India
[3]Professor, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India
[4]Professor & HOD, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India

---***---

Abstract -*The secured data sharing is provided between the information owner and user supported the user's attribute. In several distributed systems a user have to be compelled to exclusively be ready to access data if a user possess an explicit set of credentials or attributes. But even data owner is allowed here to completely management the access policy associated with his data to be shared. However, if any server storing the information is compromised, then the confidentiality of the information are aiming to be compromised. System for realizing complicated access management on encrypted knowledge that we tend to decision Ciphertext-Policy Attribute-Based .CP-ABE is limited to a possible security risk that's called key written agreement downside, whereby the key keys of users ought to be issued by a sure key authority. to get rid of the written agreement downside proposing associate degree improved two-party key provision protocol will guarantee that neither key authority nor cloud service supplier can compromise the entire secret key of a user one by one. Therefore, each storage price and coding quality for a ciphertext are alleviated. The performance analysis and therefore the security proof show that the projected theme is ready to attain economical and secure knowledge sharing in cloud computing.*

Key Words: Secure data sharing, attribute-based encryption, removing escrow, weighted attribute, cloud computing.

1. INTRODUCTION

Cloud computing has become a groundwork hot-spot because of its distinguished long-list blessings (e.g. convenience, high scalability). one amongst the foremost promising cloud computing applications is on-line knowledge sharing, like ikon sharing in On-line Social Networks among over one billion users and on-line health record system. An information owner (DO) is sometimes willing to store massive amounts of information in cloud for saving the price on native data management. with none knowledge protection mechanism, cloud service supplier (CSP), however, will totally gain access to all or any knowledge of the user. This brings a possible security risk to the user, since CSP could compromise the information for industrial advantages.

Accordingly, the way to firmly and expeditiously share user knowledge is one amongst the toughest challenges within the state of affairs of cloud computing. Ciphertext-policy attribute-based secret writing (CP-ABE) has turned to be an important encryption technology to tackle the challenge of secure data sharing. In a CP-ABE[3][7], user's secret key is described by an attribute set, and ciphertext is associated with an access structure. DO is allowed to define access structure over the universe of attributes. A user can decrypt a given ciphertext only if his/her attribute set matches the access structure over the ciphertext. Employing a CP-ABE system directly into a cloud application that may yield some open problems.

Firstly, all users' secret keys need to be issued by a fully trusted key authority (KA). This brings a security risk that is known as key escrow problem[5]. By knowing the secret key of a system user, the KA can decrypt all the user's ciphertexts, which stands in total against to the will of the user.

Secondly, the quality of attribute set is another concern[2]. As so much as we all know, most of the present CP-ABE schemes will solely describe binary state over attribute, as an example, "1 - satisfying" and "0 - not-satisfying", however not coping with arbitrary-state attribute.

2. LITERATURE REVIEW

In 2005, Sahai and Waters introduced fuzzy identity-based encryption (IBE)[5], which is the seminal work of attribute-based encryption (ABE)[4]. After that, 2 variants of ABE were proposed: key-policy ABE (KP-ABE) and CP-ABE, counting on if a given policy is related to either a ciphertext and a key. Later, several CP-ABE schemes with specific options are given within the literature. for instance, given a completely unique access management theme in cloud computing with economical attribute and user revocation. The machine overhead is considerably eliminated from

O(2N) to O(N) in user key generation by up CP-ABE theme, wherever N is that the variety of attributes. the dimensions of ciphertext is roughly reduced to 1/2 original size.

However, the protection proof of the theme isn't totally given. Most of the prevailing CP-ABE schemes need a full sure authority with its own master secret key as input to come up with and issue the key keys of users.Thus, the key escrow issue is inherent, such that the authority has the "power" to decrypt all the ciphertext of system users[7]. Chase and Chow presented a distributed KP-ABE scheme to solve the key escrow problem in a multi-authority system. In this approach, all authorities, which are not colluded with each other, are participating in the key generation protocol in a distributed way, such that they cannot pool their data and link multiple attribute sets belonging to the same user. Because there is no centralized authority with master secret information, all attribute authorities should communicate with others in the system to create a user's secret key. But, a major concern of this approach is the performance degradation.

It leads to O(N2) communication overhead on each the system setup part and any rekeying part. It conjointly needs every user to store O(N2) extra auxiliary key parts additionally to the attribute keys, wherever N is that the range of authorities within the system . Chow later planned Associate in Nursing Associate in Nursing anonymous non-public key generation protocol for IBE wherever a Ka will issue non-public key to an documented user while not knowing the list of the user's identities. It appears that this approach will properly be employed in the context of ABE if attributes area unit treated as identities. However, this theme can not be adopted for CP-ABE, since the identity of user could be a set of attributes that isn't publically unknown.

