A lightweight Multi-tier Authentication Method in Cloud Computing

[1]Mayank Gaurav, [2]Jasvinder Pal Singh, [3]Gaurav Shrivastav
[1,2,3]Dept. of CSE, RKDF IST, Bhopal, MP, India

Abstract
Cloud computing has great potential of providing robust computational power to the society at reduced cost. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Cloud storage moves the user's data to large data centers, which are remotely located, on which user does not have any control. This unique feature of the cloud poses many new security challenges which need to be clearly understood and resolved. A key area in security research is authentication. Authentication means to check the identity of the user, which means whether the person is same which he pretends to be. This paperpresents overview of different authentication methods and then proposes a scheme in which authentication process is carried out in two levels or two tiers. The advantage of this work is that it does not require any additional hardware and software. So this can be used and accessed from anywhere across the globe

Keywords
Cloud Computing, Cloud Security, Authentication

I. Introduction

Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure.
Among the biggest commercial providers of cloud computing are Amazon, Google,Force.com and Microsoft have their own definitions. The NISThas introduced a broad definition, which contains most of the definitions given by cloud computing providers.

According to the National Institute Standards and Technology (NIST) [3], Definition of cloud computing is:
" Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"
As mentioned in the definition, cloud computing is typically known by five essential characteristics which are on-demand self-service, broad network access, Resource pooling,Rapid elasticity and Measured service. The four deployment modelsare private cloud, community cloud, public cloud and hybrid cloud. These deployment models tell about the different usage of cloud computing.The services [4] provided by cloud computing are mainly of three types, namely infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

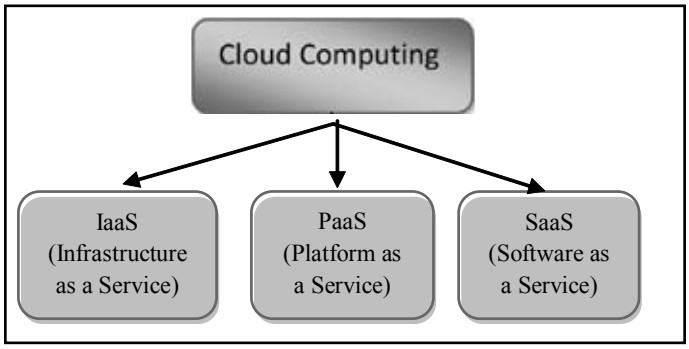


Fig. 1: Taxonomy of Cloud Computing Models

This paper presents overview of Cloud computing in Section 1 as introduction. Section II presents literature review. Proposed Multi-Tier authenticationscheme is described in Section III. Section IV shows results carried out andfinallySections 5conclude the paper and talks about future plans.

II. Literature Review

With the rapid development of cloud computing technologies, more and more computers connect together to exchange great information and share system resources. Security is then an important issue for computer networks. To prevent the information from being accessed by illegitimate or unauthorized users, authentication of users is certainly one of the most important services. User authentication is the essential security mechanism to establish the trust relationship under open network environments.
Authentication [5] is a process of validating who are you to whom you claimed to be or a process of identifying an individual. Even before computers came along, variety of distinguishing characteristics were used to authenticate people. Computer systems have applied characteristics for user authentication.
The authentication approaches can be classified into three types according to the distinguishing characteristics they use, as presented in fig. 2:

- What the user knows—knowledge-based authentication(e.g., password, PIN, pass code)
- What the user has—possession-based authentication(e.g., memory card and smart card tokens)
- What the user is—biometric-based authentication: physiological (e.g., fingerprint) or behavioral (e.g.,keyboard dynamics) characteristics.

