A Secure Data Access Mechanism for Cloud Tenants

Chunming Rong
Department of Electronic Eng & Computer Science
University of Stavanger, 4036, Stavanger, Norway
Stavanger, Norway
Chunming.rong@uis.no

Hongbing Cheng
Department of Computer Science & Technology
Nanjing University
Nanjing, China
cheng.hongbing@uis.no

***Abstract*—As the future big data storage center for tenants, cloud computing has been a hot issue recently, it consists of many large datacenters which are usually geographically distributed and heterogeneous, secure data access from cloud computing platform is a big challenge for cloud tenants. In this paper, we present a secure data access mechanism based on identity-based encryption and biometric authentication for cloud tenants. We review briefly about identity-based encryption and biometric authentication firstly and then we proposed a data access mechanism for cloud tenants, the mechanism set double protection for confidential data of cloud tenants, encryption will make the tenants data secure against the peekers and biometric authentication will eliminate the maloperations over tenants data by root administrator in cloud service. We compared the proposed mechanism with other technology and schemes through comprehensive analysis and experiment data; the results show that the proposed data access mechanism is feasible and suitable for cloud tenants.**

Keywords—Cloud computing; Big data center; Data access; Data security.

I. INTRODUCTION

As the big data center for tenants, cloud computing [1] platforms have many particular types of datacenters, or most commonly, groups of datacenters. Cloud service providers not only offer applications including search, entertainment, email and other services that Internet can provide, but also they have expanded offerings to include compute-related capabilities such as virtual machines, storage, and complete operating system services for science computing and research. At the same time, cloud computing has been proven to be a hopeful application platform and paradigm to provide potential consumers with valuable information technology services over the Internet and these services should be efficient, secure and rapid. In order to meet the above services requirement, cloud computing resources should be rapidly deployed and easily scaled. In cloud computing all processes, applications and services supplied "on demand," no need to regard user's geographic location and computer devices.

Currently, many public and private cloud services are available for tenants. Generally, private cloud computing platforms are for special intention and will not offer servicefor others, but public cloud computing platforms are available to every one with Internet access. According to the type of service provided, public cloud platform include Software as a Service (SaaS) clouds like IBM LotusLive™ [2], Platform as a Service (PaaS) includes Google AppEngine [3], Infrastructure as a Service (IaaS) like the Amazon Web Services (AWS) [4] and famous Apache hadoop [5]. Hadoop includes some subprojects such as Mapreduce and hadoop distributed file system (HDFS) and has developed many open-source software's for reliable, scalable, distributed computing. Private clouds are owned and used by a single organization or department. They provide many of the same services as public clouds, and they give the owner organization greater flexibility and control. What is most important is that private clouds can provide lower latency than public clouds during rush time of Internet occupation. Considering the benefits of the two kinds of clouds, many organizations embrace both of them by integrating the two platforms into hybrid cloud computing models. These hybrid clouds are designed to meet some specific commercial, science and technology requirements, helping to optimize security and privacy for customers in minimum investment

Cloud storage is an excellent solution for tenants' big data, and it is a promising technology and the benefits of it are obvious, but, as a commercial platform, security is the most important. To develop proper security mechanisms for cloud implementations is a big challenge. Except for the usual challenges of developing secure information technology systems, cloud computing is under some special risk [6], because essential services are often performed by a third party that .is unknown to cloud computing platform or users. These "unknown" aspects of cloud outside environment make it harder to maintain data integrity and privacy. In fact, cloud computing always transfers much of the control over data and applied operations from the tenant organization to their cloud providers, in some extent, it is similar with that organizations entrust part of their information processing operations to outsourcing other companies or agent platforms. Even the basic tasks processing, such as applying data updating and configuring network protocols may become the responsibility of the cloud service providers, not the tenants. So, in this circumstance, tenants must establish trust relationships with cloud computing service providers and understand security risk in terms of how these service providers should undertaketheir responsibility, deploy and manage security on their behalf. This kind of relationship between cloud service providers and tenants is critical because the tenants are obliged to be ultimately responsible for integrality and protection of their critical data and information, even if that tasks processing or programs have moved to the cloud computing platforms. In fact, it is the most difficult to determine the physical location where tenant data is stored inside the cloud computing environment. Security processes and issues that were once visible for tenants are now hidden behind fuzzy structure by cloud computing. This invisibility can arouse a number of security and compliance problems. On the other hand, the massive sharing of infrastructure with cloud computing creates an evident difference between cloud data security and other traditional platforms data security. Tenants who come from different organizations with different security anticipation and privilege often interact with the same set of cloud computing computation resources. On the other side, data-access security concern, cloud resource balancing, changing service-level agreements and other updating dynamic information technology environments will provide intentional-destroyer with more opportunities for misconfiguration. At the same time, data compromise and malicious conduct [7] by adversary, root users or administrator are the risk that the tenants must face. Data access calls for a high degree of standardized and strict operating rules, which can help improve data access security by eliminating the risk of supervisor operator error and intended maloperation. Therefore, the risks inherent with a massively shared infrastructure mean that cloud computing platforms and their secure data access have to pay more attention on identity and authentication.

