CLOUD DATA DISTRIBUTION AND FILE SAFETY BASED ON HIERARCHICAL METHOD

Mr.M.Ramasamy

S.Keerthiga
IT-Final year
Jei Mathaajee College of Engineering Kanchipuram

M.Radhika
IT-Final year
Jei Mathaajee College of Engineering Kanchipuram

M.Yamuna
IT-Final year
Jei Mathaajee College of Engineering
Kanchipuram

ABSTRACT: One of the most promising application platforms is cloud computing it is used to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control is paramount as it is the first line of defense that prevents unauthorized access to the shared data. In this method user can share a sensitive information, such as the business financial records, research data, or personally identifiable health information etc. The encrypted outsourcing data as to provide end to- end data confidentiality assurance in the cloud . One of the hardly noticed problem for client is key exposure, but it is inherently existed in previous research. Furthermore, enormous client decryption overhead limits the practical use of ABE. The proposed collaborative Mechanism effectively solves both key escrow problem but also key exposure.

Meanwhile, it helps markedly reduce client decryption overhead. However making the computation over the encrypted data is very hard problem. The proposed scheme not only achieves scalability but it is more secure than previous scheme .The proposed scheme having a mutual key supervision procedure for cloud data distribution

and file safety based on hierarchical method.

KEYWORDS- Key management ,CP-ABE, security, efficiency, cloud data sharing

1.INTRODUCTION

Authority accepts the user enrollment and creates some parameters in cloud computing. Cloud service provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. User downloads and decrypts the interested ciphertext from CSP. The shared files usually have hierarchical structure. That is, a department of files are divided into a number of hierarchy sub departments located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved. Presently a day's more number of plans utilized encryption for control the information in Cloud. It empowers clients with restricted computational assets to outsource their expansive calculation workloads to the cloud, and monetarily appreciate the monstrous computational power, data transfer capacity, stockpiling, and even proper programming that can be partaken in a compensation for each utilization way. Distributed computing is a progressive registering worldview which empowers adaptable, on-request and minimal effort utilization of figuring assets. Those points of interest, unexpectedly, are the reasons for security and protection issues, which rise in light of the fact that the information claimed by various clients are put away in some cloud servers rather than under their own control. The security issue of distributed computing is yet to be settled. To manage security issues, different plans in light of the Attribute-Based Encryption have been utilized. From one perspective, the outsourced figuring workloads often contain sensitive information, for instance, the business money related records, prohibitive research data, or eventually identifiable prosperity information et cetera. To fight against unapproved information spillage, sensitive data must be mixed before outsourcing so as to offer end to-end data protection affirmation in the cloud and past. Regardless, normal data encryption procedures by and large shield cloud from playing out any critical operation of the essential figure content game plan, making the count over encoded data a troublesome issue. The proposed plot not simply achieves flexibility due to its dynamic structure. We give the protection secure out in the open social distributed computing. In our venture we actualize progressive property base security the pecking orders are Cloud specialist, Domain expert and clients. Cloud expert can just have benefit to make or expel the domain (private cloud specialist) in cloud and they can keep up every one of the points of interest in general cloud Domain expert can make or evacuate the clients inside the area this clients are called private clients. Clients are two sorts private cloud client and open cloud client's Private cloud clients are depends the space Public clients under cloud specialist. Clients can transfer the documents in two ways: Public and Private. On the off chance that the private client transfer general society document, the record deceivability and availability is just inside area itself and same space clients can get to that document with no security validation If the general population client transfer people in general document, the record deceivability and openness is constantly open any cloud client can get to that document. For Private transfer If private client transfer the private document implies that record deceivability is just inside space yet document openness is who have the emit key (OTP) implies who have benefit to get to the record If general society client transfer the private document implies that document deceivability is open anybody can obvious the document yet who have a benefit (OTP) to get to they just can get to the document.

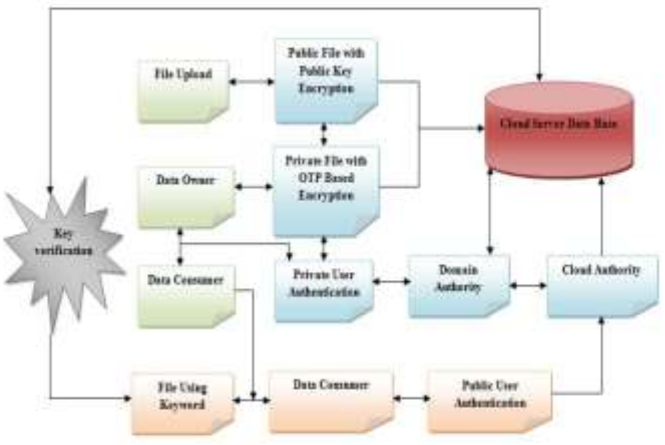
2.EXISTING SOLUTION

- In this scheme the shared data files must characteristic of multilevel hierarchy and this is used particularly in the area of healthcare and the military.
- The hierarchy structure of shared files hasn’t been explored in CP-ABE. Using Cipher text-policy attribute based encryption to secure the cloud storage part.
- The authority for file access control in which authorized of all operations on cloud data can be managed in the entire manner.

