An Efficient Attribute Encryption for Secure Data Sharing and Storage in Public and Private Clouds-A Survey

Jayasudha. M, Subbulakshmi T

ABSTRACT--- ***Cloud computing, a type of computing paradigm that highly depends on shared data resources rather than local data resources which allow the devices to handle the applications. With the rapid development of cloud data services, the data in cloud was stored and shared across numerous users. Since the shared data can be accessed and modified by multiple users, this new paradigm poses huge challenges in keeping the integrity of the shared data. Several studies about the secure data retrieval focuses heavily on providing strict security for the data stored in the third party domain. However, strict security on third party domain will requires stupendous cost and security issues on cloud service provider which inevitably affects the efficient data retrieval in clouds. In this paper, we propose an effective scheme that supports the efficient retrieval of data stored in clouds. This paper is a survey of specific issues brought by the use of attributes based encryption system in a cloud computing system.***

Index Terms —Cloud Computing, Data Storage, Data Sharing, Attribute-based Encryption

I. INTRODUCTION

Cloud computing is a promising and emerging computing paradigm in which resources are provided as services and enables users to remotely store their data in a cloud. Since this new computing technology requires users to entrust their important data to cloud providers, there have been growing security and privacy concerns on outsourced data. The idea of cloud computing is based on a very major principal of reusability of IT capabilities. The variation that cloud computing brings compared to traditional computing concepts is to broaden horizons across organizational boundaries. The component of cloud computing includes on-demand self-service, broad network access, resource pooling, rapid elasticity and consistent service. On-demand self-service means that patrons can request and manage their own computing resources. Broad network access allows services to be provided over the Internet or private networks. Pooled resources means that patrons draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and patrons are billed accordingly.

Each provider delivers a unique function, giving users higher or lesser control over their cloud depending on the type. While choosing a provider, our need has to be compared with the available cloud services. Cloud needs will vary depending on how we intend to use the space and resources associated with the cloud. There are three types of cloud providers: Software as a Service and Platform as a Service and Infrastructure as a Service. These three types vary in the amount of control that we have over the information, and conversely, how much we can expect the provider to do for us. Software as a Service (SaaS) provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for us to have a physical copy of software to install on our devices. SaaS also generates it easier to have the same software on all of our devices by accessing it on the cloud. In a SaaS agreement, we have the least control over the cloud. Platform as a Service (PaaS) system goes a level above the Software as a service setup. A PaaS provider entry the subscribers to access the components that they require to develop and operate applications over the internet. Infrastructure as a Service (IaaS) agreement deals primarily with computational infrastructure. In an IaaS agreement, the subscriber totally outsources the storage and resources, such as hardware and software that they need. The cloud provider has lesser control in an IaaS system than with a SaaSagreement.

The information hold on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of intimate information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it crucial for us to understand the security measures that your cloud provider has in place, and it is equally critical to take personal precautions to secure your data. The first thing we must look into is the security measures that cloud provider already has in place. These vary from provider to provider and among the various types of clouds. A small business user may have slightly more room to discuss the terms of their contract with the provider and will be able to raise these questions during that time. There are many questions that we can raise, but it is significant to choose a cloud provider that considers the security of our data as a majorconcern.

Deploying cloud computing can vary depending on requirements, and the following four deployment models have been classified, each with unique characteristics that support the needs of the services and users of the clouds in peculiar ways. Private Cloud: The cloud infrastructure was deployed, maintained and operated for a specific organization. The action may be in-house or with a third party on the location; Community Cloud: The cloud infrastructure is shared among a number of organizations

Revised Manuscript Received on May 15, 2019.

Jayasudha M, School of Computing Science and Engineering, VIT University, Chennai, T.N, India.

