Volume 5, Issue 1, January 2015 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 Security Framework in Cloud Computing

Prachi Soni, (Asst. Prof.) Monali Sahoo
Computer Science & Engineering
Takshshila Institute of Engg & Tech., Jabalpur (M.P.)
R.G.T.U Bhopal (M.P.) India

Abstract- Data Security is the most critical issues in a cloud computing environment. Authentication is a key technology for information security, which is a mechanism to establish proof of identities to get access of information in the system. Traditional password authentication does not provide enough security for information in cloud computing environment to the most modern means of attacks. In this paper, we propose a new multi-factor authentication framework for cloud computing. 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, Multi-factor Authentication, Cloud threats, Data Security, Cloud Trust

I. INTRODUCTION

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 [11]. 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 data centre and information, and this increase conciliation of data considerably [12]; 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 [13].
Cloud model is composed of three service models, four deployment models and five essential characteristics.

1.1. 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].

1.2. 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].

1.3. 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**.**

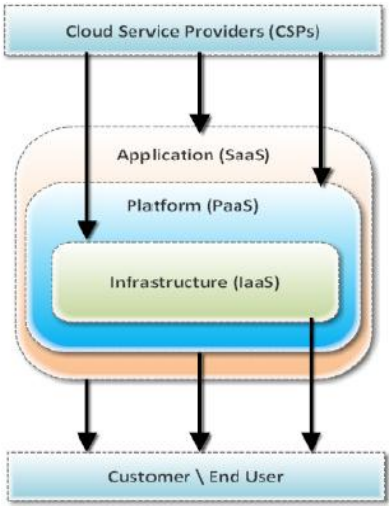

Fig 1.1 Cloud Architecture Reference Model

II. 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

2.1 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.
2.2 Availability issues: These concerns centre 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 Flexi Scale's 18-17 hour outage on October 31, 2008 (Flexi scale 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.
2.3 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.

III. 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.

3.1 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.

3.2. 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.

3.3 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.

3.4 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.

3.5 Biometric authentication: Biometrics is a method by which a person's authentication information is generated by digitizing measurements (encoded value) of a physiological or behavioural 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.

3.6 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.

IV. 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.

4.1 Knowledge factor

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).

4.2 Possession factor

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 pass code 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 phone's 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.

4.3 Inherence factor

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.

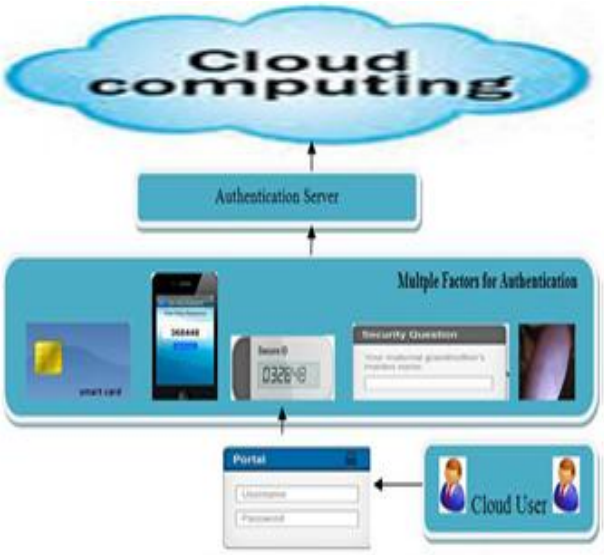

Fig 4.1 Multifactor User Authentication

V. MULTIFACTOR AUTHENTICATION

1). Registration Phase

Client registers with the cloud application by providing all information required for authenticating the user.

2). Login Phase

Client uses login form to access the cloud application and its services. This accepts username and password. And submits username and password.

3). Key generation Phase

Once the client logins with username and password the key K is generated. For the key generation, the CSP accesses matching attributes of user from Registrar. Mi is the set of matching attributes and μi is the corresponding signatures. CSP finds the aggregate by computing.

4). Split Phase

The M value is the key K and is splitted as two parts K1 and K2. The K1 is send to the email id provided by the client in the process of registration and K2 is send as SMS to the mobile phone no. provided at the time of registration of the user. This information is stored at the registrar.