- The key authority must be completely trustworthy, as it can decrypt all the cipher text using a generated private key without permission of its owner.
- To avoid unauthorized information leakage, sensitive data have to be encrypted before outsourcing. Role based encryption is used for encrypting the data based on the authority provided.
- Existing system can't secure computation outsourcing data.
- To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing.
- Plaintext data in cloud does not having a security by using ordinary data encryption technique.
- Making the computation over encrypted data a very hard problem. Complex of access control policies.
- Cipher-texts are not encrypted to one particular user as in traditional public key cryptography.
- Assigning multiple values to the same attribute.

3.OUR WORK:

- We offer the security of social cloud computing. In this paper we put into practice hierarchical security, Cloud authority, Domain authority and users. Cloud authority can only have a privilege to create or remove the province in cloud and they can preserve all the details in overall cloud Domain authority can create or eliminate the users contained by the domain this users are called private users .
- Two type users will be there. One is private cloud user and another one is public cloud users. Private users are rely on the domain, Public users under cloud authority. User has a two way of uploading files Public and Private.
- If one file uploaded by private user, file visibility and convenience having only within domain without confirmation. If some file should uploaded by public user's then, file access privileges having all the users.
- To enhance both security and efficiency of key management in cipher text policy attribute-based encryption for cloud data sharing system
- If file uploading the private user means file visibility is only within field but file accessibility is who have the secrete key (OTP) means who have license to access the file If the public user upload the private file means that file visibility is public anyone can noticeable the file but who have a privilege like one time password to access they only can access the file.
- Existing system can't secure computation outsourcing data.
- Sensitive data have to be encrypted before outsourcing due to unauthorized information leakage
- Ordinary data encryption techniques can't secure cloud underlying plaintext data.
- Making the computation over encrypted data a very hard problem.
- Complex of access control policies.
- Cipher-texts are not encrypted to one particular user as in traditional public key cryptography.
- Assigning multiple values to the same attribute.



IDE:Net Beans 7.0.1

Net Beans is an integrated development environment (IDE) for developing primarily with Java, but also with other languages, in particular PHP, C/C++, and HTML5. It is also an application platform framework for Java desktop applications and others. The Net Beans IDE is written in Java and can run on Windows, OS X, Linux, Solaris and other platforms supporting a compatible JVM.

The Net Beans Platform allows applications to be developed from a set of modular software components called modules.

Applications based on the Net Beans Platform (including the Net Beans IDE itself) can be extended by third party developers The Net Beans Team actively supports the product and seeks feature suggestions from the wider community. Every release is preceded by a time for Community testing and feedback.

Net Beans IDE provides first-class comprehensive support for the newest Java technologies and latest Java specification enhancements before other IDEs. It is the first free IDE providing support for JDK 8 previews, JDK 7, Java EE 7 including its related HTML5 enhancement and Java FX .With its constantly improving Java Editor, many rich features and an extensive range of tools, templates and samples, Net Beans IDE sets the standard for developing with cutting edge technologies out of the box. An IDE is much more than a text editor. The Net Beans Editor indents lines, matches words and brackets, and highlights source code syntactically and semantically. It also provides code templates, coding tips, and refactoring tools.

The editor supports many languages from Java, C/C++, XML and HTML, to PHP, Groovy, Java doc, JavaScript and JSP. Because the editor is extensible, you can plug in support for many other languages. Keeping a clear overview of large applications, with thousands of folders and files, and millions of lines of code, is a daunting task. Net Beans IDE provides different views of your data, from multiple project windows to helpful tools for setting up your applications and managing them efficiently, letting you drill down into your data quickly and easily, while giving you versioning tools via Subversion, Mercurial, and integration out of the box. When new developers join your project, they can understand the structure of your application because your code is well-organized. Net Beans provides static analysis tools, especially integration with the widely used Find Bugs tool, for identifying and fixing common problems in Java code. In addition, the Net Beans Debugger lets you place breakpoints in your source code, add field watches, step through your code, run into methods, take snapshots and monitor execution as it occurs.