DrSubbulakshmi T, School of Computing Science and Engineering, VIT University, Chennai, T.N, India.

with similar importance and requirements. This may help reducing the capital expenditure costs for its formulation as the costs are shared among the organizations. The action may be in-house or with a third party on the location; Public Cloud: The cloud infrastructure is available to the public on a monetary basis by a cloud service provider. This empower a consumer to develop and deploy a service in the cloud with very little financial investment compared to the capital expenditure requirements normally linked with other deployment options; Hybrid Cloud: The cloud infrastructure consists number of clouds of any type, but the clouds have the scope through their interfaces to allow data and/or applications to be lifted from one cloud to another. This can be a combo of private and public clouds that support the requirement to preserve some data in an organization, and also the need to offer services in the cloud.

There are some noticeable challenges associated with cloud computing, and some of these may cause a delay when delivering additional services in the cloud, most also can bring opportunities, if resolved with due responsibility and attention in the planning stages. The challenges faced in cloud computing are security and privacy, lack of standards, continuously evolving and compliance concerns. For service developers, making services accessible in the cloud dependsonthetypeofserviceandthedevicesbeing used to access it. The process may be as simple as a user clicking on the required website, or could associate an application using an API accessing the services in the cloud. Cloud-based communications services enable businesses to enclose communications capabilities into business applications, such as in Enterprise Resource Planning and in Customer Relationship Management systems. For travelling business people, these can be achieved through a smartphone, supporting expanded productivity while moving away from the office. These services are over and above the support of service deployments of VoIP systems, combination systems, and conferencing systems. They can be accessed from any premises and linked into current services to extend their capabilities. In terms of social networking, using cloud-based communications provides click-to-call capacities from social networking sites, access to messaging and video communication systems, improving the interlinking of people within the socialcircle.

In this paper, we first reviewed the existing schemes using attribute based encryption in cloud computing. Guiyi and Jun [5] proposed an efficient data sharing protocol for the outsourcing of data in cloud and Guojun and Minyi [6] proposed a hierarchical attribute based encryption scheme for achieving fine grained access control and high performance. The existing scheme has two major drawbacks. First, these schemes bring additional decryption and encryption burden to the data owner. The data owner who is required to be online all the time for the secure transfer and retrieval of data's in cloud. Second, if a third party is allowed to fulfill data search task, this requires the party to be fully trusted by providing the secret key of the data owner. The leakoftheinformationdisgracestheprivacyofthe data owner and this approach is undesirable due to loss of privacy and confidentiality.

The remainder of this paper is organized as follows: Section 2 discussed related works; Section 3 introduces the system model, security model and our design goal; Section 4 provides the details of our proposed scheme; finally Section 5 provides the concluding remarks of the paper

II. RELATED WORK

In this section, we review the concepts of attribute based encryption and provide an abrupt overview of various schemes adopted by existing controls.

A. Attribute Based Encryption

In order to improve the compliance of users to share their data in cloud, Sahai and Waters [1] introduced the concept of Attributed-Based Encryption (ABE) in which the user's keys and ciphertexts are defined with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a connection between the attributes of the ciphertext and the user's key. The cryptosystem of sahai and waters permits for decryption when at least k attributes overlapped between a ciphertext and a private key. Goyal [2] proposed a fine grained ABE scheme and defined two complimentary notations: Key Policy ABE and Ciphertext Policy ABE. ABE defines the identity as a set of attributes (key-policy ABE - KP-ABE) or policies defined over a group of attributes (Ciphertext-policy ABE - CP-ABE). The main issue is that decryption of ciphertext is possible only if the person holds a key for matching attributes where user keys are always issued by some trusted party. Bethencourt [3] introduced Ciphertext Policy ABE scheme in which the user's private-key is associated with a set of attributes and a ciphertext determines an access policy over a defined universe of attributes within the system. A user will able to decrypt a ciphertext, if and only if his attributes satisfies the policy of the respective ciphertext. Various schemes proposed by researchers in [11 & 17] use CP-ABE with identity-based encryption (IBE) for achieving constant computational cost and constant size cipher texts. In this scheme, there are four algorithms to be executed: Setup, KeyGen, Encrypt and Decrypt.

B. Proxy Re-Encryption

Proxy re-encryption, introduced by Blaze [4] allows a proxy to transfer an encrypted message under A's public key into one more encrypted message under B's public key without viewing the message in plaintext. The proxy does not need the private key of A to encrypt the message and encrypt it under B's public key again. Yangiang and Jian [9] formed the idea of conditional proxy re-encryption (CPRE) which enables fine grained encryption of cloud data through user revocation. Bharath and Sanjay [8] introduced an efficient and secure data distributed framework using homomorphic encryption and proxy re-encryption schemes that prohibit the leakage of unauthorized data when a revoked user joins the system.

III. PROBLEM STATEMENT

A. SystemModel

In the system model as shown in Fig. 1, we assume the cloud computing system

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

mainly composed on following parties: The data owner; whom stored the data in the cloud and depends on the cloud for data maintenance. The authorized user; who accesses the data shared by the data owner, downloads the data and decrypts it using his secret keys. The cloud provider (CP) provides a high quality service using a number of servers with considerable storagespace.

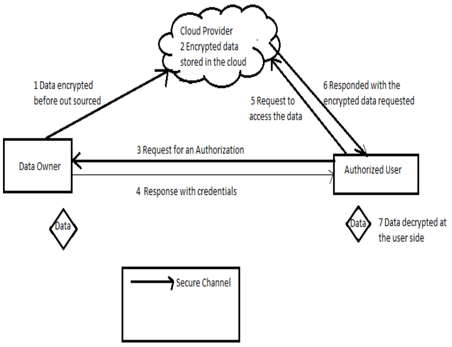

Cloud Provider
2 Encrypted data stored in the cloud
1 Data encrypted before out sourced
5 Request to access the data
6 Responded with the encrypted data requested
3 Request for an Authorization
4 Response with credentials
Data Owner
Authorized User
Data
Data
7 Data decrypted at the user side
Secure Channel

Figure 1: System Model

B. Security Model

In the security model, we assume that the cloud provider is untrusted in the manner that it may collude with malignant users to harvest file contents stored in the cloud for its own interest. There are two main attacks under such a circumstance; one is external attacks initiated by unlawful outsiders, and internal attacks initiated by an honest but curious CP as well as malignant end users. The malignant end user needs to access the data that he is ineligible to decrypt. We assume that the CP will not collude with the end users, since the CP is considered to be honest butcurious.

C. Design Goals

The main design goal of our system is to provide a security model with a secure and private policy for data sharing in cloud computing. Especially we want to enable the data owner to share his/her data with the designated authorized sharers such as the shared files, transformed files and re-encryptionkeys.

IV. PROPOSED MODEL

In proposed show, trait based encryption plot coordinates with a safe decentralized code to frame a safe shared capacity framework. The encryption conspires bolster encoding tasks over scrambled messages and advances the activities over encoded and encoded messages. The solid reconciliation of encoding, encryption, and sending makes the capacity framework advantageously meet the prerequisites of information quality, information privacy and information sending. Achieving the osmosis with thought of a mutual structure is testing. In this plan, a novel ABE System is suggested that bolsters catchphrase private inquiry and encoded information sharing together. We pick an ABE framework with quick decoding as a beginning stage. The reason of utilizing ABE is that ABE can give high enunciation to information offer and watchword look contrasted and other encryption frameworks. To accomplish the protection of catchphrase seek, concrete ABE framework was stretched out into uneven pairings. A token identified with a watchword to be developed through collaboration between Private Key Generator and a framework client. The development of the token is like that of the mystery key of the client and the token won't empower its holder to decode the figure content related with same catchphrase. This is vital necessity for accessible encryption. The proposed plan coordinates four randomized calculations: begins with System introduction, at that point continue with Encryption and Key age, Decryption to accomplish secure information partaking in cloud.

Cryptography is becoming famous day by day because it is the art and science of securing the data as well as a message, which will be stored in a database or may transferring the secret message or data in the secure form. Sender and receiver are two ends of using the data but the line in which they are communicating must be secured So, in this place, cryptography come into the picture. In cryptography, CIA(Confidentiality, Integrity, and Authentication) is the main pillar. Through which the message can be confidential and access by the authorized person only.

