Multi-Authentication for Cloud Security: A Framework

Satish Kumar
Department of Computer Science
HPU Shimla, India
171005
skumar.hpu@gmail.com
+919459037786

Anita Ganpati
Department of Computer Science
HPU Shimla, India
171005
anitaganpati@gmail.com
+919459132308

Abstract-Cloud computing is a multi-tenant computational paradigm that offers an efficient, elastic and scalable business model for organizations to adopt various information technology (IT) resources i.e. software, hardware, network, storage, bandwidth etc. There are various aspects of security problem in cloud computing field which include data security, privacy and users' authenticity. The purpose of this research paper is to construct a framework for secure and more advanced authentication scheme for executing secure transactions in a cloud environment. For any cloud service which deals with personal and private information exchange, single tier authentication is not adequate. Authentication schemes that imply more than one tier for authentication are comparatively safer than single tier authentication scheme. This work proposes a scheme in which authentication process is carried out in two levels or two tiers. First tier uses simple username and password on a standard cloud user's interface. Second tier is use of any personal device like mobile which have a unique id and in possession of the authenticated user only. The advantage of this scheme is that it enhances the strength of authentication as if cloud server has to authenticate the standard user password and id as well as the associated device's id and password simultaneously with each other.

Keywords: Cloud Security, Multi-authentication, IaaS, Multitenancy, Paas, SaaS, Virtualization, two-tier.

I. INTRODUCTION

Cloud computing is a flexible way to allocate Information Technology (IT) resources i.e. storage, software, infrastructure and bandwidth etc. hp universitysout of a pool, enabling to consume processing power according to user's needs [13]. It makes easy to set up and use server instances, allowing the size of the infrastructure to grow when there is a need to scale up business while saving costs when the users do not need the extra power anymore.

As information technology is growing rapidly, there has been very fast advancement in various computing technologies like multimedia, internet technology etc. With the advancement of internet technology, many works are done online. This includes banking, shopping, e-learning, entertainment, chatting, information retrieval and financial transactions etc. All these online activities require some type of authentication. Authentication means to check the identity of the user, which means whether the person is same which he pretends to be. In case of financial transactions, security of information is required to carry out secure transaction. Information in case of online financial transaction includes individual's authentication parameters and some other account related information etc. There are various authentication techniques that are already in use, e.g. user name, passwords, biometric face recognition, public key infrastructure and symmetric key based authentication schemes etc. Authentication schemes are key techniques to verify the correctness of the identities of all communication entities [6].

Authentication is quite challenging and difficult in the case of cloud computing. In cloud computing, a third party is responsible for providing computational power, storage space and application support etc. Every data which is used by a user is stored in cloud database. Cloud database is maintained by third party cloud provider, so user hesitates to keep his data at cloud database. In order to utilize the resources of cloud, user has to provide some identity stating that it is valid person seeking permission to use their resources. If a user needs to use or control a remote server or process financial transactions, the user needs to pass the authentication phase first [18].

A. *DEFINITION OF CLOUD COMPUTING*

The most widely used definition of the cloud computing model is introduced by National Institute of Standards and Technology (NIST) [13] as "a model for enabling 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."

According to Electrical Engineering and Computer Sciences (EECS) University of California at Berkeley, cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centres that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The data centre hardware and software is what we will call a cloud [11].

B. *CHARACTERISTICS*

Main characteristics of cloud computing are shared infrastructure, broad network access and handle metering which are defined below [3]:

1) Shared Infrastructure: Cloud environment uses an effective software model that allows sharing of physical services, storage and networking capabilities among users. The cloud infrastructure is to find out most of the available infrastructure across multiple users [3].

2) Network Access: Cloud services are accessed over a network from a wide range of devices such as Personal Computers (PCs), laptops, and mobile devices by using standards based Application Programming Interfaces (APIs) [3].

3) Handle Metering: Cloud service providers store information of their clients for managing and optimizing the service and to provide reporting and billing information. Due to this, customers are payable for services according to how much they have actually used during the billing period [3].

