ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing

Dhaval Jain[1], Piyush Daga[2], Rahul Jangir[3], K.B.Satpute[4]

Student, Department of Computer Engineering, Sinhgad College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India[1,2,3,]

Professor, Department of Computer Engineering , Sinhgad College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India[4]

ABSTRACT: Decentralizing multi-authority Attribute-Based Encryption has been adopted for solving problems arising from sharing confidential corporate data in cloud computing. For decentralizing multi- authority Attribute-Based Encryption 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 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. User identities are unique by combining a user's identity with the identity of the Attribute Authority 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 Attribute Authority outside the domain, which will enhance privacy and security. In addition, the key issuing protocol between Attribute Authority is simple as result of the trust relationship of Attribute Authority. Moreover, extensibility for authorities is also supported by the scheme presented in this essay. The scheme is based on Composite Order Bilinear Groups. A proof of security is presented that uses the Dual System Encryption methodology.

I. INTRODUCTION

Cloud computing enables users to store their sensitive data into untrusted remotely cloud service providers to achieve scalable services on-demand. For basic Identity-based encryption (IBE) and ABE, all private keys are managed by an authorized center. In basic ABE systems, the information shared is always within one domain or organization. However, in reality, information such as drivers' licenses and registration information in universities are organized by different government departments. 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 wherein authorities do not trust one another.

Scope

Provide Security to data using de-centralized system that is using more AA in project rather than one.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

II. LITERATURE SURVEY

1. "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems" **Seed Idea:** An access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability.
Limitations: Huge issue in Enforcement of authorization policies and the support of policy updates.

2. "Efficiently Revocable and Searchable Attribute-Based Encryption Scheme for Mobile Cloud Storage"
Seed Idea: The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.
Limitations: The access policy is not support to multiple domain.

3. "Improving Privacy and Security in Decentralizing Multi-Authority Attribute- Based Encryption in Cloud Computing "
Seed Idea: Achieve the security from multiple domains using multi-authority ABE for access policy.
Limitation: It does not support to de-duplication.

III. PROPOSED SYSTEM

In the proposed system, the DMA system: DO (Data Owner), AA (Attributes Authority), Cloud storage provider (CSP), CO (Company Owner). Company owner is responsible for calculating public key, defining access policy and encrypting data under the access policy. Furthermore, the company owner needs to upload the encrypted data to the remote cloud storage server. AA (Attribute Authority). AA plays the role of attributes distribution and employee authorization. It computes employee' attributes based on the public parameters and distributes them to CO and employees for access policy definition. Every AA can manage multiple attributes and has full control over those attributes. Cloud Server Provider (CSP). CSP is considered as a semi-trusted storage media that stores data. It is also responsible for updating the cipher-text when attribute revocation occurs. The CSP does not have the secret keys, so it can't decrypt the cipher-text. Employee. Cipher-text on the cloud server can be accessed freely by employee. But only when the employee's attributes satisfy the access policy that defined in the cipher-text, can he/she decrypt the cipher-text. Employee's attributes are distributed by a number of authorities according to the user privileges so that it can achieve cross-domain access control. And as contribution we also split data into the blocks and secure individual block with the help of encryption so that security can be achieved. The results indicate that the proposed system is efficient and secure with the help of encryption techniques used in the data outsourcing systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

