A Review Report On Searchable Attribute Based Mechanism for Efficient Data Sharing for Secure Cloud Storage

Prachi U.Bhatkar, Gunjan SAkhare, Trupti B.Radke, Monali P. Chandankhede

Student, Information Technology, SIPNA’S COET Amravati, prachibhatkar@gmail.com
Student, Information Technology, SIPNA’S COET Amravati, gunjan130595@gmail.com
Student, Information Technology, SIPNA’S COET Amravati, truptiradke99@gmail.com
Student, Information Technology, SIPNA’S COET Amravati, monalichandankhede22@rediffmail.com

ABSTRACT

Encryption is used to securely transmit data in open networks. Each type of data has its own futures; therefore different techniques should be used to protect confidential data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data but they are not as much as protective and easily crack their security key by hackers. In this technique we use the algorithm which provides searchable attribute based data encryption technique for secure cloud storage with the help of keyword update technique. It is a new attribute based searchable encryption approach, by which we develop cloud based searching and data sharing application for corporate companies etc.

Keywords: Searchable attribute-based encryption, keyword update, encrypted data sharing.

INTRODUCTION

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet [1]. Data encryption is widely used to ensure security however, most of the available encryption algorithms are used for encrypting data.

We will use Attribute-Based Encryption (ABE) with a significant reason that it provides fine-grained expressiveness in data share and search. After storing data to a cloud server, cloud server delivers the services rather than a product, whereby shared resources, software and information provided to devices as a metered service over a network. The data owner usually needs two necessary operations: one is data searching and the other is data sharing. The services which provided by the cloud server are broadly divided into three categories software-as-a-service, platform-as-a-service, infrastructure-as-a-service.

Another interesting behaviour is the keyword update or shared encrypted data which is not supported by traditional method like KABE, CABE. By using this approach we protect the privacy of search including data and keyword.
ATTRIBUTE BASED ENCRYPTION

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a large amount of data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection. In attribute based searchable encryption, attributes and searchable keywords of the documents will be stored in separate XML files to increase security as well as to prevent key escrow and cipher text enlargement problem. The attributes and searchable keywords of every document will be stored in encrypted format using AES (Advanced Encryption Standards) then the XML files will be stored on cloud server along with original documents.

“Attribute based encryption” is a type of public key encryption in which secrect key of user and the cipher text are dependent on attribute example The country he lives or the kind of subscription in such system the decryption of cipher text is possible only if the set of attribute of user key matches the attribute of the cipher text. A crucial security aspect of attribute-based encryption is collusion-resistance: an adversary that holds multiple key should only be able to access data if at least one individual key grants access.

Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients attribute. This primate can also be used for broadcast encryption in order to decrease the number of keys used. Although ABE concept is very powerful and promising mechanism.

ATTRIBUTE-BASED KEYWORD SEARCH

To hide search contents as well as search keywords from cloud server, Boneh et al. [6] introduced the notion of Public Key Encryption (PKE) with keyword search, in which a user delivers a special Gaps Between ABE Keyword Search and Data Share. Usually, an ABKS supporting keyword search does not simultaneously provide decryption service, such as [38]. This is due to a technical limitation in the construction method of trapdoor token (used for searching). Specifically, a trapdoor token consists of a user's "re-randomized" secret key. By using this information, the token holder (i.e. a cloud server) can easily recover the data from a ciphertext encrypted under the decryption policy matching the key. Although the server may use the re-randomized secret key to fulfill data sharing
WORKING DIAGRAM

WORKFLOW
### Work Flow

**Tenant creation**
- Registration
- Approval by cloud
- Branch creation
- Employee login creation

**Uploads**
- Upload documents
- Storage in encrypted format
- Upload searchable keywords in xml documents
- Specify attributes for access permission in XML

**Searching and Download**
- Specify keyword
- Search data as per the attributes and keywords mentioned in xml files
- SEO wise re-ranking
- Result delivery
- Get key on email
- Download document using correct key

### TECHNOLOGIES REQUIRED

**Deployment Platform**: Windows

**Application Server**: Apache Tomcat/GlassFish

**Technology**: JavaEE

**Development Tools (Serverside)**: Servlets & JSP, Java Beans

**MVC framework**: Struts

**Database technologies**: MySQL, JDBC

**Web Development**: XML, HTML, DHTML, Javascript, AJAX

**Development Tool**: NetBeans IDE
CONCLUSION

We defined a new notion searchable attribute-based proxy re-encryption with keyword update, and proposed a concrete construction satisfying the notion. We also proved the new scheme CCA secure in the ROM. The scheme is the first of its type to integrate searchable attribute-based encryption with attribute-based proxy re-encryption, which is applicable to many real-world applications. Although the new system enjoys its valuable advantages, it motivates some interesting open problems, e.g., how to reduce the size of search token, how to allow a secret key holder to generate search token individually and how to provide more expressive keyword search.

ACKNOWLEDGEMENT

We are very much grateful to department of Information Technology. SIPNA’S college of Engineering Amravati to give us opportunity to work on Searchable Attribute Based Mechanism for Efficient Data Sharing For Secure Cloud Storage. We sincerely express their gratitude to director SIPNA’S college of Engineering Amravati, head of the dept. Information Technology, SIPNA’S college of Engineering Amravati, for giving constant inspiration to carry out research work.

REFERENCES:


