ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Multi-Factor Authentication Scheme for E-Services in Cloud Computing

Mallika Roy, Prof. Ashok Verma

Research Scholar, Gyan Ganga Institute of Technology and Science, Jabalpur [M.P] India

Associate Professor & HOD, Dept. of Computer Science Gyan Ganga Institute of Technology and Science

Jabalpur [M.P] India

ABSTRACT: The current day web offers a wide range of e-Governance, e-commerce and other online services that require strong authentication mechanisms to safeguard user's account. In addition, these services require that a user be verified during registration to prevent duplication of accounts in cases where a fraudulent user creates multiple accounts with different credentials to avail the welfare services. Therefore, the challenge is to protect the e-services using secure multi-factor authentication methods with one account per user without compromising the usability. This research discusses a multi-factor authentication (MFA) scheme which uses password, mobile token and question set as multiple factors for authentication. Earlier the idea of static passwords was being used but most of the users try to use easily guessable, weak passwords or keywords from their personal information, which makes it easy for the intruders to guess their passwords in few combinations using Brute Force attack. Thus idea of using Multi-Factor Authentication has been introduced in the world of internet to harden the security of network and make it difficult for the attackers to crack systems. In this mechanism, users are required to provide some extra information along with their login Id and password. Most popular is using time based One-Time Passwords that are generated randomly and valid only for single login and even for short duration of time. One-Time Passwords can be generated either online or offline via various mechanisms. Along with one time password we are using set of questions on the basis of user activities, which need to be answered in given time. If user scores sufficient, then user is authenticated by the system and the user can further access the system for present login.

KEYWORDS: Multi-factor Authentication (MFA), Static Password, Time-based One Time, Passwords (TOTP) and Questions based Authentication.

I. INTRODUCTION

In the world of computer science, during the 60s and 70s, the computation has been done by client-server architecture (Centralized Computing). This technology has been changed to distribute computing with the development of computing technologies. However, nowadays, the computing technologies again going back to the virtual centralized computing (Cloud Computing). The cloud computing concept was first proposed by Eric Schmidt in 2006.

Cloud computing model allows access to information and computer resources using a delivery of computational services (e.g. Online file storage, social networking sites, webmail and online business applications) which allows to access software and hardware that are managed by a third party at remote locations.

The following definition of cloud computing is given by NIST: "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's interaction and has been developed very quickly in the recent years [6]." This new paradigm came up with essential characteristics, service models and deployment models.

1.1 Essential Characteristics [6] [7] [8]

On Demand Service:

The customer or consumer can easily get provided by the resources like Storage, Computing Power etc. according to their needs without any communication with the human in between.

Broad Network Access:

As we know that the internet is provided us many facility like business, storage etc. and the user can facilitate through thick or thin clients like Mobile user, Tablet user, Laptop user or Desktop users. Broad network access also includes the private, public or hybrid clouds in it along with their facilities.

Resource Pooling:

We all know that the cloud services provides facility to multiple users at same time by following the model called Multi-Tenant model in it which assigned the resources according the user needs. He also uses the resources without knowing that where actually the resources are located. Resources for the users include storage, servers, computing powers etc.

Rapid Elasticity:

Rapid Elasticity can be explained like that, in cloud computing whenever the customer demand for the resources than according to the increase or decrease in demand, the customer assigned with the resources immediately. This is called Rapid Elasticity. Deliver the customer unlimited resources and at any time.

Measured Service:

Cloud Services are the measured services mean the capacity and the performance of the cloud system is measured by the service providers. Each company has their own measurement tools for their cloud. While measuring, the company kept some level of abstraction suitable for the types of service providing. Usage of resources can be observed, control and report send to provider by maintaining transparency between provider and the customer.

1.2 Service Models [6]:

Infrastructure as a Service (IaaS): The consumer is able to deploy and run any application onto the fundamental resources which is provided by IaaS providers. This model has lowest service abstraction and highest resource visibility. The consumer has control over operating system and application, but doesn't have control over the underlying cloud infrastructure. Example: Amazon AWS [6] [9].

Platform as a Service (PaaS): This model provides a platform to the developer to develop and deploy applications onto the cloud infrastructure by providing programming construct and tools, which can be supported by the providers. This model provides higher service abstraction than SaaS and lower resource visibility than SaaS. Deployed applications can be controlled by a consumer, but has no control over the underlying cloud infrastructure. Example: Google App Engine [6] [9].

