Privacy Protection based various Data Privacy Protection Schemes in Cloud Computing

Singampalli.Sankeerthi[1], Thunuguntla.Sai Manikanta[2]
[1, 2] Department Of Mca
[1, 2] St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India

Abstract- *Cloud Computing is suitable a well-known buzzword nowadays. Many companies, such as Amazon, Google, Microsoft and so on, accelerate their paces in developing Cloud Computing systems and enhancing their services to provide for a larger amount of users. However, security and privacy issues present a strong barrier for users to adapt into Cloud Computing systems. In this paper, we investigate several Cloud Computing system providers about their concerns on security and privacy issues. We find those concerns are not adequate and more should be added in terms of five aspects (i.e., availability, confidentiality, data integrity, control, audit) for security. Moreover, released acts on privacy are out of date to protect users' private information in the new environment (i.e., Cloud Computing system environment) since they are no longer applicable to the new relationship between users and providers, which contains three parties (i.e., Cloud service user, Cloud service provider/Cloud user, Cloud provider). Multi located data storage and services (i.e., applications) in the Cloud make privacy issues even worse. Hence, adapting released acts for new scenarios in the Cloud, it will result in more users to step into Cloud. We claim that the prosperity in Cloud Computing literature is to be coming after those security and privacy issues having be resolved we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature (IABS) which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud-based services.*

Keywords- access control; data sharing; privacy protection; cloud-based services

I. INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, we need to develop an effective access control solution. Nowadays, the technology has been developed based on the human population in the world. Lots of technologies are invented today and each one serves to people in different ways. This technologies requires resources like hardware, software for the effective utilization. From the effective utilization it is processed with huge amount of data. The amount of data to handle in this world is completely panic. This situation brings us into a solution cloud computing. Cloud computing is a model for enabling convenient ubiquitous and on demand network access to a shared pool of configurable computing resources. This model provides different services and deployment models. The service models are provided as, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). The deployment models are provided as Public cloud, Private cloud, Community cloud and Hybrid cloud [1]. Storage of data becomes a major consideration in the technical world. The amount of data to store and maintain is only easier with the help of cloud data storage services. This helps to store any large size of the data at different storage locations. Each location is operated in independent manner. The data storage part is handled by the Cloud Service Provider (CSP). The CSP is a responsible person to monitor and meter for accessing the data. The data storage service offers vary by companies and individuals. The client outsource the data in to the cloud storage. The outsourced data travel from client machine to storage server. A specific cloud service is selected for the outsourced data with suitable platform model. The virtual machine manager will put the data into any managed Virtual Machine (VM) locations. These virtual machines are created and maintained by the Virtual Machine Manager(VMM). A service model for corporations provided as Storage as a Service (STaaS). This is a business model for large size corporations to maintain the business data on a subscription basis. Google, Amazon, IBM are some examples of companies providing cloud data storage services. Outsourcing of data brings out security issues. It is an responsibility by CSP to provide security to the outsourced data and ensure the reliable service to its customers. The data storage must satisfies the Confidentiality, Integrity and Availability (CIA) property of security mechanism. The data must be accessed by the person who is authorized. It is safe to make the data in unknown form. The data must not be modified by unknown or any other persons than owner. These three security properties ensure the data storage service provided in a effective manner.

Privacy

In general privacy refers the condition or state of hiding the presence or view. There is a need to attain this state in the places where the confidential things are used such as data and files. In cloud data storage the privacy is need to attain for the data, user identity and on controls. Violation of privacy leads to major failure in the system. To maintain the data privacy, it is possible for a successful deployment and usage of any service.

Privacy issues in cloud

Data in the cloud data storage has maintained at several distributed locations. CSP is the responsible person to maintain all the data securely. If proper security mechanism is implemented the security is violated at the storage service. Data can be accessed only by the person who is authorized. It is possible in this cloud model a CSP can read the client data for his purpose. Some competitor companies of data owner can give some amount to the CSP and get the access for the data. Internal workers in the CSP organization may access the data and give it to the business people for money. Government related data files like tender services, investigation documents, property checks may need by the industrialist. So the person contact the CSP and ask for the data. CSP can give it to the person on the basis of money or any other service. Identity of the famous person data like, Prime Minister, world famous sportsman, Actors personal data are accessed by the malicious persons to do such criminal activities. The access of a user is theft for performing some operation using their data. Some attackers are remove the data from the storage. Threats, malicious software are introduced to this storage for getting access and gain knowledge about the data.

