Volume 6, Issue 5, May 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# A Survey of Security Issues and Authentication Mechanism in Cloud Environment with Focus on Multifactor Authentication

**Jyotika Chhetiza**[*], **Nagendra Kumar** (Assistant Professor)
CSE Department, Shri Ram Institute of Science and Technology, Jabalpur,
Madhya Pradesh, India

***Abstract** - Cloud computing provides shared processing resources and data to computers and other devices on demand over the internet. Any configurable computing resource like, servers, networks, storage, applications and services can be provided immediately and released with lowest management effort. Although it seems highly useful and coherent, there is always the security and privacy concerns related to cloud as service providers can access the data in it at any time. Information could be altered or deleted or shared with third parties if required for the purpose of law and order without any prior notice.Authentication plays a majority role for information security that is a mechanism to find identity proof to get system access. In this paper we perform a survey of various security issues, existing user authentication techniques for cloud and discuss the growth as well as scope of multifactor authentication method in particular.*

***Keywords:** Cloud Security, Security Issues, Security Threats, Authentication, Multifactor-Authentication*

## I. INTRODUCTION

Cloud computing may be of different use to individual consumers such as for those of us who just work at home or in small-to-medium offices and use the Internet on a regular basis.Whereas, some businesses implement cloud computing techniques via different operations, one of them being Software-as-a-Service (SaaS), where the business subscribes to an application it accesses over the Internet. There's also Platform-as-a-Service (PaaS), where a business can create its own custom applications for usein the company. In the mighty Infrastructure-as-a-Service (IaaS)[1],companies like Amazon, Microsoft, Google and Rackspaceprovide a backbone that can be leased outby other companies.

