RESEARCH ARTICLE OPEN ACCESS

User Security in Cloud Using Password Authentication

Deepika Singh[1], Puran Gour[2], Rajeev Thakur[3]
M.Tech Scholar NRI Institute of Information Science & Technology Bhopal (M.P)-462021, India

Abstract
Cloud computing technology is an open standard, service-based, Internet-centric, safe, convenient data storage and network computing services [8]. Cloud computing is an internet based model for enabling convenient, on demand network access to a shared pool of configurable computing resources [9]. The software and data that you access for your work doesn't exist on your computer instead it's on the server. This concept of using services not stored on your system is called Cloud Computing.
In this paper, we are implementing a technique to enhance the security of cloud. We create an algorithm based on the selection of username and generate a password to strengthen the security in cloud.

Keywords- Cloud computing, cloud architecture, front end, hybrid cloud, IaaS, PaaS, private cloud, SaaS.

I. Introduction to Cloud Computing

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything- from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service wherever and whenever you need[19].

The Internet is commonly visualized as clouds; hence the term "cloud computing" stands for computation done through the Internet. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources.

Cloud computing is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and de-provisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices [12].

Key Cloud Computing providers: IBM, HP, Google, Microsoft, Amazon Web Services, Salesforce.com, NetSuite, VMware etc.

Examples of Cloud Computing services include Google Docs, Office 365, Drop Box, SkyDrive etc.

II. Cloud computing architecture:-

The Cloud Computing architecture comprises of many cloud components, each of them is loosely coupled. We can broadly divide the cloud architecture into two parts:

1. Front End 2.Back End

The following diagram shows the graphical view of cloud computing architecture:

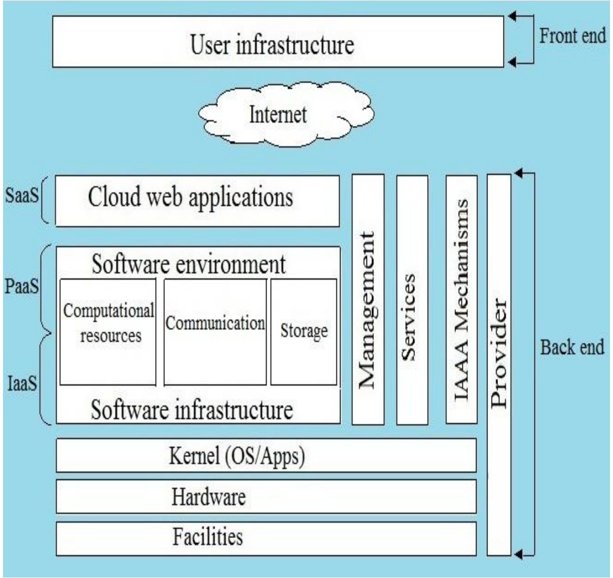

Fig1. Cloud computing architecture

Each of the ends are connected through a network, usually via Internet.

1. ***Front End:*** - Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser.
2. ***Back End:*** - Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

Figure 1 shows the cloud computing architecture. The services provided by cloud computing can be divided into three categories.

Service Models: - The service models are explained below:

Infrastructure as a service (IaaS): The simplest of cloud computing offerings. It involves the delivery of huge computing resources such as the capacity of storage, processing, and network. It is the ability to remotely access computing resources. The major advantages of IaaS are pay per use, security, and reliability. IaaS is also known as hardware-as-a-service. An example of IaaS is the Amazon Elastic Compute Cloud (EC2) [1].

Platform as a service (PaaS): supports a set of application programs interface to cloud applications. It has emerged due to the suboptimal nature of IaaS for cloud computing and the development of Web applications. Many big companies are seeking to dominate the platform of cloud computing, as Microsoft dominated the personal computer (PC). Examples of PaaS are Google App Engine and Microsoft Azure [1].

Software as a service (SaaS): provides a service that is directly consumable by the end user. It is a software deployed over the Internet. This is a pay-as-you-go service. It seeks to replace the applications running on a PC. A typical example of SaaS is Salesforce.com [1].

