# Secure Cloud Transaction Using Password Encryption With Tree

**Gurusharan Kaur, Dr. Rizwana Jamal**

**Abstract— Cloud computing technology is an open standard, service-based, Internet-centric, safe, convenient data storage and network computing services. Cloud provides have three service models IaaS, PaaS and SaaS. Cloud computing is an internet based model for facilitate convenient, on demand network access to a shared pool of configurable computing resources. The software and data that you are using all instead of save on your computer save on server. This concept of using services not stored on your system is called Cloud Computing.**

**A graphical authentication password is a verification program that works when the customer uses proposed table on the basis of which data is substituted. Table is original and it can be used by both sender and receiver to protect data. The proposed algorithm is not easy to crack and enhanced security of the cloud from malicious users.**

***Index Terms***— Cloud computing, IaaS, PaaS, SaaS, authentication

## I. Introduction to Cloud Computing

Now a days the Internet is commonly envision 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.

The whole application, software updations is now handled by cloud providers. You have pay for this as per metered services.

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 used 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, EMC etc.

**Examples of Cloud Computing** services includes Google Docs, Office 365, Drop Box, SkyDrive, facebook 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:

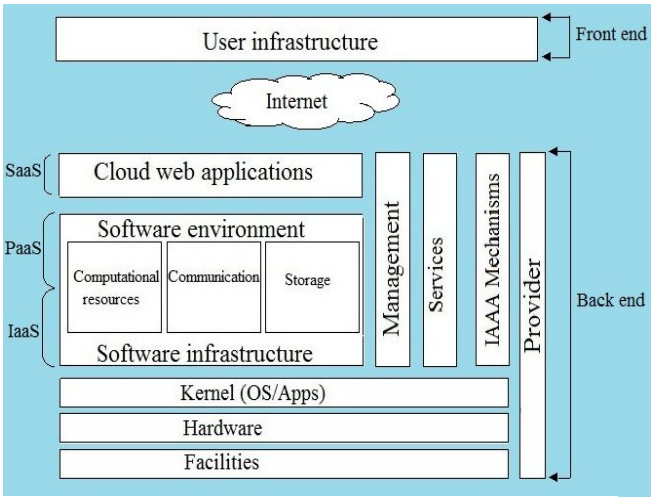



**Fig1. Cloud computing architecture**

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

1. ***Front End:*** - The interface provided to the client. Actually Front End refers to the client part of cloud computing system that consists of interfaces and

**Manuscript received July 19, 2014**

**Gurusharan Kaur**, Department of Mathematics Barkatullah University, Bhopal , India

**Dr. Rizwana Jamal**, HOD, Department of Mathematics Safia Science College Bhopal, India

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):** Cloud users have no need to update and take care of the hardware part need to access any application. The service provided by cloud computing 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):** It 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. Cloud provider has their own data center to provide various services to the users. 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):** It offers 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].

**Deployment Models:-**

***1. Private cloud:*** **-** The cloud infrastructure is provisioned for restricted use by a single organization includes multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, may 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, may a third party, or some combination of them. 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).

## III. Graphical passwords vs Alphanumeric passwords

The authentication system includes the text password and graphical passwords. Typically, text passwords are string of letters and digits, i.e. they are alphanumeric. Such passwords have the disadvantage of being tough to remember .Weak passwords are exposed to dictionary attacks and brute force attacks where as strong passwords are hard to memorize. Hence we are using textual passwords for less confidential data. Though, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and secure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, that is using a proposed table which is not easy to guess.

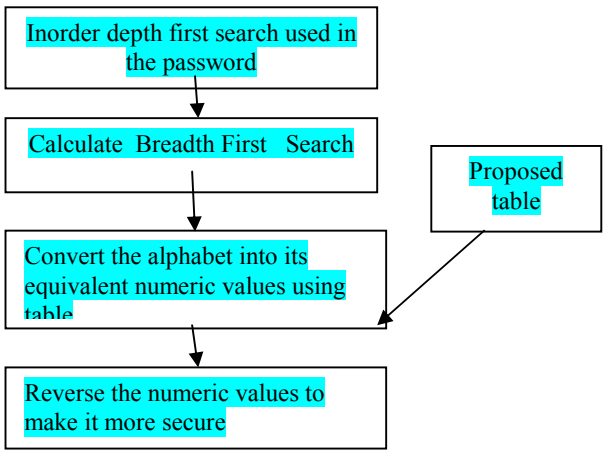



Fig2. Classification of authentication techniques

**Problems with alphanumeric passwords:-**

The main problem with the alphanumeric passwords is that once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. If a password is not frequently used it will be even more prone to forgetting. The recent surveys have shown that users select short, simple passwords that are easily guessable. For example, personal names of their family members, names of pets, date of birth etc [4]. The most important issue is having a password that can be remembered reliably and input quickly. They are unlikely to give priority to security over their need to get on with their work.