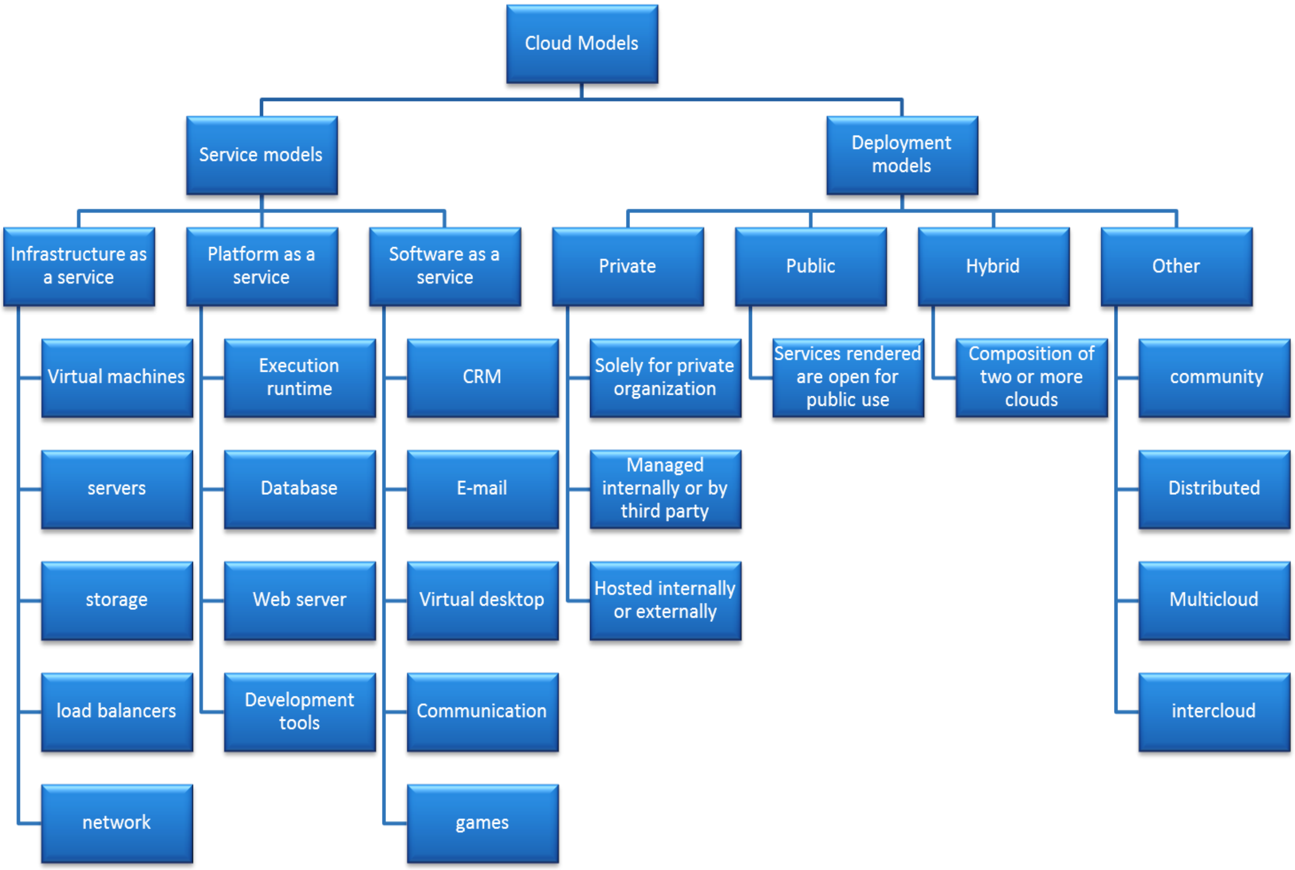

Figure 1: Cloud Models

Cloud security is a developingsub-realm of security in computers, networks and more specifically of information security. It encompasses a widerange of policies, technologies, and controls applied to protect data, applications, and the associated infrastructure of cloud computing. When an organization selects to store data or host applications on a public cloud, it cannot physically access the servers hosting its data.In order to make less usage of the resources, decrease costs and maintain efficiency, cloud service providers store data ofmultiple customers on the same server. As a result, it becomes possible that one user's private data to be viewed by other users. To look after such sensitive situations and avoid data leakages and hacks, cloud service providers should manage proper data isolation and logical storage sorting[2].It is needed that information security controls be selected and implemented according to the risks, typically by assessing the threats, vulnerabilities and effects.

Authentication is a process in which the credentials provided are compared to those in thedatabase of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. Strong authentication is a commonly used term which could be described as any method of verifying the identity of a user or device that is intrinsically stringent enough to ensure the security of the system it protects[3].

Multifactor authentication ("MFA") is an extension of two-factor authentication and a method of boosting IT security thatmandates end users to provide multiple methods of identification to confirm their identity for attaining access to corporate resources and applications, as well as perform online transactions[4]. By requiring an additional authentication factor beyond a simple password for example as software on a smartphone, a fingerprint, a voiceprint, a key fob or a security code etc. MFA technology makes it more difficult for hackers to exploit the login process and create blunders by stealing corporate, customer or partner data, even when a password has been compromised or shared among a number of different services by an end user.

## II. CLOUD SECURITY ISSUES

Security in Cloud computing is the set of control-based technologies and policies designed to adhere with regulatory compliance rules and to protect information, data applications and infrastructure associated with the use of cloud services[5]. Owing to the cloud's very nature of a shared resource, identity management, privacy and access control are of particular concern with the security point of view. With more organizations using cloud computing and associated cloud providers for data operations, appropriate security in these operations and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider.

Security issues fall into two broad categories - issues faced by cloud providers, i.e.organizations providing software, platform or infrastructure-as-a-service via the cloud and issues faced by their customers i.e.companies or organizations who use or host applications or store data on the cloud[6]. The responsibility for a safe and secure connection and communication is mutual for both parties i.e. cloud providers and the users. Here, the provider must ensure that their infrastructure is protected and that their clients' information and applications are secured while the user must take steps to vitalize their application and use strong passwords and authentication schemes.