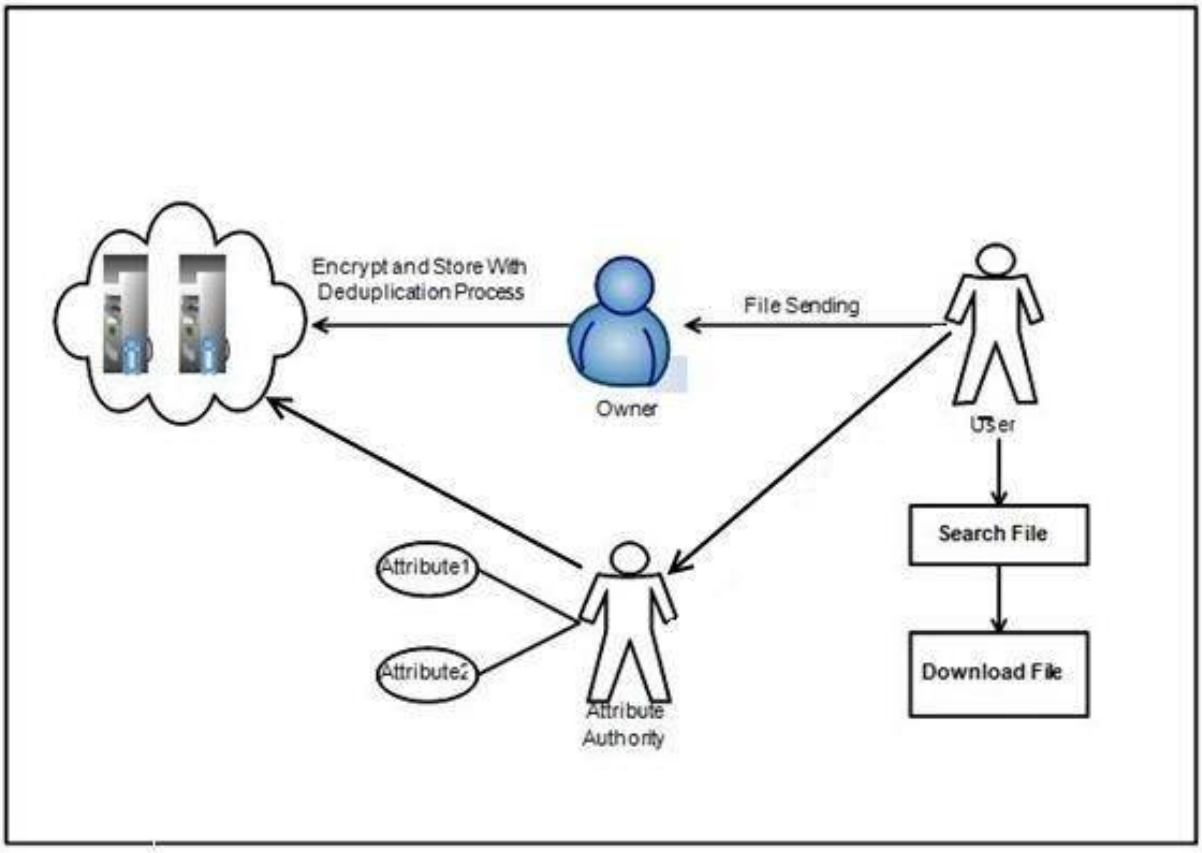

Fig 1: Proposed System Architecture

IV. IMPLEMENTATION

Cloud computing enables users to store their sensitive data into untrusted remotely cloud service providers to achieve scalable services on-demand. For basic Identity-based encryption (IBE) and ABE, all private keys are managed by an authorized center. In basic ABE systems, the information shared is always within one domain or organization.

1. Maintain the security of sensitive data stored on cloud.
2. Encryption and decryption technique used to protect data of user.
3. To fulfill requirements, proposed system implements IBE and ABE algorithms for protecting the data.
4. ABE algorithm Access multiple attributes from multiple domains using trusted attributes authority (AA).
5. Using the de-duplication concept we store the memory from duplicate files.

Encryption / Decryption: Encrypting / Decrypting Part of a Byte Array. The Java Cipher class encryption and decryption methods can encrypt or decrypt part of the data stored in a byte array. You simply pass an offset and length to the update () and / or doFinal () method.

IBE algorithm: IBE algorithm is used in same domain for sending file. Like if user1 sending file to user2 then user1 know n's its own identity like email so he send file to user1 using the attribute that is email of user2 with encrypt format if user2 satisfy this attribute i.e. email then he can download it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

ABE algorithm: After getting the clear concept I got we use the CP-ABE algorithm because we upload file with some attributes like {manager, designer, etc} and then checking the Access Policy when user2 download the data.

V. MATHEMATICAL MODEL

S=fs, e, X, Y,_g Where,
s = Start of the program.
1. Log in with webpage.
2. Load Files on cloud. e = End of the program.

Provide security to data and improve performance. X = F,Nb,A
X = Input of the program. F = File.
Nb = Number of blocks A-Attributes
Y = Output of the program.
File firstly store on cloud with encryption with some attributes. At the time of storing it create blocks and store. If some user wants to download that file the AA of that domain checks attributes and authorize users and give permissions.
X, Y 2 U

Let U be the Set of System. U= fClient, E, Ag
Where User, E,H are the elements of the set. User=Data Owner
E=Encryption of File A=Attributes

Space Complexity:
The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity.