The rest of the paper is organized as follows; in Section II, security concern on data access is described and in Section III, a secure data access for cloud tenants is proposed. In Section IV, we give a detail analysis and experiment results of the proposed mechanism. Conclusions are drawn in Section V.

II. SECURITY CONCERN ON DATA ACCESS

Generally, in terms of the service level agreements (SLAs) between tenants with Internet Service Providers (ISPs) or Cloud Service Providers (CSPs), we can categorize Internet or cloud services as below [8]:

◆ *Infrastructure as a Service (IaaS):* Under this kind of service model, ISPs allows tenants to use their database and some public services, at the same time, the tenants can rent computation, storage, networks, and other resources what they do not have to perform science research and commercial operations, such as Amazon and Hadoop. The tenant can directly deploy and run the guest OS and applications provided by ISPs. In general, the tenants have not the privilege to manage or control the underlying cloud infrastructure but have privilege tocontrol OS, storage, deployed applications, and networking components configuration.

◆ *Platform as a Service (PaaS):* This service model can provide the tenants to deploy and run their tasks and application program onto the platform infrastructure. For example, IBM also provides the tenants this kind of cloud service platform to build their programs based on some popular programming languages and software tools. The tenants can not manage or control the underlying cloud system when they perform their tasks on the platform.

◆ *Software as a Service (SaaS):* It is a common model that has been adopted by most of ISPs. In this mode, the tenants are passive and only can use what the providers provide. Such as websites browsing, email, and others, service providers undertake all of the responsibilities and develop attractive software and services for the tenants, the tenants make use of these services under some risk because the service providers maybe leak their information or critical data kept on the servers of the infrastructure The advantage of using this kind of service is that there is no upfront investment in servers or software licensing.

Cloud tenants do not want others to access or fetch their confidential data stored in cloud storage [9], so secure data access control is even more critical for data integrity and privacy. On the other hand, in general, there are two critical roles in clouds computing service called privileged users and the third-party system, privileged users refer to root users or administrators who working for the cloud providers. Privileged-users perform physical monitoring, resource scheduling, background checking. Privileged-users must have the capabilities to coordinate authentication and authorization with the tenants and enterprise back-end or third-party systems. The third-party system is a partner of the cloud service providers, it cooperates with cloud provider to easily and quickly leverage cloud services for end users.

It is evident that most famous organizations, enterprises and even general tenants cite data protection as their most important security consideration when using cloud computing service. Typical security concerns [10] include the way how data is stored, accessed and released. Tenant sensitive or regulated data needs to be properly segregated and kept on the cloud storage infrastructure, including important archived data. Finding a suitable way of encrypting and managing encryption keys of data in transit to the cloud platforms or the service provider’s data center are critical to protect data privacy ,integrity and usability. The encryption of data and the ability to securely share those encryption keys between the cloud service provider and consumer is an important way that ensures security of data access. On the other hand, it is very expensive to transfer large volumes of data quickly over the Internet, so,

ISBN: 978-1-61208-216-5

it is very critical to protect the data security when transferring the data from tenants to cloud storage platform. When sending data to the cloud service providers, it is critical that the data is encrypted and that only the cloud service providers and tenants have access to the encryption keys. But when the cloud service providers stealthily violate the agreement and to obtain some information about the transferring data using the encryption keys. So, some significant restrictions regarding with secure data access must be established for both sides to comply with.

How to set the restrictions depends on the feature of the data and the importance of the data to tenants, such as commercial value, personal privacy et. Several member states[11] of the European Union (EU) have set rules to forbid the nonpublic personal information of its citizens to leave their state borders. So, in a full shared cloud computing environment, all parties of the cloud computing participators must agree on their responsibilities to secure data and perform these security policies on a regular basis. These parties must take the responsibilities to make a secure data access environment for each participator in the cloud computing.