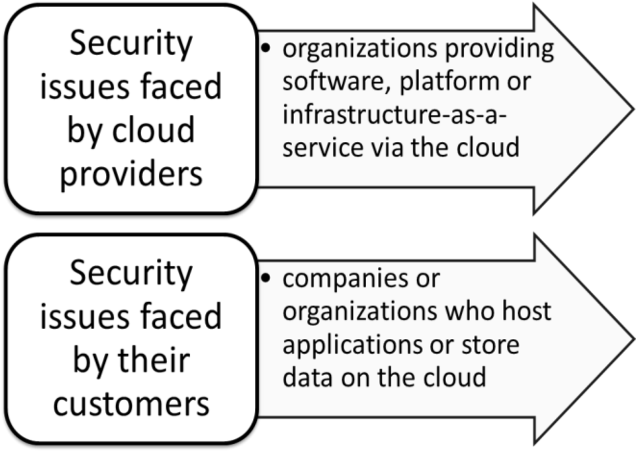
Security issues faced by cloud providers
• organizations providing software, platform or infrastructure-as-a-service via the cloud
Security issues faced by their customers
• companies or organizations who host applications or store data on the cloud

Figure 2: Security Issues

## III. CLOUD SECURITY THREATS

A leading cloud security group, 'The Cloud Security Alliance' (CSA) has put together a list of twelve most severe threats to cloud computing in 2016[7]. To analyse the data security hazards, the CSA working group evaluated Microsoft based STRIDE threat model and the categories are as follows:

S – Spoofing Identity

T – Tampering Data

R – Repudiation

I – Information Disclosure

D – Denial of service

E – Elevation of Privilege

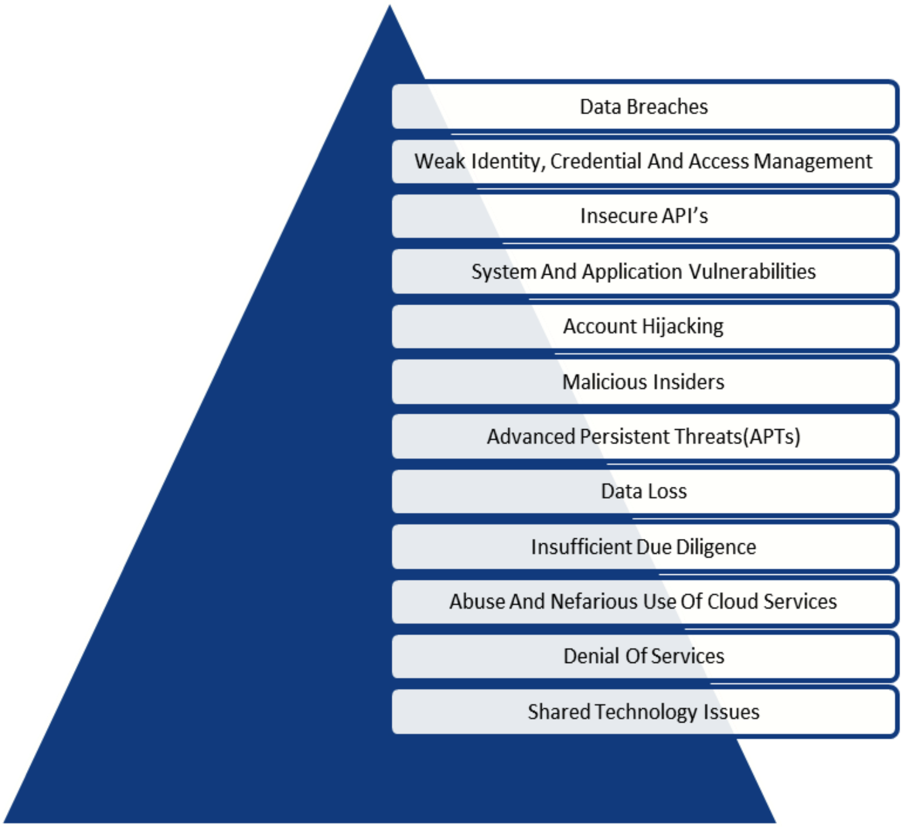
Data Breaches
Weak Identity, Credential And Access Management
Insecure API's
System And Application Vulnerabilities
Account Hijacking
Malicious Insiders
Advanced Persistent Threats(APTs)
Data Loss
Insufficient Due Diligence
Abuse And Nefarious Use Of Cloud Services
Denial Of Services
Shared Technology Issues