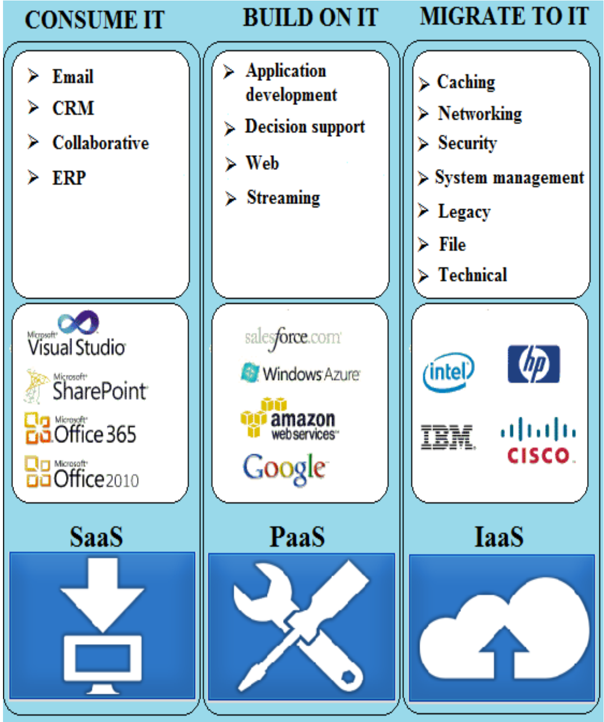

Fig2. Cloud services

There are a specific set of sub-services that describe specializations of the above cloud computing service models. These sub-services are described in the table below [21]:

TABLE1 Cloud sub-services

Sub-Service Type	**Description**
IaaS: DataBase as a Service (DBaaS)	DBaaS allows the access and use of a database management system as a service.
IaaS: Compute Capacity as a Service (CCaaS)	CCaaS is the provision of “raw” computing resource, typically used in the execution of mathematically complex models from either a single “supercomputer” resource or a large number of distributed computing resources where the task performs well.
PaaS: Storage as a Service (STaaS)	STaaS involves the delivery of data storage as a service, including database-like services, often billed on a utility computing basis, e.g., per gigabyte per month.
PaaS: Desktop as a Service (DTaaS)	DTaaS is the decoupling of a user’s physical machine from the desktop and software he or she uses to work.
SaaS: Communications as a Service (CaaS)	CaaS is the delivery of an enterprise communications solution, such as Voice Over IP, instant messaging, and video conferencing applications as a service.
SaaS: Monitoring as a Service (MaaS)	MaaS refers to the delivery of second-tier infrastructure components, such as log management and asset tracking, as a service.
SaaS: SECurity as a Service (SECaaS)	SECaaS is the security of business networks and mobile networks through the Internet for events, database, application, transaction, and system incidents.

Deployment Models:-

1. Private cloud: - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises [7].

***2. Community cloud:* -** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises [7].

***3. Public cloud:* -** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider [7].

***4. Hybrid cloud*: -** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [7].

III. Authentication in cloud

Cloud computing is not secure by nature. Security in the Cloud is often intangible and less visible, which inevitably creates a false sense of security and anxiety about what is actually secured and controlled. The off-premises computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services [16].

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 prove with 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 [20].

Authentication is the process of establishing confidence in user identities. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved. A growing number of cloud providers support the SAML (Security Assertion Markup Language) standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information between cooperating domains [17], [18].

IV. Problem Formulated

In this paper, we have made an attempt to enhance the security of cloud computing by using Password Authentication technique. Even though Cloud Computing offers various benefits and newer services, everyone has different opinions about the security aspects of it. Because of these security concerns, it is still not gaining its full momentum. Many organizations are stepping back as they don't want to take the security risk. Thus, it is essential to have more standard security measures for cloud computing in order to gain complete acceptance from all levels of organizations.

V. Proposed Methodology
VI.

A. How to start

When one starts the cloud service they will be provided with options to select. For registration user have to pass through authentication process. In that on the basis of username, process will be started at the server-side. Set of images which will be provided to user are based on result of calculation.

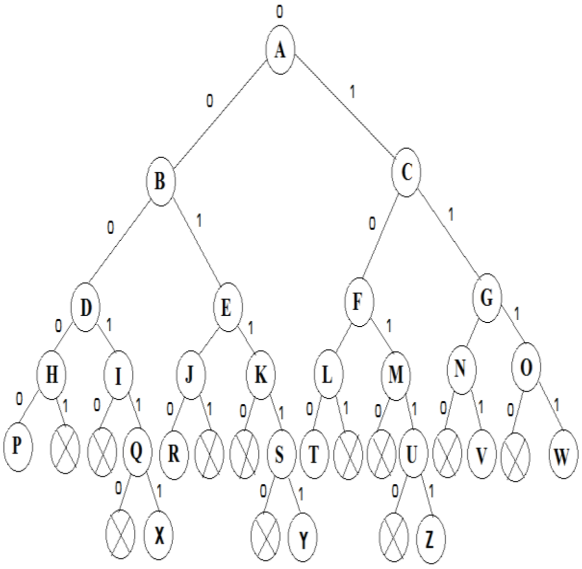

Fig3.Tree diagram of alphabets & its position

From the above tree diagram we can find the values of alphabets depending upon the position of alphabets in the tree. For e.g.:-

A = 0, Left sub-tree of A is B which is 00 & right sub-tree is C which is 01.