Time Complexity:
Check No. of patterns available in the datasets= n
If (n¿1) then retrieving of information can be time consuming. So the time complexity of this algorithm is O(n_n).
_= Failures and Success conditions.

Failures:
1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

VI. RESULTS

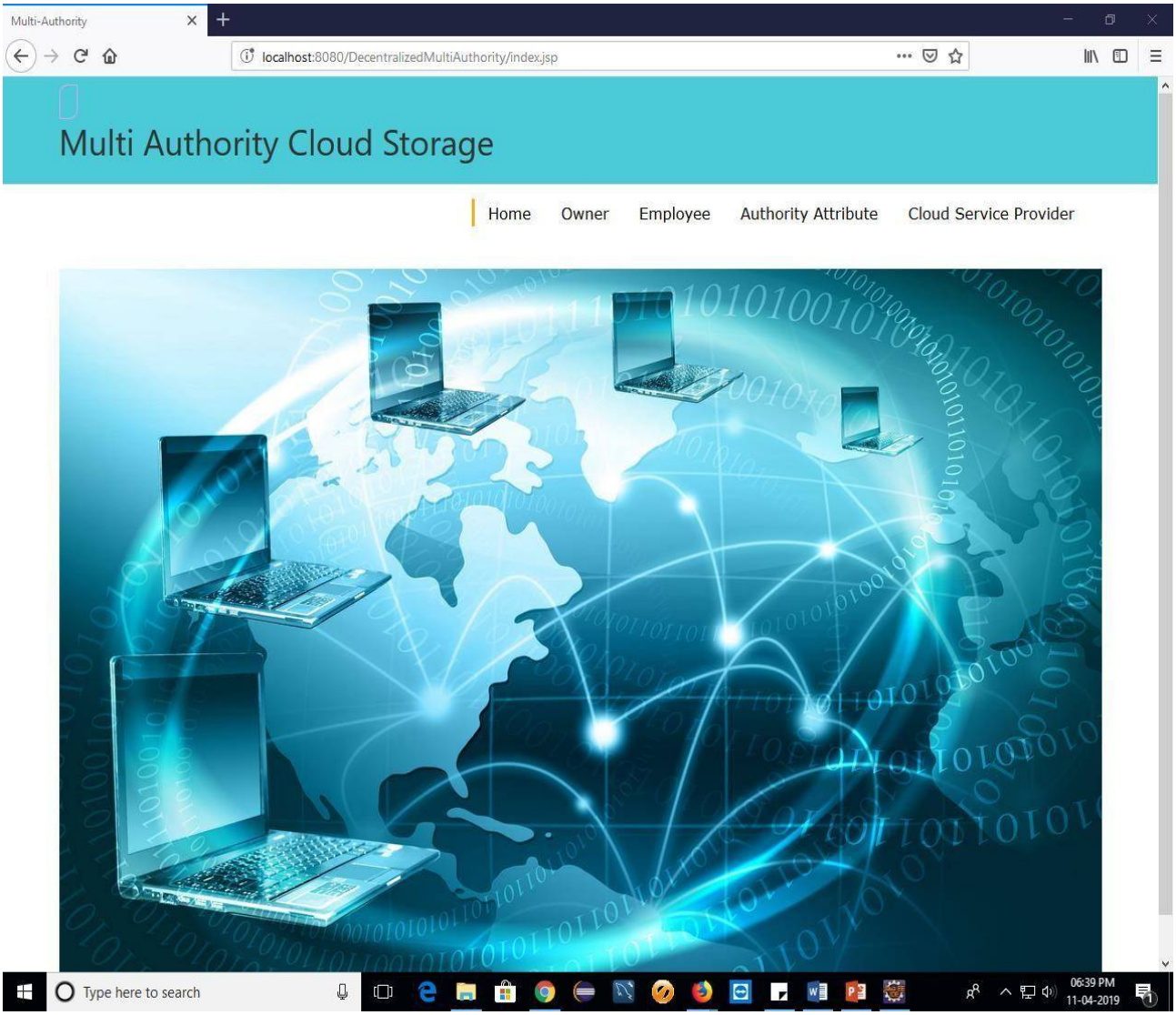

Fig 2: Main Home Page GUI

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Table of the results

Table 1: File Uploading With Security Time

Time(ms)	File Size(KB)
15000	0.52
16300	1.554
1700	0.025
1100	15.031

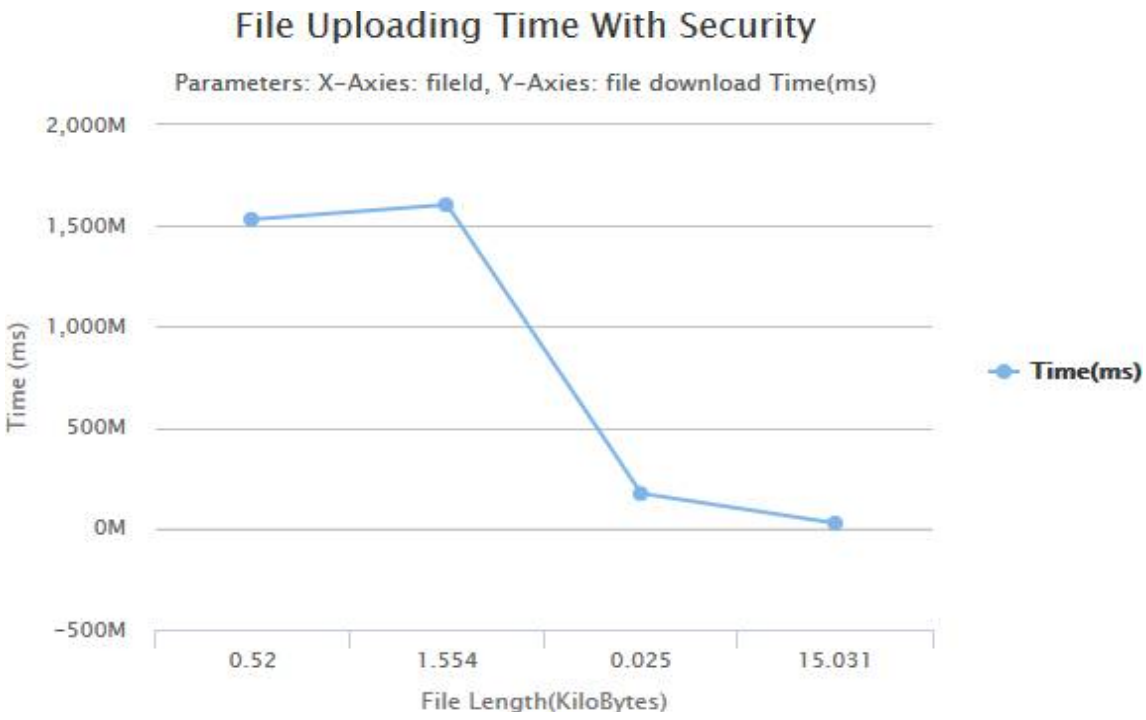

Fig 3: File Uploading With Security Time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

VII. CONCLUSION AND FUTURE WORK

Conclusion

Propose system achieve security by using ABE and IBE algorithm. In ABE uses multiauthority ABE, it solve many issues of privacy requirements of sharing data on clouds. We utilize get to tree that oversee credits which has a place with various specialists to accomplish cross-area data storage and access control. The system achieve cipher text access control, preventing collusion attacks between users and authorities as well as improve the efficiency of cipher text encryption and decryption. So the proposed system can access data from cross domain with encryption and decryption.

Future Work

1. In future we can implement system for uploading media files.
2. Also we improve project as checking the location of user and give access to only business branch location.

REFERENCES

1. Junbeom Hur and Dong Kun Noh, Member, IEEE 2011, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems”.
2. Shangping Wang, Duo Zhang, Yaling Zhang, And Lihua Liu 2018, “Efficiently Revocable and Searchable Attribute-Based Encryption Scheme for Mobile Cloud Storage”.
3. YAN YANG1,2 , XINGYUAN CHEN1,2,3, HAO CHEN4 , AND XUEHUI DU, 2018, “Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing”