Securing Sensitive Data in Public Cloud by Using Attribute Based Encryption and Digital Watermarking

[1]Vishnu S,[2]Mrs. Krishnaveni S.
[1]Student, [2]Assistant Professor
SRM University, Kattankulathur,Chennai, India

Abstract **- The secure transaction of sensitive data stored on semi trusted servers like public cloud and focus on addressing the complicated and challenging key management issues. To protect sensitive data stored on a public server, system uses attribute based encryption (ABE) as the main encryption technique. Using ABE, access policies are expressed based on the attributes of data, which enables users to share sensitive data by encrypting the file under a set of attributes without the need to know a complete list of user group. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. To improve the performance the attribute selection is based on ranking algorithms. The digital water marking technique provide data authentication so that the men in middle attack and other data hijacking techniques fails in our proposed system.**

IndexTerms**–Attribute based encryption,Digital watermarking,Cloud computing, Data security.**

I. INTRODUCTION

Now a day's security become the primary constrain for the digital world. The emergence of cloud computing opens a wide range of possibilities for the world to handle data. In cloud mainly three deployment models are used , public cloud, private cloud and hybrid cloud. Cloud computing is a model for delivering information technology services whichuses pol of information retrieved from the internet through web rather than a directconnection to a server. There are some security issues associatedwith cloud computing but these issues fall into two broadcategories: Security issues faced by cloud providers andsecurity issues faced by customers [3]. In most cases, theproviders must ensure that their infrastructure is secureand that their clients' data and applications are protectedwhile the customer must ensure that the provider hastaken the proper security measures to protect their information [4].
There are mainly 14 security domains in cloud security according to CSA cloud security guideline v.3.0. Our system focus on the Information management and data security (domain 5). Our system focus on the storing sensitive data in the cloud and check the authoritiesthatuse the data. We use a combined mechanism of attribute based encryption and digital watermarking for this.

II. EXISTING SYSTEM

In the existing system the Cipher-Text attribute based encryption (CP-ABE) is used which is a variation of attribute based encryption scheme. The data owner is uploading the data to the cloud server after encrypting the data according to the access control policy [5] defined with the set of attributes. This encrypted data can be decrypted by the user only if the attributes of that user satisfies the access control policyIn proposed system two trusted authority system is used for the attribute issue purpose, the trusted authority (TA1) for the professional domain and the Trusted Authority (TA2) for the social domain, but the patient can act as this second authority. The reputation of the user is here used for generating the secret key for the users of the social domain [5].

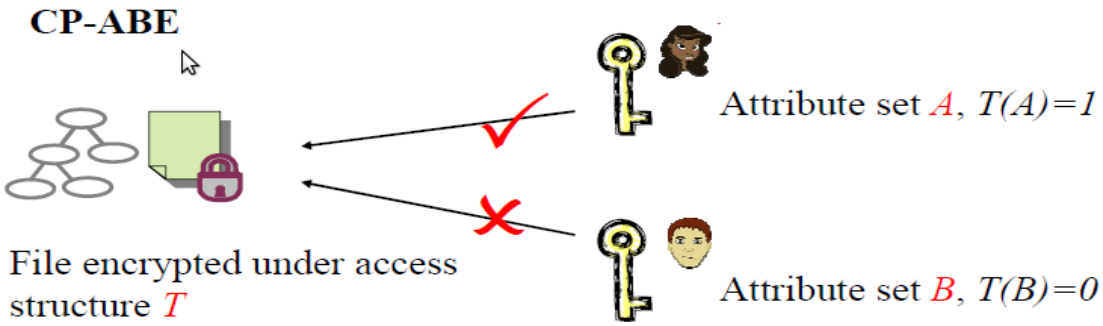


Figure 1: CP-ABE schema

The working principle and algorithm for the existing system is given as follows:

- At first the key-generation algorithm will run by the both the trusted authority by using CP-ABE scheme.
- The professional domain users will obtain their secret keys according to their attributes defined in the system.
- The patient will create the measurement data by the help of devices and tools and which will send to the application hosting devices like personal computer or mobile phones.

- The hosting device will encrypt this data after the categorization according to an access policy P.
- The encrypted data will send to the web PHR repository.
- When the user wants to see this data, they can download the encrypted data from the server and can decrypt them locally by using the secret key.
- When a request get by the patient for the data access grant permission the patient will make a decision by checking the requester's reputation score generated by the reputation engine.
- The data owner will generate the secret key for that requester according to his reputation ranking only.

The CP-ABE scheme consists of four algorithms. The following are the four algorithms [6], [7]:

- **Setup Algorithm (MK, PK)**: This algorithm run by the trusted authority and it will take input a security parameter k, and output a master secret key MK and a master public key PK.
- **Key Generation algorithm (SK)**: It also run by the trusted authority and takes input a set of attributes and MK. It has the output a user secret key SK associated with the attribute set.
- **Encryption algorithm (CT)**: It is run by the encryption engine of the system. It has the input a message m, a master public key PK, and an access control policy p, the output of the algorithm is a cipher text CT, under the access policy P.
- **Decryption algorithm (m)**: It is run by the decryption engine. The input for the algorithm is the cipher text CT to be decrypted and the user secret key SK. The output of the algorithm is the message m, if and only if the secret key of the user satisfies the access policy P, under which the message was encrypted. It shows an error message if the secret key doesn't satisfy the access policy P, under which the message was encrypted.

III. PROPOSED SYSTEM

In our proposed system we divide the user group into two category, one is public domain(PUD) and other is private domain (PSD).There are multiple SDs, multiple data owners, multiple AAs, and multiple data users. In addition, two ABEsystems areinvolved: for each PSD the YWRL's revocableKP-ABE scheme [7] is adopted; for each PUD, revocable MA-ABE is

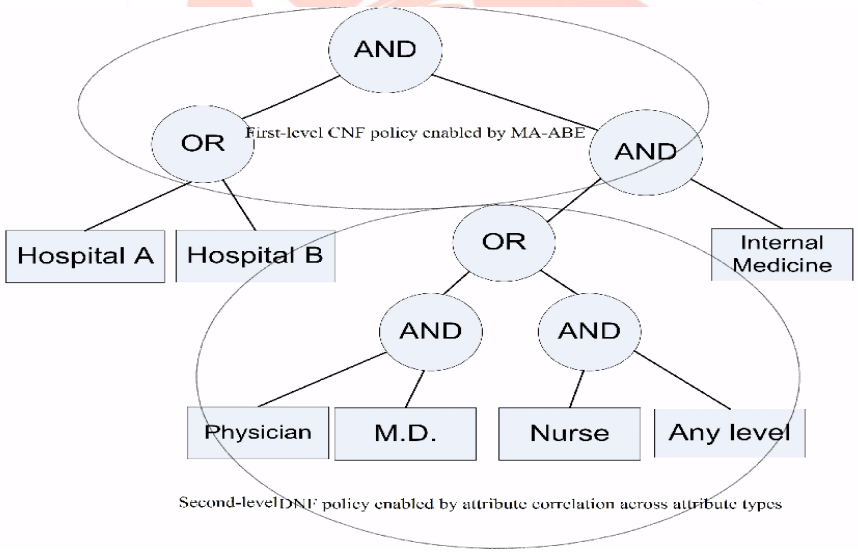
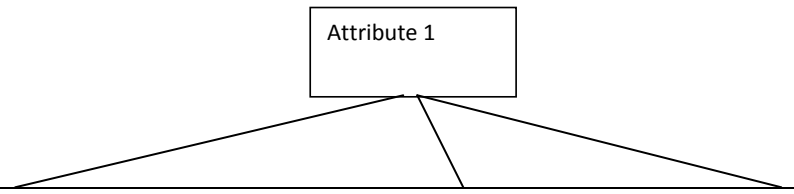


