TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing

Sultan Ullah, Zheng Xuefeng and Zhou Feng

School of Computer and Communication Engineering, University of Science and Technology, Beijing
sultan.ustb@yahoo.com, zxf.ustb@yahoo.com, zhou.uztb@yahoo.com

Abstract

The countless advantages of cloud computing has brought a massive change to the lifestyle and the way to cope with the world today, yet the cloud has to reach maturity. However, the main barrier to its widespread adoption is the security and privacy issues. In order to create and maintain mutual trust among the customers and the cloud service providers, a well – defined trust foundation should be implemented. The data stored in the cloud remotely by individual customer or an organization, so they lost control over the data, thus creating a security dilemma. The most challenging and hot research area in cloud computing now a day is the data security and access control. An effective measure to protect cloud computing resources and services in the start is to implement an access control mechanism. In this paper the features of various access control mechanisms are discussed and a novel framework of access control is proposed for cloud computing, which provides a multi - step and multifactor authentication of a user. The model proposed is well-organized and provably secure solution of access control for externally hosted applications.

Keywords: *Cloud Security, Access Control, Cloud Trust, Data Control, Multi – Factor Authentication*

1. Introduction

Even though cloud computing endow with a lot of benefits that consist of economy of size, active stipulating, amplified litheness and near to the ground principal expenses, yet it also bring in a variety of new-fangled security threats. The widespread apprehensions in relation to cloud computing are the privacy and security. A cloud user can access cloud services from any location. It is of most importance that to uncover new means of privacy and security to protect data and privacy for the cloud computing. One of the approaches normally in use is the common authentication procedure in which a user needs only a user name and password, in other to make use of an authentication and authorization system in which every client has the right to access the data and applications which are only appropriate to his or her job [1, 2].

Every cloud has central server administration systems, which govern the structure and operation of the cloud; make a balance among the supply and demands of the client resources and monitor in going and outgoing traffic. One of the concerns of the customer is about the storage to data in the cloud. It is a universal approach to store data of several customers in one common place in cloud computing, other concern is the access to the data in the cloud environment. The cloud services are provided by commercial service providers and the above mentioned concerns are very common from

the customers, as it is outside the trust domain of the customers [3]. It is the responsibility of the cloud service provider to implement a well – organized mechanism of data confidentiality and access mechanism.

The owner of the information has a great concern over the risk of data lose when they liberate the information for processing to the cloud, because they don't have the control over the information. The customers have no physical control over the infrastructure of the datacenter and information, and this increase conciliation of data considerably [4]; on the other hand, advantages (reduction in the overall operating costs and amplified availability of availing the services of cloud computing may be momentous enough to justify the risks [5].

It is a well known fact that for the last twenty years many efforts are made, and numerous solutions have been provided to secure data, messages and other resources available on computer networks. Efforts are also made that the privacy of the users, integrity, availability and reliability could be ensured for computing environments. Despite all these requirements, activities, enduring efforts, and above all the solutions that we have, it is a common belief that the trust in today's cloud application is not sufficient. In this paper a novel framework of access control is proposed for cloud computing, which provides a two - step multifactor authentication of user. The model proposed is well-organized and provably secure and can also provide single sign on solution for externally hosted applications [6].

The major issue confronted by most of the organization regarding adoption of the cloud architecture is the security. A lot of techniques and technologies have been developed and implemented to ensure a high level of security in the cloud. A lot of cryptographic methods are employed to realize security, however owing to the complexity of accomplishment; it seems that the performances lessen. Only a few methods are present that not only perform the registration and classification but perform the monitoring and tracing of users' transactions.

In order to provide the data or applications in cloud environment a comprehensive mechanism of security is, desists the unauthorized access in the first step, which is possible by implementing a strong authorization mechanism for the user. In general the principles or course of actions that refrain, allow or confine access to a system is known to the access control. It may possibly, as well, observe and document all attempts made to access a system, and identify the users who are unauthorized and attempting to access the system. It is considered to be the most important mechanism of protection in computer security [7]. The process of identifying a user uniquely through the verification of their credentials is called authentication, and upon the validation of the identity, a trust relationship is established for further interactions.