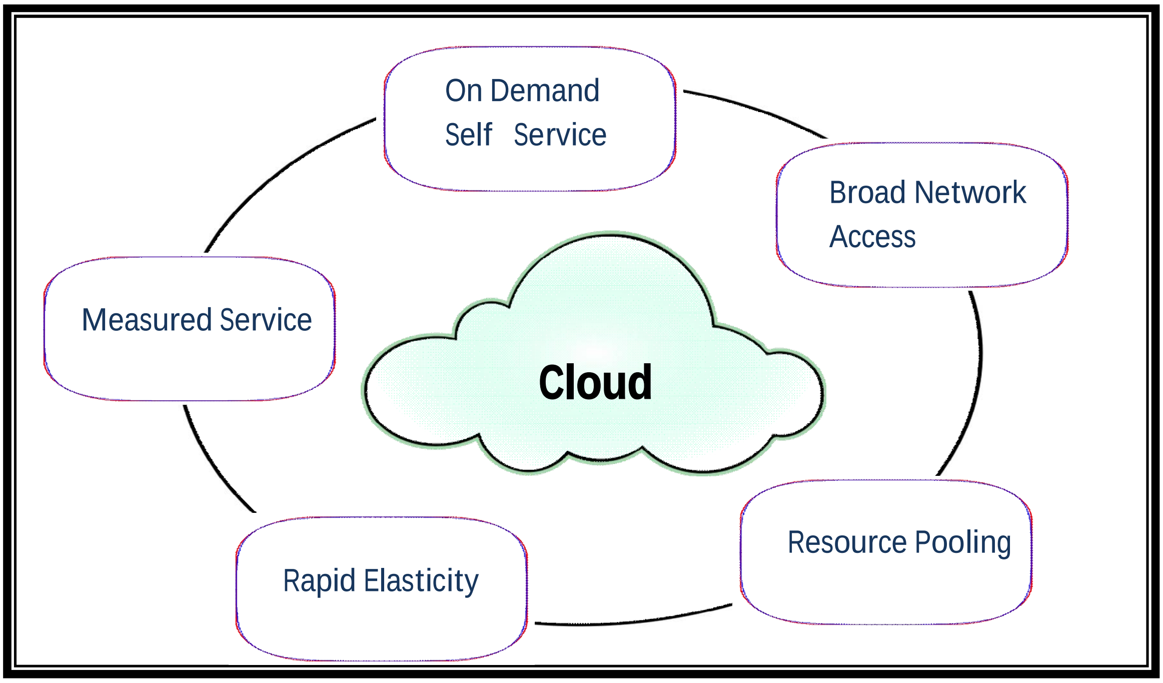

Fig. 1.1 : Essential Characteristics of Cloud [3]

Software as a Service (SaaS): Service providers deploy services to the web which provides remote access to the end user for accessing capabilities. The end user can utilize these services through the web interface. This model provides highest service abstractions and lowest resource visibility. This model hides the implementation of the application to the consumer. Services and underlying cloud infrastructure are not managed or controlled by the consumer. Example: gmail.com [6] [9].

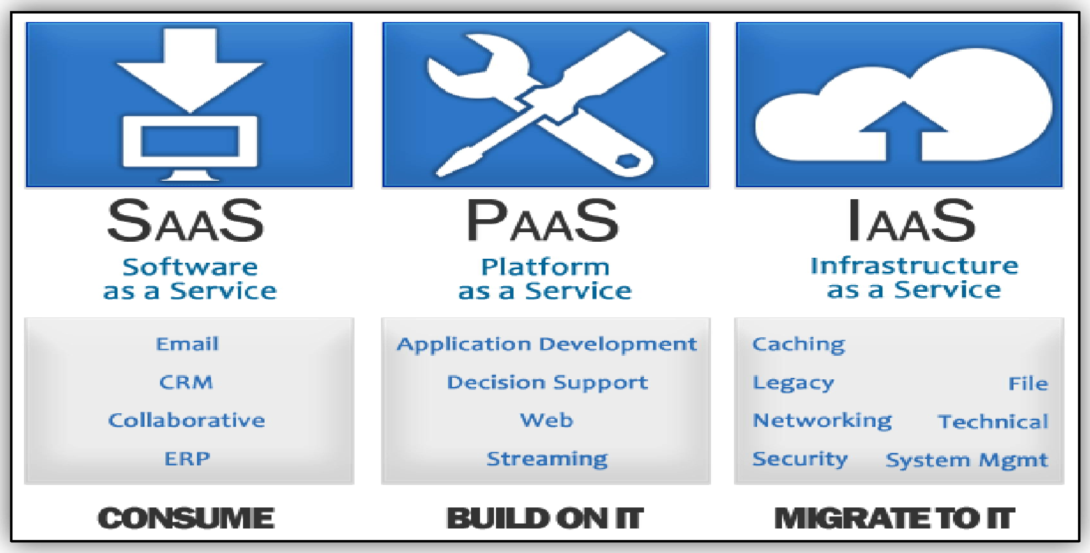

Fig. 1.2: Service Models of Cloud [4]