Figure 3: Top Cloud Computing Threats in 2016

**Data breaches** come under the category of information disclosure (I).
**Feeble Identity, Credential and Access Management, System Vulnerabilities, Account Hijacking, Insufficient due diligence** comprises of all the categories mentioned in STRIDE
**Insecure interfaces and API**'s threat evaluation confirms data tampering (D), repudiation (R), disclosure of information (I) and elevation of privilege (E).
**Malicious Insiders** satisfies with spoofing identity (S), data tampering (T) and Info disclosure (I).
**Advanced persistent threats** and **Shared technology Issues** come under (I) and (E).
**Data loss** deals with (R) and (D).
**Abuse and nefarious use of cloud computing** is a Denial of Service (D) threat.

## IV. THE MOST IMPORTANT SECURITY ISSUE - AUTHENTICATION IN THE CLOUD ENVIRONMENT

All of the security threats mentioned above take place in the absence of proper authentication mechanism and could be avoided if one deploys any of the following authentication mechanisms[8].

### 1) Working of Authentication on a private network

While logging on to the machine and then trying to access a resource, either a file server or database, it needs to be assured that ourlogin credentials are valid. If it is a Windows machine, this authentication is performed by a component called the Local Security Authority Subsystem Service ("LSASS"). If we run Windows Task Manager and list the running processes for all users, we see a program called "lsass.exe". Similarly, in a Linux/UNIX/Mac machine, it is called "lsassd"[9].

Authentication of a user could be done in either one of two ways: using local credentials or using Active Directory ("AD") credentials. If the machine is "joined" to AD, we will typically log on with the AD account. If the machine is not joined to AD it is in work group mode and we log on using local credentials. With latter, the username and password are validated against account information stored on user's own machine[10]. In the AD case,LSASS authenticates the user's credentials using the Kerberos protocol to talk to an AD domain controller.Kerberos is an essential thing to mention for authentication. It can authenticate credentials without ever transmitting the password in either clear or hashed form. This is important because it makes it impossible to perform offline password cracking. Kerberos also supports single sign-on, which forms the base for any authentication check. Once we are logged on to the machine, we have a special "ticket" that can be used toacquire additional tickets for other services.

### 2) Identity management

At the core of an identity management system are policies defining which devices and users are allowed on the network and what a user can accomplish, depending on his device type, location and other factors[11]. The solution for ID management in Cloud is Cloud ID which links the confidential information of the users to their biometrics and stores it in encrypted manner[2]. Making use of an encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

### 3) Authentication techniques

Existing User Authentication Techniques are shown in the figure below which takes different criteria to authenticate the users in Cloud[12].

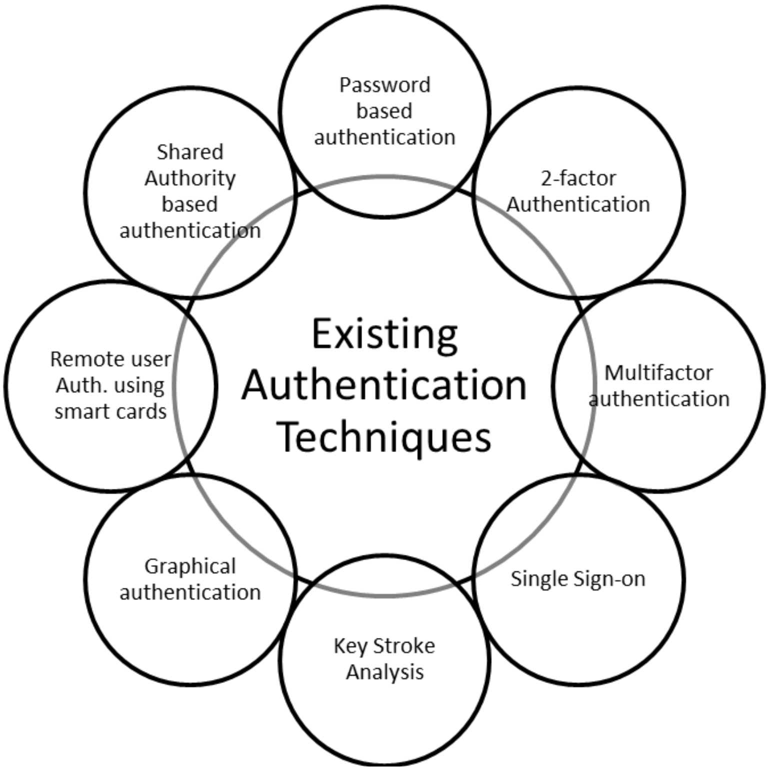
Password based authentication
2-factor Authentication
Multifactor authentication
Single Sign-on
Key Stroke Analysis
Graphical authentication
Remote user Auth. using smart cards
Shared Authority based authentication
Existing Authentication Techniques