Encryption is basically the set of the process which makes the text or message in a secret form. The process of encryption is applied for transforming the plain text into cipher text. It is the portion of cryptography that is why it is considered as the subset of cryptography. The conversion of plain text into some other form that is created or takes some random value which is meaningless and unintelligible.

It can also be said that encryption is the process of transforming plaintext (Which is human readable and meaningful form) into the cipher text (this is a random character and not meaningful text) where plaintext is the input to the encryption process and the ciphertext is the output of the encryption process.

The proposed algorithm is based on the highest prime factor of the ASCII Value of the character. The process of encryption is defined in the following steps: -

- ➢ Plain text is provided to the encryption part of the algorithm.
- ➢ Then the plain text is converted to the corresponding ASCII Value.
- ➢ Prime factor process is run on the ASCII Value and the prime factors are temporarily stored into a temporary variable.
- ➢ After each ASCII prime factor process, the prime factor is compared with the temporary prime factor and the highest prime factor for that particular ASCII Value is stored.
- ➢ Then the ASCII value and the highest prime factor is retrieved from the temporary storage.
- ➢ The ASCII Value is divided by the highest prime factor and the quotient is stored in an array.
- ➢ Then the quotient is added with a numeric value (random value).
- ➢ After adding random value add the position of that character.
- ➢ The result is the final key which is stored.
- ➢ The ciphertext is the corresponding text of the ASCII Value of the final key.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

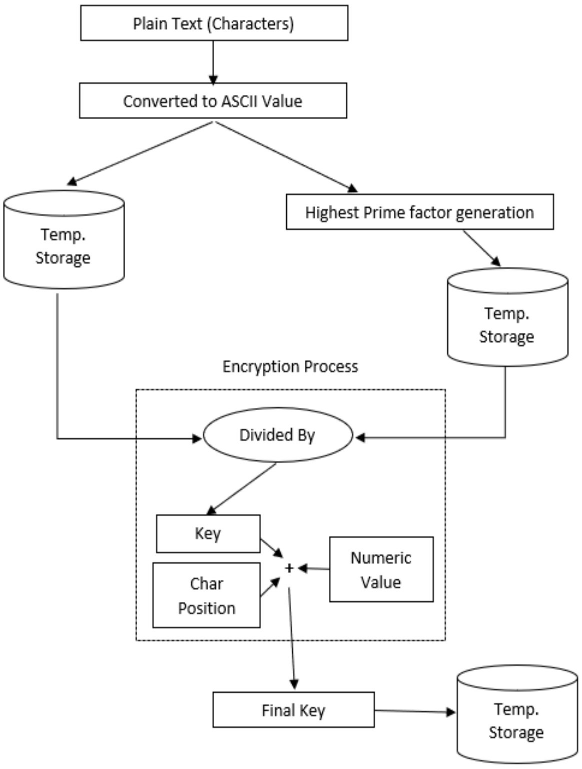


Figure 2:Proposed Encryption Architecture

One part of the algorithm is completed and the plain text is now converted to the ciphertext. The ciphertext and the final key is sent to the receiver. Using the final key receiver can decrypt the ciphertext to the plain text.

Following are the steps involved in the decryption process: -

- ➢ Now the receiver side contains the final key and ciphertext.
- ➢ The numeric value which was added in the encryption process is now subtracted in the decryption process.
- ➢ Numeric value and Position of that character is subtracted from the final key value and is stored to a temp variable.
- ➢ Then the final key is multiplied with the highest prime factor.
- ➢ The value is the ASCII Value of the character.
- ➢ And ASCII Value is converted back to the character (plain text).

Now after the decryption process, the receiver gets the plain text which the user sends along with the final key.