C. *CLOUD COMPUTING MODELS*

Basically there are two types of models of cloud computing which depends upon the way how these models are deployed and services they provide. These are known as deployment models and service models. Each of these models is described below:

1) *Deployment Models*

According to NIST [13], deployment models refer to those models which are based upon the deployment of different computing resources. There are following type of deployment models defined by NIST [13]:

a) Private cloud: The cloud infrastructure is operated solely for an organization. A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings [13].

b) Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns e.g. mission, security requirements, policy and compliance considerations. The goal of a community cloud is to make realize the participating organizations about the benefits of a public cloud such as multi-tenancy and a pay-as-you-go billing structure but with the added level of privacy, security and policy compliance usually associated with a private cloud [13].

c) Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. In a public cloud model resources such as applications and storage, can be accessed by the general public over the internet. Public cloud services may be free or offered on a pay-per-usage model. The main advantage of the public model will be that user have to pay only for what we need, hence no resource wastage [10].

d) Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. A hybrid cloud includes a variety of public and private options with multiple providers. Private cloud customers can store personal information on their private cloud and use the public cloud for handling large amount of processing demands [10].

2) *Service Models*

A cloud can provide access to software applications such as email or office productivity tools (the Software as a Service or SaaS, service model), or can provide a toolkit for customers to use to build and operate their own software (the Platform as a Service or PaaS, service model), or can provide network access to traditional computing resources such as processing power and storage (the Infrastructure as a Service or IaaS, service model) [13]. The different service models have different strengths and are suitable for different customers and business objectives. Generally, interoperability and portability of customer workloads is more achievable in the IaaS service model because the building blocks of IaaS offerings are relatively well-defined e.g. network

protocols, Central Processing Unit (CPU) instruction sets, legacy device interfaces. There are following type of cloud service models:

a) *Cloud Software as a Service (SaaS):* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure through a thin client interface such as a web browser e.g. web-based email. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [15].

b) *Cloud 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 and tools supported by the provider [8]. PaaS services are software design, development, testing, deployment, and hosting.

c) *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provide processing, storage, networks, and other fundamental computing resources (such as virtual machine, disk image library, and file-based storage, firewalls, load balancers and Internet Protocol addresses) where the consumer is able to deploy and run arbitrary software, which include operating systems and applications. In IaaS most of the services are provided virtually on Virtual Machines (VMs) e.g. data storage, firewalls and networks etc. [12].

D. *NEED OF THE STUDY*

Like all computing systems, security of cloud computing systems is also a very critical issue which must be examined very earlier from the initial stages i.e. requirements stages and design stages of its development process. As we know that cloud relies in a multi-tenant environment and thus multiple users can store and access information on the same cloud, authenticity of different users is an important security aspect. Hence there is a need of having strong authentication technique for cloud users. The focus of this research paper is based on existing literature and to define a strong multi-authentication framework for cloud providers that will help them in cloud users' authentication, which is of high importance.

There must be a strong authentication mechanism to check the authenticity of all cloud users and hence to prevent the unauthorised access to the stored information on the cloud.

E. *OBJECTIVES OF THE STUDY*

The objective is to develop an effective and secure authentication method for cloud computing system which will help cloud providers to avoid unauthenticated access to the cloud.

II. LIITERATURE REVIEW

Cloud computing security challenges and issues are discussed by various researchers. In this section various literature reviews of different researchers are presented.

Subashini et al. [17] discussed the various security challenges of the service delivery model in cloud computing, which were focused on the SaaS and also analyzed critical areas of cloud computing. They derived a set of best practices for the cloud providers, cloud users and cloud security vendors to follow in each domain.

Brian Hay et al. had focused on data authentication, data integrity, querying and outsourcing the encrypted data. They clarified issues using the digital forensics techniques namely the ephemeral nature of cloud resources and seizing a "system" for examination [5].

Sarbjeet Singh and Maninder Singh proposed a multi-authentication scheme for cloud security in which authentication process is carried out in two tiers. First tier uses general username and password. Second tier is pre-determined series of steps. The advantage of this scheme is that it does not require any additional hardware and software. So this can be used and accessed from anywhere across the globe. They concluded that the strength of any authentication technique depends upon the probability of breaking that technique [16].

Amlan et al. proposed a framework which provides identity management, mutual authentication and session key establishment between the users and the cloud server. They proposed a scheme that verifies the user authenticity using two-step verification, which is based on password, smartcard and out of band authentication. The advantage of this scheme is that certain authentication control lies towards client side. Disadvantage of this technique is requirement of additional hardware and software to carry out the processes, which make it little hectic [2].