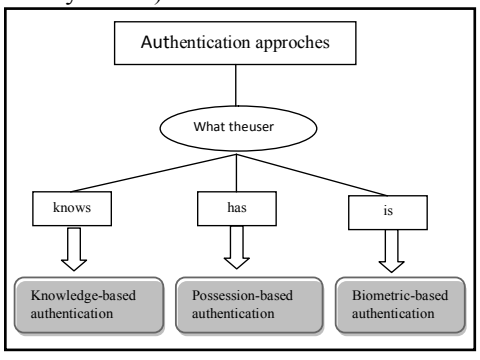


Fig. 2: Classification of Authentication Methods

The most widely used type of authentication is knowledge based authentication[6]. Examples of knowledge-based authentication include passwords, pass phrases, or pass sentences graphical passwords and Personal Identification Numbers (PINs). In this scheme the user enters or logs in into the system through his username and password. The system first authenticates the user from the user database and on the basis of authentication of the user and then grants the access to the system is granted.

Possession-based authentication [7], referred to also as token-based authentication, is based on what the user has. It makes use mainly of physical objects that a user possesses, like memory card and smart card tokens.

Biometric-based authentication [8] is based on what the user is i.e. based on the fact that certain physiological or behavioral characteristics of a person reliably distinguishable. Thus, it is possible to establish an identity based on who the user is, rather than on what the user possesses or knows and remembers.

In choosing an authentication method a number of factors [2]need to be considered: security effectiveness, ease of implementation,ease of use, and user attitude and acceptance. Erlich, Z.et.al.[11]shows ranking of authentication types based on above four factors as in Table 1.

Table 1: Ranking of Authentication Types From 1 (Low) to 3 (High)

Factor / Authentication type	Security effectiveness	Easy of implementation	Easy attitude of use	User and acceptance
Knowledge Based	1	3	3	3
Possession-Based	2	2	2	2
Biometric-Based	3	1	1	1

Authentication types canbe implemented alone or in combination. FFIECL et.al.[5],William E. Burr et al.[9], Dineshaet.al. [1] shown that multitierauthentication schemes are more secure than single-tierschemes. Single-tier schemes are prone to insider attack.So it is desirable to have more than one tier authentication.

To strengthen the authentication process, a simple approach is to use one/combination of the above techniques in multi-level authentication, so that, probability of breaking such a password is reduced to a large extent. A knowledge based authentication technique is more liked and accepted by user, so paper proposed a secure authentication technique by using core featuresof knowledge based and multi-level authentication.

III. Proposed User Authentication

The proposed authentication work is divided into two tiers. First tier takes UserId and a VarSent (variable length string) and sends it to cloud server. The VarSent is not pre-defined. In second tier user submits the password and a VarToken (string token, based on the VarSent).After verifying the credentials, user is allowed to use services.

In proposed work some notations are used. List of those notations and their meaning are listed in Table 2.

Table 2: Terminology Used in Our Authentication Scheme

Notation	Meaning
UserId	User Identification
Pwd	Password
VarSent	Combination of words or Phrase
VarToken	Combination of characters associated with VarSent
SessId	Session associated with UserId
AuthServer	Authentication Server
AuthWin	Authentication Window

This technique authenticates the cloud access in two tiers. Here UserId and Password are not sent together. At first tier user sends only UserId along with VarSent. A VarSent is a group of words or a phrase,which user can memorized easily. Every time user can choose different VarSent. On receiving UserId and VarSent, AuthServer saves the VarToken and creates a session, say SessId. Here, VarToken is initial letters of each word of VarSent. Now,AuthServer sends SessId to user with next Authentication window. On receiving Authentication window, user enters his password and VarToken. When password and VarToken is matched at the AuthServer for corresponding session against SessId, user is authenticated and allowed to use services.

As shown in fig. 3 the basic idea of the proposed work is as follows:

First user registered with the cloud service provider and gets its UserId and Password. Whenever the user wants to communicate with cloud Server, he must go through the following steps to authenticate himself.

STEP 1: User enters his UserId and a VarSent. Here, VarSent is a group of any variable length phrase which is not predefined i.e. every time when user wish to login he can choose VarSent by his choice.

STEP 2: At Server side, UserId is checked and if UserId is found, corresponding VarSent is saved for that UserId. Here, server also generates the SessId. After that Server sends Authentication window to the user.