RESPONSIBILITY	IaaS	PaaS	SaaS
Data Classification & Accountability	Cloud Customer	Cloud Customer	Cloud Customer
Client & End Point Protection	Cloud Customer	Cloud Customer	Cloud Customer
Identity & Access Management	Cloud Customer	50% Cloud Customer 50% Cloud Provider	50% Cloud Customer 50% Cloud Provider
Application Level Controls	Cloud Customer	50% Cloud Customer 50% Cloud Provider	50% Cloud Customer 50% Cloud Provider
Network Control	Cloud Customer	50% Cloud Customer 50% Cloud Provider	50% Cloud Customer 50% Cloud Provider
Host Security	Cloud Provider	Cloud Provider	Cloud Provider
Physical Security	Cloud Provider	Cloud Provider	Cloud Provider

Table 1.1: Responsibility of Cloud Services

1.3 Deployment Models [6]:

Public cloud: The cloud infrastructure is available to the general public with shared purpose which can be owned or managed by third parties who are providing cloud services.

Private cloud: The cloud infrastructure is managed or controlled by the particular organization or third party which is operated for particular an organization [9].

Community cloud: The cloud infrastructure is shared by several organizations for particular concerns like mission, security requirements, policy which can be owned or managed by third parties or the organization [6].
Hybrid cloud: An organization can use the combination of any two or more of the above models to cloud deployment for taking advantages of individual deployment model.

Researchers mainly concentrate on hardware and software from the past few decades for improving the technologies. Due to the improvement of the technologies, the internet technologies are growing very fast across the world. So many works and services have been done online. These services include entertainment, gathering information about different things, emails for keeping in touch with friends, communicate with friends, whether conditions. It requires some type of authentication for all these services.
Security is one of the major issues in cloud infrastructure for adapting the cloud computing technology in IT industries. In cloud computing paradigm, the third party is providing processing capabilities, space for storing information, support for services, etc. Many organizations are storing their crucial information in the cloud database in a cloud environment. Third party maintains the cloud database. The user has to prove their identity to the service provider for seeking.

DOI: 10.15680/IJIRCCE.2017. 0501181

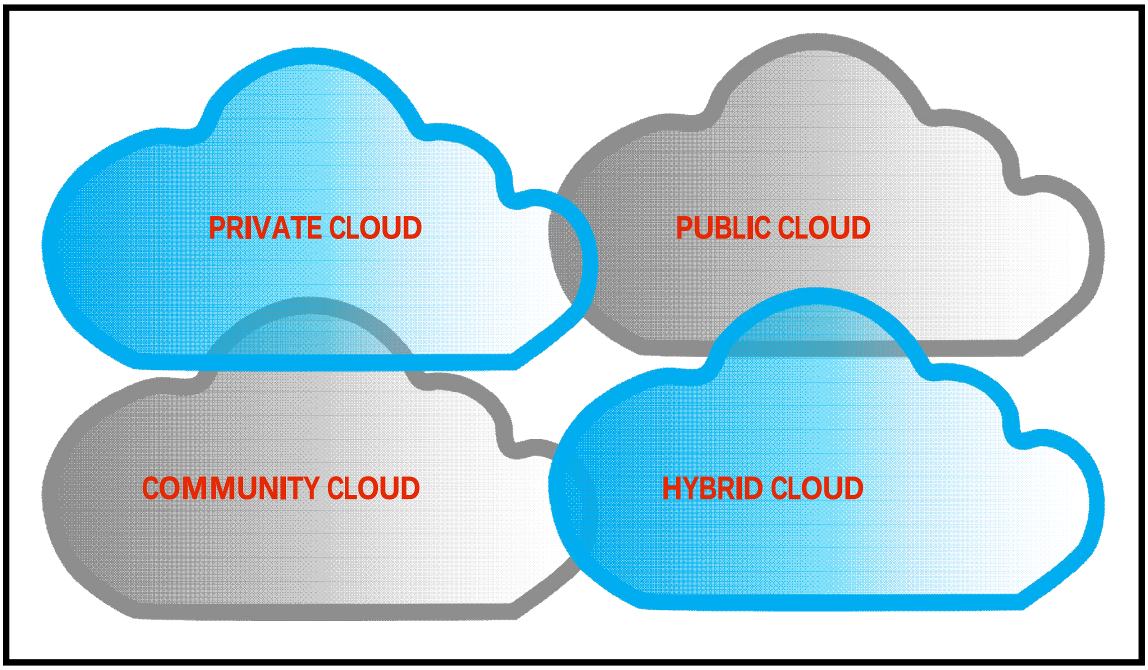

Fig. 1.3: Deployment Models for Cloud [7]

