International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 04, April 2016
www.ijates.com
ijates
ISSN 2348 - 7550

STUDY ON SECURITY MANAGEMENT WITH OTP USING CLOUD COMPUTING

Praveen Kumar Shrivastava[1], Vibha Sahu[2], Dr. S.M.Ghosh[3]

[1,2]Rsearch Scholar, Department of Computer Application,
Dr. C.V.Raman University, Bilaspur Chhatishgarh (India)
[3]Professor, Department of Computer Science & Engineering,
Rungta College of Engineering & Technology,Bhilai, Chhatisgarh,(India)

ABSTRACT

For the information security issues of cloud computing, this paper study's the security management methods of cloud computing authorized user, analyzes the vulnerabilities of OTP and proposed security authentication scheme based on OTP authentication in cloud computing application. This authentication enables two-way authentication between the user and the service provider, effectively prevent middleman attack, reduce information leakage and relies secure communications. This paper also deals the authentication management like security audit mechanism, access control mechanism with the use of OTP.

Keywords: Security Management Method, Cloud Computing, Anonymous OTP, Authorized User.

I.INTRODUCTION

Cloud computing is an Internet-based computing, via Network provides individuals and businesses demand is taking computer resources anytime, anywhere access to the network, storage, server and application software, programs, etc. can be configured with large-scale, virtualized, scalable resistance, high reliability, dynamic allocation, affordable, etc., for people to provide a huge market space, the new information service model, but because of its large number of users, information resources highly concentrated. The security issues brought by cloud computing have become a hot field of security, and authentication is the foundation of information security, the security system is the first hurdle, but also to ensure the security of cloud services is an important aspect. OTP is a simple authentication technology that can be quickly loaded onto the system without the need for any additional hardware. It uses a one-time pad method can effectively guarantee the security of user identity, at the same time, it does not require third-party notarization low cost, suitable for network environment is not yet mature, but its existence decimal vulnerable to attack, middle attack security vulnerabilities, therefore, requires the use of certain methods to make it safe and reliable .

II.THE AUTHENTICATION BASED ON CLOUD COMPUTING

In the identification of cloud storage, the user as long as the cloud storage server information to prove their identity to access cloud, is a one-way authentication, secure cloud identity authentication methods are mainly based on the user identity module (SIM) authentication (using the Global system for Mobile

Communications GSM \ GPRS General Packet Radio Service subscriber identification module), based on public key infrastructure (PKI) authentication and password-based authentication three authentication methods. Which is the traditional password authentication, allowing the user to provide a password can prove their identity, in the transmission process vulnerable to third party attacks, for which there has been the challenge and response authentication based on one-time passwords. OTP authentication, the user initiates an authentication to the server each time, when random numbers and messages are transmitted in clear text and therefore cannot resist the middleman spoofing attacks seeds and hackers to intercept the server iteration value coming ', and modify the iteration value, using known Kazakh dilute function H ( ) successively larger iterative calculation values obtained subsequent one-time password to the user to achieve the decimal attack 'an improved method for the above-mentioned problems are: the use of two random numbers, so that each authentication the data is more difficult to guess and forgery, while using elliptic curve cryptosystem on-line transmission of plaintext, a random number, user information such as encryption secret phrase, achieve mutual authentication of users and servers, there by preventing the middleman spoofing attacks.

III. THE DEFINITION AND CHARACTERISTICS OF OTP

One-time password (abbreviated OTP) authentication technology based on the cryptography basis, by adding uncertainty factor in the certification process, so that every time a user authentication password authentication are not the same, and each authentication password is used only once. OTP authentication technology authentication method for one-time pad can effectively ensure the security of user identity. Compared with static password authentication technology, the main features of OTP authentication technology are as follows:

- Dynamics : A one-time password can be set with equal time or event variables change automatically, without human intervention.
- One-time : Password again effective, so too the password cannot be reused, even if the password is tapped, it will not cause great danger, therefore, it has a good anti-wiretapping.
- Random : Randomly generated one-time password, without the law, the increase the difficulty of cracking.
- Multiple security: A single static password authentication in different ways, OTP one-time password authentication technology with a user name and static password and other multiple factors combined to achieve certification.