The authentication of the user is obligatory, as soon as, the user endeavor to access the services or data. Even some time, while, the applications create a link to distant services or attempt to access data held locally. If the deployment selected is central for data or an application, then it need more importance to be secured, consequently it can only be accessible to authorized users. The servers are required to authenticate the users first to see whether they are the authorized to access data/service or they are not the legitimate users. The majority business enterprises which are security – cognizant, employed various types of authentication and authorization mechanisms in order to access computing resources over a network. The advantages of the approach are evident.

Authentication can be put into practice by numerous methods. The significance of choosing a suitable authentication technique is conceivably the most critical judgment in scheming protected systems. A number of authentication schemes are based on

simple password authentication, which needs effortless implementation, except primeval and commonly weak. Some of the authentication techniques which may be more complicated and necessitate added time to developed and preserved, except offer tough and trustworthy means of authentication [2].

Normally the factors which can be used for authentication fall into three categories; apiece authentication feature swathe up an array of aspects, utilize to authenticate, or prove a person's uniqueness preceding to establish an access, supporting an operation demand, marking a document, giving away right to others, and ascertaining a string of powers. These factors of authentication consist of: the things which are in the ownership of a user, the things which are related with the knowledge base of the user, and personal intrinsic factors [8, 9].

Authorization is the next step after authentication, which permit or confines the rank of right to use and utilize allowable to that unit, which is based on the identity of the user. The elemental objective of either of the access control technique is to make available a provable scheme for assurance the safety of information from improper access. All this is done by employing some policies regarding safety regulation. In broad, the policy to the implementation of access control techniques rely on the type of policy, but it will include at least one of these control, *i.e.*, either the confidentiality or integrity.

2. Related Work

There are various types' of access control techniques that also utilizes cryptographic algorithms depending on the availability of the computing resources. Numerous cryptographic access schemes have been defined and implemented in cloud computing. A cryptographic based access control model is proposed, and the basis of our model also depends on the model depicted in [9, 10]. The system model of the cryptographic based access control is shown in Figure 1.

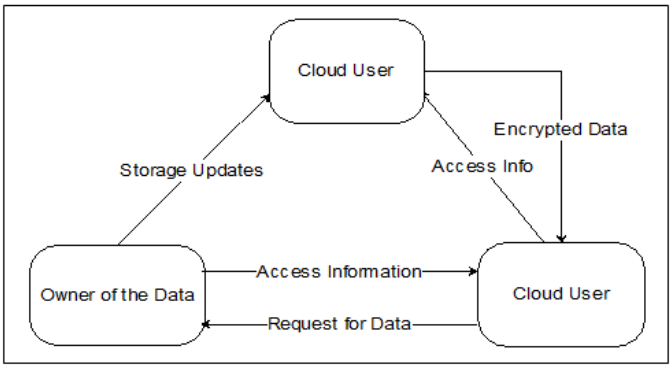

Figure 1. Encrypted Data Access Model

There are three contributor in the model illustrated above, *i.e.*, the Owner of the Data, the provider of the Could Services, and Cloud User. The owner outsourced its data to the cloud services, as the cloud is a multitenant environment and untrusted the data outsourced by the owner is encrypted, and the cloud user desires to access the data. The owner of the data sends the keys and an authentication certificate required to access and decrypt data when it receive the request from the user of the cloud. The authentication certificate is then presented to the CS for verification; upon the

successful validation by cloud services, then user receive the data in encrypted form. The model depicted above assured that the confidentiality will be achieved, integrity will be maintained and authentication will not be compromised, yet it suffers. The owner will always be online in order to entertain the request of user, which is the main weakness of the model [11]. It is difficult to maintain keys and certificates for all the communicating entities. The situations even get worse when the owner has poor computing capabilities.