Q Wang et al. described that cloud computing has been envisioned as the next generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy. They studied the problem of ensuring the integrity of data storage in cloud computing. They first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in their protocol design [14].

Abdul Ghafoor and Sead Muftic designed a secure software distribution system which was based on well-established standards and protocols like FIPS-196 based extended strong authentication protocol and SAML based authorization security policies. They also designed secure execution environment which is capable to execute signed and encrypted software modules, supports standard security services and network security protocols [1].

Gansen Zhao et al. summarized the security concerns in cloud computing and proposes five service deployment models to ease these concerns. The proposed models provide different security related features to address different requirements and scenarios and can serve as reference models for deployment. They stated that while making decisions on adopting cloud computing related solutions, security has always been a major concern. [9].

Dimitrios Zissis and Dimitrios Lekkas aimed at two points; first to evaluate cloud security by identifying unique security requirements and second to attempt to present a viable solution that eliminates these potential threats. This paper proposed introducing a trusted third party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure (PKI) operating in concert with Single Sign-On (SSO) and lightweight directory Access Protocol (LDAP), to ensure the authentication, integrity and confidentiality of involved data and communications [7].

According to B. Zou and H. Zhang, trusted cloud can be obtained through system security and trusted environment. Trusted Cloud Group (TCG), a group of cloud computing professionals, proposed an authenticated boot and platform attestation function which is implemented by Trusted Platform Model (TPM). A caveat to this model is that the security component of the proposed solution is only meant for service users and not for service providers [4].

III. EXISTING SINGLE AUTHENTICATION FRAMEWORK IN CLOUD

In single authentication technique, user is provided with a single user id and password which he uses to sign-in to the cloud website. In this authentication system, insider attack can be more successful as it is easy for an insider to get first tier authentication credentials (i.e. user id and password). This single authentication system is shown in Figure 1 below:

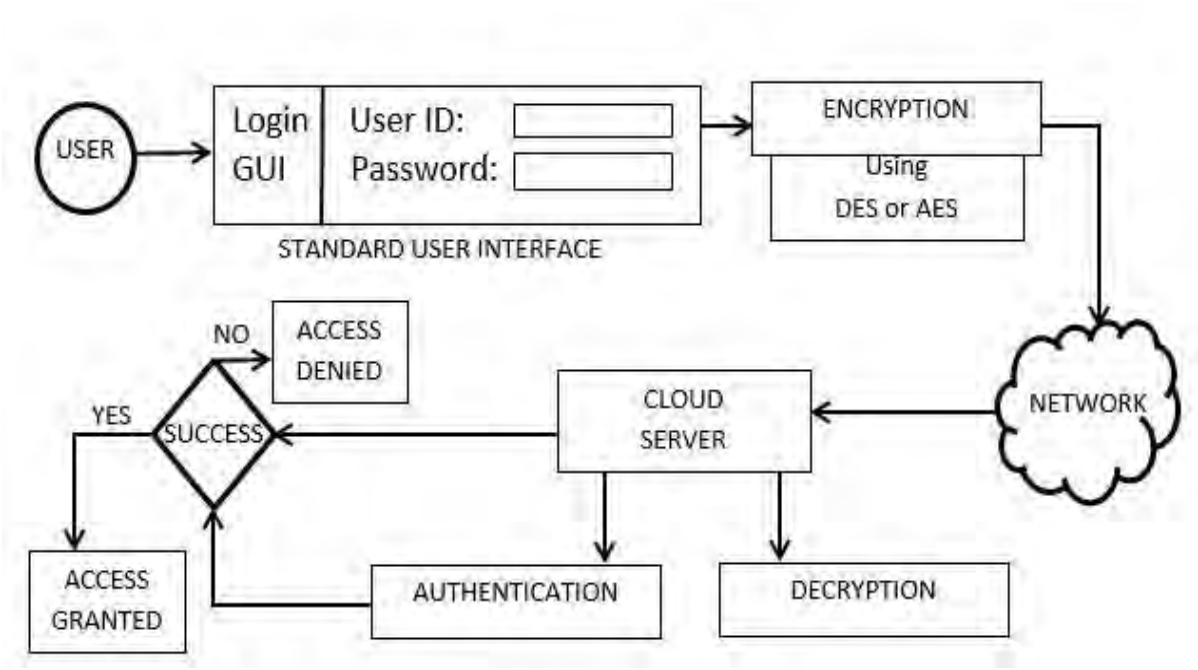

Figure 1. Single authentication framework in cloud

In the existing authentication system, single authentication is not enough for the cloud security. As shown in Figure 1, suppose if you are using only one authentication credential like user id and password only and if the hacker is able to get this information (i.e. user id and password), he will surely get access to the stored data at cloud. So we need such an authentication system in which even if the hacker is able to get one credential, still he should not be able to access the user data and that is where multi-authentication plays role.