Privacy preservation

Privacy deals with accessibility and availability of sensitive information to the intended recipients. Outsourced data accessed and modified only by the users who are having appropriate access privileges. Consider an organization have prepared and outsource their data in cloud. The outsourced data contents are given to the local administrator to place in cloud. It is recommended to ensure that the administrator cannot view or modify the data contents. After file outsourcing, no one including service provider can view or modify the contents. If service provider or local administrator is trying to read the file contents, it must not be done. Privacy preservation deals with the kind of security in outsourced data. This could be ensured by using Cryptographic techniques.

II. LITERATURE OF REVIEW

Greveler et al. designed a Privacy preservation model to protect cloud and local administrators [43]. The machine readable rights and expressions are needed for accessing the data. That is a database is created with set of controls such as roles for users, are defined at the time of application launch. It is unchangeable. author found that a work is to secure the hard disk with set of decryption keys. Keys are to be stored at some space in the system. Microsoft Bit locker is worked based on this approach [19], [22] To store the decryption keys on separate space bit locker uses Trusted Platform Module chip (TPM) [41]. eXtensible Access Control Markup Language (XACML) is an eXtensible Markup Language (XML) based language used to define a fine grained access control policy [26], [27]. A tamper proof hardware token is used to provide access control [8]. Privacy manager with XACML policies are the techniques to provide controls. The author found that these techniques are not safeguarding against attacks as impersonation. The author work is based on some of the methods like TPM on Linux, XML signatures, XML Encryption, and Encryption proxies. Encryption proxy is a system model containing TPM, user and rule engine. Cloud database is stored with user credentials and metadata table information. Users can access the cloud data through the encryption proxy. Full disk encryption is performed with TPM protected key file and stored in proxy's secure storage. If user wants to access the data, he/she need to follow encryption proxy. If the user doesn't have control on existing rule, then access is restricted. This work is combined with several mechanisms. This leads to performance overheads. Each time there is a need for re calculation or redefining such rules. It gives confusion on huge requests. Entire control is on the encryption proxy. Compromising the proxy leads the system failure.

Nabeel et al. provides a fine grained access control with fine grained encryption technique for cloud data [39]. Some other models proposed by various researchers are also encrypting the data before outsourcing. But, it gives a computation and communication overhead. Author proposes a Two Layer Encryption (TLE) technique to address the findings. Coarse grained encryption performed at user side, fine grained encryption at the cloud server side. This model faces an issue on the decomposition of Access Control Policies (ACPs) at the time of two layer encryption. A group key management scheme is used here to addressing it. Some works are applying fine grained access control over encrypted data [12], [16]. For each group communication different symmetric keys are used. Distribution of these keys affects the relationship between data items. The re encryption of data gives computation overhead and the distribution of the keys gives communication overhead. Some approaches limiting the issues by the broadcast key management schemes. These schemes are performing single layer encryption. For user access control policies distribution, thowner needs to maintain at each add/revoke [35], [39], [50]. The fine grained access control allows a user for selective access to content. This task has done using expressive specification of policies. The two model of fine grained access control are, push based and pull based models. Push based models distribute the keys at the time of registration [12], [16]. So, it is difficult to maintain the key secrecy in a dynamic data sharing system. Redistribution of key is overcome but the support of expressive access control policies is not supported [35]. Pull based models required the data publisher to stay online to grant access. Such works ensures this, using third party storage services. Some other works enforce the data owner has the responsibility to enforcing the access control policies and the user privacy from data publisher. Multiple encryption technique is followed in some models. Such works are not concentrating on encrypted data when user is removed, access control policies are changed. Such models are following the Attribute Based Encryption (ABE) technique and some other based on proxy re encryption technique [20], [32]. Basic building blocks of this system are broadcast encryption [4] oblivious commitment based envelope protocols [21] privacy preserving attribute based group key management based on [39], [55], [35], [50], and Single Layer Encryption (SLE) [39]. Then policy decomposition and two layer encryption are discussed. Two layer encryption techniques has six phases as identity token issuance, policy decomposition, identity token registration, data encryption and upload, data downloading and encryption, encryption evolution management. Discussion of experimental results is concern on policy decomposition algorithms and single, two layer encryption techniques. Analysis performed as SLE vs TLE and on security, privacy concerns. This work enlarges the view on privacy issues and techniques followed to overcome it. It performs the two layered encryption with group key management policy to ensure the privacy on outsourced data. It has such overhead on computation at server side and in the access control policies. The author concluded that the attribute based keys, access control policies decomposition are the key to success of this model. And also the future work plan is to extend this model with alternate two layer encryption technique with minimal computation cost for access control policies.