Figure 2: An example policy realizable under our framework using MAABE,following the enhanced key generation and encryption rules [1].

used.We term the usershaving read and write access as data readers andcontributors, respectively.System setup and key distribution. System willdefines a common universe of data attributes shared byevery PSD. An emergency attribute isalso defined for break-glass access. Everydata owner's clientapplication generates its corresponding public/master keys.Thereare two ways for distributing secret keys. First, when firstusing the data service, a data owner can specify the accessprivilege of a data reader in PSD, and let applicationgenerate and distribute corresponding key to the latter, in away resembling invitations in GoogleDocs. Second, a readerin PSD could obtain the secret key by sending a request(indicating which types of files she wants to access) to the data owner, and the owner will grant a subsetof requested data types. The policy engine ofthe application automatically derives an access structure,and runs keygenerator of KP-ABE to generate the user secret keythat embeds access structure based on this. In addition, the dataattributes can be organized in a hierarchical manner forefficient policy generation, see Figure 3.



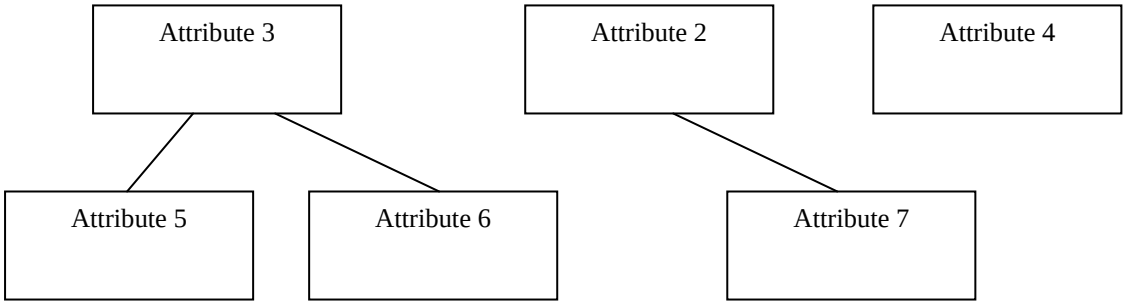


Figure 3: Attribute hierarchy

When the user isgranted all the file types under a category, accessprivilege will be represented by that category instead. System defines role attributes for the PDU, and areader in a PUD obtains secret key from AAs, which bindsthe user to claimed attributes/roles. Inpractice, there exist multiple AAs each governing a differentsubset of role attributes.

Data encryption and access.

The owners upload ABEencrypted data files to the server. Each owner's data file is encrypted both under a certain fine-grained and role based access policy for users from the public domain to access. Selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the data files, excluding the server.

User revocation.

Here, consider revocation of a data reader access privileges. The possible cases are:

1. Revocation of one or more role attributes of a public domain user;
2. Revocation of a public domain user which is equivalent to revoking all of that user's attributes. The AA will done these operations that the user belongs to, where the actual computations can be delegated to the server to improve efficiency.
3. Revocation of a personal domain user's access privileges;
4. Revocation of a personal domain user. These can be initiated through the data owner's client application in a similar way.

Policy updates.

A data owner can update sharing policy for an existing document by updating the attributes in the cipher text. Operations include add/delete/modify that can be done by the server on behalf of the user.

Break-glass.

To handle emergency situation, the regular access policies may no longer be applicable, break-glass access is needed to access the victim's data for this situations.

Digital Watermarking Process

The digital watermark is used as authentication and authorization model to avoid the unauthorized data storageand unauthorized data access. The authentication is ended with simple entry of username and password. If a person knows the username and password, then the person will access the data and make some modification, alteration or may some offense things too.The figure 4 explains the process of assigning and accessing a model of data which was taken place in thestorage part. The user 1 sends data to the cloud storage. The data is verified and digital watermark was fixed with the databy the digital watermark assigning server. Later the digitally watermarked data were stored in multiple servers which werelocated in different places. And the servers are interconnected for the data availability and data redundancypurpose. If another user wants to access the data which was stored in the cloud storage, he will be authorized by the digital watermark verifying server.