IV. PROPOSED FRAMEWORK FOR USER MULTI-AUTHENTICATION IN CLOUD

The proposed authentication scheme is divided into two tiers. First tier authentication uses the encryption decryption mechanism as followed in normal authentication schemes. The second tier authentication requires the user to input another password from his personal device like mobile which have a unique id (such as

International Mobile Station Equipment Identity (IMEI) in case of mobile phone) which will be generated from cloud server and sent over to the user's personal device. When the login screen appears in the user interface of computer and user enters the required cloud id and password, a One-Time Password (OTP) must be generated from the server and sent to the cloud user's registered personal device. Then user must enter that password in the personal device and send to the cloud server. User may send this device through simple Short Message Service (SMS) or may use any standard cloud mobile application of specific cloud server. Then both the standard user password entered in computer's login interface as well as the password entered in user's personal device's interface is authenticated at the (cloud) server end. If any of the authentications fails, the cloud access will be denied. The overall working is explained in 9 steps as shown in Figure 2.

A. Step wise working of proposed framework is explained below:

Step 1: User enters the URL of cloud provider website in his browser. Login GUI is loaded in the browser.

Step 2: User enters his first tier credentials (username and password). These credentials are passed to the cloud server for validation as shown in Figure 2.

Step 3: Cloud server checks for first tier credentials. If the username and password are correct then cloud server sends One-Time Password (OTP) to the client (cloud user).

Step 4: Upon receiving OTP at the client end, user enters the password in his registered personal device's interface and send back to the cloud server.

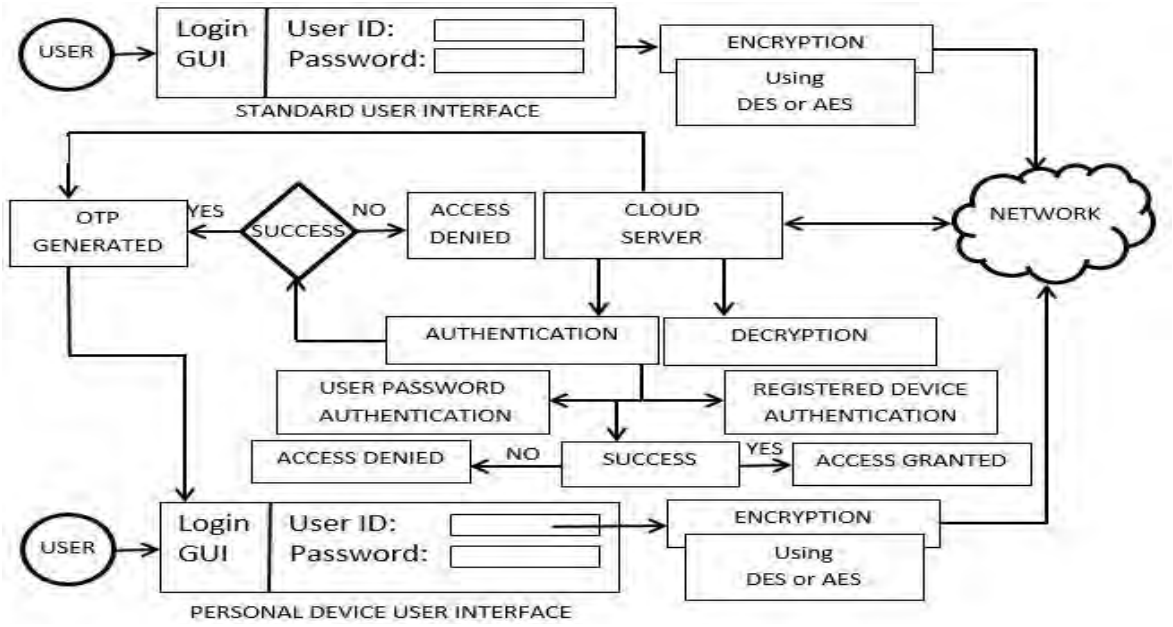

Figure 2. Working of proposed multi-authentication framework

Step 5: Cloud server checks the password as well as the device's id for authentication.