Table2 Position of alphabets

A = 0	N = 0010
B = 00	O = 0111
C = 01	P = 00000
D = 000	Q = 00011
E = 001	R = 00100
F = 010	S = 00111
G = 011	T = 01000
H = 0000	U = 01011
I = 0001	V = 01101
J = 0010	W = 01111
K = 0011	X = 000111
L = 0100	Y = 001111
M = 0101	Z = 010111

B. Calculation of data to be sent

Enter username not more than 6 characters.

Example 1

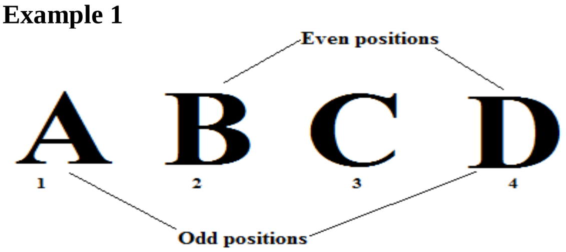

Fig4. Even & odd positions in username ABCD

For username ABCD (4 characters username)

A	B	C	D
0	00	01	000

Rearranging the odd & even positions separately:

A	C	B	D
0	01	00	000

Insert redundancy bits 11111(5 times 1)

So the data username will become
0111110111111100111111000

Example 2

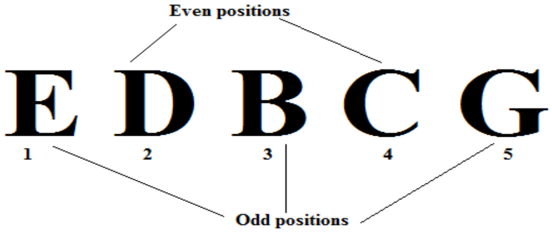

Fig5. Even & odd positions in username EDBCG

For username EDBCG (5 characters username)

E	D	B	C	G
001	000	00	01	011

Rearranging the odd & even positions separately:

E	B	G	D	C
001	00	011	000	01

Insert redundancy bits 11111(5 times 1)

So the data username will become
0011111100111110111111100011111101

Algorithm for sender (Encryption):-

Step 1. Design tree for alphabets A to Z.
Step 2. Start from A, assign left sub-tree as 0 and right sub-tree as 1.
Step 3. Repeat the procedure up to Z.
Step 4. Enter the username.
Step 5. Re-arrange the alphabets according to even and odd positions.
Step 6. Arrange odd position alphabet first and even position at last.
Step 7. Assign values to the alphabet in the username i.e. A=0, B=00, C=01 etc.
Step 8. Insert redundancy bits between the values of the username.
Step 9. Send the data username with added redundancy bits.

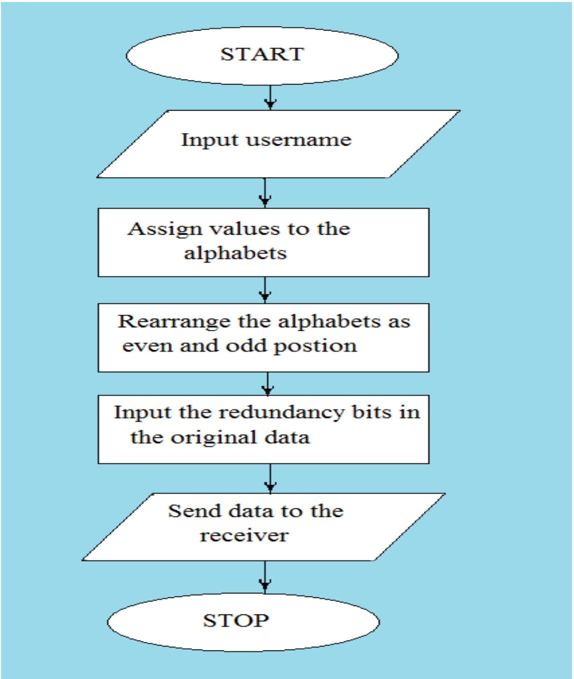
START
Input username
Assign values to the alphabets
Rearrange the alphabets as even and odd postion
Input the redundancy bits in the original data
Send data to the receiver
STOP

Fig6. Flow chart for sender

Algorithm for receiver (Decryption):-

Step 1. Received data find with redundancy bits.
Step 2. Start from A, assign left sub-tree as 0 and right sub-tree as 1.

Step 3. In our example, redundancy bit is '11111' (5 times 1), which is used to represent the end and start oh the values.
Step 4. Fetch the actual data after detecting the redundancy bit from the received data.
Step 5. Assign the alphabet to the numeric values in the received data.
Step 6. Rearrange according to odd and even position in alphabetic order.

