IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10724

IMPROVING PRIVACY AND SECURITY IN DECENTRALIZING MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION IN CLOUD COMPUTING

Kishanth E[1], Madhusoodhanan P[2]

BE, CSE, Anand Institute of Higher Technology, Affiliated to Anna University, Chennai[1,2]

Abstract: Decentralizing multi-authority attribute-based encryption (ABE) has been adopted for solving problems arising from sharing confidential corporate data in cloud computing. For decentralizing multi authority ABE systems that do not rely on a central authority, collusion resistance can be achieved using a global identifier. Therefore, identity needs to be managed globally, which results in the crucial problems of privacy and security. A scheme is developed that does not use a central authority to manage users and keys, and only simple trust relations need to be formed by sharing the public key between each attribute authority (AA).

User identities are unique by combining a user's identity with the identity of the AA where the user is located. Once a key request needs to be made to an authority outside the domain, the request needs to be performed by the authority in the current domain rather than by the users, so, user identities remain private to the AA outside the domain, which will enhance privacy and security. In addition, the key issuing protocol between AA is simple as the result of the trust relationship of AA

Keywords:

- AA Attribute Authority
- CP-ABE Cypher text- Attribute Based Encryption
- IBE Identity-based encryption
- HIBE Hierarchical Identity-based encryption
- HABE Hierarchical Attribute Based Encryption

I. INTRODUCTION

Cloud computing enables users to store their sensitive data into untrusted remotely cloud service providers to achieve scalable services on-demand. Prominent security requirements arising from this means of data storage and management include data security and privacy and require the use of strong encryption techniques with fine-grained access control for data security in cloud computing.

Attribute-based Encryption (ABE) is an efficient encryption system with fine-grained access control for encrypting out-sourced data in cloud computing. With the emergence of sharing confidential corporate data on cloud servers, data are generated by several organizations, and access policies can be defined by several authorities. Single-authority ABE cannot meet the demands of decentralized distribution, and decentralizing multi-authority ABE have been proposed to solve those problems. For basic Identity-based encryption (IBE) and ABE, all private keys are managed by an authorized center. However, in practice, this will present a performance bottle-neck requiring evaluation due to the huge numbers of requests. In addition, concentrated attacks seem to be more easily from happening. Therefore, Hierarchical IBE (HIBE) and Hierarchical ABE (HABE) are now being used.

HIBE and HABE are also called leveled multi-authority IBE and ABE. According to the main concept, the authorized center is managed at different levels, and domains or users at higher levels can use their private keys to generate private keys for the domain or users at lower levels. HIBE or HABE, when applied at various levels, can solve the key distribution load problem.

Because roots are ultimately trusted sources, authorized centers at each level are based on a single trusted root. In addition, system efficiency can be improved dynamically because identity authentication and key transmission can be performed locally.

Decentralizing multi-authority ABE is used to solve the access problem in which user attributes belong to different authorities. Those authorities differ from that for a leveled multi-authorized ABE, for which the leveled multi-authority ABE has one trust root. There is no trust between organizations, and attribute management and key distribution always

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 7, July 2021
DOI 10.17148/IJARCCE.2021.10724

are performed separately from each other. For some specified work reasons such as sharing confidential corporate data on cloud servers, trust relationships can be made between organizations.
Single-authority ABE primarily randomizes private keys, and the secret values are separated based on the part in the users' private keys (referring to a different attribute), and decryption is performed by reconstructing the secret values. In Single-authority ABE, each user's keys are generated using different random and secretly shared values such that keys generated for different users cannot be combined, which prevents collusion attacks. For decentralizing multi-authority ABE, the private keys of users can be generated by different authorities that do not communicate. Thus, the crucial technical challenge for decentralizing multi-authority ABE is constructing a secret-sharing value to resist collusion attacks. The Global Identifier (GID) and central authority originated to solve the resist collusion attacks. All early schemes used central authority to deliver secret splitting, thereby assuring collusion resistant under circumstances where in authorities do not trust one another. However, a central authority should be globally trustworthy.
Therefore, in order to avoid the security weaknesses resulting from the use of central authorities, schemes that do not employ central authorities have been published. There is no reliance on single trust centers, and although each authority distributes its own attributes and keys, they still need common support parameters for distribution by related organizations, or complicated trust relationships need to be formed between each authority. User's GID is published globally in early schemes will breach the user privacy. In order to solve the question, some schemes used anonymous key issuing protocol to enhance user privacy, but the protocols usually are complex.

OBJECTIVE:

Cloud offers **benefits** such as reduced **costs** and complexities, better agility etc. However, your business needs to identify and decide upon security challenges, transparency needs, availability and integration has to be carefully balanced.

