Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multi-factor Authentication in Cloud Computing for Data Storage Security

Deepa Panse
Assoc. Prof. CSE Dept.
GCET, Keesara
JNT University, Hyderabad, India

P. Haritha
Asst. Prof. CSE Dept.
GCET, Keesara
JNT University, Hyderabad, India

Abstract: Cloud computing is an internet-based computing, where a set of resources and services such as applications, storage and servers are delivered to computers and devices through the Internet. It incorporates large open distributed system, virtualization, internet delivery of services, dynamic provision of reconfigurable resources and on-demand operations. Cloud Computing is continuously growing and showing consistent growth in the field of computing. The major challenging task in cloud computing is the security and privacy issues caused by the outsourcing of infrastructure, sensitive data and critical applications and its multi-tenancy nature. The security for Cloud Computing is emerging area for research work and this paper discusses various types of authentication methods and multi-factor user authentication.

Keywords: Cloud Computing, Multi-factor Authentication, Cloud threats, Data Security.

I. INTRODUCTION

As per the definition provided by the National Institute for Standards and Technology (NIST)[3], Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud model is composed of three service models, four deployment models and five essential characteristics.

A. Service Models

1) ***Software as a Service (SaaS):*** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
2) ***Platform as a Service (PaaS)****:* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
3) ***Infrastructure as a Service (IaaS):*** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications [3].

B. Deployment Models

1) ***Private cloud:*** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2) ***Public cloud:*** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
3) ***Hybrid cloud:*** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
4) ***Community cloud:*** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises [3].

C. Essential Characteristics

1) ***On-demand self-service****:* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2) ***Broad network access:*** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3) ***Resource pooling:*** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.
4) ***Rapid elasticity:*** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
5) ***Measured service:*** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [3].

Figure 1 show the Cloud Architecture reference model composed of three service models, four deployment models and five essential characteristics**.**

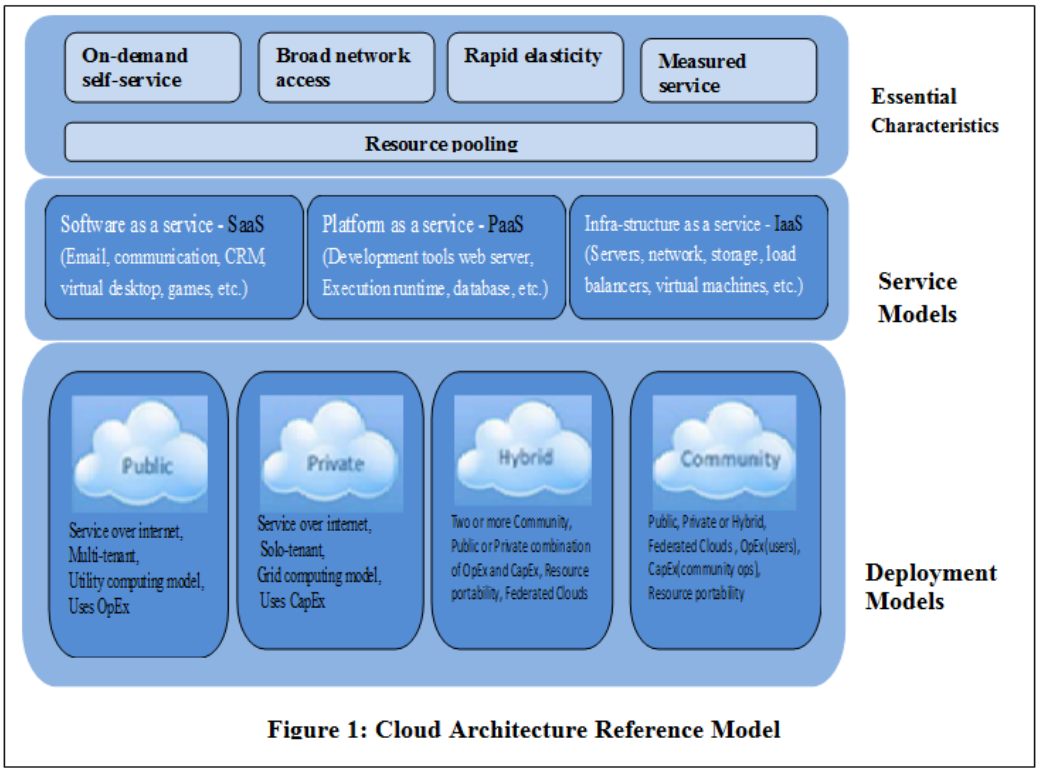

Figure 1: Cloud Architecture Reference Model

II. SECURITY THREATS IN CLOUD COMPUTING

Top nine security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) [7] published in February 2013 are:

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

Cloud service users use delivered services and resources through service models. The lack of a clear definition and classification of responsibility among cloud service users and Providers may induce conceptual conflicts. The security threats [10] in cloud computing can be categorized into the following two classes:

- Threats for Cloud Service Users
- Threats for Cloud Service Providers

A. Threats for Cloud Service Users:

The Security threats in this category include Responsibility Ambiguity, Loss of Governance, Loss of Trust, Service Provider Lock-in, Unsecure Cloud Service User Access, Lack of Information/Asset Management, Data loss and leakage etc.