Figure 4: User Authentication Techniques

**Password based Authentication** is also called single-factor authentication. In this method, user should insert username and password to login to the system and can access to the data in cloud service provider. This mechanism in present may not be considered the best security practice as leaked passwords can lead to data breaches[13].

**Two-factor authentication** is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized, such as a security code[14].

**Single Sign-On**("SSO") is a session/user authentication process that permits a user to enter a name and password in order to access multiple applications. Credentials for authorization are stored on a dedicated SSO policy server.Although single sign-on is a convenience to users, it present risks to enterprise security. If an attacker gains control over a user's SSO credentials, he will be granted access to every application the user has rights to, which increases the amount of potential damage[13].

**Key Stroke Analysis** uses the fashion and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the user's typing pattern for future authentication [15].

**Graphical Authentication**system works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). A graphical password is easier than a text-based password for most people to remember.

**Authentication using smart card**: A biometric authenticated card which allows the user with both logical and physical access is a long cherished dream of any corporation. The connection of a smart card chip is via direct physical contact with a machine which could read smart cards. However, USB tokens are way more easy and convenient to carry, less susceptible to breakage and could be read by any PC having USB ports.

**Shared Authority based privacy preserving authentication protocol** ("SAPA")is attractive for multi-user collaborative cloud applications. Shared access authority is attained by anonymous access request matching mechanism with security and privacy considerations i.e., authentication, data anonymity, user privacy, and forward security[16].

## V. MULTIFACTOR AUTHENTICATION TECHNIQUES

Multifactor Authentication ("MFA") is security structure that needs multiple forms of authentication from autonomous classes of credentials to check the identification of the user for login or other activities. MFA incorporates two or more autonomous credentials: password - what the user realize and security token – what the user retains and biometric verification – who the user is. The objectives of MFA is to device a covered defence and makeit extra troublesome for an unwarranted user to access the object such as a physical location, computing apparatus, network or database. If any one of the multiple factors is damaged or compromised then the hacker still at least needs to successfully break an additional authentication factor for breaching into the target[17].

Further, we take a look on comparative study of different authentication factors and based implemented technologies with examples. Also, the comparison of techniques proposed by different authors and applied algorithms.

Table 1: Multifactor Authentication Technologies Based On Authentication Factors

| **Authentication factor** | **Description** | **Examples** | **Implemented technologies** |
|---|---|---|---|
| Knowledge factor | Information that a user must be able to provide in order to log in. | Usernames/IDs, passwords, PINs, Answer to secret questions | Password-based authentication/Single-factor authentication |
| Possession factor | Anything that a user must have in their possession to log in | Security token, OTP, employee ID card, Mobile's SIM card | Hardware security tokens - Small hardware devices that the owner carries to authorize access to a network service in the form of a smart card or may be embedded in an easily-carried object such as a USB drive.<br>Software based soft tokens - applications that generate a single-use login PIN, often used for multifactor mobile authentication. |
| Inherence factor | Biological traits the user has that are confirmed for login | Retina scans, iris scans, fingerprint scans, facial recognition, voice recognition, hand geometry, earlobe geometry | Biometric Authentication based on geometry of user's body parts. |
| Location factor | User's current location | Users typically carry their phones and most smartphones have a GPS device, enabling reasonable surety confirmation of the login location | GPS smartphones can also provide location as an authentication factor with this on board hardware. |
| Time factor | Current time of login. Verification of employee IDs against work schedules could prevent some kinds of user account hijacking attacks | A bank customer can't physically use their ATM card in America, for example, and then in Russia 15 minutes later. These kinds of logical locks could prevent many cases of online bank fraud. | Employee ID and customer cards, including magnetic strip and smartcards used for logging in at particular time. |