L.A. Dunning et al. proposed an algorithm for anonymous sharing of private among N number of parties [49]. The ID numbers are assigned iteratively to the nodes from 1 to N. The received identities are unknown to the other members of the group. It is also verified that there is no collision in private communication channels use. This is distributed without using a trusted central authority. The newer algorithms are developed over a secure sum data mining operation using Newton‘s identities and Sturm‘s theorem. Markov chain process is used to realize the statistics on the required number of iterations. The computer algebra gives the results closer to the completion rates. Author found that some cloud based tools used for website management are providing access for a server to saw the visitor actions on a site. In a secure multiparty communication, it is allowed for multiple parties on a network to jointly take over a computation which depends on each user, while it is held by other but unknown to the parties [3], [2]. For network nodes, such applications are there for requiring dynamic unique ID [6]. This ID is required in sensor network services for administration activities or for security to the individual nodes [30]. It is not an anonymous network, the participants known and identifiable by each others. In mobile network anonymous communication, methods for assigning and using set of pseudonyms have developed [31], [37]. An algorithm for sharing simple integer data on top of secure sum is build. This is used with the anonymous ID assignment (AIDA) algorithm. It requires a large number and varied iterations. The author prescribing a review on secure sum, specified method of transmitting simple data with power sum, sharing complex data with an AIDA, and how to find an AIDA. Comparison of various AIDA like Slot selection AIDA, Prime modulus AIDA, Sturm‘s Theorem AIDA are discussed. Communications Requirements of AIDA methods are defined. Author concluding that the use of newton identities reduce the communication overhead greatly. So the use of many slots with less number of rounds is needed. The polynomial solution can be avoided by applying sturm‘s theorem. The non cryptographic algorithms are simulated. The requirements are based only on the secure algorithm chosen.

H. Liu et al. reviewed that the existing solutions focus on the illegal access of data not on privacy issues when data sharing to others [57]. Author proposed a Shared

Authority based Privacy preserving Authentication protocol (SAPA). This protocol achieved the shared access authority by anonymous access matching mechanisms with privacy and security considerations. An attribute based access control is used to prove that the user can only access own data fields. Proxy re-encryption is applied to prove data sharing among multiple users. A universal composability model [11], is established for multiuser applications. Anonymous ID based data sharing algorithm for the systems under distributed computing and multi party oriented. This gives an integer data sharing algorithm gives a unlimited number of anonymous assignment. Theorems of newton and sturm are used for data mining[49]. Multi owner data sharing scheme is derived for dynamic groups in cloud applications. It assures the user can share the data securely to dynamic user groups through a untrusted cloud server. A granted user is able to decrypt the files. No interaction required for accessing the data from its owner. Revocation of user is achieved by the revocation list. This list is not updating the secret keys of other users. Applied access controls are ensuring that any user in the group can use the resources anonymously. This gives computation overhead are not based on the amount of user [51]. A zero knowledge proof (ZKP) based authentication scheme supports the sharing of personalized contents and network services through TCP/IP network. A trusted third party can handle decentralized instructions [42]. A broadcast group key management scheme (BGKM) developed to improve the weakness of symmetric key cryptosystem in the public cloud models. It ensures that no need for a user depending public key cryptography. One can derive the symmetric keys dynamically at the time of decryption. An attribute based access control method used to attain user who are having the identity attributes can decrypt the contents. This BGKM is a feature of adding revoking users and access control policies [50]. A decentralized framework developed, to track or account the user data usage in the distributed data storage. An object centered approach that provides logging services with the user data and with policies. Jar program ensures that the data access authentication and auditing mechanisms described to strengthen the user data control. The author proposes that a protocol authenticating the data access and authorizing the privacy preserving access authority sharing. ABAC and proxy re-encryption techniques are applied for authentication and authorization. The SAPA model has system initialization with bilinear pairing. Protocols are described for access challenges and responses, data access control, access request matching and data access authority sharing. Security analysis with universal composability model is performed as security model, ideal functionality, real protocol, and security proof for sharing. The author concluding that a newer privacy issue is identified to achieve sharing of privacy preserving access authority. Through the wrapped values transmission data anonymity is achieved. Session identifiers are used for preventing the session correlation. This work is based on a novel security issue. The models defined are combined with a force. Security analysis shows that this work is secure.