1.4 The verification process has been done by one of the three types of confirmations:
Something known: Secret thing is only known to the user that can be verified by the service providers. Examples are pin no, password, private key.

Something possessed: Something that verifies the users' identity. Examples are ATM card, drivers' license, smart card.

Something inherent: Something that is inherent properties of a user. Examples are fingerprinted, retina scan, and voice.

There are three major techniques for authentication:
Password based authentication: The oldest and simplest method of authentication for accessing the resources in which user has to provide a password which is only known to the user.

Challenge-Response authentication: In this technique, users have to prove that they know the secret without sending it to the service provider. The challenge is any time stamp value which is sent by the service provider and user applies a function on challenge to send response to the service provider.

Zero-Knowledge authentication: In this technique, the user does not disclose anything that might take a chance to the confidentiality of the secret. The user proves to the service provider that they know the secret without disclosing it to the service provider. User and service provider exchanges some messages to each other for authentication. After exchanging these messages, service provider somehow knows that the user knows the secret.
Single-tier authentication can be implemented using one these techniques, but still single-tier authentication is not enough to secure the resources of the service providers in a cloud environment because this technique is suffering from many security attacks like, brute-force attack, insider attacks, in a cloud environment. For making more secure authentication model, the researcher came up with multi-tier authentication (also known as multi-factor authentication). This new technique leads to less probability of breaking the authentication system which provides

more security to the resources of the cloud providers. The multi-tier authentication technique uses two or more verification process to verify the user.

II. LITERATURE REVIEW

This chapter introduces the single-tier and multi-tier authentication techniques and study related to its security analysis for strengthening the existing authentication techniques. It also describes the study about existing authentication techniques and its deficiencies with respect to cloud environments.
For securing confidential information of the user, authentication is a crucial security parameter. If the system is not using any authentication techniques, then confidential information can be accessed by the unauthorized persons who can use this information for making fraud in the system, or also user uses this crucial information for cheating in the financial transactions in the business perspective. Unauthorized users make the access of crucial information to crashing the system or causing the system.

2.1 Review of different authentication techniques

Multi-Factor Authentication on Cloud, Salman H. Khan, M. Ali Akbar

To address MFA Salman H. Khan, M. Ali Akbar implemented a verification system that combines human inherence factor (handwritten signature biometrics) with the standard knowledge factor (user specific passwords) to achieve a high level of security. The major computational load of the aforementioned task is shifted on a cloud based application server so that a platform-independent user verification service with ubiquitous access becomes possible. Custom applications are built for both the iOS and Android based devices which are linked with the cloud based two factor authentication (TFA) server. The system is tested on-the-run by a diverse group of users and 98.4% signature verification accuracy is achieved. Due to the recent security infringement incidents of single factor authentication services, there is an inclination towards the use of multi-factor authentication (MFA) mechanisms. These MFA mechanisms should be available to use on modern hand-held computing devices like smart phones due to their big share in computational devices market. Moreover, the high social acceptability and ubiquitous nature has attracted the enterprises to offer their services on modern day hand-held devices. In this regard, the big challenge for these enterprises is to ensure security and privacy of users.

Multi-Factor Authentication as a Service Andreas, U. Schmidt, LakshmiSubramanian

U. Schmidt design architecture for providing multi-factor authentication as a service is proposed, resting on the principle of a loose coupling and separation of duties between network entities and end user devices. The multi-factor authentication architecture leverages Identity Federation and Single-Sign-On technologies, such as the OpenID framework, in order to provide for a modular integration of various factors of authentication. The architecture is robust and scalable enabling service providers to define risk-based authentication policies by way of assurance level requirements, which map to concrete authentication factor capabilities on user devices.