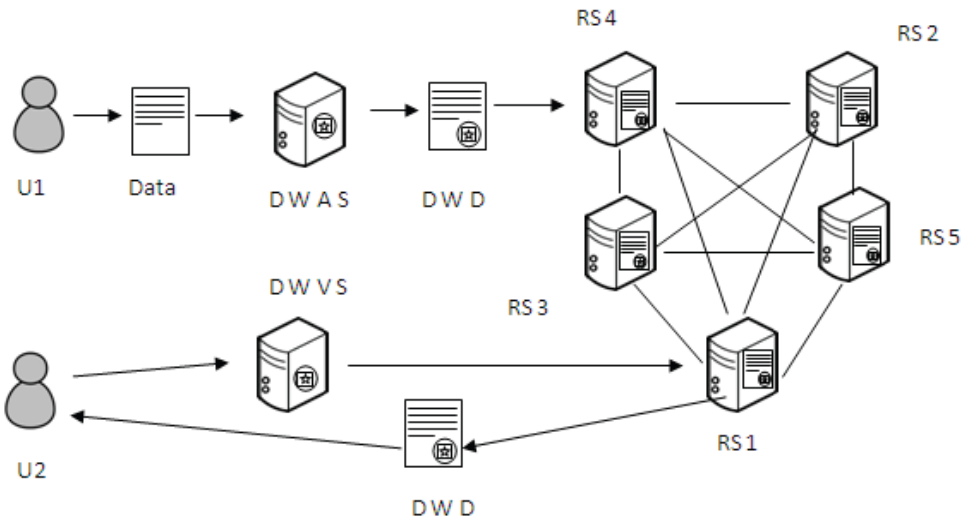


Figure 4: Digital Watermarking Process of Data Storage and Data Access

The user is authorized person to access the data then onlythe user permits to get the access to the data which wasdigitally watermarked and stored in cloud storage. TheFigure.4 explains the process.
U1: User 1, U2: User 2, D W A S: Digital WatermarkAllocation Server, D W V S: Digital Watermark Verification Server, D W D: Digital Watermarked Data, RS1:Replication Server 1, RS2: Replication Server 2, RS3:Replication Server 3, RS4: Replication Server 4, RS5: Replication Server 5.

Digital Watermarking Working Principle

1. User1 sends data to the storage through DWAS.
2. The DWAS assign the DW.
3. The DW assigned data stored in server.
4. Data stored in server was replicated.
5. User2 sends the request to DWVS for access the data.
6. DWVS verifies the DW and allow the User2
7. DW data get accessed by User2.

IV. ANALYSIS

The Secured Cloud Storage mechanism is using the ABE algorithm for sensitive data storage in cloud. So the users canencrypt the file using their private key and stored the file in the public cloud service provider using public key. The public key is used to store and access the file from the public cloud service provider. The important thing is the public key is only used to access the file. The user required private key to decrypt the file.
We compare our proposed system with the existing techniques with three criteria.
First the Key management policy of the algorithms. Here we can see that CP-ABE scheme has more key management complexity than the proposed system and MA-ABE scheme.
Second we compare the three techniques on the basis of processing steps. In this comparison we can see that the CP-ABE scheme have less steps than MA-ABE scheme which have less steps than our proposed scheme. In the CP-ABE scheme usually use a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrowproblem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys
Third we compare the three techniques based on the data security it provide, here then we can see that CP-ABE scheme and MA-ABE scheme are provide almost same data security but our proposed scheme give more data security than the other two. Our system will prevent more hacking techniques than the other two.