STEP 3: On receiving the Authentication window, user enters his pwd and VarToken. Here, VarToken is associated with VarSent.

STEP 4: Received pwd and VarToken is verified at the server for UserId. After verification user is allowed to access data.

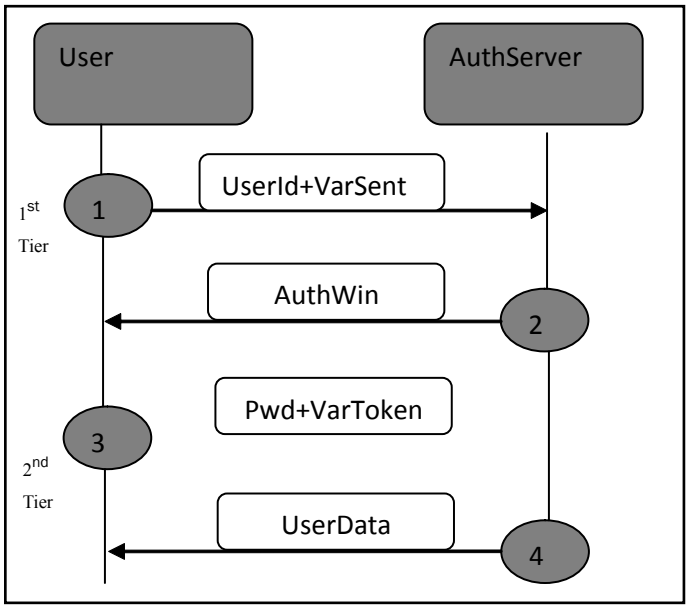


Fig. 3: Login and Authentication Phaseof Proposed Work

IV. Result Analysis

The multi-tier authentication technique proposed has been implemented on oracle cloud and Eclipse IDE (Integrated Development Environment). Development of application on cloud server has been made using Eclipse IDE by installing oracle SDKplug-in package .The analysis of various parameters of results has been checked on oracle cloud server. This is divided into two sections. First section 4.1 is about security and space analysis and second section 4.2 gives some general features of proposed work.

A. Security and space requirement analysis for proposed work is as follows:

Security Analysis

Probability of breaking multi-tier authentication to access data can be formulated by using the probability theory [10].

1. Let probability of successfully authentication at first tier is P1 and at second tier is P2 then for multi-tier system probability (say P3) of success becomes P1*P2.

Table 2 is drawn for some values for P (1) and P (2).Table's cell values is probability of success P(S) calculated by using P (3) =P (1)*P (2).

Table 3.Probability of success P (3) at multi-tier based on 1stand 2nd tier's Probability P1 & P2

value of P(2) \ value of P(1)	0.01	0.02	0.03	0.04	0.05
0.01	0.0001	0.0002	0.0003	0.0004	0.0005
0.02	0.0002	0.0004	0.0006	0.0008	0.001
0.03	0.0003	0.0006	0.0009	0.0012	0.0015
0.04	0.0004	0.0008	0.0012	0.0016	0.002
0.05	0.0005	0.001	0.0015	0.002	0.0025

Based on Table 3, a graph is drawn as shown in fig. 5. Value of P (2) is also shown in the graph.

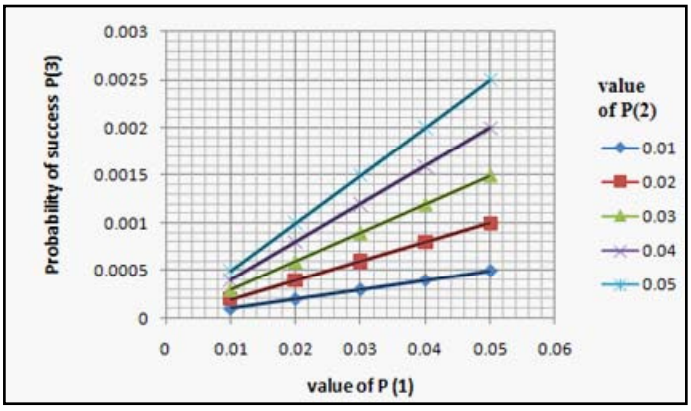


Fig. 4: Probability of Success P(S) Where x-Axis Shows Probability at 1SttierP(1) and y-axis Shows Probability at Multi-tier.P (2) is Probability of Success at 2nd tier