J. Zhou et al. proposed a protocol for preserving privacy in cloud assisted e-healthcare storage systems [61]. e-healthcare facilitates monitor, model with latest inventions [24], [5]. Sharing the resource from various locations is accessed through mobile or any other devices, and it is uploaded into the cloud data storage. It is generally stored as person health information (PHI) into the cloud data storage. Providing this data to the untrusted, leads to security and privacy issues. The author found that the existing schemes are focusing the fine grained privacy preserving static model for text access and image analysis. The works proposed provide a secure privacy preserving data mining for dynamic data with image feature extraction scheme. As basis privacy preserving fully homomorphic data aggregation is derived for the proposed privacy preserving data mining model. Then the outsourced disease modelling and earlier intervention achieved by devising an efficient privacy preserving function correlation. A privacy preserving data aggregation supporting multivariate polynomial evaluation without secure communication channel proposed with a respect of aggregator model and participants only model [43]. By the use of paillier‘s cryptosystem [7] an image feature scheme is proposed with privacy preserving scale invariant feature transform (SIFT) [45]. The usage of this cryptosystem directly onto the images deviates the actual process. It is further exploited. It's in efficiency but it is not adaptable to resource concerned devices. It doesn‘t applied to outsourced medical image extraction. Since paillier‘s cryptosystem supports homomorphism of addition. Local extrema extraction through encrypted data comparison with an encrypted data of the same scale doesn‘t prevent chosen plain text attack. So the differences of guassian images and the thresholds are under the same randomness. A simple and provable additive homomorphic stream cipher is proposed to perform efficient aggregation of encrypted data. It is done by replacing the exclusive-OR (XOR) function operations found in stream cipher with modular addition [28]. A concealed data aggregation scheme is proposed based on the property of additive homomorphic encryption based on elliptic curve ElGamal cryptosystem. But it is required to perform the ElGamal encryption on each individual data [7]. An efficient privacy preserving data aggregation scheme in smart grid communications is proposed. It reduces the cost of ElGamal encryption on each data. But it only supports additive homomorphism [61]. Fully Homomorphic Encryption (FHE) [34], [13], [29], [33], [38], [36] provides a solution to secure outsourcing operations in addition and multiplication formats in the encrypted data. Most works are constructed with polynomial-bounded hard problems. The plain text has to be encrypted as bit by bit. So it can not applied to the small devices. It gives computation overhead [34], [29], [38]. A privacy preserving data aggregation model is proposed but it supports only statistical computation. The addition and multiplication aggregation operations are independent. It gives an additional burden for users [48]. A newly developed full homomorphic data aggregation is proposed. It supports addition and multiplication with unified mechanism from n individual data in the encrypted domain, needed to perform any such one way trap door function computation only once. The author describes the network architecture and security model. The proposed work functions are, privacy preserving data aggregation, Privacy Preserving Data Mining 1 (PPDM) for dynamic medical text mining, PPDM2 for medical image feature extraction. Security and performance analysis are performed using various factors. The comparison with [45] shows this work has reduced overheads. Author concludes that the model supports privacy preserving fully homomorphic data aggregation from any such one way trapdoor function. The dynamicity of data is still a questionable. The homomorphic function is not effectively used.