5). Zero Knowledge Proof Protocol

According to the Zero Knowledge Proof protocol, the client randomly picks y, s in [1, ..q], computes d = (mod p), and sends d, μ, M, Mi , 1 <= i <= t, to the CSP. The CSP sends back a random challenge e [1, .., q] to the client. Then the client computes u = y+em(mod q) and v = s+er (mod q) where m = m1 + . . . mt and r = r1 + . . . rt and sends u and v to the CSP. The CSP accepts the aggregated zero knowledge proof. If this case then CSP conforms to the correctness of user identity.

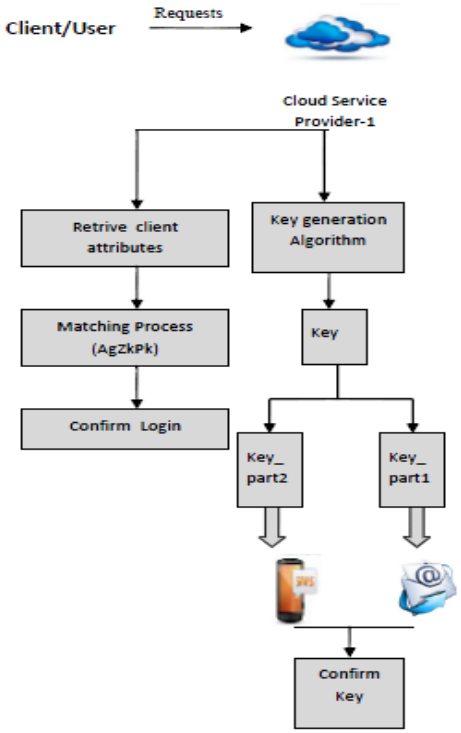

Fig 5.1 Attribute Based Multifactor Authentication System

VI. SYSTEM IMPLEMENTATION

Algorithms used in the implementation

Generating elliptic curve points

gen_points (p,a,b) [11]

{

x=0;

While(x<p)

{

W=(x3 + ax + b) mod p

If(w is a perfect square in Zp)

display ((x,sqrt(w)),(x,-sqrt(w)))

X=x+1

}

}

Generating public key [11]

1. Select a point E(a,b) with an elliptic curve over GF(p).
2. Select a point on the curve, e1(x1,y1).
3. Choose an integer d.
4. Calculate e2(x2,y2)=d * e1(x1,y1)
5. Combination of E(a,b), e1(x1,y1) and e2(x2,y2) is key.

Encryption process:

Select P, a point on the curve, as plain text, P. Then calculate a pair of points on the text as cipher text.

Process of proposed system implementation:

1. Compute where m is identity attribute, r is random number in
2. g ,h are the generators of group G of elliptic curve.
3. Now find the M as product of for n attributes.
4. Find the μ as the product of for n attributes. This value is used as signature of registrar.
5. Now split the M value and send parts of key to mobile and email accounts.

6. As another factor of authentication, according to the ZkPk client selects y,s in [1,.., q].
7. Client calculates d= (mod p)
8. Client sends d, μ,M,Mi to the CSP service.
9. CSP sends a value e to the client. Then client calculates u,v as follows and sends to CSP.

u= y + em(mod q) where m=m1+m2+....+mt

v= s + er (mod q) where r=r1+r2+.....+ rt

10. If = then authentication is confirmed by CSP.

VII. ANALYSIS OF THE PROPOSED FRAMEWORK

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

7.1 Authentication and Authorization

The user is authenticated and authorized by a multi – factor and multi step approach at the cloud service centre. 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.

7.2. 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.

7.3 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 centre. 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 [14, 15, 16]. 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.

VIII. CONCLUSIONS

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. This system provides less complex and efficient privacy policy for cloud based applications. If the user is unable to access mobile phone or email account then the system provides alternate ways by checking all the identity attributes of the user. The method 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] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage", NDSS, (2005).

[16] R. Blom, "An optimal class of symmetric key generation systems", In Advances in Cryptology, Springer Berlin/Heidelberg, (1985), pp. 335-338.