III. THE PROPOSED DATA ACCESS MECHANISM

Firstly, we review the identity-based encryption and biometric authentication technology and then we show the proposed data access mechanism for cloud tenants.

3.1. PRELIMINARY

A. *Identity-based Encryption*

Adi Shamir proposed the concept of identity-based cryptography [12] in 1984 firstly. Shamir's original motivation for identity-based encryption was to simplify certificate management in e-mail systems. When Alice sends mail to Bob at bob@company.com she simply encrypts her message using the public key string "bob@company.com". There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted mail he contacts a third party, which we call the Private Key Generator (PKG). Bob authenticates himself to the PKG in the same way he would authenticate himself to a Center of Authentication (CA) and obtains his private key from the PKG. Bob can then read his e-mail. Note that unlike the existing secure e-mail infrastructure, Alice can send encrypted mail to Bob even if Bob has not yet setup his public key certificate. Also, note that key escrow is inherent in identity-based e-mail systems: the PKG knows Bob's private key.

The distinguishing characteristic of identity-based encryption is the ability to use any string as a public key. The functions that compose a generic IBE can be specified as follows.

In 2001, Boneh and Franklin proposed a practical algorithm[13] firstly, based on IBE technique. To describe the Boneh and Franklin IBE algorithm, from here on, we use Z_q to denote the group $\{0,\cdots q-1\}$ under addition modulo q. For a group G of prime order we use G^* to denote the set $G^* = G \mid O$ where O is the identity element in the group G. We use Z^+ to denote the set of positive integers We give first some definitions and then the basic IBE scheme.

Definition 2.1 A map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ is called a bilinear pairing if, for all $x, y \in G_1$ and all $a, b \in Z$, we have $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$.

Definition 2.2 The Bilinear-Diffie-Hellman problem (BDH) for a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ such that $|G_1| = |G_2| = q$ is prime is defined as follows: given $g, g^a, g^b, g^c \in G_1$, compute $\hat{e}(g,g)^{abc}$, where g is a generator and $a,b,c \in Z$. An algorithm A is said to solve the BDH problem with advantage ε if

$$\Pr[A(g, g^a, g^b, g^c) = \hat{e}(g,g)^{abc}] \geq \varepsilon$$

where the probability is over the random choice of $a, b, c, g,$ and the random bits of A

Definition 2.3 A randomized algorithm G that takes as input a security parameter $k \in Z^+$ is a BDH parameter generator if it turns in time polynomial in k and outputs the description of two groups G_1, G_2 and a bilinear function $\hat{e}: G_1 \times G_1 \rightarrow G_2$, with $|G_1| = |G_2| = q$ for some prime q. Denote the output of the algorithm by $G(1^k) = < G_1, G_2, \hat{e}, q >$.

Definition 2.4. We say that G satisfies the BDH assumption if no probabilistic polynomial algorithm A can solve BDH with non-negligible advantage.

The detail on the basic identity-based encryption algorithm can obtain in [13]

B. *Biometric Recognition*

Biometric recognition is a process of automatically recognizing the identity of a person based upon one or more intrinsic physiological or behavioral traits that the person possesses. Physiological characteristics are related to the shape of the body and the widely deployed ones include fingerprint, face, iris and hand geometry[14]. Behavioral are related to the behavior of a person and voice and gait are among the mostly researched.

From the viewpoint of pattern recognition, biometric recognition is a typical classification problem, which generally includes two main modules: feature extraction and classification. Through feature extraction, discrimitive and compact digital representation of biometric sample is generated. In classification, statistical techniques are generally applied to learn biometric pattern for each person during training, and make decision on identity during test by using the learned patterns.

A biometric recognition system can operate in two modes: verification and identification. Verification (orauthentication) accepts or rejects the identity claim of a person (for example, Bob). Identification determines which of the registered persons a given biometric data comes from. The idea can be described as follows, when any person say, q, want to use authentication system, first, he must get a legal ID from system and pass the system check by sys_checker. Then, uses the ID to create his biometric template, all of the created templates are storied in system database such as sys_database. In verification phase, q's template is sent to the system matcher to match with the extracted biometric feature from q. Otherwise, in identification phase, the q's extracted biometric feature will have a match with all the storied templates in the system database. Algorithm 1 describes the process of biometric authentication.