Y. Wang et al. designed a privacy preserving cloud data storage using array Belief Propagation (BP) - Xor codes [60]. Technique of Belief Propagation decoding process is used with Low Density Pair Check (LDPC) and with Luby Transform (LT) codes [49], [57]. It is used for sharing secrets. Secret sharing schemes are BP-XOR secret sharing scheme, pseudo BP-XOR secret sharing scheme, and Threshold LDPC sharing secret scheme. Threshold LDPC [50] scheme is designed by utilizing array coded design. For reconstruction and distribution of a secret less number of XOR operations are utilized from the BP-XOR/LDPC scheme. In a threshold scheme number of participants can know the secret by grouping them. It is very difficult to handle it. In the secret sharing scheme reconstruction and redistribution is a hard task. Author explain about various number of codes and about the schemes construction. Threshold based secret sharing scheme is defined for privacy protection of cloud data. It uses only XOR operations so the updates and error recovery are easily performed. It overcomes update complexity of Shamir secret sharing scheme. This scheme guaranteed that data file is not required for any checking. Performance is better compared to existing schemes. Because this scheme is based on XOR operation. Author gives importance to the schemes rather than the cloud model. It requires more computation for operations performed with encryption texts and collude attacks are possible. The system has setup, user key generation, and access authentication algorithms. Proof of Knowledge model is designed to support proof check. Security analysis and various threat models are defined.

J.K Liu et al. designed a fine grained two factor authentication access control system for the computing services based on web [61]. Attribute based access control scheme is designed by taking secret key and a device. Both are required to get access, (i.e) the same computer is required for every access. Personal usage system like e-Banking services is an suitable application. The device used must support algorithm functions and tamper proof. This scheme supports

A. fine grained attribute based access control. Mediated cryptography was designed for the immediate revocation of public keys [4]. A Security Mediator (SEM) model is designed based on this cryptography. But it gives a pressure that this SEM always stay to perform any transactions. Modified version of this model designed as security mediated certificate less cryptography. In this system, user has secret key, public key, identity, and signing algorithm. Secret key and SEM model are also needed. It solves the revocation problems. User is anonymous to this model. So it leads to a security issue. Key insulated cryptography is used to store long term keys in a secured device and short term signatures in unsecured device. All users are needed to update the key for every time and the device is requested to do this task [20]. Bilinear pairing algorithm is used as initial step. (Boneh-Boyen-Shacham) BBS signature scheme used to check the credentials. It requires less amount of requirements. Performance analysis and security analysis are performed. It enables a security system model to provide privacy support for the data. It always requires the device to ensure the privacy. So it is not effective under different cloud services storage mechanism.

III. RELATED WORK

As shown in Fig.1, our system model consists of Data owner, users in PSD, and users in PUD, root authority CA, regional authority AA and cloud service provider, which are defined as follows.

1. The cloud service provider consists of two parts: data storage server and data service management. Data storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding ciphertext.
2. In the actual cloud environment, CA manages multiple AA, and AA each manages attributes in their

own field. The attributes owned by the user are issued by different authority.

3. Personal domain (PSD), in which users have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows the user's identity, which is easy to manage.
4. Public domain (PUD), which owns a huge number of users with unknown identity and a lot of attributes owned by the user.
5. Data Owner, based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server.