In 2013, provided associate improved security information sharing theme supported the classic CP-ABE. The key written agreement issue is self-addressed by victimization associate escrow-free key supply protocol wherever the key generation center and also the information storage center work along to get secret key for user[1]. Therefore, the procedure price in generating user's secret key will increase as a result of the protocol needs interactive computation between the each parties. Besides, Liu et al. bestowed a finegrained access management theme with attribute hierarchy, wherever and area unit engineered, severally. within the schemes, the attributes area unit divided into multiple levels to realize fine-grained access management for class-conscious attributes, however the attributes will solely specific binary state. Later, Fan et al. projected associate arbitrary-state ABE to resolve the problem of the dynamic membership management.

2.1 Cloud Service Model

Cloud Software-as-a-Service: Software–as-a-Service is a software distribution scheme which gives right to access the software and its functions remotely as a web-based service. Software-as-a-Service permits organizations to get into business functionality a very low cost normally less than paying for licensed applications since SaaS charges are built on a monthly fee. As so the software is hosted remotely users do not require paying for additional hardware. Software-as-a-Service eliminates the all possibilities for organizations to handle the installation, set-up, daily preservation and maintenance.

Cloud Platform-as-aService: the capability provided to the users to deploy onto the cloud infrastructure. PaaS model, cloud suppliers brings a computing platform, naturally comprising Operating System, Programming Language execution environment, database and wed servers. Application developers can develop and run their software results on cloud platform with no cost and difficulty of acquiring and handling of the main hardware and software films, for examples Oracle cloud platform-as-a-service, Oracle provides the Database as platform. And other example is windows azure.

In other means Platform-as-a-Service is the facility to offer to the users to deploy user-designed or obtained applications on the cloud infrastructure. PaaS can largely be characterized as application development environments proposed as a „Service" via the cloud supplier. Users uses these platforms which is being normally have Integrated Development Environment (IDE), so as it comprises the editor, compiler, build/execute and deploy features to develop their applications.

And users deploy their applications on the infrastructure provided by the cloud supplier. Cloud Infrastructure-as-a-Service: The cloud infrastructure such as hardware, servers, routers, storage, and other networking modules all are granted by the IaaS supplier. The end user takes on these offered services based on their requirements and pay for what they have used. The end user is capable of deploy and run any software, which comprise Operation Systems, applications. The end user does not supervise or monitor the core cloud infrastructure, but has hold over the operation systems and deployed application.

At this juncture the end user needs to experience the resource requirements for the precise application to make use of IaaS properly. Flexibility and scaling are the liabilities of the end user, not the supplier. Moreover IaaS is small task performing - it-yourself information hub so as you would require to form the means (server, storage) and make the task completed. Waiting right away, small end users did not have the investment to make a purchase of immense computing resources and to make sure that they had the space they wanted to manage unpredicted spikes during load.

2.2 Cloud Deployment Model

Public Cloud-A cloud is to be entitled as public cloud when the services (like applications, storage) are being provided over network that are available publically, anyone can access it. Public cloud's benefits may be taken as on a pay per usage mode or other purchasing schemes. Private Cloud – A private cloud is an infrastructure that provides the services to a single organization, whether managed by internally or by a third party. Cloud which is hosted externally is termed as "externally hosted" private cloud and other hosted by third party are termed as "on premise" private cloud. Community Cloud-It comprises sharing of computing infrastructure between organizations of identical community. Hybrid Cloud-A hybrid cloud is a collection of private as well as public cloud options.) That remains unique entities but is bound together by standardized or proprietary technology.

2.3 Cloud security issues

While cost and ease of use are the two main strong benefits of the cloud computing, there are some major alarming issues that need to be referenced when allowing moving critical application and sensitive data to public and shared cloud environment[6]. The main aspect describing the achievement of any new computing technology is the height of security it provides whether the data located in the cloud is protected at that level that it can avoid any sort of security issue. So that Security and privacy are the key challenges in the cloud computing.

2.3.1 Data availability issue

When keeping data at remote location which is owned by others, data owner may face the problem of system failure of the service provider. And if cloud stops working, data will not be available as the data depends on single service provider. Threats to data availability are flooding attacks causes deny of service and Direct /Indirect (DOS) attack. Cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system.

2.3.2 Data integrity issue

As the word itself explains the "completeness" and "wholeness" of the info that is that the basic and central wants of the knowledge technology, that integrity of information is very important within the info equally integrity of information storage is very important and necessary demand within the cloud, it's the key issue that agitated the performance of the cloud. the info integrity proofs the validity, consistency and regularity of the info. it's the right methodology of writing of knowledge in a very secure means the persistent data storage which might be reclaim or retrieved within the same layout because it was keep later. So cloud storage is changing into in style for the outsourcing of regular management of information .So integrity observation of knowledge| within the cloud is additionally important to flee all potentialities of information corruption and data crash. The cloud supplier ought to offer surety to the user that integrity of their information is maintained within the cloud.