Algorithm 1. Biometric authentication process for the Person q

```
Bio_Au_process(Person q){
    sys_checker ←q.ID
    if (sys_checker){
     for(i=0;  ;i++)
      {Template[i]←Extract Biologic feature of q
            sys_database ←Template[i]}
                    }
     //create personal biologic feature template
  if someone p claims that he or she is q
      {p.tmp←Extract Biologic feature of  p
           matcher ←p.tmp
           matcher ←Template[i]
     //send p's biologic feature template to matcher
           If matcher (p.tmp == Template[i])
               p is q
                    }
   else  {p.tmp←Extract Biologic feature of  p
           matcher ←p.tmp
           matcher ←Template
     //send all biologic feature templates to matcher
            for(j=0; ;j++)
            {If matcher (p.tmp == Template[j])
               p has passed authentication
                    }
                      }
              return
                 }
```

Biometric authentication is a statistical hypothesis testing problem involving in a tradeoff between two error types: false reject and false alarm. The performance measures of such system are the false reject rate (FRR) and the false alarm rate (FAR) which can be adjusted by an acceptance threshold. FRR is the proportion of genuine users that are incorrectly rejected. FAR is the proportion of impostors that are incorrectly accepted as genuine users.

The performance of identification is measured asidentification rate which is significantly influenced by population size among other things. For face recognition, it is found that identification rate decreases linearly in the logarithm of the population size.

Being easy-to-use and non-intrusive, biometric recognition technology is widely deployed to control access to restricted services, for example, banking and databases. In the initial phase, users are required to enroll in a system, namely, to give examples of their biometric data to the system so that it can build models for them and this should be done only once. This is similar to the sign up procedure to establish ID and password. In the verification phase, the identity claim is accepted or rejected; or in identification phase, the identity is determined. Each time when a user accesses to the service, verification or identification is performed.

Design of a biometric system needs to take into consideration such factors as the available sensors, the performance of various biometric recognition technology, existing security infrastructure, and cost and user acceptance.

With the recent advance in biometric recognition techniques and low-cost sensors, we can expect the increasing deployment of biometric recognition in many fields including cloud computing.

3.2. The Proposed Data Access Mechanism

We design a secure data access mechanism for cloud tenants based on Boneh-Franklin IBE algorithm and biometric authentication, the detailed mechanism is as follows.

Step1: Setup cloud side parameters

1. initialization

On the cloud service side, given a security parameter $k \in Z^{+}$, the algorithm works as follows:

Run G on input k to generate a prime q , two groups G_1, G_2 of order q , and an admissible bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ .Choose a random $\alpha \in G_1$ .Pick a random $s \in Z_q^*$ and set $\beta = \alpha^s$. Choose cryptographic hash functions for some n , $H_1 : \{0,1\}^* \rightarrow G_1^*$, $H_2 : G_2 \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*$, $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ .For the security proof, we view all the hash functions as random oracles. The message space is $M = \{0,1\}^n$. The ciphertext space is $C = G_1^* \times \{0,1\}^n$. The output system parameters are $\pi = \{q, G_1, G_2, \hat{e}, n, \alpha, \beta, H_1, H_2, H_3, H_4\}$. The master key is $s \in Z_q^*$. Where q is a prime number, G_1 and G_2 are two groups of order q , $\hat{e}: G_1 \times G_1 \to G_2$ is a bilinear map, n is the length of plaintext, $\alpha \in G_1$, $\beta = \alpha^s$, $s \in Z_q^*$ is the master key, H_1 , H_2 , H_3 , and H_4 are four hash functions with random oracles respectively. The master key should be kept in a secret place and the parameters can be distributed to all nodes.

2. key generation

When tenants are registered in cloud computing providers, each tenant will obtain a unique identity to identify him or her. In our proposed mechanism, the obtained identity is same with the one used in IBE algorithm. For a given tenant identity $ID \in \{0,1\}^*$ (ID is the cloud tenant's public key. It could be a random string and so it is very convenient and easily realized). According to IBE algorithm, the private key of the tenant can be calculated as following:

Compute $Q_{ID} = H_1(ID) \in G_1^*$ .Set the private key of the tenant K_{ID} to be $K_{ID} = (Q_{ID})^s$,where s is the master key.

The phase generates private key corresponding to given registered ID of every tenant in cloud computing.