From fig. 4, we observed that calculated value of P(3) is less than value of P(1) and P(2),that shows probability of success is less for P(3). As probability of success P (3) decreases which means it requires more trials for successful access, thus it can be concluded that security at multi–tier enhanced.

2. Let VarSent has N words and it contains D distinct characters.

thenpossible number of VarToken is D!/(D-N)!

so probability of success P(S)=1/(D!/(D-N)!),

Here, we assumed VarToken contains no repeated characters.

Table 3 is drawn for some values N and D as x and y axis respectively. Table's cell values is probability of success P(S) calculated by using P (3) = 1/ (D! / (D-N)!).

Table 4: Probability of Success for Different no. of Words (N) and Characters (D)

no of word s(N) \ no. of characters(D)	5	7	9	11	13	15	17
3	0.016667	0.004762	0.001984	0.00101	0.000582751	0.000366	0.000245
4	0.008333	0.00119	0.000331	0.000126	5.82751E-05	3.05E-05	1.75E-05
5	0.008333	0.000397	6.61E-05	1.8E-05	6.47501E-06	2.78E-06	1.35E-06
6	null	0.000198	1.65E-05	3.01E-06	8.09376E-07	2.78E-07	1.12E-07
7	null	0.000198	5.51E-06	6.01E-07	1.15625E-07	3.08E-08	1.02E-08
8	null	null	2.76E-06	1.5E-07	1.92709E-08	3.85E-09	1.02E-09
9	null	null	2.76E-06	5.01E-08	3.85417E-09	5.51E-10	1.13E-10

Based on Table 4, a graph is drawn as shown in fig. 5. From the figure 5, it is clear that as number of words N in VarSent or number of distinct characters D increases, probability of success P(S) decreases and tends to zero which means it requires more trials for successful access. Thus it enhanced security at multi–tier.

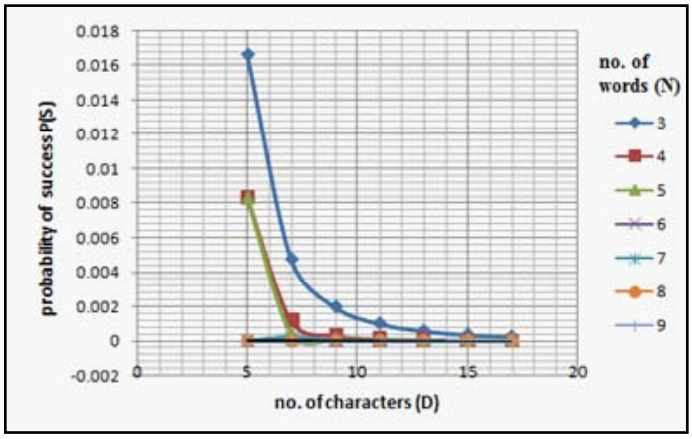


Fig. 5: Probability of Success P(S) Where x-Axisshows no. of Characters N and y-axis shows P(S).N is no. of words.

From above two analyses, it can be concluded thatproposed work provides better security.

Space Requirements

The space is another parameter which is analyzed for theproposed work. UserId and password is saved for every user so, in proposed work extra overhead is only VarSent. On an average, Let a single user credentials UserId and password size is 150 bytes and VarSent size is 200 bytes. VarSent is stored for user every time user logins,total 250 bytes is required for single user at server.If at any time 100000 users are registered, then serverwould need 100000*200 = 20000000 (19.07 MBapprox.) bytes of additional storage, which is not a bigissue in comparison to more security provided by multitiertechnique.