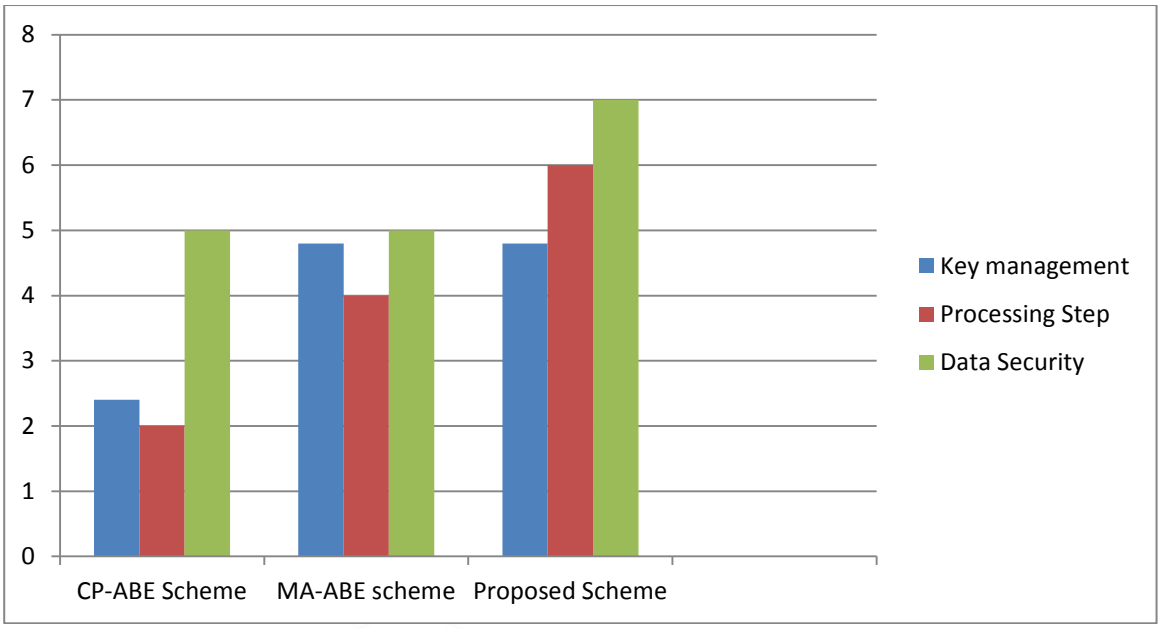


Figure 5: Comparison of three methods

V. CONCLUSION

The proposed system which include the MA-ABE (multiple-authority attribute based encryption) and the digital water marking techniques. The proposed system is more secure than the existing systems. It will take the best mechanism from the MA-ABE scheme and add the extra layer of digital water marking to the sensitive data so that the unauthorized access to the data can be prevent. The system will take more processing time because it have more steps than the existing methods but when we consider the protection of sensitive data which need more security the proposed system is better than the other two.

REFERENCES

[1] Ming Li,Shucheng Yu, Kui Ren, Wenjing LouandYao Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" IEEE transactions on parallel and distributed systems, vol. 24, no. 1, January 2013.

[2] Boopathy D andM.Sundaresan2"Data Encryption Framework Model with Watermark Security for Data Storage in Public Cloud Model", 978-93-80544-12-0/14/$31.00_c 2014 IEEE

[3] "Swamp Computing a.k.a. Cloud Computing", Web Security Journal, 2009-12-28, Retrieved 2013-10-25.).

[4] Philip Wik, "Thunderclouds: Managing SOA-Cloud Risk",Service Technology Magazine, 2011-10.

[5] M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[7] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," LectureNotes in Computer Science. Berlin, Germany: Springer, pp.1-12, vol.5451, 2009.

[8] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[9] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACMSymp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[11] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW'10), pp. 47-52, 2010.

[12] https://cloudsecurityalliance.org