Step2: Generate tenant's biometric template

Cloud computing is a pervasive service environment for tenants, different tenants have different security requirement. To these tenants who have special security concern on data can generate their biometric template and be stored in cloud database. Biometric authentication must be needed when someone wants to access the data. Modern mobile and video technology make the generation of tenant's biometric template very convenient and easy, many tenants can finish the process on the cloud interface through iphone and other mobile devices. The process of generation tenant's biometric template is described in part of Algorithm 2.

Step3: Encrypt cloud data

Input: cloud data (which is created by cloud tenants and stored in the database of cloud platform), a private key (the cloud service providers), and an ID (the cloud tenant who want to access the data); output: encrypted cloud data. The detailed operation is as following.

Input: A cloud data message $m \in \{0,1\}^*$, a private key d_A , an identity ID_B , and the system parameters. Choose a random $\mu \xleftarrow{R} \{0,1\}^n$, compute $r = H_3(\mu, m)$ and $s := e(d_A, H_2(B))$ then output the encrypted cloud data ciphertext $c :=< r, \mu \oplus H_1(r,s), E_{H_4(\mu)}(m) >$.

Step4: Biometric authentication

As an excellent storage scheme for tenants' big data, cloud computing has been a hot issue for a lot of consumers, generally, tenants' different data should be processed by different security modes. Biometric authentication has the advantage of exclusive for tenant in data access. When any registered cloud tenant say, p, want to access the data stored in cloud, first, he must pass the cloud system check such as cloud_sys_checker. Then, cloud tenants use registered identity ID to create their biometric template and all of the created templates are stored in cloud_sys_database. In cloud data access, cloud tenant p must pass the biometric authentication performed by biometric matcher in cloud computing. Part of algorithm 2 describes the process.

Algorithm 2. Biometric authentication for tenant p to access cloud data

```
Cloud_Bio_Au(Person p){
  //generation of cloud tenant p biometric template
     Cloud_sys_checker ←p.ID
    if (Cloud_sys_checker){
     for(i=0;  ;i++)
  {Template[i]←Extract Biologic feature of tenant p
               Cloud_sys_database ←Template[i]}
                        }
  //biometric authentication for cloud data access
  If cloud tenant p want to access cloud data
         {  p.tmp←Extract Biologic feature of  p
            matcher ←p.tmp
           matcher ←Template
             for(j=0; ;j++)
              {If matcher (p.tmp == Template[j])
                 p has passed authentication
                          }
                             }
              return
                   }
```

Step5: Decrypt cloud data

Input: encrypted cloud data ciphertext (which is generated in Step3), an ID (the cloud service provider's), a private key (the cloud tenant who want to access the data), and output: the corresponding plaintext i.e. cloud data. The detailed operation is as follows.

Input: An encrypted cloud data c, an identity ID_A, a private key d_B. Compute $s := e(H_2(A), d_B)$, $\mu := V \oplus H_1(U, s)$, $m := D_{H_4(\mu)}(m)$. Check whether $U = H_3(\mu, m)$ holds. If not, reject the ciphertext; otherwise output the plaintext *m* i.e. the cloud data that tenantaccess. Consistency is clear since $e(d_A, H_2(B)) = e(H_2(A), H_2(B))^a = e(H_2(A), d_B)$ by bilinearity.

IV. ANALYSIS AND COMPARISON

In this section, we mainly focus on analysis of feasibility and security of our mechanism. At the same time, we will compare our mechanism with other relational technology including cryptography and Role Based Access Control (RBAC) scheme.

1) Feasibility analysis and comparison

(1) Cloud computing will provide its legal tenants with pervasive communication service anytime and anywhere. Recent development of wireless communication technology has gained a rapid progress, many wireless standards and modes emerged, including 3G, Wi-Fi, et. At the same time, wireless communication devices also have made a quick development; some advanced wireless communication devices, such as iphone and iPod, equipped with many high-class functions that only possessed by lap-top class device before. All of these advances make access of Internet by wireless connection become more and more dominant. In many public places, more and more people rely on such mobile devices to browse web page, to download multimedia and to interact with Internet.

When applied our data access mechanism in cloud computing, latest communication technology can support the running of the proposed data access mechanism well. Users can operate mobile devices on touch screen and push technology. On the other side, the advanced wireless communication devices can be used as camera, can deal with massive multimedia data packet and run a lot of complicated software and program. All of these are fundamental for the proposed data access mechanism and it is possible for the mechanism to be applied in practice.