B. Threats for Cloud Service Providers:

The Security threats in this category include Responsibility Ambiguity, Protection Inconsistency, Evolutional Risks, Business Discontinuity, Supplier Lock-in, License Risks, Bylaw Conflict, Bad Integration, Unsecure Administration API, Shared Environment, Hypervisor Isolation Failure, Service Unavailability, Data Unreliability and Abuse Right of Cloud Service Provider etc.

III. SECURITY ISSUES IN CLOUD COMPUTING

The security issues [1, 9] in cloud computing can be categorized into the following three classes:

- Traditional security issues
- Availability issues
- Third party data control-related issues

A. Traditional Security Issues:

These security issues involve computer and network attacks or intrusions that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their safety measures and security processes are full-grown and tested than those of the usual company. Concerns in this category include VM-level attacks, Cloud service providers' vulnerabilities, Phishing cloud provider, expanded network attack surface, Authentication and authorization, Forensics in the cloud.

B. Availability issues:

These concerns center on data and critical applications being available. Well-publicized incidents of cloud outages include Gmail's one-day outage in mid-October 2008 (Extended Gmail Outage), Amazon S3's over seven-hour downtime on July 20, 2008 (Amazon S3 Availability Event, 2008), and FlexiScale's 18-17 hour outage on October 31, 2008 (Flexiscale Outage). Maintaining the uptime, preventing denial of service attacks (especially at the single-points-of-failure) and ensuring robustness of computational integrity (i.e. the cloud provider is authentically running and giving applicable outcome) are some of the major issues in this category of threats.

C. Third Party Data Control:

The legal implications of applications and data being held by a third party are complex and not well understood. There is also a potential lack of control and precision when a third party holds the data. Part of the publicity of cloud computing is that the cloud can be implementation-independent, but in reality, regulatory compliance requires transparency into the cloud. Various data privacy and security issues are prompting several companies to build clouds to avoid these issues and yet maintain some of the benefits of cloud computing. However, concerns like Due diligence, Auditability, Contractual obligations, Cloud provider espionage, Cloud provider espionage, Transitive nature of contracts need to be addressed properly.

V. COMMON AUTHENTICATION METHODS

Authentication is a method by which a system verifies and validates the identity of a user of the system who wishes to access it. Authentication [4] ensures and confirms a user's identity through a code such as a password and verifies genuineness of a document or signature, to make it effective or valid. It is the measure employed to ensure that the entity requesting access to a system is what or who it claims to be, and to counter any inappropriate or unauthorized access. Authorization is the method of giving individuals access to system objects like information, application programs etc. based on their identity.

A. Password and PIN based authentication

Using password (a secret word or string of characters that is used for user authentication) or Personal Identification Number (PIN which is a secret numeric password and is typically used in ATMs) to login is the most common knowledge-based authentication method. It is mandatory for the user to provide knowledge of a secret in order to authenticate the process.

B. SMS based authentication

SMS is used as a delivery channel for a one-time password (OTP) generated by an information system. There are two types of one-time passwords, ***a challenge-response password*** which responds with a challenge value after receiving a user identifier and ***a password list*** which makes use of lists of passwords which are sequentially used by the person wanting to access a system. User receives a password through the message in the cell phone, and enters the password to complete the authentication. This SMS-based authentication method is used in the login process of Internet banking system to authenticate the process.

C. Symmetric-key authentication

In symmetric key authentication, user shares a secret, unique key with an authentication server. The user may be asked to send a randomly generated message (the challenge) encrypted by the secret key to the authentication server. If the server can found the match for received encrypted message (the response) using its shared secret key, the user is authenticated and server authorizes user's access to the system.

D. Public-key authentication

In Public-key cryptography a pair of private key and public key is used. A private key is kept secretly by the user, while the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is made available to others for sharing the public key among different users. The private key is used to encrypt the messages send between the communicating machines and both encryption and verification of signature is accomplished with the public key.

E. Biometric authentication

Biometrics is a method by which a person's authentication information is generated by digitizing measurements (encoded value) of a physiological or behavioral characteristic. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware device. The device scans the physical characteristic, extracts critical information, and then stores the result. Biometric authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic.