The Net Beans Profiler provides expert assistance for optimizing your application's speed and memory usage, and makes it easier to build reliable and scalable Java SE, Java FX and Java EE applications. Net Beans IDE includes a visual debugger for Java SE applications, letting you debug user interfaces without looking into source code. Take GUI snapshots of your applications and click on user interface elements to jump back into the related source code. Net Beans IDE 7.0.1, which has full support for the official release of the Java platform.

MODULES:

- Data Owner
- Data Consumer
- Domain level Security
- Attribute based security
- Secret file accessing

Data Owner

In the data server, data can be upload by the data owner. For the purpose of security the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. The data owner can set the access privilege to the encrypted data file. Data Owner to delegate most of the computational overhead to cloud server . The use of KP-ABE provides fine-grained access control gracefully. The encrypted data file is stored. With the corresponding attributes and the encrypted . If the associated attributes of a file stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted, which is used in turn to decrypt the file. For the purpose of sharing a data with consumer, data owner can encrypt their data and store it in the cloud . Each data owner consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner.

Data Consumer:

The user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Domain authority and the Data users are controlled by the Domain Authority only. Users may try to access data files either within or outside the use of their access privileges, so unauthorized users may collude with each other to get sensitive files beyond their privileges. Data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. Data consumers will be always online. They come online only when necessary, while the cloud service provider, the trusted authority, and domain authorities are always online. The cloud is assumed to have abundant storage capacity and computation power. In addition, we assume that data consumers can access data files for reading only.Data consumer create the account and then login to access the cloud storage information and data consumer entry level based on the hierarchical manner.

Domain level Security:

The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain. We assume that communication channels between all parties are secured using standard security protocols.

Domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. Top-level organization corresponds to a each top-level domain authority, such as a federated enterprise, while each lower-level organization corresponds to a lower-level domain authority, such as an affiliated company in a federated enterprise. Data owners/consumers may correspond to employees in an organization. Each domain authority is responsible for managing the data owners/consumers in its domain.

A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain.

Trusted authority, multiple domain authorities, and numerous users corresponding to data owners and data consumers are available in system model. The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.

Attribute based security:

By applying a delegation algorithm to ASBE , the HASBE using a hierarchical structure of a system user. HASBE also achieves efficient user revocation because of multiple value assignments of attributes. We proved that the security of HASBE based on the security of CP-ABE. A hierarchical attribute-set-based encryption (HASBE) scheme is used for access control in the cloud computing. HASBE extends the cipher text-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

Secret files accessing:

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. The cloud server provider is untrusted in the sense that it may collude with malicious users (short for data owners/data consumers) to harvest file contents stored in the cloud for its own benefit. In the hierarchical structure of the system users given in each party is associated with a public key and a private key, with the latter being kept secretly by the party. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. The traditional method to protect sensitive data outsourced to third parties is to store encrypted data on servers, while the decryption keys are disclosed to authorize users only.

CONCLUSION:

In this paper, we introduced the HABSE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The HABSE scheme incorporates a hierarchical structure of system users by applying a Homomorphic algorithm to ABSE We formally proved the security of HABSE based on the security of CP-ABE Finally, we implemented comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

REFERENCE:

[1]K. Liang, M. H. Au, J. K. Liu, W. Susilo , D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie , “A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, October 2014.

[2]T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo , and J. Zhou, “ktimes attribute-based anonymous access control for cloud computing,” IEEE Transactions on Computers, vol. 64, no. 9, pp. 2595–2608, September 2015.

[3]F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, “CP-ABE with constant-size keys for lightweight devices,” IEEE Transactions on Information Forensics and Security, vol. 9, no 5, pp. 763–771, May 2014.

[4]T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, “Privacy preserving cloud data access with multi-authorities,” in Proc. IEEE INFOCOM, Apr. 2013, pp. 2634–2642.

[5] J. Hur, and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Trans. Parallel Distrib . Syst., vol. 22, no. 7, pp. 1214-1221, 2011.

[6] N. Oualha , and K. T. Nguyen, “Lightweight attribute-based encryption for the Internet of Things,” in Proc. ICCCN, 2016, pp. 1-6.

[7] S. Easwarmoorthy , F. Sophia, and A. Karrothu, “An efficient key management infrastructure for personal health records in cloud,” in Proc. WiSPNET, 2016, pp. 1651-1657.

[8] D. Pletea, S. Sedghi, M. Veeningen, and M. Petkovic, “Secure distributed key generation in attribute based encryption systems,” in Proc. ICITST, 2015, pp. 103-107.

[9] G. Zhang, L. Liu, and Y. Liu, “An attribute-based encryption scheme secure against malicious KGC,” in Proc. TRUSTCOM, 2012, pp. 1376-1380.