(2) In the proposed data access mechanism, biometric authentication is an important secure measure for cloud data. On general impression, biometric authentication is complicated and costly for common applications, it is only available in some crucial situations, such as bank counter, airport security, etc., but it is not true now, rapid progress of electronics technology make it realistic to produce cost-efficient and multifunctional mobile communication devices which can read and process tenant's some feature information such as fingerprint, face and iris, etc. It is reported that only the users of iphone in the world will exceed 100 million till 2012 [15]. Now, in some public places of many countries, these kind of advanced multimedia mobile devices are available for tenants free to use. Therefore, all of these prosperous situations make it feasible and convenient to apply the proposed data access mechanism in cloud computing environment.

2) Security analysis and comparison

(1) As we know, except for key leaking, the security of key not only is related with key length, but also depends on encryption algorithm. Symmetric encryption algorithm DES with 64-bit key (DES-64) has been cracked for about 20 years and RSA algorithm with 768-bit key (RSA-768) was cracked in 2009 by some scientists in Switzerland [16]. So, for the sake of making data access secure in cloud computing, we have to find suitable secure encryption algorithm and secure key length. Identity based encryption algorithms are based on Elliptical curve cryptography (ECC). Related research results [17] show that the traditional asymmetric RSA algorithm with 1024-bit key (RSA–1024) provides the currently accepted security level, in order to reach the same security level, ECC key length is 160-bit (IBE-160) and symmetric key length is 80 bits. On a PC with Redhat Linux 9.0, P42.8G processor and 512M DDR, we tested the average encryption and decryption time for different encryption algorithm, these time cost does not include keys distribution and parameters setup, the comparison is listed in Table 1.

TABLE 1 COMPARISON OF DIFFERENT ENCRYPTION ALGORITHM

algorithm	key (bit)	Average encryption cost(s)	Average decryption cost(s)	Has been cracked
RSA	1024	21.2261	34.4025	RSA-768
IDES	80	0.0028	0.0028	DES-64
IBE	160	0.1279	0.1279	NO

From the results in Table 1, we can conclude that the proposed data access mechanism is the safest for cloud tenants. Although symmetric encryption algorithm has some advantage in key bit and time cost, the fatal weakness is that encryption key and decryption key are same and kept by different parties, in addition, the RSA encryption and symmetric encryption had been cracked and the attempt for cracking more bits of them will continue.

(2) Biometric authentication technology has been developed for decades and many of them have been applied in some security scenarios successfully. In detection of criminals, biometric authentication such as finger-print and face recognition have made many pernicious cases come out in the wash. As the rapid development of social economy and technology, biometric authentication can be applied in more and more situations. Of all the biometric authentication technology, the face recognition is a convictive representative. In 1993, the American government launched a project called FERET [18] to found a series of technology development efforts and evaluation cycles, the face

recognition community benefited a lot from this project and built a large datasets collected to test face recognition technology, the large datasets push the research of technology forward quickly. Figure 1 show that from the beginning of the Facial Recognition Technology (FERET) program to the Face Recognition Vendor Test 2006 (FRVT 2006). The remarkable improvement of face recognition has five important milestones since 2003. To each representative algorithm, they wereevaluated on the false reject rate (FRR) at a false accept rate (FAR) of 0.001 (1 in 1000). The algorithm for 1993 was Turk and Pentland's eigenface algorithm [18] and for 1997 is Sept97 FERET evaluation [19]. The 2002 evaluation result is from the FRVT 2002 and the 2006 and 2010 is from the FRVT 2006 and FRVT 2010.

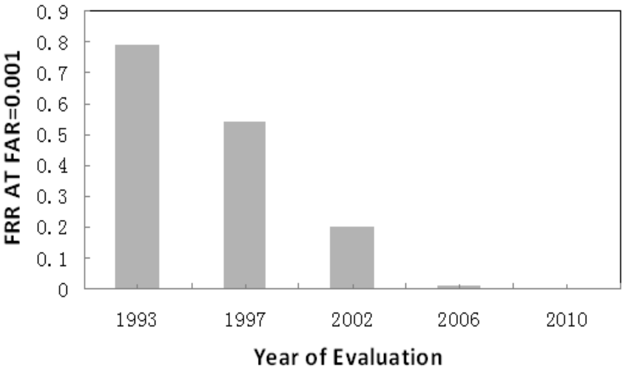

Figure 1 Improvement of face recognition from 1993 to 2010

From the evaluation results in Figure 1, we can conclude that as the representative of the biometric authentication technology, the face recognition attained an enormous improvement these year, especially, from 2002 to 2010, the improvement was very evident. The factors on the improvement due to advancement in algorithm design, advanced multimedia devices and more deep understanding of image processing. So, the low false reject rates (FRR) at a false accept rate (FAR) of the biometric authentication will enhance the security of the proposed data access mechanism.

