Avoiding the Security Violation in Accessing the Cloud Resources Using Modified-Hierarchical Attribute Based Encryption

S. Praveen Kumar[1], Dr. B. Swaminathan[2]

[1]*P.G. Scholar,* [2]*Professor*

Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, Tamil Nadu, India

***Abstract*: Cloud computing is an internet- based computing pattern through which shared resources are provided to device on demand. Sharing the user data should be secured and integrity it must be achieved on cloud. Data sharing should be a secure transferable functionality in cloud security. The proposed system provides how to maintain integrity, confidentiality and availability to data sharing. To achieve data security, we use M-HABE (Modified-Hierarchical Attribute Based Encryption). Modified Hierarchical Attribute Based Encryption is a recent cryptographic primitive which has been used for access control. M-HABE also provide fine grained access control and reduce the communication overhead on the internet.**

***Key Terms*: Cloud computing, M-HABE, key generation, Encryption, Decryption, access control, fine-grained access**.

I. INTRODUCTION

Cloud computing is a collection of resources available to use as per the requirements of the user to store and share their data over the internet.

This defines novel approach of providing the services. In cloud computing the services are offered huge number of benefits to the organizations for their data management. The group of resources in cloud computing provided by service provider of cloud to the end user based on their demand through the internet. The virtual environment created by cloud computing for the user it will allow the end user to use the resource in cloud virtually. The common example of cloud services such as Google search engine, oracle cloud, Microsoft office 360. Cloud resources as challenge such as availability, reliability and the important research problem is security. In traditional cloud services and platform are the main concern is the absence of data security method.

M-HABE (Modified-Hierarchical Attribute Based Encryption) is one of the best approaches for public key encryption which is process for key management it is done by human intelligible attribute such as email address, IP address and unique name. It is direct encrypt message with the attribute of receiver attribute. The receiver achieve the private key is allocate with the corresponding attribute from the private key generator (PKG) is available to decrypt the cipher text.

M-HABE method to minimize the computation overhead at PKG with CSP (cloud service provider) entrusted. The key generation process handled during the process for the key issue and key update to KU-CSP (key updated cloud service provider).

Cloud is providing various application services to satisfy users requirement for providing the application services to the end user, the data has to make the flexible and scalable access control policy so that only authorized user can access. The cloud environment is inherently insecure in nature. To protect the data, it must be encrypted before uploading it on cloud storage.

The security violations in cloud environment user do not have knowledge about the term where the data is saved, who will manage the data as well as vulnerabilities. The security data is achieved by data placing to legitimate and authorized user. CSP using a multi-tenant cloud application cost reduction with use of virtual machine. The personal and private information accessing is threat to the security in the cloud.

II. SECURITY VIOLATION IN CLOUD

2.1 Data confidentiality

The Data confidentiality in the system before uploading data to the cloud, the data was encrypted by the data owner. Therefore, unauthorized parties including the cloud computing cannot know the information about the encrypted data.

2.2 Fine grained access control

The system granted the different access right to the individual user. Users are in the same group, but each user can be granted the different access right to access data even for users in the same group, their access rights are not the same.

2.3 Scalability

Scalability in the system defines that when the authorized users increase, the system can work efficiently. The number of authorized users cannot affect the performance of the system.

2.4 User accountability

In user accountability the authorized user may be deceptive, user would be share the attribute of the private key with another unauthorized user. It causes the problem that the unauthorized key would share among the unauthorized users.

III. RELATED WORKS

[1]Mrs. Rupali Sharma and Dr. Bharti joshi conducted study on Identity-Based Encryption (IBE) for the cloud security with outsourced revocation. The problem associated with IBE is overhead on PKG (Private Key Generator) for computation during user revocation. In cloud security the research problem is needed security improvement in IBE and efficient IBE revocation. To achieve the strong security they combine the IBE and ABE (Attribute-Based Encryption) along with cloud user identity, attribute through that IBE encryption, decryption then revocation occur. In IBE the KU-CSP (Key Update-Cloud Service Provider) is presented for user revocation. It can be performed by public cloud and third party will run it. A PKG service is standardized along with network.

The proposed is to solve the security enhancement problem with efficient revocation. IBE method they contribute the properties of ABE encryption and decryption process with original function of IBE key generation, encrypt and decrypt are redefined and modified with time component.