IV.SECURITY ANALYSIS OF OTP AUTHENTICATION MECHANISMS

Password authentication mechanism security threats mainly from eavesdropping attacks, password guessing attacks, replay attacks and password leaks and other. OTP authentication mechanism for static password authentication mechanism insecurity put forward, therefore, the defense said in password security threats than static password authentication mechanism has a higher security. However, there are some security issues of OTP authentication mechanism, including [3].

A. There is no two-way authentication:

OTP authentication mechanism is a one-way authentication mechanism, only one-way authentication server to the client, the server cannot guard against counterfeit deceive legitimate users. If an attacker intercepts the authentication server information, he could use the database to steal passwords and other means of reproduction posing server deceive clients.

B.It is vulnerable for decimal attacks:

OTP authentication mechanisms vulnerable to attack decimal specific process: When a client requests authentication to the authentication server, an attacker can eavesdrop on information intercepted by a network authentication server transmits the challenge and modify the internet to a small value, then the server will intercept counterfeit seed and smaller internet to clients. Clients use the attacker's Seed and internet transmission time password calculated and transmitted to the server. Again attacker intercepts one-time password sent by the client, and using the known one-way hash function to calculate a one-time password sequentially larger internet, access to user passwords successor series, so the attacker can impersonate legitimate users this is the decimal attacks.

C.It is difficult to resist the middle attack:

OTP authentication mechanism is difficult to resist the middle attack, specific process: An attacker located between the client and server-side authentication information may be intercepted, one fake client and server-side connection, on the other hand fake server connections with clients. Client login transfer one-time password to the server, an attacker can intercept one-time password, so that the client cannot log on, causing the network connection is lost, the connection timeout illusion, at the same time, you can use the intercepted one-time password to log into the fake client Service-Terminal. In addition to the main security issues, OTP authentication mechanisms are also other security issues, such as: storage of client and server-side data, lack of confidentiality of sensitive security measures, illegal theft of easily; the mobile client frequently is reinstalled, it will not appear Iteration synchronization problems cause cannot achieve certification. Security risks OTP authentication mechanism mainly involved in one-time password generated random number and authentication information are transmitted in clear text, so if you take cryptosystem random number and the authentication information is encrypted, attackers bound to bring great difficulties.

V. THE MAIN SECURITY MANAGEMENT MECHANISM OF CLOUD COMPUTING AUTHORIZED USERS AUTHENTICATION MECHANISM

The rapid development of cloud services brings massive access authentication request and complex authentication scenario, a variety of certificate-based security authentication technology. "Cloud" stores a lot of sensitive data, once the user identity is phishing, likely to cause data leakage. How cloud services confirm the true identity of the user, such as ensuring the physical identity and digital identity visitor consistency problem is a cloud service provider primary problem. Usually it is identified by the identification of those who share the same secret, such as passwords and so on. Cloud terminal interacts with the user to obtain information about their identity, and information submitted to the authentication server, the authentication server for user identity information and database information obtained for comparison to determine the user based on comparison results identity is legitimate. Cloud services to confirm user identity, to

a certain extent, to ensure the integrity, confidentiality, and security access control data .In the user authentication process, objects covered include: user providing identity information is verified by; the authentication server to verify the identity information is legitimate; third-party service providers offer arbitration and mediation; data assailant attempt disguise the identity of the impostor; authentication device user computing hardware and software device password. User authentication is generally through multiple factors come together to identify, the more discriminating factor authentication greater reliability. Three common factors include: the user knows a password and password; the user has a credit card or U Shield; the user has fingerprint, Signature, retina, etc. Currently password-based password authentication technology is the most widely used, it has the advantage that without the aid of third-party service providers, the authentication mechanism is simple to use. The disadvantage is that the password mechanism is simple, cloud server once being attacked, the user password is easy to be exposed to the attacker. To improve the security of authentication, password-based authentication can be based on two factors, the user only to have the private key file, but also to know the private key, both of which must be met in order to pass the identification, but this requires a third-party CA to ensure its trusted content. The problem is that if untrusting third-party service providers can not ensure the security key. Deploying cloud services make data security beyond the scope of performance beyond the control of the computer field, extending to the cloud service provider in the field. Users of cloud services to lose control of the information, trust relationships between users and other organizations are now ported to a cloud environment, so cloud service providers can obtain identity information resulting in data loss. Authentication technology exists in its three service models each level security requirements for cloud computing, but with different security problems IaaS, PaaS and SaaS service model on each face. No matter how perfect the authentication mechanism, it is in a complex environment of cloud computing will always face new challenges.