V. CONCLUSIONS AND FUTURE WORK

Cloud computing has been a hot issue recently, as the future big data storage center for tenants, cloud computing is an Internet-based pervasive information infrastructure to provide tenants with data storage and service on demand it consists of many large datacenters which are usually geographically distributed and heterogeneous, secure data access from cloud computing platform is a big challenge for cloud tenants., how to design a secure data access mechanism for cloud computing is a main concern for service providers and their tenants.

In order to seek a secure data access method for cloud tenants, we presented a secure data access mechanism based on identity-based encryption and biometric authentication in this paper, the mechanism set double protection for confidential data of cloud tenants, encryption will make the tenants data secure against the peekers and biometric authentication will eliminate the maloperations over tenants data by root administrator in cloud service. We compared the proposed mechanism with other technology and schemes through comprehensive analysis and experiment data, the results show that the proposed data access mechanism is feasible and suitable for cloud tenants. In future work, We will make our proposed scheme more efficient and put it into practice.

ACKNOWLEDGMENT

This work was supported in part by the 973 Project under the Grant No. 2011CB302903, the National Natural Science Foundation of China under Grant No. 60873231, by the "Six Kinds Peak Talents Plan" project of Jiangsu Province under Grant No. 11-JY-009 ; the Nature Science Foundation of Jiangsu Normal Higher University under Grant No. 11KJB510003; China Postdoctoral Science Foundation funded project under Grant No.2012M511252 and Jiangsu Province Postdoctoral Science Foundation funded project Grant No.1102014C.

References

[1] "Cloud Computing- The BlueCloud Project ", www.ibm.com/developerworks/websphere /zones /hipods /, Oct. 2007.
[2] http://www.ibm.com/developerworks/lotus/library/lotuslive-intro/. [retrieved; June, 2012].
[3] http://code.google.com/intl/zh-CN/appengine/.[retrieved; June, 2012].
[4] http://aws.amazon.com/ . [retrieved; June, 2012].
[5] http://hadoop.apache.org/.[retrieved; June, 2012].
[6] Cloud Security Alliance, "Security guidance for Critical Areas of Focus in Cloud Computing", April 2009.
[7] J. Girard and J. Pescatore, " Teleworking in Cloud: Security Risks and Services" – A Gartner Report, May 15 2009.
[8] J. Viega, "Cloud Computing and the Common Man", IEEE Computer Magazine, Aug. 2009, pp. 106-108.
[9] R.L. Grossman, "The Case for Cloud Computing," IT Professional, vol. 11, no. 2, 2009, pp. 23–27.
[10] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," Nat'l Inst. of Standards and Technology (NIST), 2009.
[11] http://europa.eu/legislation_summaries/consumers/consumer_information/l21253_en.htm, [retrieved; June, 2012].
[12] A. Shamir, "Identity-based cryptography and signature schemes," [J].Advances in Cryptology, CRYPTO'84, Lecture Notes in Computer Science, vol. 196, 1985, pp. 47-53.
[13] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," [J]. in Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, 2001,pp. 213-229.
[14] A.K. Jain, "Biometric recognition," Nature, vol. 449, 2009, pp. 38-40.
[15] http://tech.sina.com.cn/t//03246615270.shtml. [retrieved; June, 2012].
[16] A.Kleinjung, K.Franke, F.Lenstra. Factorization of a 768-bit RSA modulus, v 1.0. International Association for Cryptologic Research ePrint archive. January 7 2010.
[17] K.Lauter, "The advantages of elliptic curve cryptography for wireless security," [J].IEEE Wireless Communications, vol. 11, no. 1, Feb 2004, pp. 62-67.
[18] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cognitive Neuroscience, vol. 3, no. 1, 1991, pp. 71–86.
[19] L. Wiskott, J.-M. Fellous, N. Kruger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," IEEE Trans. PAMI, vol. 17, no. 7, 1997, pp. 1-23.