A Review Paper on Security in Cloud Computing

Priyanka S P
Department of Computer Science and Engineering ,AIET
AIET, Mangalore, India

Ranjith
Department of Computer Science and Engineering ,AIET
AIET, Mangalore, India

Shridevi Prabhu B S
Department of Computer Science and Engineering ,AIET
AIET, Mangalore ,India

Nalini
Department of Computer Science and Engineering, AIET
AIET, Mangalore ,India

Prof.Vasudev S Shahapur
Department of Computer Science and Engineering ,AIET
AIET, Mangalore ,India

***Abstract* - There is a significant increase in the amount of data loss in corporate servers in the cloud environments. This includes password compromise in the cloud and account hijacking, thus leading to severe vulnerabilities of the cloud service. Current authentication methods require the users to use their credentials to gain access to cloud service. However once the credential is compromised, the attacker will gain access to the cloud service easily. This paper proposes a novel scheme that does not require the user to present his password, and yet is able to prove his ownership of access to the cloud service using a variant of zero-knowledge proof. A challenge-response protocol is devised to authenticate the user, requiring the user to compute a one-time pad (OTP) to authenticate himself to the server without revealing password to the server.**

Index Terms - Cloud computing, zero-knowledge proof, one-time pad.

I. INTRODUCTION

Cloud is a ubiquitous computing technology dependent on geographically distributed computing entities like storage servers, dedicated systems and software. A cloud environment has dedicated systems, servers to provide the service promised by the service providers [1]. Cloud computing is an infrastructure in which computing power and storage are managed by remote servers to which users connect via a secure Internet link. A desktop or a laptop, a mobile phone, a tablet computer and other connected objects have become access points to run applications or view data hosted on these servers [6] Cloud computing have characteristics such as: 1) Device and location independent: these are enable user to access system using a web browser regardless of their location or what they use (e.g., PC mobile phone).and access via the internet, users can connect to it from anywhere. 2)
Maintenance: on each user's computer no need to install cloud computing application. These are access from different places. 3) Multitenancy: resources are share across large number of users [3]. As cloud computing is gaining more popularity, more importance is given to security issues such as, authentication, access control, storage, storage security and virtualization. Secure user authentication is one of the main necessities of cloud computing in order to avoid loss for a cloud service provider and to provide secure service to the valid user [1].

The major problems associated with cloud system are:

1. Data Breaches

Data breach is an incident that has potential to disclose sensitive information to an unauthorized party. Data breaches may be caused by a variety of reasons such as theft. In the era of cloud computing, data breaches is one of the major security concerns found in the literature. There were plenty of incidents of this kind in the history of computing and of late the cloud computing[9]

2*. Hijacking of Accounts*

Account or service hijacking is a kind of identity theft has evolved to be one of the most rapidly increasing types of cyber attack aimed at deceiving end user's.[11]

3. *Insider Threat*

A severe threat, that modern information systems and critical infrastructures need to address, is the insider threat. In general, the insider threat is defined as a person who has the appropriate access rights to an information system and misuses his privileges.[10]

4. *Malware Injection:*

In Cloud Malware Injection Attack an attacker tries to inject malicious service or virtual machine into the cloud. In this

type of attack attacker creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and try to add it to the Cloud system. Then, the attacker has to behave so as to make it a valid service to the Cloud system that it is some new service implementation instance among the valid instances. If the attacker succeeds in this, the Cloud automatically redirects the requests of valid user to the malicious service implementation, and the attacker code starts to execute. The main scenario behind the Cloud Malware Injection attack is that an attacker transfers a malicious service instance into cloud so that it can achieve access to the service requests of the victim's service.

5. *Abuse of cloud service*

The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties. In some cases this practice affects both the cloud service provider and its client. For example, privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider.

6. *Vulnerable Systems and APIs*

Cloud APIs (Application Programming Interfaces) represent an open door for public to your cloud application. Exploiting a cloud API can grant an attacker considerable access to cloud resources. Cloud Service Providers (CSP) exposes a set of software user interfaces or APIs that customers use to interact with cloud services. Those APIs should be designed to protect against accidental and malicious attempts.[12]

7. *Denial of Service Attacks*

A DoS (Denial of Service) attack as shown in Figure 3, effects the availability of a system. In a DoS attack, there is only one source machine from which the attack originates and it is susceptible to mitigate. DoS attacks are designed to prevent legitimate users of a service from being able to access their data or applications.[12]