3. SYSTEM ARCHITECTURE

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

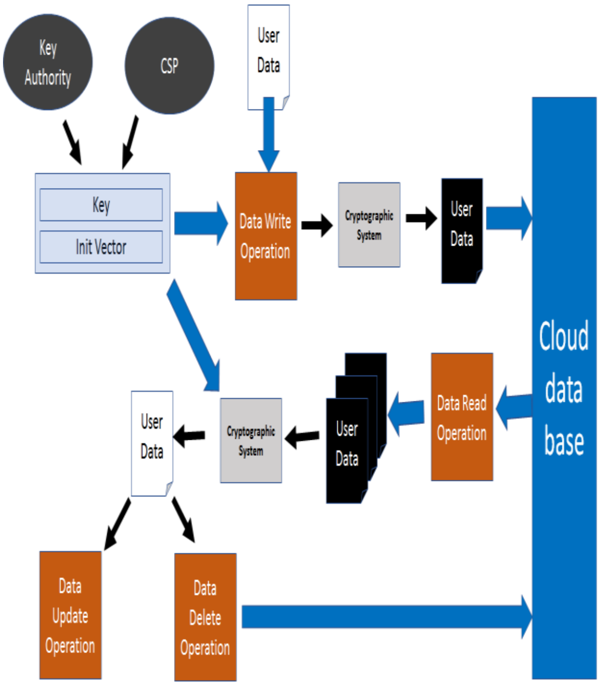

Fig 1: Proposed system Architecture

3.1 Data Access Layer

Data access layer is the one which exposes all the possible operations on the data base to the outside world. It will contain the DAO classes, DAO interfaces, POJOs, and Utils as the internal components. All the other modules of this project will be communicating with the DAO layer for their data access needs

3.2 Account Operations

Account operations module provides the following functionalities to the end users of our project.

- Register a new seller/ buyer account
- Login to an existing account
- Logout from the session
- Edit the existing Profile
- Change Password for security issues
- Forgot Password and receive the current password over an email

3.3 Key and Init Vector Generation

This module generates the Key and Init vectors which will be used for performing the encryption and decryption operations using the AES algorithm. A key is something you keep secret. Anyone who knows your key (or can guess it) can decrypt anydata you've encrypted with it. An IV or initialization vector is, in its broadest sense, just the initial value used to start some iterated process. Here, both the key and Init vector will be a random alphanumeric string of 16 characters each.

4 CONCLUSIONS

The improved key supply protocol was bestowed to resolve the key written agreement downside. It enhances knowledge confidentiality and privacy in cloud system against the managers of Hindu deity and CSP similarly as malicious system outsiders, wherever Hindu deity and CSP square measure semi-trusted. Additionally, the weighted attribute was planned to enhance the expression of attribute, which may not solely describe arbitrary state attributes, however conjointly cut back the quality of access policy, so the storage value of ciphertext and time value in coding may be saved.

5. FUTURE WORK

Future lines of research include the analysis of novel cryptographic techniques that could enable the secure modification and deletion of data which is in the Cloud. This would give permission to extend the privileges of the authorization model with more actions like edit and delete. Future lines of this research work include extending the encryption algorithm to PDF and image files, and also to integrate the storage with big data processing technologies.

ACKNOWLEDGMENT

Our thanks to my teachers who have contributed towards development of this paper.

REFERENCES

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid,” IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[2] A. Balu and K. Kuppusamy, “An expressive and provably secure ciphertext-policy attribute-based encryption,” Inf. Sci., vol. 276, no. 4, pp. 354–362, Aug. 2014.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[4] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in proc. 14th ACM Conf.Conf. Comput. Commun, Secure, 2007,pp. 456-465.

[5] S.S. M. Chow, “Removing escrow from identity-based encryption,”in Proc. 12th Int.Conf. Pract.Theaory Public Key Cryptogr,, 2009,pp.256-276.

[6] C.-K. Chu, W,-T, Zhu, J, Han, J,-K,Liu, J, Xu, and J,Zhou, “Security conerns in popular cloud storage services,”IEEE Pervasive Comput., vol. 12,no. 4,pp. 50-57, Oct/Dec,2013.

[7] H. Deng et al., “Ciphertext-policy hierarchical attribute-based encryption withshort ciphertexts,” Infs. Sci., vol. 275, no. 11,pp. 370-384,Aug, 2014.