V. RESULTS AND DISCUSSION

The algorithm is implemented in C++ language. Following is the pseudocode: -

```
1.    string s; // Take the input (String)
2.    arr [] =s; //Store the string in a temporary array.

for(i=0;i<n;i++)  //Encryption Process
{
      temp=ch[i];
      arr1[i]=temp; //ASCII Code of Character
      for(k=2;k<=temp;k++)  //Prime Factors of the ASCII Code
      {
            if(temp%k==0)
            {
            flag=1;
            for(j=2;j<=k/2;j++)
            {
                  if(k%j==0)
                  {
                        flag=0;
                        break;
                  }
            }
          if(flag==1)
          {
                  if(k>temp1)
                  {
                        temp1=k;
                  }
            }
        }
      }
      arr[i]=temp1; //Storing highest prime factor in
      Another array
      temp1=0;
}
```

3. Repeat step 3 until all the prime factors for all the characters are found.

```
for(i=0;i<n;i++)  //Generating of final key
{
      arr1[i]=arr1[i]/arr[i];
      arr1[i]=arr1[i] + key + pos_char;
      ch[i]=arr1[i];
}
```

4. Repeat step 5 until final key for all characters are received.

```
for(i=0;i<n;i++)  ///Decryption Part
{
      int t= arr1[i] – key – pos_char;
      arr1[i]=t*arr[i];
      ch[i]=arr1[i];
}
```

Here, pos_char is position of character in file. It is use to assign unique value for each character, weather it is same character or different. Key is any random value which can be taken as fixed random value for both encryption and decryption.

Let, discuss the performance of the algorithm.

File Size (in characters length)	Compilation Time (in sec)	Exited time (in sec)
41	0.50	0.03398
750	0.50	0.04387
1801	0.50	0.07838
70239	0.64	0.335
210717	0.66	0.6296

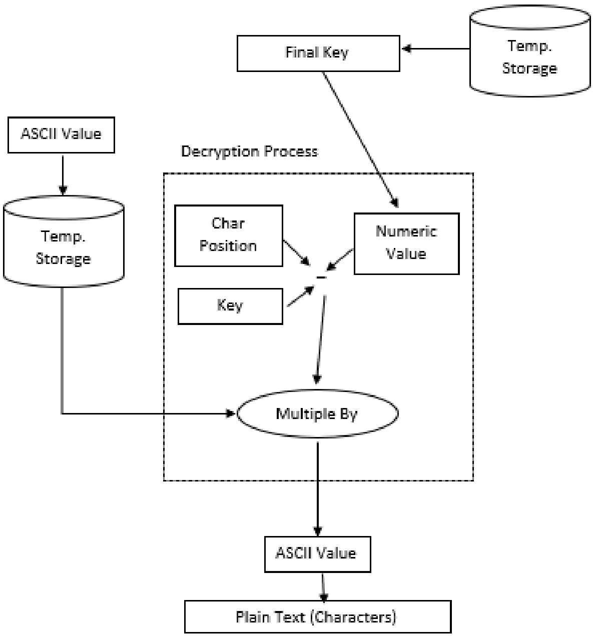
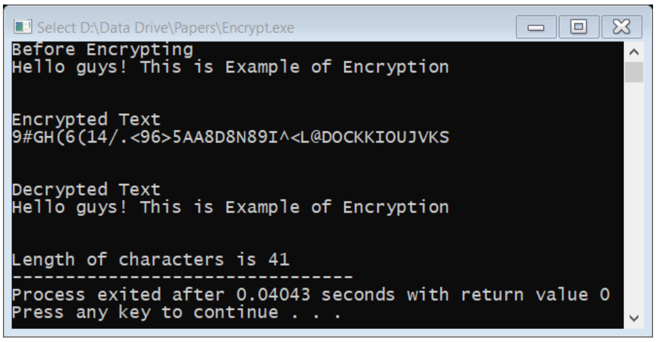


Figure 3: Proposed Decryption Architecture



```
Before Encrypting
Hello guys! This is Example of Encryption

Encrypted Text
9#GH(6(14/.<96>5AA8D8N89I^<L@DOCKKIOUJVKS

Decrypted Text
Hello guys! This is Example of Encryption

Length of characters is 41
--------------------------------
Process exited after 0.04043 seconds with return value 0
Press any key to continue . . .
```

Figure 4: Output

Above, the table is showing the execution speed of the proposed algorithm with compilation time and Exited time. Compilation time is the time taken for checking the index as well as assigning memory to a program and Exited time is the time for calculating encrypting as well as decryption time both.