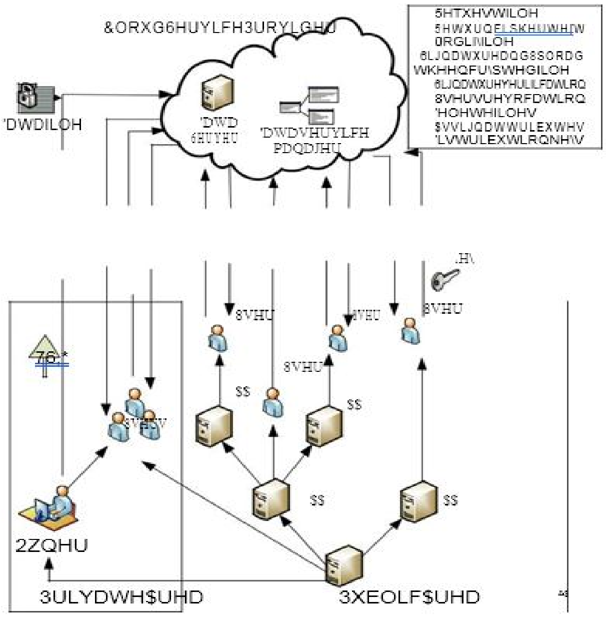

Figure 1. System framework

IV. PROPOSAL WORK

Read Access Control

The PSD has a small number of users, and their identities are known to the owner. In general, the data owner only wants the users to access or modify parts of data files, and different users can access and modify different parts of the data. For example, the blogger can allow his friend to browse part of his private photos; enterprises can also authorize employees to access or modify part of sensitive data. This requires the data owner to grant users read or write access permission to some data. In Chen’s MAH-ABE scheme, the CP-ABE is used to achieve the read access permission, but there are some defects to be considered. Firstly, since in the PSD, the users are all have a close relationship with the owner and the number is small, there is no need to use the CP-ABE which is applicable to the scenario which has a lot of users, and their identities are unknown to the owner, while the KAE scheme is set for the small users with certain identities. Besides, the distribution and management of keys and attributes, encryption and decryption process of CP-ABE are much more complex compared with the KAE scheme. Therefore, the KAE is exploited to implement the read access permission which improves the access efficiency.

Based on the above analysis, the paper uses the Aggregate Key Encryption scheme to encrypt the data files to realize different read access control. The specific application process of the KAE algorithm is as follows.

1. System setup and file encryption. The system first runs Setup of KAE to establish the public system parameter and master key. Each owner classified the file by its data attribute, such as “photo files”, “blog files” and “game files”. Fig.2 shows the way to classify the files. Choose and label the files,

Denotedby i
i ^1 , 2 ,..., n`, note that a file class i cannot be the subset of another file class j
j ^1 , 2 ,..., n`. Then the owner’s client application runs Encrypt of KAE using the public key and the number of classification file to encrypt the PHR files and sends them to the cloud.

2. Access and key distribution. When the user send access request to the cloud server, and his file index number is i , then the cloud server returns the corresponding encrypted classification file to the user. The owner authorized users access permission with the file index number denoted by j and sent the collection S of all the index number j to CA, CA generate an aggregate decryption key for a set of ciphertext classes via Extract of KAE and sent it to the corresponding user, Finally, any user with an aggregate key can decrypt any ciphertext whose class is contained in the aggregate key via Decrypt of KAE.

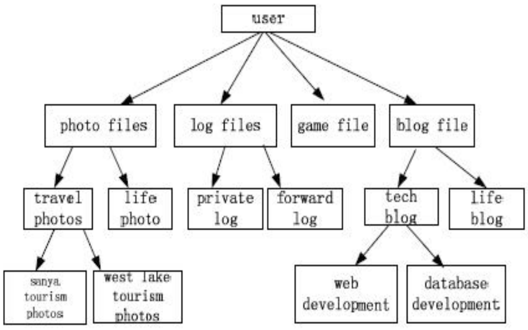

Figure 2. Data file classification

B. Write Access Control

As Chen's MAH-ABE scheme does not refer to the write access control, and in the PSD some cases exist, for example, the owner needs his friends to modify his file after he read it. So we proposed the write access permission in the PSD. For the user, the public key and file class label are all known, he can implement the algorithm to encrypt the files after he modified, and then upload them to the cloud. But whether the cloud server saves the modified file is decided by the write access control policy. On the one hand, in the complex cloud environment, if a user's modification operations are very frequent, maybe he is very important to the user, so that the user may be stricken from outside attacks. Therefore, the user worries the leak of identity after the signature. On the other hand, in the data sharing scheme, the separate access of read and write to the file is extremely important. In PSD, not all users who have read permissions also have write permissions to the files. Whether the user has write permissions to the file is decided by the data owner. Therefore, this paper selects the improved attribute-based signature (IABS) to determine the user's write permission.