Table 2: Comparative Study of Multifactor Authentication Schemes based on Issues, Algorithms, Advantages and Limitations

| Authors | Authentication Issues | Implemented Algorithm(s) | Advantages | Limitations |
|---|---|---|---|---|
| Hoonjae Lee, Pardeep Kumar[18] | Identity management, mutual authentication, session key establishment between the users and the cloud server. | Public key and Mobile out of band based authentication algorithm | Resistance to replay attacks, man-in-the-middle attacks and denial of service attacks. Security over basic two-factor authentication | Absence of a formal security proofing technique. |
| Vishal Paranjape[19] | Better password solution, two-factor OTP authentication solution, easy-to-understand registration system | mOTP Authentication Algorithm | Use of time based OTP's, internal clock generates passwords that depends on the current time | Vulnerable to attacks due to absence of other standard privacy and security algorithms. |
| Wenyi Liu[20] | Privacy-preserving multi-factor authentication system utilizing the features | Multiple Access with Collision Avoidance("MACA"), fuzzy hashing | MFA providing privacy and usability based on hybrid profile of user | Cannot be implemented as a full-proof solution to all authentication and |

| | | | | |
|---|---|---|---|---|
| | of big data | encryption algorithm | behaviour combining the features of big data | security problems in cloud. |
| Jiangsham Yu[21] | Upgrading 2-factor mechanism to formal 3-factor scheme. | Fingerprint based fuzzy vault system | Highly secure under three-factor requirements, low registration cost, use of biometrics | Asymmetric key encryption/decryption and digital signature signing/verification are still required. |
| S.H Khan, M.A Akbar[22] | Verification system combining human inherence factor with standard knowledge factor | Signature matching system(feature extraction, distance measurement) | Scalable and available to use in mobile platforms like android and ios, low cost and resource requirements. | Verified only for a small group of users.Evaluation for large scale clients on cloud is not yet tested. |

## VI. CONCLUSION

MFA products can contribute compelling benefits to an enterprise, but the technology being so complex and the mechanism itself can differ vastly from vendor to vendor. Many of the leading MFA products are already out for commercial space. In this paper we have broadly discussed about security factors, threats, authentication strategies and Multifactor Authentication mechanisms in significance. Along with password or PIN as the baseline authentication standard, additional layers of security and verification can be pulled from a wide pool of sources. Although its implementation may be a little expensive for naive users; secure, usable and affordable MFA is still possible in the future.

## REFERENCES

[1] H. F. Rashvand And Y. S. Kavian, Using Cross-Layer Techniques For Communication Systems, Hershey, Pennsylvania: Igi Global, 2012, Pp. 328-348.

[2] M. Haghighat, S. Zonouz And M. Abdel-Mottaleb, "Cloudid: Trustworthy Cloud-Based And Cross-Enterprise Biometric Identification," Expert Systems With Applications, Vol. 42, No. 21, Pp. 7905-7916, 30 November 2015.

[3] A. Ruiz-Martinez, R. Marin-Lopez And F. Pereniguez-Garcia, Architectures And Protocols For Secure Information Technology Infrastructures, Hershey, Pennsylvania: Igi Global, 2013, Pp. 1-45.

[4] Y. Shah, V. Choyi And L. Subramanian, "Multi-Factor Authentication As A Service," Mobile Cloud Computing, Services, And Engineering (Mobilecloud), Pp. 144-150, 2015.

[5] A. S. Raja And S. A. Razak, "Analysis Of Security And Privacy In Public Cloud Environment," In International Conference On Cloud Computing (Iccc), Riyadh, 2015.