User-Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services, Reza Fathi

Reza Fathi design authentication architecture suggests a progressive manner to leverage access to different levels of cloud services. At each level, the architecture asks for authentication factors by considering the perceived hardship for users. To increase the security and user convenience, the architecture also considers implicit authentication factors in addition to the explicit factors. Our evaluation results indicate that authentication using the proposed architecture decreases the users' perceived hardship up to 29% in compare with other methods. The results also reveal that our proposed architecture adapts the authentication difficulty based on the user condition. Clouds are becoming prevalent service providers because of their low upfront costs, rapid application deployment, and high scalability. Many users outsource their sensitive data and services to cloud providers. Users frequently access these sensitive services through devices and connections that are vulnerable to thieving and eavesdropping. Therefore, users are desperate of robust security measures to protect their data and services privacy in clouds. In particular, robust authentication techniques are demanded by users for safe access to cloud services. One technique is to utilize multiple authentication factors (a.k. a multi-factor authentication) to access cloud services. However, the challenge is that the multi-factor authentication technique is not effective as it causes user frustration and fatigue. To address this challenge, in this study, we propose a multi-factor authentication architecture that aims at minimizing the perceived authentication hardship for cloud users while improving the security of the authentication.

III. PROPOSED SCHEME

We made some modification to the authentication technique proposed by Singh, Maninder, and Sarbjeet Singh et al. [5] to overcome the problems in the existing technique. We proposed an authentication technique by modifying the existing two-tier authentication model to three-tier authentication with including the one extra authentication factor for verifying the intended user to overcome the insider attack and providing single-sign on access of the registered services.

The proposed authentication technique works on four phases. In the first phase, the users register themselves with the first-tier and second-tier authentication credentials. The first-tier authentication credentials are simple like username and password whereas the second-tier authentication credentials are like pattern matching or text field activity like in the existing technique [5]. We took the pattern matching as the second-tier authentication credentials to simulating the proposed scheme. For the third-tier authentication, the user does not need to provide the authentication credentials like first-tier and second-tier authentication. We are using the email secret code as the third-tier authentication code. This secret code is valid for some amount of time to access the requested service. We provide the time limit with the secret code. After the time limit expires, the user can not access the requested service with that secret code. The user needs another secret code for accessing the requested service. The figure 3.1 shows the abstract model of the proposed multi-tier authentication technique for single-sign on (SSO) access of cloud services.

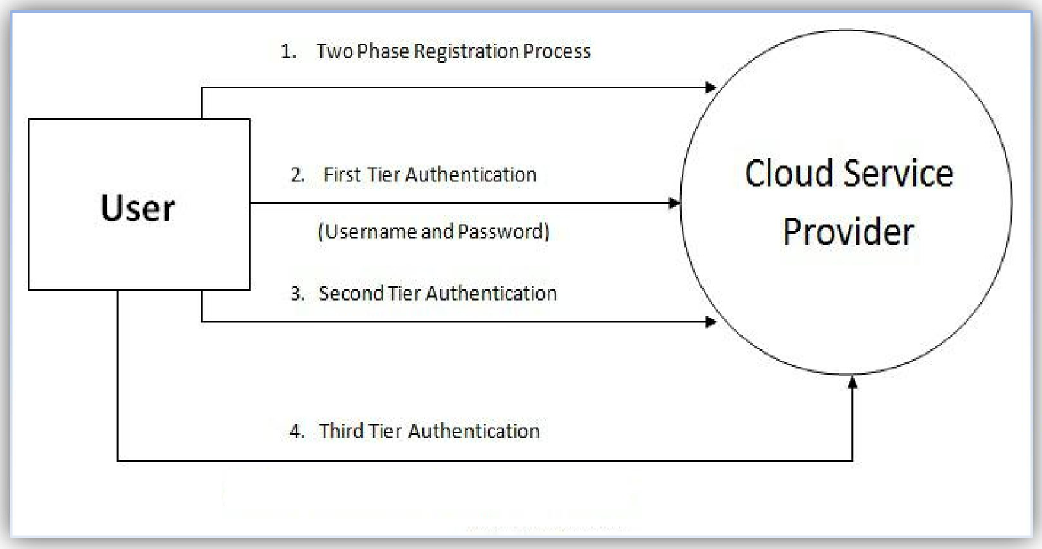
1. Two Phase Registration Process
User
2. First Tier Authentication
(Username and Password)
3. Second Tier Authentication
Cloud Service Provider
4. Third Tier Authentication

Figure 3.1: Abstract design of proposed authentication model

In the first phase, the proposed model verifies whether the intended user or not. After the first phase, the second-tier credentials are used to authorize the requested user by listing the registered services. It lists the registered services by the user. Finally, the third-tier authentication credential is used to authenticate the requested user again and provide the access the requested service. Once the two phases of authentication is completed, the user does not need to provide the other services. For accessing the other service after the two phases, the user has to provide the mobile secret code to the authentication system.