A system to accomplish a protected, fine – grained and capable of being easily upgraded or expanded and to provide on demand access control was introduced for cloud computing environment [3]. This system was based on the different methods of encryptions which are, proxy re – encryption, attribute – based encryption and lazy re – encryption. The features which are having an important effect on each others are coupled to a file in the situation of user's concern. The mechanisms for every user, to be authorized to access have a distinctive logical expression based over the features, which shows the capacity of the data file for which the user is authenticated to access. For every attribute a public key element is generated. These public keys are used to encrypt all of the data files analogous to the attributes. The users are assigned private analogous keys to the access rights, in order to make them capable of decrypting a cipher text if and only if the attribute of the data file authenticate his access rights. A key problem concerning this mechanism is the derivation of a distinctive logical expression for all users, because the cloud store enormous amount of data logical expression based on the attribute of the file becomes multifaceted. Furthermore, the re-encryption also becomes an issue as the updating of the user secret key for every user excluding the revoked one is tough procedure when the there are lot of users.

A system of authentication which is based on the combination of identity and combined key and hardware encryption technology is proposed, implemented and tested [12]. This mechanism is composed of web – server subsystem, authentication subsystem and client subsystem.

A robust ID – Based system on Elliptic Curve Crypto System (ECCS) for remote user authentication is proposed in [13]. The model proposed is a system separated into three phases; the first phase is the system initialization phase, the second phase is about the registration of the user, phase and in the third phase the authentication of the user along with the mutual key agreement takes place. The authentication system based on ECCS has some limitations. The first one: a key authentication center is needed to maintain certificate for user's public keys. The second: a large storage space is needed when the number of users is increased as in the case of cloud to store the public keys and certificate of the users. The computation and energy cost of the devices become very high, as the users need additional computations in order to verify the certificate of others.

A new model based on the dynamic firewall operation and using the three way TCP handshake for the authentication of the users is proposed in [14]. The firewall exploits the available information to approve the establishment of associations during the sessions which is supported by user's demonstrated distinctiveness. The inadequacy of the model is the conception and fortification of the certificates, which is inappropriate for cloud environment. The performance of the overall system is reduced due to complex cryptographic methods.

The use of certificate at different levels which enable the secure transfer and access of data is revealed by the model presented in [15]. The different types of certificate demonstrate the type of user, the type of application and the type of hardware. The main

weakness of the mechanism is the maintenance of the certificates at diverse levels and to create a trust relationship between these certificates.

The model of multitenant platform that guarantees to block any faulty or malicious code from any tenant, which interfering the normal execution of the other tenant or code or the platform itself is proposed in [16]. The challenging concerns are separation, possible harms like visibility of object orientation from fluctuating position of classes and overcrowding throughout communal data structures.

Access control on available XML documents by the use of various cryptographic keys on different level of XML tree is presented in [17]. Special nodes of metadata were also introduced in the technique to impose access control. The key management and the generation of the XML tree are the only complexities of this approach.

The Identity – Based Hierarchical Model for Cloud Computing is proposed in [18]. This mechanism is used for the authentication of cloud users. The successive encryption and signature mechanism are used to be able to access the service of the cloud. The only problem with method is that it consumes a lot of bandwidth.

The initiative for authentication of the user through billing information by the clouds service providers, and make use of X.509 certificate or PKI/SSH infrastructure [19] [20]. The model only allows chosen operating system and kernels to run, which is the only drawback.

To secure data on untrusted servers a new technique is proposed, which is based on the encryption of data with a symmetric key and all of the users are assigned a secrete keys [21]. The owner of the data then creates pubic token, which contain the decryption key which is derived by the user using his secrete key. The number of secrete keys and encryption keys are much reduced in this approach, yet it has suffered from the issue of complexity in operations, *i.e.*, the number of file creation and user access requests is directly proportional to number of users, which leads to the non – scalability issue.

The applied mechanism for user authentication and authorization are different security measures to safe the platforms. The techniques which are used to delimit the access of a process in one operating system and not to come within the reach of the other process are proposed in [22]. The solution proposed has not complex computation on the client side, the authentication and validation is performed at service provider and data center's location.