Step 6: If authentication is successful, direct communication between client and cloud server is established and user is allowed to access the cloud data.

B. Security Analysis

In this section, security of proposed multi-authentication framework is analysed and presented. It is shown here that proposed authentication framework for cloud computing system is much stronger than existing single-tier authentication framework.

1) *Single-tier Authentication Security Strength:* In a single-tier authentication if hacker, anyhow, able to hack the password or any insider attacker reveals or steal the cloud user id and password, he will surely get access to the stored cloud data, because there will be no other way to stop him or authenticate him again to access cloud data. Now suppose there are "n" numbers of cloud users at a time trying to login and access their data on cloud. Let the probability of success of hacking is "p". Now the probability of success for hacker to get any cloud user's credentials (user id and password) is 1/n.

Now let us take some values of "n" and see how probability of success varies with this value "n". These values are shown in Table I below:

TABLE I. VARIATION OF PROBABILITY OF SUCCESS W.R.T NUMBER OF CLOUD USERS IN SINGLE-TIER AUTHENTICATION SYSTEM

Value of "n"	Probability of Success "p"
10	0.1
100	0.01
1000	0.001
10000	0.0001

It is clear from the above table that the probability of success of hacker is inversely proportional to the number of cloud user. As number of cloud user increases, probability of success of hacking decreases and vice versa. For the same table, a graph is drawn in Figure 3 below which shows the variation of probability of success of hacking with respect to the number of cloud users.

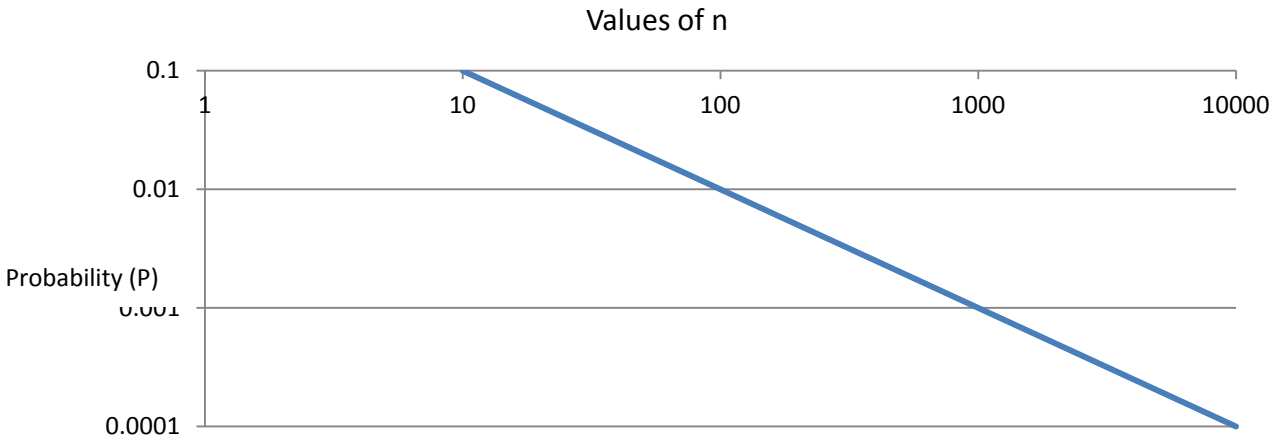

Figure 3. Probability of success of hacking versus number of cloud users in single-tier authentication framework

2) *Proposed Multi-authentication System Strength:* In proposed scheme, the second password is generated from cloud server and is also for one time use only, that is, it will be One-Time Password (OTP), and so it will be more secure. Now suppose if cloud user enters id and password in the standard user interface and even if it is hacked in the network, the hacker will not be able to get the control and access the cloud user's data. Because as if first tier authentication is successful, the cloud server will send the One-Time Password (OTP) to the cloud user's registered personal device and will wait for its reception and authentication. Then only if both tiers' authentication is successful, access will be granted to the cloud user.