[2] Zhiguo wan, Jun'e liu and Rorth. Den'g conducted research on ABE (Attribute-Based Encryption) security in cloud environment. The proposed is for security on access control with outsourced data. Hierarchical Attribute-Set Based Encryption (HASBE) by extending Cipher text-policy Attribute-Set Based Encryption (CP-ASBE) with a hierarchical structure of user. It achieves scalability and flexibility and Fine grained access control. It analyzes its performance and computational complexity. The security of HASBE based on the security of CP-ASBE by Bethencourt. The performance analysis will be system setup, Top-level domain authority grant, new user/domain authority grant, new file creation. The implementation of HASBE will be setup, key generation, key deletion, key update, encrypt, decrypt and revocation.

[3] Minu Geroge, Dr. C. Suresh Gnanadhas, K. Saranya conducted survey on Attribute-Based Encryption (ABE) in cloud computing. The cloud consumer and Cloud Service Provider (CSP) have the different trusted domain. Security and privacy of data are the issues for the data storage. They analyze various schemes for encryption and for their solution. It consists of ABE (Attribute-Based Encryption), KP-ABE (Key policy-ABE), CP-ABE (Cipher text policy-ABE), HABE (Hierarchical Attribute Based Encryption), MA-ABE (Multi Authority-Attribute Based Encryption), ABE with non-monotonic access structure. After analysing different ABE scheme they conclude HABE(Hierarchical Attribute Based Encryption) will have good fine grained access control, efficiency is flexible and have good collusion resistant. It also enables dynamic modification of access policy to support on demand user/attribute revocation.

[4]Jia Yu, Kui Ren, Fellow and Cong Wang conducted study on cloud storage audit with key update of outsourcing verification author focus to make the key update for the client as transparent and proposed a new approach called cloud storage with verifiable key update outsource. The client only needs to download the secret key from the Third Party Auditor to decrypt. The salient features are designed carefully for the client to make the key exposure transparently. The key-update is performed by authorized party. Client can verify the validity of the secret key for encryption. It undergo algorithm to do these salient feature they are system setup, encrypted key update, encrypted key verification, secret key decryption, authentication generator, proof generator and proof verification. The main aim of the author to make the key update of verifiable outsourcing is transparent to the client.

[5]Vetripriya and Anand conducted study on Attribute Based Encryption (ABE) with privacy in cloud application. In cloud computing privacy and security are main concern. The symmetric key algorithm uses the same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes attributes and secret keys to all users. A new approach of decentralized access control for storing secure data in clouds that supports unidentified authentication. The validity of the user who stores the data is also verified. The proposed is that an attack is replayed by resilient. The Secure Hash algorithm for authentication purpose, SHA is one of the best cryptographic hash functions, used to verify that a file has been unmodified. The Blowfish and Pailier crypto system is a probabilistic asymmetric algorithm for public key cryptography.

Blowfish algorithm is used to encrypt the data that are stored in cloud. The Pailier algorithm used for access policy creation then accessing and restoring the file process.

[6]Prof. Dipa Dharmadhikari, Sonali Deshpande conducted study on the Key policy-Attribute Based Encryption (KP-ABE) in the cloud storage. Sharing the data is the important process in the cloud storage. The proposed provide to maintain integrity, confidentiality and availability while sharing of data. ABE (Attribute Based Encryption) cryptosystem which generate both encryption and decryption with time along with size. Work of proposal is explaining the encryption with ABE then file is split into chunk. Hash key is

generated for every data chunk which must be unique. SHA (Secure Hash Algorithm) is used for hash key generation. For decrypting the data file is searched on cloud with private key then it is decrypted. SHA is applied with ABE. The author made analysis on encryption and decryption of that time calculation with both IBE and ABE according to the file size. Creation of hash key for every chunk must be unique. It is asymmetric key approach. Key set is used for the both encryption and decryption process. Through cloud space data is stored and is available for the everyone.