F. Zero-knowledge proofs

Zero-knowledge proofs [11] make it possible for a Host to convince another Host to allow access without revealing any secret information by communicating several times to finalize authentication. The client creates a random but difficult problem and solves it using information it has, commits the solution using a bit-commitment scheme and sends the problem and commitment to the server. The server then asks the client to either prove that the problems are related or open the committed solution and prove that it is the solution. The client complies with the request. Typically, about ten successful exchanges will be required to take place before the authentication process is complete and access is granted. This method utilizes a one-way hash function where the committing answers are based on the output of that hash function. The number of proofs needed is generally larger (64 or more), to avoid brute-force attacks.

G. Digital Signatures

A digital signature is a digest calculated from a signed document (typically a one-way hash function) which is then signed (encrypted with private key). The client verifies the digest signature by decrypting it with the server's public key and compares it to the digest value calculated from the message received. The signature can also be used by the server to verify data the client is sending. Digital signature is used to assure that the downloaded data is genuine and not malicious or invalid information.

VI. MULTI – FACTOR USER AUTHENTICATION IN CLOUD COMPUTING

Multi-factor authentication (MFA) is an approach to authentication which requires the production of two or more of the three following independent authentication factors:

1. Knowledge factor
2. Possession factor
3. Inherence factor

After submission, each factor must be validated by the other party for authentication to occur. Multifactor authentication (MFA) [4] is a security system that requires more than one form of authentication to validate the authenticity of a transaction. Multifactor authentication requires two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification).

Previously, MFA systems typically based upon two-factor authentication. Because customers are more and more using mobile devices for banking and shopping, however, physical and logical security concerns have converged. This, in turn, has formed more interest in three-factor authentication.

A. Knowledge factor *("something only the user knows"):*

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate like password (a secret word or string of characters that is used for user authentication), PIN (A personal identification number (PIN) is a secret numeric password and is typically used in ATMs) and Pattern (Pattern is a regular or stochastic sequence or array of sets of information as e.g. in a single dimensional barcode or in a two dimensional matrix code or in a finger print like set in any n-dimensional stack in any physical representation).

B. Possession factor *("something only the user has"):*

Possession factors have been commonly used for authentication from many years, in the form of a key to a lock. The basic principle is that the key holds a secret which is common between the lock and the key, and the similar principle is used for possession factor authentication in computer systems. A number of types of pocket-sized authentication token are available which display a changing passcode on an LCD or e-ink display, which must be typed in at an authentication screen, thus avoiding the need for an electronic connection. This can be done one in the forms such as sequence-based token, time-based token, and the token may have a small keypad on which a challenge can be entered. The challenge can take one of following tokens:

1) ***Connected tokens****:* The connected type tokens are available in the form of Magnetic stripe cards, Smartcards, Wireless RFID-based tokens, USB tokens and Audio Port tokens.
2) ***Soft tokens (computer-simulated software-based tokens):*** The functionality of any disconnected token can be emulated as a soft token on a PC or Smartphone using deployed software, where that device itself becomes the possession factor.
3) ***One-time pads:*** A one-time pad is a password used only once. Schemes based on a one time pad have been described but are rarely deployed due to the need to supply a new password or pad for each authentication.
4) ***Mobile phones:*** A new category of TFA tools transforms the PC user's mobile phone into a token device using SMS messaging, an interactive telephone call, or via downloadable application to a Smartphone.
5) ***SMS one time password:*** SMS one time password uses information sent to the user in an SMS as part of the login process.
6) ***Smartphone push:*** The push notification services offered by modern mobile platforms, such as phones' APNS and Android's C2DM/GCM, can be used to provide a real-time challenge/response mechanism on a mobile device. Upon performing a sensitive transaction or login, the user will instantly receive a challenge pushed to their mobile phone, be prompted with the full details of that transaction, and be able to respond to approve or deny that transaction by simply pressing a button on their mobile phone.
7) ***Mobile signature:*** Mobile signatures are digital signatures created on a SIM card securely on a mobile device by a user's private key. In such a system text to be signed is securely sent to the SIM card on a mobile phone. The SIM then displays the text to the end-user who checks it before entering a PIN code to create a signature which is then sent back to the service provider. The signature can be verified using standard PKI systems.

C. Inherence factor *("something only the user is"):*

1) ***Biometrics:*** Biometric authentication satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault. For many biometric identifiers, the actual biometric information is rendered into string or mathematic information. The device scans the physical characteristic, extracts critical information, and then stores the result as a string of data. Comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved.

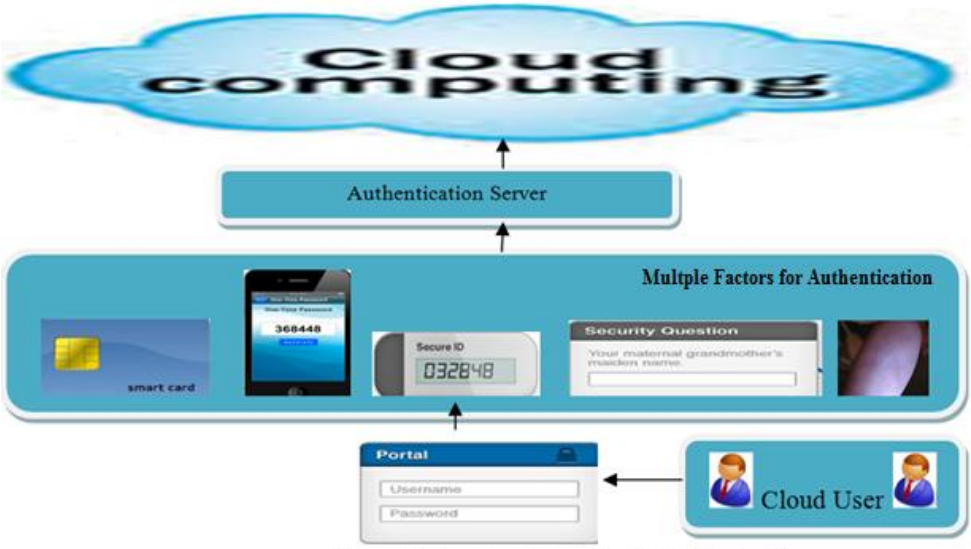

Figure 2 Multi-factor User Authentication for cloud Data Secutiry

VII. TOKEN THREATS

An Attacker [4] who can achieve control of a token will be able to masquerade as the token's owner. Token threats can be categorized based on attacks on the types of authentication factor:

A. ***Possession factor*** may be damaged, lost, stolen from the owner or cloned by the Attacker. For example, an unauthorized user who gains access to the owner's computer might duplicate a software token. A hardware token might be duplicated, stolen, tampered.

B. ***Knowledge factor*** may come to knowledge of an Attacker. The Attacker might guess or estimate a password or PIN. Where the token is a shared secret, the Attacker could access to the computer system or Verifier and acquire the secret value. An Attacker may set up malicious software (e.g., a keyboard logger) to reveal the secret. Additionally, an Attacker may find out the secret through offline attacks on network traffic from an authentication attempt.

C. ***Inherence factor*** may be produced or replicated. An Attacker may obtain a duplicate copy of the token owner's fingerprint and construct a replica.

Multiple factors lift up the threshold for successful attacks. If an Attacker wishes to acquire a cryptographic token and guess a password, then the work to find out multiple factors may be too high. The goal of MFA is to create a layered security and make it more complicated for an unauthorized person to access an object such as a physical location, computing device, network or database. If one factor is broken or compromised, the attacker still has at least one more difficulty level to go by before successfully breaking into the target.

VIII. CONCLUSION

Cloud provides open interoperation across (proprietary) cloud solutions at IaaS, PaaS and SaaS levels, manages multi-tenancy at large scale and in heterogeneous environments with dynamic and seamless elasticity from in-house clouds to public clouds for unusual (scale, complexity) and/or infrequent requirements. The explosive growth of cloud computing has made the provision of adequate and effective security challenges. Multi- factor user Authentication is an effective technique for preventing unauthorized access. A major weakness in the security of cloud data is that, the provision of physical security controls is impossible. As a result, strong access control and authentication becomes very important for providing effective security. In this paper, we explore the feasibility of introducing MFA to ensure authentication for cloud access control as Multiple factors raise the threshold for successful attacks. However, there are still other security issues to be addressed in the future. This includes:

- Confidentiality
- Integrity
- Availability and
- Anonymity

Future research should give consideration to all of the above in the context of the cloud security.

REFERENCES

[1] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011 , 316-322 .

[2] Z. Wang, "Security and Privacy Issues Within Cloud Computing" IEEE Int. conference on computational information sciences, Chengdu, China, Oct. 2011.

[3] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus, NIST Special Publication 800-63-1 " Electronic Authentication Guideline" [online] Available.

[4] Peter Mell, Timothy Grance, NIST Special Publication 800-145 "The NIST Definition of Cloud Computing" [online] Available.

[5] Mathisen, "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea, 31 May -3 June 2011.

[6] Greveler U, Justus b et al. (2011). A Privacy Preserving System 2. for Cloud Computing, 11th IEEE International Conference on Computer and Information Technology, 648–653.

[7] CLOUD SECURITY ALLIANCE (CSA)'s The Notorious Nine: Cloud Computing Top Threats in 2013 Available Online at: http://www.cloudsecurityalliance.org/topthreats.

[8] John Harauz, Lorti M. Kaufinan. Bruce Potter, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Co published by the IEEE Computer and Reliability Societies, July/August 2009.

[9] Cong Wang, Kui Ren, Qian Wang and Wenjing Lou "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, vol 5, no. 3, pp 220-232, 2011.

[10] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