Internet is considered to be the infrastructure of universal communication for the providers of the cloud services [23]. It uses the well – defined TCP / IP protocols for the identification of the users' on the cloud. The drawbacks of this approach are same as to addressing mechanism of the physical computer on the internet; the virtual machines also have IP addresses. A malevolent entity, irrespective of its identity, can locate this address. In this situation, the physical server running the virtual machine can be located, and the malevolent user implant a false virtual machine at that physical location to initiate an attack.

A protected system of distributed storage based on the techniques of proxy re – encryption is proposed in [24]. The block of data is encrypted with content symmetric keys by the owner of the data; all of the content keys are then encrypted by the owner

with a master public key. The proxy re – encryption keys are generated by the owner of the data by using the user's public key and his own private key. The problem faced by this mechanism is that, even a single untrusted server or malevolent user possibly could exposed all the decryption keys for the cipher text and the overall security of the system is compromised.

3. The Proposed Model

In our proposed model, it is assumed that the components which make the system operational is composed of an owner of the data, a lot of entities which will used the data created by the owner of the data called the user of the data and the provider of the cloud services and data center. The authentication of the user is a multistep process, and after the successful authentication the user will only access the data file store by the owner, in a confidential manner by the implementation of the digital certificate. It is also assumed that it is not necessary for the user or owner to be online all the time. The owner comes online when it needs to register a new user or make some update to the certificate available on provider of cloud service, and the provider of cloud services is assumed to be online all the time to provide access to the data store at data center. Another assumption that we make is that the owner of the data will be able to perform / implement binary codes at cloud services for administration of data along with the storing of such data in encrypted type. All the communication, whether it is between the cloud service and user or between the user and owner and vice versa will use cryptographic means, *i.e.*, the use of RSA for encryption and along with digital certificate. The idea behind the choice of RSA encryption involving user and the cloud service is, since RSA encryption will need all associations to generate digital certificate for all users, and which is only one of its kind for every user. By implementing this mechanism of RSA encryption we are able to accomplish a protected data communications for all latest session. The RSA is considered to be more efficient, safe and sound mean of encryption, and also the digital certificate are make use of an encrypted session, therefore the rest of the users are unable to observe the data or information which is in transit over the network. The user is refraining from accessing other's data files, as the access provided by the owner has put some limitation on the user because of their capabilities.

The proposed framework and its operational architecture are presented in this section. The overall all working model is presented in Figure 2. The data which will contain request of the user for the data and his identification credentials are sent to cloud services, and checked it with the available information in the validation information at data center and also the communication between owner and provider of cloud services ought to be secured during the transaction, to oppose any attack. The framework proposed, will clarify they way to attain the level of security required and controlled the mechanism of access.

The authentication of the user is a multi – step process. In the first step the user can sign in to CS by providing her / his username and password, along with the IP address

of the terminal. Then the user will be asking for entering the biometric (Finger Prints) data. Upon the successful authentication, the user will be sent an email containing the access code for the session, which adds an extra layer of security around the user account. After completing the login process every user will get an authorization certificate based the attribute. The high level diagram of the proposed framework is shown on Figure 2 and the detail diagram is shown in Figure 3.

The steps required for the registration of new users comprises of a request for registration send to the owner of the data with identity details i.e User ID, IP address / Terminal ID, timestamp and the right to access data file. This is shown in Figure 4.