The proposed scheme follows the following steps to authenticate the user for accessing the requested services.

For accessing the services, the user provides the URL of the cloud service provider in the web browser which sends the request to the cloud server for loading the Login GUI of the cloud service provider.
The user provides the registered username and password (first-tier authentication credentials) at the login GUI for verifying themselves to the cloud server.
If the username and password provided by the user to the cloud server is correct, then the cloud server sends the reply of validation at the user side. The application program or observer gets this validation reply at the user side

IV. IMPLEMENTATION

To solve the problem of secure authentication, we are using the concept of multi tier and multifactor authentication. In the proposed security model one time password has been used with user name and password for authenticating the user. Along with these credentials, we are using set of random questions; these questions are based upon the user's activities on web. User has to give correct answers for authenticate themselves and for getting the access.

The user sign up process starts with first tier user authentication process, user sign up interface where the user enters its static username and password details. This information moves for verification to the system's database. Once it is verified, the system generates one time password for next level authentication. This OTP is sent to user's registered email account. The OTP is valid only for 2 minutes time. The one time password is time synchronized with both the end. The session value is also attached with this OTP for better security. In next event, user has to reply with their email OTP within given time limit. If user is unable to reply with OTP within time limit, then user can request new OTP from the System.
Ones user validates two levels of authentication, system continues with next tier authentication process. In this, system generates set of eight questions randomly from their database; user has to give six correct answers of the set of questions. User has to give all the six correct answers within 2 minutes of time. For this level authentication, there will be two scenarios can occur:

i. User's time limit expires.

ii. User replies less than six correct answers.

In both the situations, user has three attempts for authentication. If user unable to authentication using three attempts, complete authentication process will start from the beginning.

Each correct answer generates a score called API score. If user's API score is greater than six, then user authentication will be successful. If user API score is less than six,then user's authentication will be failed. At this level, if user authentication fails, then the complete authentication process will restart from tier one level. If user succeeds to authenticate, then user can access services from service provider.

V. RESULT AND COMPARISON

5.1 Security Analysis

The proposed authentication technique uses three phases of authentication. First phase used to verify using the password, second phase authorizes the user using pattern matching and finally the user authenticated with the secret code.

Let Success (S) and Failure (F) be the two outcomes of the requested cloud services.
So, the outcomes of the three authentication levels are SSS, SSF, SFS, SFF, FSS, FSF, FFS, FFF and N (O) = 8 for our proposed authentication model, where, O = outcomes.

Now, let, the p = probability of the success for accessing the services at each authentication level So, success, SSS, for breaking the whole authentication system, i.e. multi-tier authentication system is denoted by P (E). Where, P (E) = p^3. This leads the failure for breaking the authentication system is 1 - P (E) = 1 - p^3.
Now, let say p = 0.2, then p^2 = 0.04 and p^3 = 0.008. It means the probability of success in breaking the whole authentication system is very less, almost zero, compared to one-tier and two-tier authentication system.
The strength of all the three tiers of the authentication system depends on the Password and pattern chosen by the user at the registration time and a secret code generated by the cloud server.
The strength of the authentication system is indirectly proportional to the probability of success in breaking the multi-tier authentication system. It means the higher the strength, the lesser the probability of success for breaking the system.

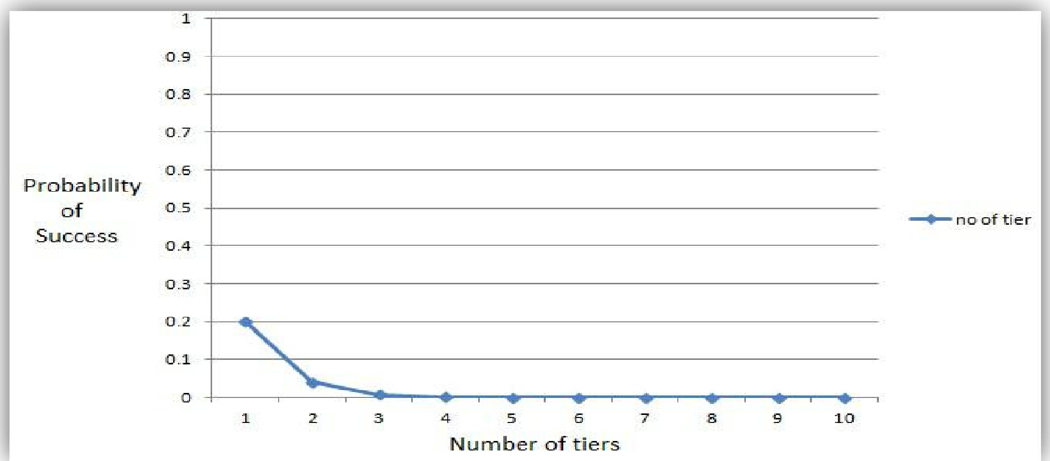

Figure 4.1: Probability of success for breaking the multi-tier authentication system

The figure 4.1 shows the relation between the probability of success and the number of tiers of the multi-tier authentication system.