SCOPE:

This system is to implement Improving privacy and security in Decentralized Multi-Authority Based Encryption using Cloud Computing, which also helps in IT industry, Commercial Purposes, Educational and Medical purposes.

ANALYSIS

SYSTEM ANALYSIS

This chapter gives an overview of the underlying technologies used to develop the project. In current scenario, cloud is the base of the development process and is integrated with the micro-services and sharing information in an encryption Frame work. The framework has predefined libraries and functions which can be inherited to Invoke existing encryption methods and on top of it the additions of the new algorithm to support Enhanced encryption.

Problem Definition

Various layouts based on attribute based-encryption are proposed to secure the cloud storage, but most of the target on the data content privacy and the access control, while less attention given to the privilege control and the identity privacy. Data sharing in the cloud is very feeble to cyber-attacks since data stored on cloud servers, and multiple users access data from unknown servers, resulting in Data security and privacy as critical issues for remote data storage. This uncertainty of Data Privacy and User Integrity is the foundation of the study.

Existing System

Confidential corporate data are not encrypted in cloud computing. Security issues in User Data. Expensive storage price. Data's are not in encrypted format. Lagging in data security. One of the main concerns regarding the security and privacy in cloud computing is the protection of data.
If the security and privacy in cloud computing is neglected, then the private information of each user is at risk, allowing easy cyber breaches to hack into the system and exploit any users' private storage data.

DISADVANTAGES

- Data is not in encrypted format.
- Lagging in data security.
- Expensive storage price.
- Security issues in User Data.
- Confidential corporate data are not encrypted in cloud computing.

Proposed System

Confidential corporate data are encrypted in cloud computing. Virtualized environment in Cloud Computing platform Online Storage for Data Handing user data in virtualized platform in highly secure way Cost Effective, Pay per use.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 7, July 2021
DOI 10.17148/IJARCCE.2021.10724

Avoid storing sensitive information in the cloud. Read the user agreement to find out how your cloud service storage works. Be serious about passwords Encrypt. Use an encrypted cloud service.

ADVANTAGES

- Avoid storing sensitive information in the cloud.
- Read the user agreement to find out how your cloud service storage works.
- Online Storage for Data, Be serious about passwords.
- Encrypt which Confidential corporate data are encrypted in cloud is computing.
- Use an encrypted cloud service.

REQUIREMENT ANALYSIS

Requirements specification and analysis identify, analyze, and model the functionality or "what's" of a prospective software system. The requirements specification and analysis phase of a software project is the most important phase of software development and should not be omitted under any condition.

Functional Requirements

Functional requirements explain what must be done by identifying the Necessary task, action or activity that must be accomplished. Functional Requirements analysis will be used as the top-level functions for functional Analysis.

Usability

Usability is the degree to which software can be used by specified consumes to achieve quantified objectives with effectiveness, efficiency and satisfaction in Quantified context of use.

Maintainability

Maintainability basically defines that how easy it is to maintain the system. This means that how easy it is to analyze, change and test the application. Maintainability of the project is simply as further updates can be easily done without affecting its stability.

Compatibility

Compatibility of this project is worldwide. It is a web application and is supported by all the web browsers.

Functionality

The system provides multiple functionality likes Time Allotment, Server Overloaded, Cloud Server Notification, Multiple Deadlines, User Notification and File Retrieval.

Efficiency

Efficiency the amount of resources required by a program to perform a specific function. This term is used to show the effort put in to develop the application and to quantify its user-satisfaction.

Security

Security is a specialized field that focuses on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts.

Safety

Safety is a risk management strategy based on identification, analysis of
Hazards and application of remedial controls using a systems-based approach.

Non-Functional Requirements

Security

The state of providing access to resource is security. The system provides sad security and authorized user cannot access the system thereby providing separate login to admin. Only authenticated user can access data thereby maintaining high security.

Portability

It is the usability of the same application in different environment. The web application can be run on any browser.

Performance

These requirements determine the resources required that deals with the performance of the system.

Flexibility

The flexibility of the project is provided in such a way that is has the ability to run on different environments being executed by different users.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10724

SOFTWARE ANALYSIS

Hardware Requirements:

A. Speed : 2 GHz core CPU.
B. RAM : 4 GB RAM or above.
C. Hard Disk : 120 GB HDD.
D. Processor : Intel i3 and above processor.