The main structure of the scheme includes five parts: an authentication center (CA), the data owner, users, mediator and cloud servers. The CA is responsible for generating master key which is sent to the owner and system parameters which are shared for all users. The mediator holds part components of the signature keys and is responsible for the validity check of attributes and users. The data owner produces the signature tree and sends it directly to the cloud server. The user encrypts the modified files and signs them using the attribute-based signature, then uploads them to the cloud server. The cloud server verifies the attribute-based signature, if the authentication is successful, the user has permission to modify files and the cloud server stores the file. Own to the limited space we will omit the specific description of the IABS scheme in PSD.

ACCESS CONTROL SCHEME IN PUD

Before introducing our proposed secure authentication protocol, we first make a statement for the notations used in the later, all of them are listed in Table I.

Table 1.

Notation	Description
PUD	Public Domain
PRD	Private Domain
CP-ABE	Ciphertext-policy Attribute-Based Encryption
MA-ABE	Multi-authority Attribute-based Encryption
HABE	Hierarchical Attribute Encryption
CK	Encryption Key
K	Key Space
PK	Public Key
SK	Secret Key
KAE	Key-Aggregate Encryption
CA	Authorization Center

A. Scheme Design

the attribute-based encryption scheme (CP-ABE) can achieve access control, it cannot meet the needs of complex cloud environment. In traditional CP-ABE scheme, there is only one authorized agency responsible for the management of attributes and distribution of keys. The authority may be a university registrar's office, the company's HR department or government educational organizations and so on. The data owner defines access policies and encrypts the data files in accordance with this policy. Each user is distributed a key related to his attribute. As long as the user's attributes meet the access policy he can decrypt the file. However, if there is only one authority in the system and all public and private keys are issued by the authority. Two problems will appear in the practical application:

a. In the practical cloud environment, there are a lot of authorities and each authority in their own field manages part of users' attributes. The attributes owned by the user are issued from different authorities. For example, a data owner may want to share his medical data with a user who owns the doctor attribute issued by medical institutions and the medical researcher attribute by the clinic practice management. Therefore, exploiting multi authority is more realistic in the practical scenarios.
b. If there is only one authority, all the distribution of the keys are handed over by one trusted authority. The frequent interaction between the user and trust authority will not only bring bottlenecks for the system load capacity, but also increase the potential security risks.

Therefore, multi authority ABE (MA-ABE) is used in this paper.

Users in PUD do not need to interact directly with the data owner, and the attributes of the user are called role attributes. Firstly the data owner uploads the attribute-based encrypted data files to the cloud server. Then after authorized, the data owner receives the corresponding decryption key and sends a data file access request directly from the cloud server. Finally, after the cloud server returns the ciphertext, users can use their own decryption key to decrypt the ciphertext. The framework of this area is shown in Fig.3.

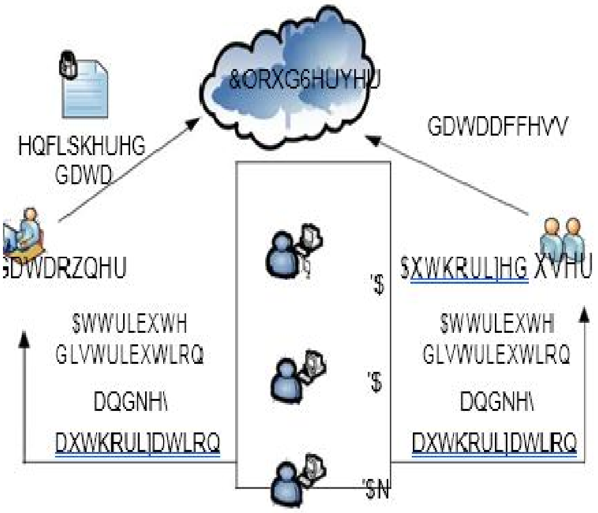
&ORXG6HUYHU
HQFLSKHUHG GDWD
GDWDDFFHVV
GDWDRZQHU
$XWKRUL]HG XVHU
'$
'$
'$N
$WWULEXWH GLVWULEXWLRQ DQGNH\ DXWKRUL]DWLRQ
$WWULEXWH GLVWULEXWLRQ DQGNH\ DXWKRUL]DWLRQ