8. Weak Authentication and Identity Management

Organizations or enterprises often encounter difficulty with identity management as they try to allocate appropriate permissions to every user's job role. The Anthem Inc data breach resulted in cyber criminals accessing 80 million records of personal and medical information. This attack was the result of stolen user credentials. Attackers masquerading as legitimate users, operators or developers can access and modify data, issue control plane and management functions, sniff data in transit, or inject malicious software that appears to originate from a legitimate source[12]

9. Shared Technology Vulnerabilities

Cloud computing provides multi-tenancy where multiple users share different cloud resources. Underlying components that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multi-tenant architecture or multi-customer applications. This can lead to shared technology vulnerabilities related to Virtual Machines (VMs), operating systems, hypervisor, etc. A vulnerability or misconfiguration in a shared platform component can allow an attacker to compromise the cloud data security of many or all customers, resulting in a data breach. Best practices around client implementation and data management help protect against shared technology vulnerabilities.[12]

10 Data Loss

It is corruption or unavailability of data which results due to natural disasters like floods, earthquakes; and simple human errors like when a cloud administrator accidentally deletes files, hard drive failure, power failure, or due to malware infection. To avoid data loss, the most efficient strategy is to backup data to multiple locations so that even when data gets corrupted or lost at one location, it can be replaced with a copy available at another location.[12]

II. RELATED WORK

In this section, a number of papers are reviewed which have worked on security parameter for cloud computing.

In Cloud computing the registration of a new user and the future login are dependent on the credit card details and the user's email address [3]. Hence there is a need for much secure authentication schemes both for the development of the Resource Provider and the user.

Dr. G. Jaspher Willsie Kathrine proposed a secure biometric based authentication scheme which provides secure user identification, mutual authentication, session key issue and proxy issue in cases where a single cloud service provider (SP) provides more than one service. Cryptographic algorithm such as Elliptic Curve Cryptography is used for secure key generation and exchange. But biometric authentication systems are not 100% accurate. There are two types of errors in a typical biometric system. A false reject (FR) error is the rejection of an authorized person trying to access the system. A false accept (FA) error is the acceptance of a person who is not in fact who he or she claims to be [1].

Shefali Ojha proposed an authentication based AES and MD5 technique to secure data and login of user over cloud. In this paper they propose present technique of encryption and decryption for data at the time of login but there is no authentication provided at the given time of login. Due to only basis of trust value security is not provided [2].

Ms. Neha Kalkhar proposed a method where privacy preserving protocol is used in cloud computing for secured access. In this work using SAPA protocol a new privacy challenge is identified during data accessing in the cloud

computing to achieve privacy preserving access authority sharing. ECC algorithm and multiple key used for reencryption purpose for sharing file with numbers of user therefore confidential transaction are achieved. A secure system for encrypted transaction is made and tested against attack [3].

Slawomir Grzonkowski and Peter M. Corcoran presented a novel authentication protocol that is suitable for cloud-based services. In comparison with existing solutions such as Kerberos, this protocol does not require physical tokens and it is not prone to replay attacks; also, there is no shared password between the user and the authentication service: this part is based on a password-based zero-knowledge proof based protocol that we developed earlier [9].
P. Tobin, L. Tobin, R. Gandia Blanquer, M. McKeever, J. Blackledge presented a paper where they we examine the design and application of a one-time pad encryption system for protecting data stored in the Cloud. Personalizing security using a one-time pad generator at the client-end protects data from break-ins, side-channel attacks and backdoors in public encryption algorithms. The one-time pad binary sequences from modified analogue chaos oscillators initiated by noise encoded client data locally.

III PROPOSED SYSTEM

This section describes the architectural overview of the proposed authentication protocol.

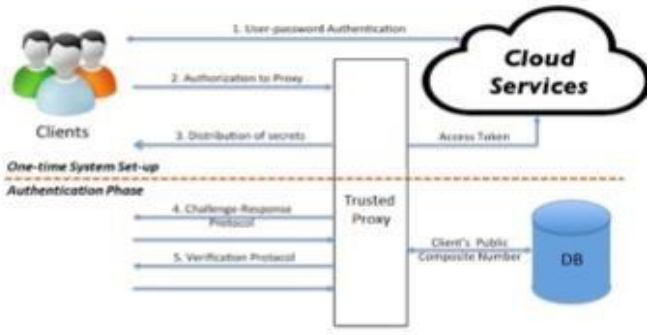

Fig. 1. System Architecture of the cloud-based authentication protocol

As illustrated in Figure 1, we introduce a trusted proxy for cloud services such as Dropbox, to handle authentication using our novel challenge-response protocol that is based on prime number factorization. The system is first set-up by requiring the client to authenticate itself to the cloud service using the normal user-password authentication protocol, and then requests for an access token. It then authorizes the trusted proxy to mediate the authentication between himself and the cloud service, by passing the access token to the trusted proxy. In this one-time set-up phase, two secrets, which are randomly generated large prime numbers are distributed to the client, together with a client secret, to be stored in a secure storage. A public composite number, which is the product of the two prime numbers is stored in the trusted proxy to identify the client. Knowing this composite number does not reveal any information about the secret prime numbers.