B. In addition from space and security analysis, the suggested work satisfies the following general features.

1. Security From Insider Attack

This parameter is basedon the assumption that it is easy for an insider to gainaccess to first tier authentication credentials .As proposed work doesn't send all credentials in first tier,so second tier authentication is also required.

B. Session Management

In proposed work, the VarSent is not saved permanently on server. VarSent is deleted from server when user terminates connection for that session. Every time for login, user has to choose a VarSent, without which he is not able to login.

C. Extra Hardware Software Needed

Some of thetechniques (possession or biometric based) require extra hardware and software. This adds overhead to the performance of thetechniques. The working of such kind of techniques depends upon the working of additionalhardware i.e. if the additional hardware fails, then theauthentication technique fails. Here extra hardware and software not required.

V. Conclusion

Probability of success is reduced to a large extent in multi-level authentication techniqueand knowledge based authentication is comparatively inexpensive, simple touse, and attractive to users. In this paper, proposed work combines features of both multi-level and knowledge based authentication techniques. Main features of proposed work are:

1. Extra software and hardware is notrequired.
2. No need toremember extra credentials except UserId and password for the users.

Thus based on above two features,proposed work is considered as lightweight.Still this work provides more security with some extended features as shown in result section.Graphical VarSent and VarTokencan be used as an alternative to alphanumeric VarSent and VarToken in which users click on images to authenticate themselves rather than type alphanumeric strings. These graphical alternatives are in the future scope of this work.

References

[1] Dinesha H.A.,"Multi-level Authentication Technique for AccessingCloud Services", International Conference on Computing,Communication and Applications (ICCCA), IEEE, February 2012, pp. 1-4.

[2] Furnell, S. M., Dowland, P. S., Illingworth, H. M., Reynolds, P. L.,"Authentication and supervision: A survey of user attitudes", Computers & Security, 19(6), 2000, pp 529-539.

[3] Mell P., Grance T.,"The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011, pp. 1-7, [Online] Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[4] CSA Security Guidance,"Guidance for Critical Areas of Focus in Cloud Computing v3.0", 2011. [Online] Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] "Authentication in an Internet Banking Environment", Federal Financial Institutions Examination Council, Government of USA, 2005.[Online]. Available: http://www.ffiec.gov/pdf/authentication_guidance.pdf

[6] Anand Sharma, VibhaOjha,"Password based authentication: Philosophical Survey", International Conference on Intelligent Computing and Intelligent Systems (ICIS), IEEE, 2010, pp. 619-622.

[7] Wen-Shenq,Juang,Sian-TengChen,Horng-TwuLiaw,"Robust and Efficient Password-Authenticated AgreementUsing Smart Cards", IEEE, Transaction on Electronics,Vol. 55, No. 6, June 2008.

[8] Haider, S., A. Abbas, A.K. Zaidi,"A Multi Technique Approach for User Identification through Keystroke Dynamics", IEEE International Conference on Systems, Man and Cybernetics, 2(s), 2001, pp. 336-1341, 2000.

[9] William E. Burr.,"Electronic Authentication Guideline by U.S. Department of Commerce", NIST Special PublicationVersion 1.0.2, April 2006.

[10] David A. Santos,"Elementary Probability", August 2007, [Online] Available: http://pareto.uab.es/mcreel/statistics/Elementary-Probability-Santos.pdf

[11] Erlich, Z., Zviran, M.,"Authentication methods for computer systems security, in Encyclopedia of Information Science and Technology", 2nd Ed., Vol. 1, USA: Information Resources Management Association, 2009, pp. 288-293.



Mr. MayankGaurav received hisB.E. degree in Computer Science and Engineering from RGPV University, Bhopal in the year 2009 and at present he is pursuing M.Tech.(2010-2013) in Software Engineering branch from R.K.D.F.I.S.T.,Bhopal, affiliated to RGPV University, Bhopal .His area of interest is Programming languages, Cloud Computing, Network Security.