IV. PROPOSED SYSTEM

1. A Modified-Hierarchical Attribute Based Encryption (M-HABE) and the propose the three attribute structure. It differing from the existing paradigms such as the HABE algorithm and the original three-layer structure, the novel pattern mainly focuses on the processing, storing and accessing of data, it is designed for the application users with legal access authorities to get relevant data and to restrict unauthorized users to get data access, the proposed promising paradigm makes it extremely suitable for the cloud computing based paradigm. Each user Using unique key for their encryption and decryption algorithm.
2. Modified Hierarchical Attribute based encryption user's identity is used as attribute after user uploaded the data and server encrypting that data using (M-HABE) algorithm.
3. Encryption is the process of transferring the plain text data (plaintext) into something that appears to be random and meaningless (cipher text).
4. Decryption is the process of converting cipher text back to plain text. To encrypt more than a small amount of data, attribute encryption is used.
5. A attribute key is used in the process during both the encryption and decryption technique for providing the security. To decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used. Attribute key is used for the authentication.
6. The access control policy is expressed by the disjunctive normal form (DNF. There are five roles in this technique: the cloud storage service, data owner, the root authority, the domain authority, and data users. The Data owner (sender) is responsible for before sharing it with others it will encrypt the original data.
7. The authority of root generates system parameters and domain keys to distribute them. The domain authority regulates the domain authority at the level of internet and all users in its domain, to delegate keys for them. It can distribute secrete keys for the users. User use their secrete key to decrypt the encrypted data and then obtaining the message. The key generation is done on hierarchically.
8. At the first level, root authority generates a root master key for authority of the domain. The system public key and the master key of the authority of the domain

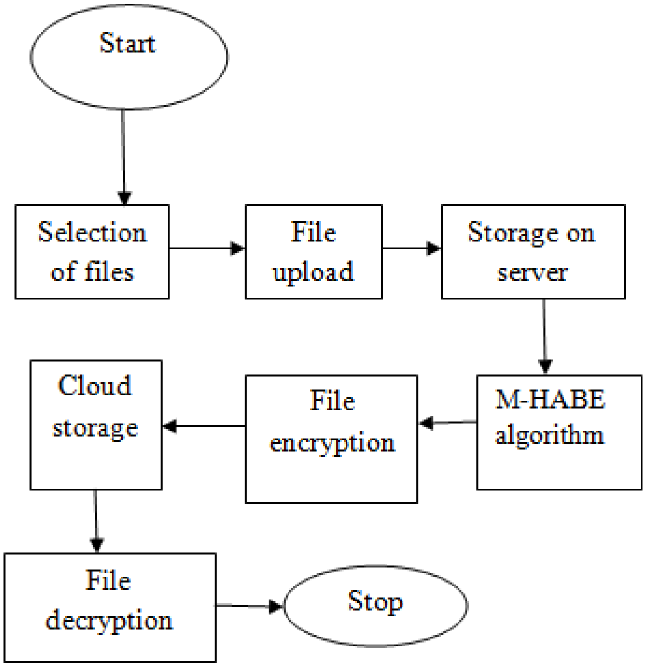

Fig -1Modified-Hierarchical Attribute Based Encryption (M-HABE) architecture

Benefits of M-HABE

- Data confidentiality.
- Asymmetric based encryption and decryption.
- Privacy with high efficiency.
- ABE can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.
- It provides a fine-grained access control.

V. CONCLUSION

AnM-HABE scheme by taking advantages of attributes based encryption (ABE) and hierarchical identity-based encryption (HIBE) access control processing. The proposed access control method using modified HABE is designed to be utilized within a hierarchical multiuser data-shared environment, which is extremely suitable for a cloud computing model to protect the data privacy and defend unauthorized access. Compared with the original HABE scheme, the novel scheme can be more adaptive to cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data and files. The scheme not only accomplishes the hierarchical access control of sensing data in the cloud computing model but protects the data from being obtained by an untrusted third party.

REFERENCES

[1]. Rupali sharma Research scholar, DR.Bharti joshi,"H-IBE: Hybrid-Identity based Encryption approach for cloud security with outsourced Revocation", International conference on Scopes-2016.

[2]. Zhiguo wan, jun'e liu and Robert h. deng: "Hierarchical Attribute-based solution for access control in cloud computing",IEEE transactions on information forensics and security, Vol-7, No-2, April 2012.

[3]. Minu Geroge, Dr. C. Suresh Gnanadhas, and Saranya .k: "A survey on Attribute Based Encryption scheme in cloud computing", International Journal of advanced research in computer and communication engineering Vol. 2, issue 11, November 2013.

[4]. Jia Yu, Kui Ren, Fellow and Cong Wang: "Enabling cloud storage auditing with verifiable outsourcing of key-update", IEEE Transaction of information forensics and security Vol.11, No.6, June 2016.

[5]. Vetripriya and Anand: "Implementation of Attribute-based encryption with privacy preserving in cloud application", International journal of emerging technology in computer science & Electronics, Vol-21, April 2016.

[6]. Dipa Dharmadhikari and Sonali Deshpande: "Key policy Attribute base encryption in cloud storage", IOSR Journal of Computer Engineering (IOSR-JCE), Vol-18, Sept-Oct 2016.