Once this proxy-based cloud authentication has been setup, all subsequent authentication will not require the user to transmit its username-password, but a security challenge will be issued to the client based on the composite number, and a residue computed based on the client's secret. Only the correct response which must be generated using the client's secrets will be accepted. The challenge is generated using a random number that is 3072 bits long, and hence ensuring that each access request is unique and will not be re-used. The database is used to store the mapping of the public composite number to the corresponding user account. Using this protocol, the clients do not need to use their username-password to perform authentication anymore.
The following sections describe the security requirements to be achieved, the procedure of generating the security parameters and the details of the challenge-response protocol for cloud authentication.

A. Security Requirements

This section outlines the security requirements for cloud authentication.

- Transmission of password – the client must not be required to transmit its password to the server for authentication.
- Storing of password – the trusted proxy which mediates the authentication should not store the user's password, but only public information that even if it is compromised, the client's confidential credential is not revealed.
- Secrets with high entropy1 – Access to the cloud services should be based on secrets distributed to the client, which have high entropy. A master password maybe required to grant access to the client to retrieve these secrets. Alternatively, the secrets may be stored using a hardware token, e.g., a secure USB that should be in possession of the client.

B. Generation of Security Parameters

The security of system is based on large prime factorization.

- Two large prime numbers (Pii, Pij) – are randomly generated for each client. The generated prime numbers must be at least 1024-bit. These two primes form two parts out of three of the client's secret.
- Public composite number (Ni) – is a product of the primes, Pii x Pij. Ni is public, and it is stored in the database hosted by the trusted proxy.
- Secret (s) – is a randomly generated number that is coprime with the composite number Ni. s is generated such that it is $1 < s < Ni$. Essentially, s forms the third part of the client's secret.
- Residue (Ii) – is generated as $Ii = s2 \bmod Ni$. Similarly, this residue is public, and it is known to the trusted proxy and is used for verification of the client's secret,

s. The primes and the secret,(Pii, Pij, s)are distributed to the client, and these secrets must be stored in a secure storage of the client, while the public information (Ni, Ii) are distributed to the trusted proxy, and they are mapped to the client's cloud service account for identification.

C. Challenge-Response Authentication Protocol Figure 2 shows the sequence diagram of the challenge response protocol for authenticating the clients. Assuming that the client has been configured with the secrets, and the public information are mapped to the client's account. When the client requests to read/write/modify/download its files on the cloud service, the trusted proxy generates a session challenge X with the following:

$X = y2 \bmod Ni$ (1)

Where y is a random number per access request, and it is typically 3072-bit. Upon receiving the challenge, the client accesses its secrets, and compute the following:

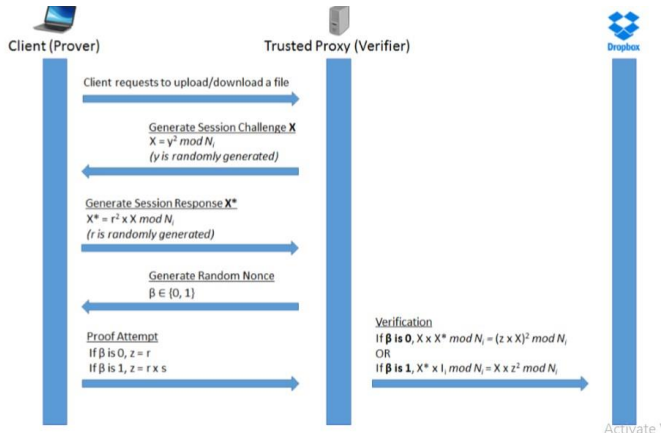

Fig. 2. Challenge-Response Protocol for cloud authentication

$X* = r2 \times X \bmod Ni$ (2) where r is also a randomly generated number with the same length as y. Ni can be derived by multiplying the two secret prime numbers in possession of the client. X* is then sent back to the trusted proxy for verification. This serves as a commitment of authentication for the access request. The trusted proxy then generate a random $\beta \in \{0, 1\}$, in order to verify the client. Depending on the value of β, the client generates a different response to authenticate itself. If $\beta = 0$, then the client returns the previously generated random number, $z = r$. Conversely, if $\beta = 1$, the client computes:

$$z = r \times s \quad (3)$$

At the trusted proxy, the verification is performed depending on the value of β. When $\beta = 0$, it does not require the client to use the third part of its secret, s, and by returning a correct $z = r$ is sufficient. This is because r which was committed as part of X* must have been generated by the correct client that possesses the authentic prime numbers (Pii, Pij). The trusted proxy verifies z such that it satisfies the following equation:

$$X \times X * \bmod Ni = (z \times X)\ 2 \bmod Ni \quad (4)$$

Essentially, this is equivalent to $y4 \times r2 \bmod Ni$. On the other hand, if $\beta = 1$, this requires the client to use the third part of its secret, s to compute the response z. The received z must satisfy the following:

$X* \times Ii \bmod Ni = X \times z2 \bmod Ni$ (5)

Which results in $y2 \times r2 \times s2 \bmod Ni$.

VI. CONCLUSIONS AND FUTURE WORK

This paper has proposed a novel challenge-response protocol to authenticate clients that utilize cloud storage in a secure and economical means. With the security concerns, we have proposed an authentication scheme similar to OTP that is based on prime factoring hard problem; we have also devised and implemented a practical challenge-response protocol to allow for each access request from the client to be authenticated without requiring the client to transmit his password.

Through preliminary experiments, we have also shown that the proposed solution incurs reasonable amount of overhead and its performance can be scaled up by deploying multiple proxy nodes, and this is particularly useful for meeting the requirements of the enterprise tenants, where it can better support performance oriented applications for large scale enterprises.

REFERENCES

[1] A secure framework for enhancing user authentication in cloud environment using Biometrics Dr. G. Jaspher Willsie Kathrine Karunya University meet.katee@gmail.comM. King, B. Zhu, and S. Tang, "Optimal path planning," *Mobile Robots*, vol. 8, no. 2, pp. 520-531, March 2001. [2] Implementation of Re-encryption Based Security Mechanism to Authenticate Shared Access in Cloud Computing Ms.Neha Mahakalkar Department of Computer Science and Engineering G.H.R.I.E.T, Nagpur Nagpur, India nehamahakalkar@gmail.com.

[3] AES And MD5 Based Secure Authentication In Cloud Computing by Shefali ojha CSE department, LNCT college Bhopal shefaliojha09@gmail.com.

[4] Token-Based Policy Management (TBPM): A Reliable Data Classification and Access Management Schema in Clouds by Faraz Fatemi Moghaddam*,†, Philipp Wieder*, Ramin Yahyapour.

[5] A multifactor authentication system using secret splitting in the perspective of Cloud of Things
Rohan H. Shah, Prof. D. P. Salapurkar Department of Computer Engineering, Sinhgad College of Engineering Savitribai Phule Pune University.

[6]TowardsaNewSecurityApproachBasedonHeartbeatAuthenticationtoEnsure Security of Cloud Data Access Hamza Hammami University of Tunis El Manar Faculty of Sciences of Tunis LIPAH-LR11ES14, 2092 Tunis, Tunisia Email:hamza.hammami@aol.fr

[7] An Effective User Revocation for Policy-Based Access Control Schema in Clouds Faraz Fatemi Moghaddam*,†, Philipp Wieder*, Ramin Yahyapour*,†

[8] A Review: Cryptography and Steganography Algorithm for Cloud Computing

[9] DATA BREACHES AS TOP SECURITY CONCERN IN CLOUD COMPUTING Govind Rao Mettu1 Dr Anitha Patil2 Computer Engineering,Pillai HOC College of Engineering and Technology,Rsayani,

Inida Computer Engineering,Pillai HOC College of Engineering and Technology,Rsayani, Inida
[10] Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E.: The insider threat to Information Systems and the effectiveness of ISO 17799. Computers & Security 24(6), 472–484 (2005)
[11] Analysis and prevention of account hijacking based incidents in cloud environment, Sreenivas Srimath Tirumala,Auckland University of Technology ,Auckland, Newzeeeland
[12]Threats and Vulnerabilities of Cloud Computing: A Review
P.S. Suryateja CSE Dept., Vishnu Institute of Technology, Bhimavaram, India