VI. SECURITY AUDIT MECHANISM

Security audit mechanism must rely on network security, data security can be improved, is an important means to ensure the security of cloud service network. All active security audit records of user access, and ultimately the formation of audit data through data analysis found loopholes in the system or the relatively weak link, it is determined whether the network is abnormal or attacked and attacked the node, which has a reference value for retroactive attack source. Security audit is similar to "black box" on the plane, it can not only forecast and warn before the crisis, but also can automatically save the user's illegal operation and operating time. Security audit mechanism will automatically record the normal operation of the user, in a cloud computing environment, some users of the normal operation of the server happens to be attacking an illegal operation. "Cloud Audit" is a service that can IaaS, PaaS and SaaS three service models audit, help solve the problem of the credibility of users of cloud computing. With the "cloud audit" to reduce the cloud data environment is unknown super-user access, data storage location is unknown, data cannot be long-term use, the data cannot be recovered, the data cannot be really isolated, data compliance checks and other risks. Security audit include detection, prevention, investigation, analysis four processes. Detection module detects the user's finger which is operating in violation of the safety rules of conduct; defense module means to ensure the security of data in the cloud through secure authentication technology; Survey

module data were analyzed by means of the detection module, the survey carried out in violation of the current operation of the user and intrusion attempts; analysis module refers to the data analysis module for the survey what protective measures have to face the same illegal operations will be taken to deal with the intrusion. Currently a large part of the cloud service provider refuses to provide real-time monitoring data and audit logs, audit information did not lead to effective assistance of safety monitoring accuracy, and data stored in the cloud to any corner of the world, users do not know the cloud service provider specific details of the operation providers to store data, security audit mechanism in a cloud computing environment also faces enormous challenges.

VII. ACCESS CONTROL MECHANISMS

Access control technology is to protect the security of cloud computing environments basic technology, which includes access control system for cloud computing, network and data resources, it is to prevent a cloud service system is the first line of defense against unauthorized access. Cloud computing systems need access control mechanisms to maintain their complex network environments while reliably support multi-user information belongs to the isolation and security of different sectors. In the access control process, objects covered include: body - their own people to perform the operation or process; object - files or other resources (such as equipment, directories, etc.). Common access control modes include discretionary access control, mandatory access control, role-based access control. Discretionary access control mechanism, the access policy is there to decide what the main object of the owner or having access to a higher authority. But discretionary access control process rights management more difficult, and cannot be applied to the number of users is large. Role-based access control access policy is determined by the user only when the subject of "permission set" consent, the subject can access an object or perform the corresponding function. Mandatory access control access policy is determined by the system, it can achieve the label assigned to each subject and object. The body of credit on behalf of its level, object label represents its access objects necessary level of trust. For example, the body to achieve access to the object, the subject must be capable of higher level label or tag and other objects. Mandatory Access Control mode is more conducive to the expansion of data security in the cloud computing environment more often.

VIII. CONCLUSION

In cloud computing environment the user has a great responsibility for the secure of cloud data. User safe behavior certification is the effective technology way to ensure cloud service system security operation. With secure authentication technology we can detect an illegal operation and malicious acts or potential security vulnerabilities. In this paper, we gave an in-depth research on the existing user security management system, analysis the categories of safety management system and characteristics of the various management techniques and provide the security management methods of cloud computing authorized users based on anonymous OTP.

REFERENCES

[1]. 5th International Conference on Computer Sciences and Automation Engineering (ICCSAE 2015).
[2]. Shen Changxiang. Information Security And Communication Security,Vol.12 (2010)No7,p.12-15.
[3]. Bian Genqing. Journal of Xi'an Jiao Tong University, Vol. 3(2005) No 6, p.335-356.
[4]. Zhang Fengzhe. Computer research and development, Vol. 46(2010) No 4,p.256-280.
[5]. Qin Zhiguang. Computer Application, Vol. 32(2010) No 3, P.118-144.
[6]. Chen Haibo: Computer Application, Vol. 12(2003) No 12, p.11-124.