Figure 4.1 clearly shows that the probability of success in breaking the multi-tier authentication system is exponentially followed with the number of tiers in the authentication system.

5.2 Space Requirements

We use the space as a second analysis parameter for our proposed authentication technique. For evaluating this parameter, we find the result of the space usage of the one-tier and two-tier authentication and analyze those results and we conclude them in the following figure 4.2. The following figure 4.2 shows the linear relationship between the spaces required to store the user's login credentials of one-tier, two-tier and three-tier authentication system.

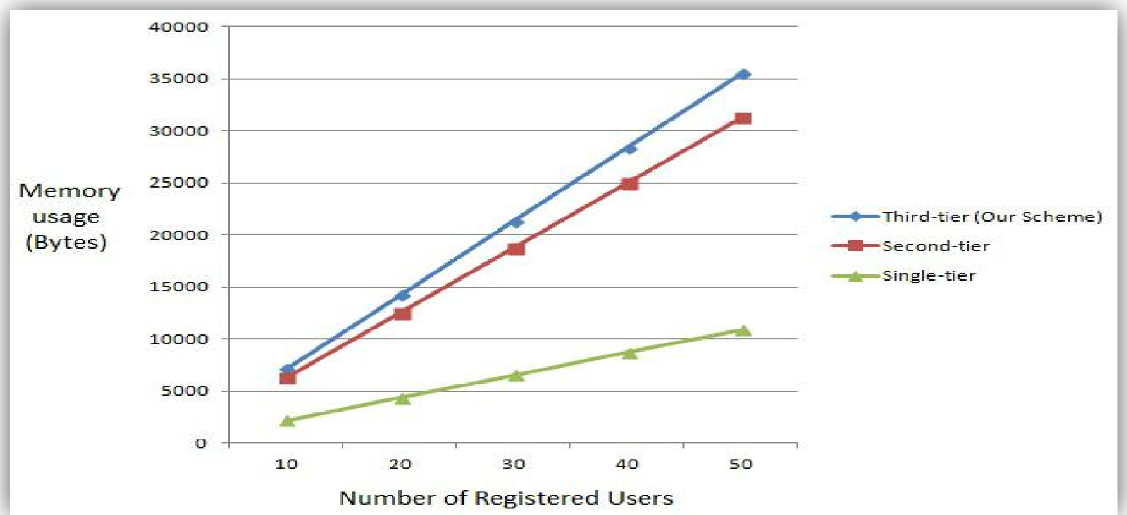

Figure 4.2: Memory space used by the registered users

From the figure 4.2, the memory space required by the user is linearly increasing as the number of users are registered themselves in the cloud application.

We find that the space is consumed by the one user's credential for one-tier authentication, two-tier authentication and three-tier authentication system.

Application required space of one user's credentials for one-tier authentication is 217 bytes, for two-tier authentication is 625 bytes and three-tier authentication (proposed technique) is 709 bytes.

If 1 million users are registered at any moment of time, then the cloud server needs 1000000 * (709-625) = 84000000 = 84MB of extra memory space to store the users' credentials. This is not a big issue while we are comparing with the security of the data.

Comparison between Existing Authentication Model and Proposed Authentication Model

The following table shows the comparison between existing authentication technique and proposed authentication technique with three comparison parameters.

Table Comparison between existing technique and proposed technique

Comparison Parameters	**Multi-tier authentication technique**	**Multi-tier authentication technique(Our Scheme)**
Probability of success (p)for breaking the authentication system (let,p=0.1)	0.01	0.001
Single-sign on access of cloud services	No	Yes
No of authentication factor	One	Two

DOI: 10.15680/IJIRCCE.2017. 0501181

VI. CONCLUSION

Any authentication system's core strength depends upon the probability of success for breaking that system for accessing the services provided by the cloud service providers. In our proposed authentication scheme, the core strength is first-tier, second-tier and third-tier authentication user credentials. For getting the access of the requested service, the attacker has to break all the authentication layers.