[6] D. Talbot, "Mit Technology Review," 21 December 2009. [Online]. Available: Https://Www.Technologyreview.Com/S/416804/Security-In-The-Ether/. [Accessed 12 May 2016].

[7] "The Treacherous 12 - Cloud Computing Top Threats In 2016," February 2016. [Online]. Available: Https://Downloads.Cloudsecurityalliance.Org/Assets/Research/Top-Threats/Treacherous-12_Cloud-Computing_Top-Threats.Pdf. [Accessed 15 May 2016].

[8] T. Harris, "Torry Harris Business Solutions," [Online]. Available: Http://Www.Thbs.Com/Downloads/Comparison-Of-Cloud-Computing-Services.Pdf. [Accessed 06 May 2016].

[9] R. Mirunadevi And A. Marimuthu, "Three Dimensional Authentication Mechanisms For Secured Transfer Of Data In Networks," International Journal Of Computer Science And Management Research (Ijcsmr), Vol. 1, No. 5, P. 1074–1079, December 2012.

[10] A. Gopal And S. Noor, "Cloud Service Authentication Verification Using 3d Graphic Signature," International Journal Of Combined Research & Development (Ijcrd), Vol. 1, No. 7, Pp. 2321-2241, November 2013.

[11] E. Chickowski, "Information Week Dark Reading," 25 October 2013. [Online]. Available: Http://Www.Darkreading.Com/Identity-Management-In-The-Cloud/D/D-Id/1140751. [Accessed 20 May 2016].

[12] N. Veeraragavan, G. Kumaresan And L. Arockiam, "A Study Of User Authentication Techniques In Cloud Computing," International Journal Of Emerging Technologies And Innovative Research (Ijetir), Vol. 2, No. 8, Pp. 3309-3314, August 2015.

[13] M. Babaeizadeh, M. Bakhtiari And A. A. Muteb, "Authentication Methods In Cloud Computing: A Survey," Research Journal Of Applied Sciences, Engineering And Technology, Vol. 9, No. 8, Pp. 655-664, 27 January 2015.

[14] S. Lee, I. Ong, H. Lim And H. Lee, "Two Factor Authentication For Cloud Computing," International Journal Of Kimics, Vol. 8, No. 4, Pp. 427-432, August 2010.

[15] Y. Deng And Y. Zhong, "Keystroke Dynamics User Authentication Based On Gaussian Mixture Model And Deep Belief Nets," Isrn Signal Processing, Vol. 2013, P. 7, 2013.

[16] H. Liu, H. Ning, Q. Xiong And L. T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol In Cloud Computing," Ieee Transactions On Parallel And Distributed Systems, Vol. 26, No. 1, Pp. 241-251, January 2015.

[17] "Techtarget," March 2015. [Online]. Available: Http://Searchsecurity.Techtarget.Com/Definition/Multifactor-Authentication-Mfa. [Accessed 20 May 2016].

[18] A. J. Choudhury, P. Kumar, M. Sain, H. Lim And H. Jae-Lee, "A Strong User Authentication Framework For Cloud Computing," Services Computing Conference (Apscc), Ieee Asia-Pacific, Pp. 110-115, 2011.

[19] V. Paranjape And V. Pandey, "An Improved Authentication Technique With Otp In Cloud Computing," International Journal Of Scientific Research In Computer Science And Engineering, Vol. 1, No. 3, Pp. 22-26, 30 June 2013.

[20] W. Liu, A. S. Uluagac And R. Beyah, "Maca: A Privacy-Preserving Multi-Factor Cloud Authentication System Utilizing Big Data," Computer Communications Workshops (Infocom Wkshps), Pp. 518-523, 2014.

[21] J. Yu, G. Wang, Y. Mu And W. Gao, "An Efficient Generic Framework For Three-Factor Authentication With Provably Secure Instantiation," Ieee Transactions On Information Forensics And Security, Vol. 9, No. 12, Pp. 2302-2313, December 2014.

[22] S. H. Khan And M. A. Akbar, "Multi-Factor Authentication On Cloud," Digital Image Computing: Techniques And Applications (Dicta), 2015 International Conference, Pp. 1-7, 2015.