Figure 3. Access control framework of PUD

B. Access Control Process

The PUD is characterized by a huge number of users, a lot of attributes owned by the user, complexity management, and indefinite users' identity. In view of the above characteristics, the user can only have the read access permission. Although

Based on the above analysis, we use a hierarchical attribute encryption scheme (HABE) to implement access control in PUD.

1. Files creation: The creating of files is completed by the data owner. In general, in order to protect the privacy of the data file, the data owner firstly encrypts data file, and then stores it in the cloud. To reduce the ciphertext size and complexity, the data owner combines the symmetric encryption scheme with public key encryption scheme, namely that each file is firstly encrypted with symmetric encryption key called CK, then CK is encrypted with the HABE program. Before the data file uploaded to the cloud, the process of creating a data file is as follows:

1) Select a unique ID for the data file.
2) Choose a random symmetric encryption keyCK □□R□ K . K means key space, and encrypt the data file with CK.
3) Define access tree T, use the algorithm HABE .Encrypt □ PKe , CK , T □ to encrypt CK and return the CT.
4) The data owner computes the CT by hash operations and signs h(CT) to get the signature SG , on the one hand to ensure the integrity of the data, on the other hand to facilitate the cloud and user to authenticate the identity of the data owner.

2. Data access: If the user wants to access a data file, he should get the file from the cloud server and decrypt the encrypted data file, which corresponds to the decryption process. There are two stages: firstly use the algorithm HABE ˜ Encrypt PK e , CK , T to decrypt the symmetric encryption key CK, then use the key CK to decrypt the data file.
3. Files deletion: If the data owner wants to delete a file, he can send the file ID and his signature SG to the cloud server, then the cloud servers delete the files after verifying the signature of the data owner.
4. Attribute revocation: The authority assigns attributes to each user and attaches the set of attributes with an expiration time T . The attributes of access control tree contain a timeattribute T c , if T ! T c and the attributes match, then this file can be access to. So the data owner can restrict users' access permissions by changing the time attributes.
5. Users' attributes Revocation: The DA calculates the minimum set of attributes A min that allows users' access revocation, and Anew A Amin , making T Amin returns null. Set a new expiration time to each attribute set, generate new private key components and return it to the client.

V. CONCLUSIONS

In this paper, we propose access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the user, we divide the users into personal domain (PSD) and public domain(PUD) logically. In the PSD, the KAE algorithm is applied to implement users read access permissions and greatly improved efficiency. The IABS scheme is employed to achieve the write permissions and the separation of read and write permissions to protect the privacy of the user's identity. In the PUD, we use the HABE scheme to avoid the issues of single point of failure and to achieve data sharing. Furthermore, the paper analyzes the scheme from security and efficiency, and the simulation results are given. By comparing with the MAH-ABE scheme, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” Proc. IEEE INFOCOM, pp. 1-9, 2010.

[2] J. Bethencourt, A. Sahai, B. Waters, “Ciphertext-policy attribute-based encryption,” Proc. Security and Privacy, pp. 321-334, 2007.

[3] J. Hur, D.K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.

[4] A. Lewko, B. Waters, “Decentralizing attribute-Based encryption,” Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.

[5] M. Li, S. Yu, Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption,” IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131-143, 2013.

[6] C.K. Chu, S.S.M. Chow, W.G. Tzeng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.

[7] J. Li, K. Kim, “Hidden attribute-based signatures without anonymity revocation,” Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.

[8] H.K. Maji, M. Prabhakaran, M. Rosulek, “Attribute-Based Signatures,” Proc. Topics in Cryptology - CT-RSA, pp. 376-392, 2011.

[9] S. Kumar, S. Agrawal, S. Balaraman, “Attribute based signatures for bounded multi-level threshold circuits,” Proc. Public Key Infrastructures, Services and Applications, pp. 141-154, 2011.