Security analysis says that increases as the number of authentication tiers in the system, the probability of success for breaking the multi-tier authentication system reaches near to the zero. Hence, by seeing the analysis of security, we can say that there is a very less probability of breaking the multi-tier authentication system. If we consider the usability of the storage space, then the proposed technique takes more space than the existing authentication technique which is very less and also we can say that it is negligible in the case of cloud environment where large amount of storage and its scalable.

Space requirement says that the as increases the number of registered users in the cloud application, the storage space consumed by the user's credentials are linearly increases and this will not cause more processing and fetching overhead to the cloud server. For handling the pressurized situations, this technique adds the fake screen concepts. This fake screen is not related to any software and hardware.

By using the secret code on SMTP protocol mechanism, the proposed authentication technique provides the single-sign on access of the cloud services provided by the service providers. The user has to provide a secret code which is getting on the registered mail id for accessing the particular requested service.

REFERENCES

[1] S Subashini and V Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1):1{11, 2011.

[2] HA Dinesha and VK Agrawal. Multi-level authentication technique for accessing cloud services. In Computing, Communication and Applications (ICCCA), 2012 International Conference on, pages 1{4. IEEE, 2012.

[3] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, and Hoon Jae-Lee. A strong user authentication framework for cloud computing. In Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, pages 110{115. IEEE, 2011.

[4] Ms. Shilpi Harnal Deepak Bagga. Single sign-on authentication model for cloud computing using kerberos. 2013.

[5]Maninder Singh and Sarbjeet Singh. Design and implementation of multi-tier authentication scheme in cloud. International Journal of Computer Science Issues (IJCSI), 9(5), 2012.

[6] Peter Mell and Tim Grance. The nist definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2009.

[7] Panagiotis Kalagiakos and Panagiotis Karampelas. Cloud computing learning. In Application of Information and Communication Technologies (AICT), 2011 5th International Conference on, pages 1{4. IEEE, 2011.

[8]Barrie Sosinsky. Cloud computing bible, volume 762. John Wiley & Sons, 2010.

[9]Rasib Hassan Khan, Jukka Ylitalo, and Abu Shohel Ahmed. Openid authentication as a service in openstack. In Information Assurance and Security (IAS), 2011 7th International Conference on, pages 372{377. IEEE, 2011.

[10]Davit Hakobyan. Authentication and authorization systems in cloud environments. 2012.

[11]David Chou. Strong user authentication on the web. http://msdn. microsoft.com/en-us/library/cc838351.aspx, August 2008.

[12]Federal Financial Institutions Examination Council. Authentication in an internet banking environment. 2011.

[13]William E Burr, Donna F Dodson, and William T Polk. Electronic authentication guideline. Citeseer, 2004.

[14] Ashish G Revar and Madhuri D Bhavsar. Securing user authentication using single sign-on in cloud computing. In Engineering (NUiCONE), 2011 Nirma University International Conference on, pages 1{4. IEEE, 2011.

[15] Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank Verma, Vijay K Chaurasiya, and Rahul Gupta. An architecture based on proactive model for security in cloud computing. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, pages 661{666. IEEE, 2011.

[16] Wenjun Zhang. 2-tier cloud architecture with maximized ria and simpledb via minimized rest. In Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, volume 6, pages V6{52. IEEE, 2010.

[17] Fengyu Zhao, Xin Peng, and Wenyun Zhao. Multi-tier security feature modeling for service-oriented application integration. In Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on, pages 1178{1183. IEEE, 2009.

[18] Zubair Ahmad, JA Manan, and Suziah Sulaiman. Trusted computing based open environment user authentication model. In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, volume 6, pages V6{487. IEEE, 2010.

[19] Ali A Yassin, Hai Jin, Ayad Ibrahim, and Deqing Zou. Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. In Cloud and Green Computing (CGC), 2012 Second International Conference on, pages 282{289. IEEE, 2012.

[20] Sanjeet Kumar Nayak, Subasish Mohapatra, and Banshidhar Majhi. An improved mutual authentication framework for cloud computing. International Journal of Computer Applications, 52, 2012.

[21] Sarbjeet Singh and Seema Bawa. A privacy policy framework for grid and web services. Information Technology Journal, 6(6), 2007.

[22] Sarbjeet Singh and Dolly Sharma. An access control framework for grid environment.

[23] Sarbjeet Singh. Trust based authorization framework for grid services.Journal of Emerging Trends in Computing and Information Sciences, 2(3):136{144, 2011.