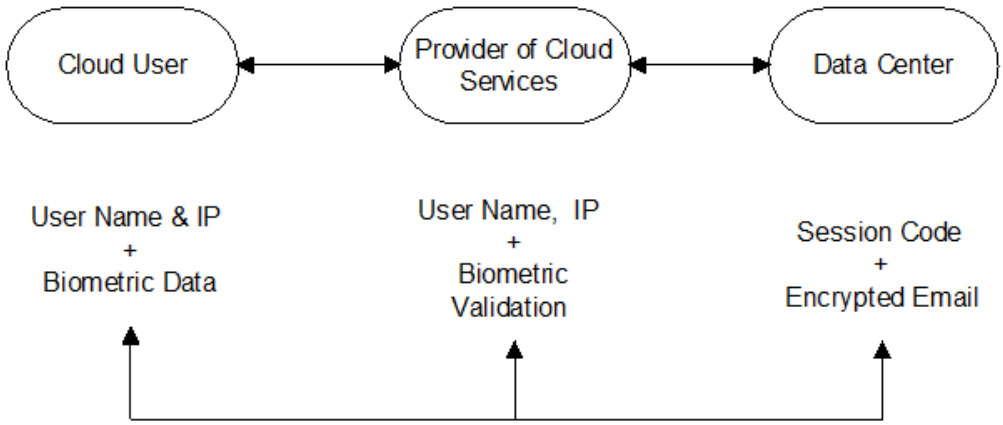

Figure 2. High Level Diagram of the Proposed Scheme

The validity of the request is checked by the owner of the data after the formal receipt of the data. To make the things at ease, we assume that that the owner has a separate course of action to check the authenticity of the client's request. The new user information is now updated by the owner at the service provider. After the updation of information at cloud service and data center, the data center now generate sends a reply message to the clients encrypted by MD5. The man – in – the – middle attack can be avoided by the use of timestamp and IP address in the reply message.

In the following set of operation it is explained how the data could be make more secure. The owner of the data encrypts every file available in the frame of reference using MD5. The owner of the data used MD5 a 128 – bit hash instead of several other mechanism, *i.e.*, SHA – 1. It is done to ensure the integrity of data and because of the putting this digest alongside the file with by means of a symmetric key. The file is again encrypted with the public of the owner of the data, which results in more strength and security of the data instead of only using the SHA – 1. The data integrity and confidentiality of data is ensured by this means between the user and the owner of the data.

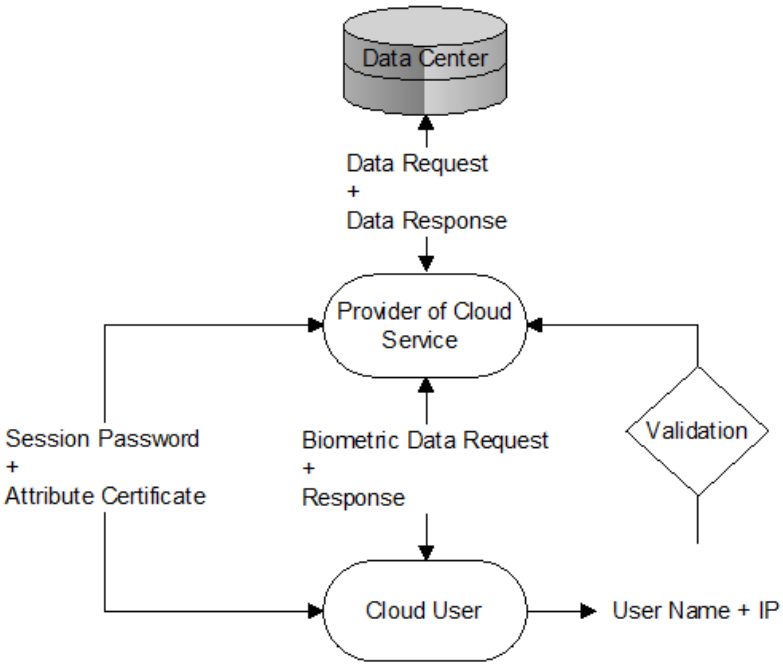

Figure 3. Multi – Step Authentication of Cloud User

The owner of the data subsequently propels the whole lot of data, encrypted with his private key, and after that employing the service provider public key in order to maintain the confidentiality and authentication among the provider of the cloud service and owner of the data. After receiving the encrypted files the provider of cloud service will use the public key of the owner of data and its own private key to decrypt the message and send the encrypted files to the data center for storage. The strength of our model is that the provider of the cloud services is unable to know the real contents of the data as the symmetric shared key is only know to the user and the owner. The design objective is accomplished by using this model as the actual data/information is only available to the data user and owner and not to the provider of cloud service, because it is to be had on a domain which is not trustworthy.