For first factor authentication, if encryption key is of length 256 bits then there are 2^{256} different combination for a particular key. In the proposed scheme, the strength of second tier authentication is as follows. Now suppose if there are "n" number of cloud users who are logging to cloud service at a time, then the probability of a specific user's account to be hacked is 1/n. In addition, as proposed in this scheme, suppose there are "k" number of registered personal devices, so probability of getting hacked the specific user's OTP is also 1/k. Furthermore, the probability of getting password hacked of the same cloud user's standard user password as well as personal device's password simultaneously is 1/(n*k). Moreover, if the registered personal device's password is hacked, hacker will not be able to send that password from that device and hence authentication will fail again.

Suppose at any time, n=10 and k=10, probability of success for hacker is 1/(10*10) which will be equal to 1/100=0.01. If n=100 and k=100, probability of success is 1/(100*100) which will be equal to 1/10000=0.0001. A table is made for some value of k and n as shown in Table II below:

TABLE II. PROBABILITY OF SUCCESS OF HACKING W.R.T NUMBER OF CLOUD USERS AND PERSONAL DEVICES IN PROPOSED MULTI-AUTHENTICATION FRAMEWORK

Number of cloud users (n)	Number of personal devices (k)	Probability of success (P)
10	10	0.01
100	100	0.0001
1000	1000	0.000001
10000	10000	0.00000001

It can be seen clearly from the above table that the probability of success for hacker decreases as the value of n and k increases. Also a graph has been drawn against number of cloud users and devices versus probability of success of hacking which is shown below in Figure 4.

On the basis of the graph it can be seen clearly that probability of success of hacking user password is inversely proportional to the number of cloud user standard devices as well as number of registered personal devices. It can also be seen that the probability approaches to zero as the value of n or k increases as shown in Figure 4 above.

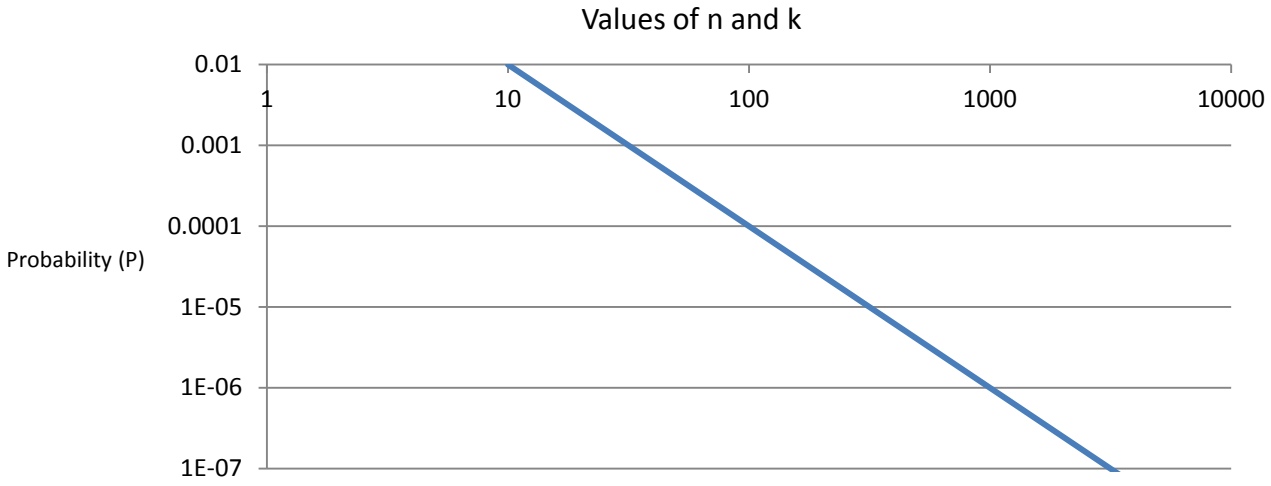

Figure 4. Probability of hacking versus n and k in proposed multi-authentication framework

C. Comparison of proposed multi-authentication system and single-tier authentication system

Suppose "n1" is the number of cloud users in a single-tier authentication system and "n2" is the number of cloud users in proposed multi-tier authentication system, where n1=n2. Now "k" is the number of registered personal devices in multi-tier authentication system. Suppose "p1" is the probability of success of hacking in single-tier authentication system and "p2" is the probability of success of hacking in proposed multi-authentication system. A table is drawn for some values of n1, n2 and k and respective probability values p1 and p2 as shown below in Table III:

TABLE III. PROBABILITY OF SUCCESS IN BOTH THE SINGLE-TIER AND PROPOSED MULTI-AUTHENTICATION SYSTEM

Number of cloud users in single-tier authentication system (Suppose n1)	**Number of cloud users and personal devices in proposed multi-authentication system (Suppose n2=n*k)**	**Probability of success of hacking in single-tier authentication system (Suppose p1)**	**Probability of success of hacking in multi-tier authentication system (Suppose p2)**
10	10*10=100	0.1	0.01
100	100*100=10000	0.01	0.0001
1000	1000*1000=1000000	0.001	0.000001
10000	10000*10000=100000000	0.0001	0.00000001

According to Table III, it can be seen that due to the introduction of another personal device which has to be registered in the cloud at the time of new registration for cloud services, probability of success of hacking decreases more than that of a single-tier authentication system.

Now finally a combined graph is constructed for both single-tier authentication framework and proposed multi-authentication framework below in Figure 5. It will help to visualize the variation of probability of success in both the frameworks (i.e. single-tier framework as well as proposed multi-authenticated framework for cloud users).

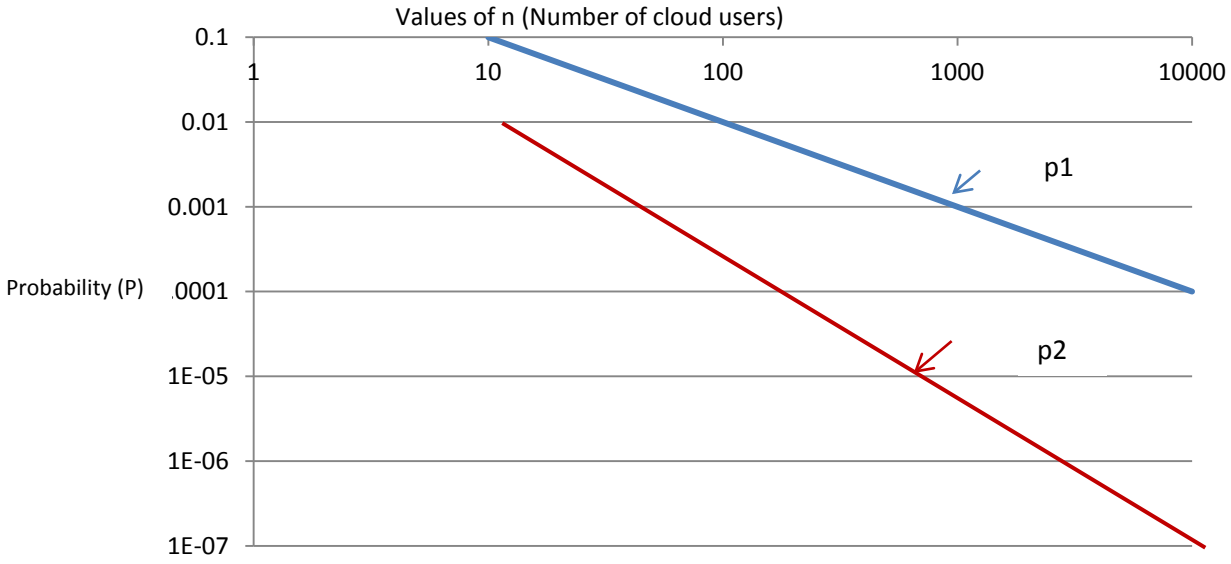

Figure 5. Probability of success of hacking versus number of cloud users in single-tier and multi-authentication system

It is clear from the graph that the probability of success of hacking in proposed multi-authentication framework decreases quite fast than that of single-tier authentication framework. The probability of success decreases "1/k" times more in the proposed multi-authentication framework. So according to the proposed framework, as the number of cloud users will increase, number of registered personal device will also increase (i.e. "k") and the probability of success of hacking will decrease correspondingly.