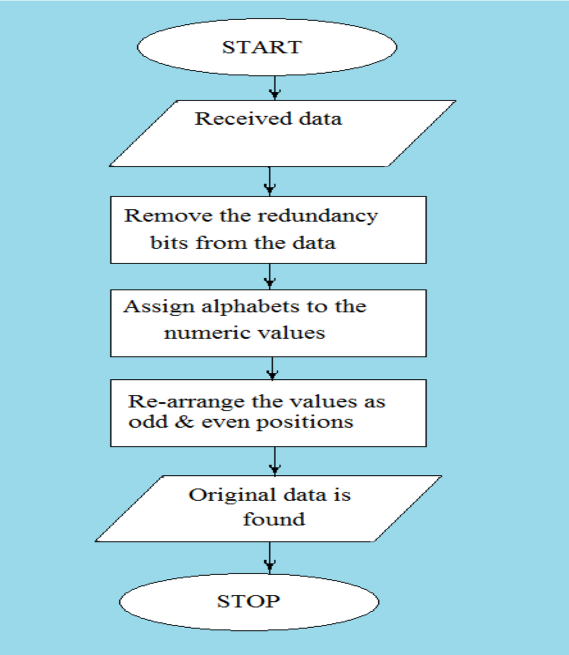
START
Received data
Remove the redundancy bits from the data
Assign alphabets to the numeric values
Re-arrange the values as odd & even positions
Original data is found
STOP

Fig7. Flow chart for receiver

Advantage of this technique:-

1. It is a unique method using simple methodology which is not easy to guess.
2. We don't need to remember long passwords.
3. Numeric values enhance the security of cloud accessing.
4. Less calculation time improve the throughput of the server.

VII. Conclusion

We conclude this technique of password authentication provides more secure authentication than the usual text password technique. The proposed algorithm can also be enhanced with more than 6 alphanumeric characters provided by the user for future work.

References

[1] Matthew N.O. Sadiku, Sarhan M. Musa, and OMonowo D. MoMOh, *Cloud computing: Opportunities and challenges, IEEE potentials, pp. 34-36, January/February 2014.*

[2] Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane and Nilesh R. Khochare, *Graphical Password Authentication Cloud securing scheme, IEEE Computer Society , pp.479-483, 2014.*

[3] Bogdan Hoanca and Kenrich Mock, *Secure graphical password system for high traffic public areas, ETRA June 2006.*

[4] Brown, Bracken, Zoccali & Douglas, Sasse et al., 2001; 2004.

[5] Chiasson, S., Biddle, R., and van Oorschot, P.C. *A Second Look at the Usability of Click-Based Graphical Passwords. Symp. on Usable Privacy and Security (SOUPS) 2007.*

[6] D. Davis, F. Monrose, and M. Reiter, —*On user choice in graphical password schemes, USENIX Security Symposium, 2004.*

[7] NIST Cloud Computing Standards Roadmap, July 2013.

[8] IEEE – The Application of cloud computing in education informatization, madern educational tech...Center Bo Wang, HongYu Xing.

[9] NISTdefinition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc

[10] Alireza Pirayesh Sabzevar, Angelos Stavrou, *Universal Multi-Factor Authentication Using Graphical Passwords, IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS) ISBN: 978-0-7695-3493-0 2008.*

[11] FABIAN MONROSE AND MICHAEL K. REITER, *Graphical Passwords, August 5, 2005.*

[12] Web-Resource http://en.wikipedia.org/wiki/Cloud_computing

[13] R. Kandukuri, R. Paturi V, and A. Rakshit, *Cloud security issues, in Proc. IEEE Int. Conf. Services Comput., Bangalore, India, 2009, pp. 517–520.*

[14] http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html, What Cloud Computing Really Means.

[15] Software as a service, Wikipedia, http://en.wikipedia.org/wiki/Software_as_a_service.

[16] Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar, *Effective Ways of Secure, Private and Trusted Cloud Computing, International Journal of Computer Science Issues (IJCSI), ISSN (Online): 1694-0814, Vol. 8, Issue 3, No. 2, pp. 412-421, May 2011.*

[17] B.Prasanalakshmi, A.Kannammal, *Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor*

Authentication using Biometrics, International Journal of Computer Applications (0975 – 8887) Volume 53– No.18, pp. 13-19, September 2012.

[18] Pradnya B. Rane, Pallavi Kulkarni, Suchita Patil, Dr. B.B.Meshram, *Authentication and Authorization:Tool for Ecommerce Security, IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, pp. 150-157, 2012.*

[19] Tejas.P.Bhatt, Ashish Maheta, *Security in Cloud Computing using File Encryption, International Journal of Engineering Research and Technology (IJERT), Vol. 1, Issue 9, November 2012.*

[20] Amlan et al., *A Strong User Authentication Framework for Cloud Computing, Asia-Pacific Services Computing Conference, IEEE Computer Society, 2011, pp 110-115.*

[21] INFORMATION SECURITY BRIEFING 01/2010 CLOUD COMPUTING http://www.cpni.gov.uk/Documents/.../2010007-ISB_cloud_computing.pdf