The accomplishment of an improved and protected data access for cloud environment, an exclusive access control is provided by means of another type of digital certificate known as the attribute certificate. The data structure of the attribute certificate is analogous to the identity certificate; on the other hand it does not contain any public key as opposed to identity certificate. Even though the sort of endorsement data possibly is positioned within additional fields of identity certificates, because does so, it has some fundamental causes. First of all, the authorities who issue these certificates are generally not accountable for the authorization information of this sort. Consequently, some additional steps are required to be taken by the certificate issuing authorities to acquire the information needed for the access control from the sources. On the other hand, the information needed for authorization may perhaps provide diverse life span for the requisite of public key and the identity. If the information of access control is placed in the extension of the identity certificate then it will shorten the life span of the certificate, whereas life span/validity prerequisite for the attribute certificate permit short and long – lived certificates.

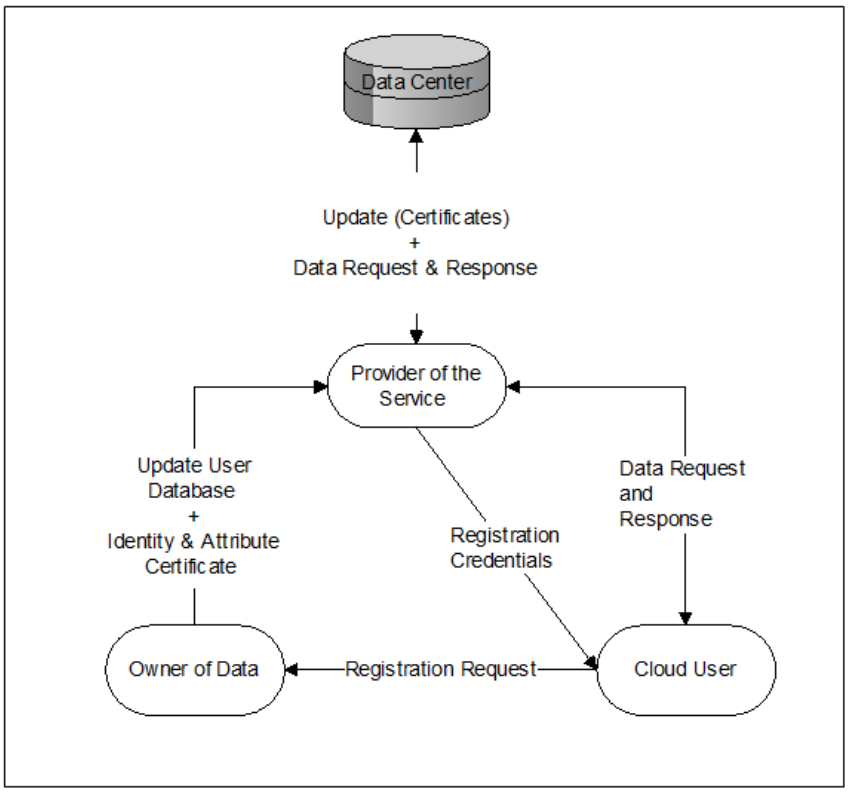

Figure 4. User Registration

The validity periods of attribute certificate generally may perhaps be calculated in hours, on contrary to identity certificate, for which the time calculated, is in months and years. The permissions for short validity periods attribute certificate can be changed in a little flexible manner if it is used in such a mechanism that no revocation is required. The attribute certificate which requires a longer life perhaps be used for authorization those are comparatively static. In such cases a common certificate issuing authority is liable to provide attribute and identity certificates. It is recommended that the attribute necessary for authorization is kept separate, but in some cases when the issuing authority is common it kept in the extension field of the identity certificate.