V. CONCLUSION AND FUTUTRE SCOPE

The strength of any authentication technique depends upon the probability of breaking that technique. As shown in the Figure 4, the probability is inversely proportional to the number of cloud users standard devices and personal registered devices. As the number of standard devices and number of registered personal devices (denoted by n and k respectively) increases, the probability of breaking the multitier authentication technique approaches zero. Hence, it can be concluded that there is very less probability of hacking the user password due to second factor (i.e. personal device password) authentication. In terms of performance, multitier authentication technique no doubt increases overhead slightly like CPU time, OTP generation and authentication time etc. but this slight overhead is negligible and can be overlooked in case of cloud computing which provides high processing power, storage capacity and scalability.

In future, we will work on the case in which the secondary device (i.e. personal user device) is lost or maybe stolen intentionally by someone to illegally access the cloud data of that user. If it happens, OTP will be send to the registered personal device and if that person has first tier credentials of cloud user already, he can surely access the cloud data. In that case there must be some security mechanism to avoid misuse of that device. Also, a secure mechanism will be built to register again the new personal device with the cloud provider. Thus this total multi-authentication system will be more secure and robust which will help in improving the security of cloud systems and will surely remove the fear of authentication issues among cloud users.

REFERENCES

[1] Abdul Ghafoor and Sead Muftic, "CryptoNET: Software Protection and Secure Execution Environment", International Journal of Computer Science and Network Security (IJCSNS), at The Royal Institute of Technology, DSV, Borgarfjordsgatan 15, SE-164 40, Kista, Sweden, VOL.10 No.2, February 2010.

[2] Amlan, "A Strong User Authentication Framework for Cloud Computing", Asia- Pacific Services Computing Conference, IEEE Computer Society, pp 110-115, September 2011.

[3] Ayesha Malik and Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", Department of Computer Science, Lahore College for Women University, Lahore, Pakistan. Vol. 3, March 2012.

[4] B. Zou and H. Zhang, "Toward enhancing trust in cloud computing environment", 2nd International Conference on Control, Instrumentation and Automation, September 2011.

[5] Brian Hay, Kara Nance and Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences, August 2011.

[6] Chun-I Fan, Pei-Hsiu Ho and Ruei-Hau Hsu, "Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications", IEEE/ACM Transactions on Networking, Vol. 18, No. 3, June 2010.

[7] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future generation computer systems, Department of product and system design engineering, University of Aegean, Greece, June 2012.

[8] European Network and Information Security Agency (ENISA), "Cloud computing: benefits, risks and recommendations for information security," November 2009.

[9] Gansen Zhao, Martin Gilje Jaatun, Chunming Rong and Frode Eika Sandnes, “Deployment Models: Towards Eliminating Security Concerns From Cloud Computing”, IEEE, Reprinted from “International Conference on High Performance Computing and Simulation”, ISBN 978-1-4244-6828-7, March 2010.
[10] Judith Hurwitz, Robin Bloor, Marcia Kaufman and Dr. Fern Halper, "Service oriented architecture (SOA for dummies)", 2nd IBM limited addition, Published by Wiley Publishing, Inc., Indianapolis, Indiana, March 2009.
[11] Michael Armbrust and Armando Fox, "Above the clouds: A Berkeley view of cloud computing”, Electrical engineering and computer sciences university of California at Berkeley, Technical Report No. UCB/EECS-2009-28, February 2009.
[12] Mohamed Al Morsy, John Grundy and Ingo Müller, "An analysis of cloud computing security problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, November 2010.
[13] Peter Mell and Tim Grance, "The NIST definition of cloud computing", at National Institute of Standards and Technology, Gaithersburg, MD 20899-28930, September 2011.
[14] Q Wang, C Wang, J Li, K Ren and W Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing”, Computer Security-ESORICS, Springer, 2009.
[15] Ristenpart, T. Tromer, E. Shacham and H. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”, In Proceedings of the 10th association of computer machinery (ACM) conference on Computer and communications security (CCS), November 2009.
[16] Sarbjeet Singh and Maninder Singh, “Design and Implementation of Multi-tier Authentication Scheme in Cloud” Published in International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 5, No. 2, at Computer Science and Engineering, UIET, Panjab University, Chandigarh, India, September 2012.
[17] S. Subashini and Kavitha, "A metadata based storage model for securing data in cloud environment", Journal of Network and Computer Applications, vol. 298, In Press, Corrected Proof, June 2011.
[18] Wen Shenq, Juang, Sian Teng Chen and Horng Twu Liaw, “Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards”, IEEE, Transaction on Industrial Electronics, Vol. 55, No. 6, June 2008.