Software Specification:

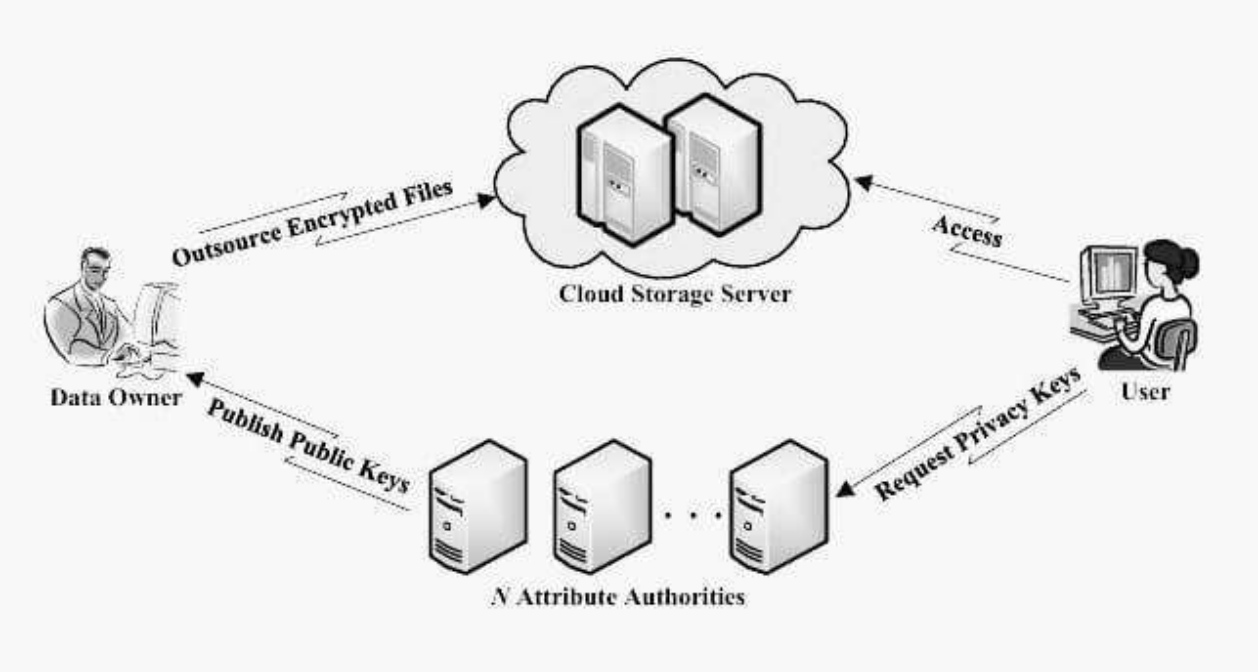
- Public Cloud account : AWS
- Operating System : Windows/Linux OS
- Front End : KMS Key Encryption
- Back End : Amazon Web Service

DESIGN

SYSTEM DESIGN

Systems design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development.

Overall Design



RESULT AND DISCUSSION

Our proposed system which provides to learn an effective latent representation, we simultaneously incorporate prior knowledge, such as temporality of wellness features aerogravity of users. Essentially, the secure search is thus a technique that allows an authorized data user to search over the data owner's encrypted data by saving encrypted query keywords in a privacy-preserving manner and is an effective intension of traditional searchable encryption to adapt for the cloud computing environment.

CONCLUSION

Our system has a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server. Moreover, in our design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually retuned by the cloud server. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed scheme.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10724

FUTURE ENHANCEMENT

Security issues in the area of cloud computing are active area of research and experimentation. Cloud services are available to achieve security with the varying techniques and methods. Cloud services are studied and analyzed to evaluate the trust value. In our project, the size of file is small and it is suited for text file. So, in future our project can be extended for multimedia file and size of the same should be refined.

REFERENCES

A. Abadi, Agrawal, (2012) "A flexible fine-grained dynamic access control approach for cloud computing environment" in Conference on Data and Applications Security and Privacy.

B. Boneh.D, Franklin, (2005) "Multi-authority Attribute Based Encryption" in Springer, Heidelberg.

C. jian weng, junjuo lai, (2014) "Fully secure key-policy attribute-based encryption with" in 9th ACM symposium on information, computer a and communications security

D. John Bethencourt, Amit Sahai, Brent Waters, (2007) "Cipher text- Policy Attribute-Based Encryption" in IEEE Symposium on Security and Privacy.

E. LanZhang, TaehoJung, PuchunFeng, Kebin Liu, Xiang-Yang, (2015) "A Lightweight Secure Data Sharing Scheme for Mobile" in IEEE Transaction on parallel and Distributed system.

F. Youwen Zhua, Zhiqiu Huang, Tsuyoshi Takagi, (2016) "Distributed Attribute-Based Encryption" in IEEE Transaction on parallel and Distributed system.