Subsequent the successful login of the user on to the cloud services, the certificate issuing authority issues identity, and attribute. The user request for the data access to data center through cloud services, the cloud service after verification of the attribute and identity certificate with the issuing authority, authorize the user to access data on the data center. Now the user is able to access the encrypted data as requested by the user. The user needs a decryption gizmo that is present in her/his personal user account. The gizmo will need a password to perform the decryption, which is automatically sent to the valid email address of the client which the access is granted to the client. The decryption gizmo will start the generation of the private key for the data encrypted, and then decrypt the data. The digest is calculated with the help of has function and check for the integrity of the message using the new digest and the one receive with the message.

4. Analysis of the Proposed Framework

The proposed scheme is being analyzed for the characteristics of security in this section.

4.1. Authentication and Authorization

The user is authenticated and authorized by a multi – factor and multi step approach at the cloud service center. All the interactions of the owner of the data and cloud service is also authenticated, the mechanism followed is, the owner uses his private key for the encryption of the scrambled data file, and the Cloud Services uses his public key to authenticate the owner of data. The authentication user of the data is performed with owner private key when adding a new client, while the owner authentication is performed at cloud service by the private encryption at cloud service with owner private key.

4.2. Data Confidentiality and Integrity

In order to perform the analyses of the data confidentiality for this proposed approach, it is compared with the already existing encryption techniques that use the symmetric keys. The provider of cloud service is unable to visualize the original data and digest of the owner as the key is symmetric and only shared among the user and data owner. The data after encryption with symmetric keys is once again encrypted with the private key of the data owner, and public key of the provider of cloud services. To wrap up the discussion that data is not available to be decrypted in to its original form by the cloud services.

The integrity is ensured for the data under consideration by employing the MD5 hash algorithm. The user of the data computes a fresh has and then match it up to the one already appended to the original data file. The integrity violation will be reported and the owner of the data will be informed accordingly, if the hash calculated by the user does not match to the original hash present in the message.

4.3. Access Control Based on Attribute Certificates

The authentication and authorization is based on a multistep process including the biometric data, other than that, in our proposed model, the access is further control on the bases of a second type of digital certificate i.e. the attribute certificate. The identity and attribute certificate can be created by owner of the data in certificate issuing authority center. The clients are issued certificates according to the nature of their request after successful login to the cloud service provide. The reason of using the attribute certificate is that, the earlier models were using access control lists, which may not be practicable for cloud computing environment [22, 23, 24]. Because the user needs are different, if one access one data file may not necessary accessed by other client so, creating of access control list for any data object is apparently difficult. In our approach we use attribute certificate which contain the necessary data structure of the data files for the access control.

5. Conclusion

The model proposed in this paper give power to the owner of the data to implement the security process on the data to be outsourced, and hence retain the control over the data. The model also proposed the combination of cryptography and access control to keep the data safe from vulnerabilities. A multistep, multi – factor authentication approach is employed for the authentication and authorization of the client, which increase the confidentiality and integrity of the data. The paper also presented the private key, hash and public encrypted ciphers among the owner, the client and the service provider which guarantee the isolation and safe execution of the cloud environment.