VI. CONCLUSION

Due to cost efficiency and less hands on management, data owners are very much interested in outsourcing their data in cloud which can access to data as a service. In this paper, we reviewed the schemes and methodologies using attribute based encryption in cloud computing and a novel proposed Attribute based Encryption system for executing data sharing and retrieval simultaneously in cloud. Further work includes the evaluation of our proposal for effective data sharing and retrieval in private and publicclouds.

REFERENCES

1. Sahai A, Waters B. 2005, ”Fuzzy identity-based encryption”. In: Proceedings of EUROCRYPT. LNCS Vol. 3494; p. 457-73.
2. Goyal V, Pandey O, Sahai A, Waters B.,2006, “Attribute-Based encryption for fine-grained access control of encrypted data.” In: Proceedings of CCSp. 89-98.
3. Bethencourt J, Sahai A, Waters B., “Ciphertext- policy attribute-based encryption.” In: Proceedings of ISSP; p. 321-34.
4. 4.Matt Blaze, GerittBieumer, Martin Strauss, 1998,“Divertible protocols and atomic proxy cryptography,”In:Kaisa Nyberg(Ed.), EUROCRYPT, In: Lect. Notes Comput. Sci., vol.1403, Springer, pp. 127-144.
5. 5.Guiyi W, Rongxing L, Jun S. EFADS:,2014, “Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re- encryption.” In: Journal of Computer and System Sciences 80 (2014); p: 1549-1562.
6. 6.Guojun W, Qin L, Jie W, Minyi G.,2011, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers.” In: Computers & Security 30 (2011); p. 320-331.
7. 7.AwsNaser J, MohamadFadli Bin Z.,2013,” Use of Cryptography in Cloud Computing.” In: IEEE International Conference on Control System, Computing and Engineering, 29 Nov – 1 Dec 2013,
8. Penang, Malaysia
9. 8.Bharath K S, Yousef E, Gerry H, Sanjay M.,2015, “A secure data sharing and query processing framework via federation of cloud computing.” In: Information Systems 48(2015); p.196-212.
10. 9.Yanjiang Y, Haiyan Z, Haibing L, Jian W, Youcheng Z.” Cloud based data sharing with fine- grained proxy re-encryption.” In: ELSEVIER Pervasive and Mobile Computing.
11. 10.VijendraRajendra A, Prabhaker L R. ,2014,”Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques.” In: International Journal of Application or Innovation in Engineering & Management (IJAIEM); Volume 3, Issue 3, March 2014.
12. 11.Xin D, Jiadi Y, Yuan L, Yingying C, Guangtao X.,2014,” Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing.” In: ELSEVIER Computers & Security 42(2014); p.151-164.
13. 12.Yuan Zhang et al,2015,”Cryptanalysis of an integrity checking scheme for cloud data sharing”In:ELSEVIER journal of Information security and applications;p.1-6.
14. 13.Boyang Wang ,Baochun Li , Hui Li , 2015,”Panda: Public Auditing for shared data with efficient user revocation in the cloud”,In:IEEE Transactions on services Computing;p.92-105
15. 14.Boyang Wang , Baochun Li , Hui Li , 2015,”Oruta:Privacy –Preserving Public Auditing for shared Data in the cloud”, In: IEEE Transaction on cloud computing;p.43-56.
16. 15.FU Jing-yi, HUANG Qin-long, MA Zhao-feng, YANG Yi-xian,2014,”Secure personal data sharing in cloud computing using attribute –based broadcast encryption”, In: The journal of china universities of Posts and Telecommunications;p.44-77.
17. 16.D.Thilakanathan , Shiping Chen, Surya Nepal and Rafael A. Calvo,2012,”Secure Data sharing in the cloud”, In: IEEE Conferences on Cloud Computing;p.1-29.