References

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: towards a cloud definition", ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, **(2008)**, pp. 50-55.
[2] S. Ullah and Z. Xuefeng, "Cloud Computing Research Challenges", In Proceedings of 5th IEEE International Conference on Biomedical Engineering and Informatics, **(2012)**, pp. 1397-1401.
[3] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing", In INFOCOM, 2010 Proceedings IEEE, IEEE, **(2010)**, pp. 1-9.
[4] L. Yousef, M. Butrico and D. Da Silva, "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, GCE '08, **(2008)**, pp. 1-10.
[5] Z. Shen and Q. Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", In Proceedings of 2nd International Conference on Signal Processing Systems, **(2010)**, pp. 11-15.
[6] R. L. Grossman, "The Case for Cloud Computing", IT Professional, vol. 11, no. 2, **(2009)**, pp. 23-27.
[7] S. Ullah, Z. Xuefeng and Z. Feng, "TCloud: Challenges and Best Practices for Cloud Computing", International Journal of Engineering Research and Technology, vol. 1, no. 9, **(2012)**, pp. 01-05.
[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, **(2011)**, pp. 1-11.
[9] Di Vimercati, S. De Capitani, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati, "A data outsourcing architecture combining cryptography and access control", In Proceedings of the 2007 ACM workshop on Computer security architecture, ACM, **(2007)**, pp. 63-69.
[10] W. Wang, L. Zhiwei, R. Owens and B. Bhargava, "Secure and efficient access to outsourced data", In Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, **(2009)**, pp. 55-66.
[11] S. Kamara and K. Lauter, "Cryptographic cloud storage", Financial Cryptography and Data Security, **(2010)**, pp. 136-149.
[12] J. Dai and Q. Zhou, "A PKI-based mechanism for secure and efficient access to outsourced data", In Networking and Digital Society (ICNDS), 2010 2nd International Conference on, vol. 1, **(2010)**, pp. 640-643, IEEE.
[13] G. Zhao, X. Hu, Y. Li and L. Du, "Implementation and testing of an identity-based authentication system", In Computing, Communication, Control, and Management, 2009, CCCM 2009, ISECS International Colloquium on, vol. 4, IEEE, **(2009)**, pp. 424-427.
[14] E. -J. Yoon and K. -Y. Yoo, "Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc", InComputational Science and Engineering, 2009, CSE'09, International Conference on, vol. 2, IEEE, **(2009)**, pp. 633-640.
[15] J. Wiebelitz, S. Piger, C. Kunz and C. Grimm, "Transparent identity-based firewall transition for eScience", In E-Science Workshops, 2009 5th IEEE International Conference on, IEEE, **(2009)**, pp. 3-10.
[16] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, **(2012)**, pp. 583-592.
[17] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software platforms", Computers & Security, **(2011)**.
[18] H. Li, Y. Dai, L. Tian and H. Yang, "Identity-based authentication for cloud computing", Cloud Computing, **(2009)**, pp. 157-166.
[19] G. Miklau and D. Suciu, "Controlling access to published data using cryptography", In Proceedings of the 29th international conference on Very large data bases, vol. 29, VLDB Endowment, **(2003)**, pp. 898-909.

[20] D. Naor, A. Shenhav and A. Wool, "Toward securing untrusted storage without public-key operations", In Proceedings of the 2005 ACM workshop on Storage security and survivability, ACM, **(2005)**, pp. 51-56.
[21] E. -J. Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing remote untrusted storage", NDSS, **(2003)**.
[22] H. Ahn, H. Chang, C. Jang and E. Choi, "User Authentication Platform using Provisioning in Cloud Computing Environment", Advanced Communication and Networking, **(2011)**, pp. 132-138.
[23] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage", NDSS, **(2005)**.
[24] R. Blom, "An optimal class of symmetric key generation systems", In Advances in Cryptology, Springer Berlin/Heidelberg, **(1985)**, pp. 335-338.

Authors

Sultan Ullah

Sultan Ullah, received MSc and MS degrees in computer science from Sarhad University, Peshawar in 2004 and 2010 respectively. He is currently a PhD candidate at the School of Computer and Communication Engineering, University of Science and Technology, Beijing. His research interest includes Access Control, Network Security, Information Security and Cloud Computing Security. He is a member of the International Association of Engineers.

Prof. Dr. Zheng Xuefeng

Zheng Xuefeng, was born in 1951, is professor and doctoral supervisor in the School of Computer and Communication Engineering, University of Science and Technology Beijing. His research interest includes Computer Control Systems Development, Computer System Security Analysis, Network Security, Information Security and Distributed Systems Security. He is the senior member of the computer society.

Dr. Zhou Feng

Zhou Feng, is an associate professor in the School of Computer and Communication Engineering, University of Science and technology Beijing. She got the PhD degree from University of Science and Technology Beijing in 2009. Her research interest includes Computer Network Technology, Network Security, and Distributed System Security. She is the member of the computer society.