**Need of graphical passwords:-**

Graphical password was originally described by Blonder I in 1996. The basic need for graphical password is that graphical passwords are expected to be easier to recall, less likely to be written down and have the likely to provide a richer symbol space than text based password. Graphical password are used which is having some unique calculation which is not to guess or crack.

## IV. Problem Formulated

In this paper, we have made an attempt to enhance the security of cloud computing by using Graphical Authentication Method. 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

Proposed Methodology shows how can data can be encrypted.

**How to start –**

**Method to Encrypt :**

1. Let we have a proper binary tree.
2. A proper binary tree is used having an ordered tree in which each internal node has exactly two children.
3. Calculate Breadth first search of the tree.
4. Convert the received alphabets into its equivalent numeric value using table.
5. Reverse the value.
6. Send the encrypted value.

**Method to Decrypt :**

1. Reverse the received encrypted value.
2. Convert the value into its equivalent alphabet.
3. Draw proper binary tree with the received alphabet
4. Find In order depth search traversal value for the given tree.
5. Receive data is the protected password that we want to extract.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | A | | | | | | | | I |
| 2 | | B | | | | | | H | |
| 3 | | | C | | | | G | | |
| 4 | J | K | L | D | E | F | M | N | O |
| 5 | | | R | | | | S | | |
| 6 | | Q | | | | | | T | |
| 7 | P | | V | W | X | Y | Z | | U |

**Table 1. Proposed table that we used to convert data**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 01 | | I | 18 | | Q | 61 | | Y | 75 | |
| B | 21 | | J | 40 | | R | 52 | | Z | 76 | |
| C | 32 | | K | 41 | | S | 56 | | | | |
| D | 43 | | L | 42 | | T | 67 | | | | |
| E | 44 | | M | 46 | | U | 78 | | | | |
| F | 45 | | N | 47 | | V | 72 | | | | |
| G | 36 | | O | 48 | | W | 73 | | | | |
| H | 27 | | P | 70 | | X | 74 | | | | |

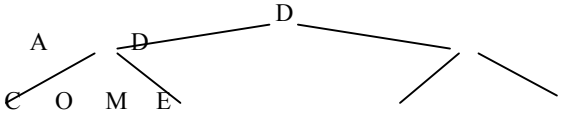
**Table 2. Values of the alphabets as per the above table**

Example to understand the Algorithm

**Example 1**

(Method to encrypt)

Let the tree be

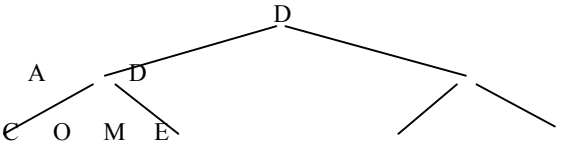



1. Calculate breadth first search traversal of the tree i.e DADCOME

2. Convert DADCOME into equivalent numeric value using given Table i.e 43014332484644
3. Reverse the received above valuei.e 44464832430143
4. Send the above received value.

**(Method to Decrypt)**

1. Received value is 44464832430143
2. Reverse the received value i.e 43014332484644
3. Convert into equivalent numeric value into alphabet using given table i.e DADCOME
4. Draw the A proper binary tree using the above data




5. Now calculate the Inorder traversal depth first search of the tree which the password. i.e CAODMDE that we have hide with the tree.

**Advantage of graphical password technique:-**

1. It is a unique method using simple methodology which cannot be estimate.
2. Don't need to memorize long passwords.
3. Numeric values enhance the security of cloud accessing.
4. Less calculation time means no burden

## Conclusion

We conclude that graphical password authentication system provides more secure authentication than the text password system. The graphical password techniques still need improvement against shoulder surfing attack and dictionary attack. But still this technique is much better than the alphanumeric password technique. The proposed algorithm is using a table to find the values of respected alphabet which can be enhanced with special characters used in password in near future.

The identification of security challenges and improved techniques in large number of services of Cloud Computing is a very challenging task. In the process of identification from research methods I had identified a satisfactory number of challenges and mitigation techniques which are being used at present and also in future Cloud Computing.

## 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. Adams, A. and Sasse, M.A. (1999). Users are not the enemy. Communications of the ACM 42, 12, 41-46.
6. Birget, J.C., Hong, D., and Memon, N. (2003). Robust discretization, with an application to graphical passwords. Cryptology ePrint Archive. http://eprint.iacr.org/2003/168 accessed January 17, 2005.
7. Blonder, G.E. (1996). Graphical Passwords. United States Patent 5559961.
   Boroditsky, M. Passlogix password schemes. http://www.passlogix.com, accessed December 2, 2002.
8. Brostoff, S. and Sasse, M.A. (2000). Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al. (Eds.), People and Computers XIV - Usability or Else, Proceedings of HCI 2000, Springer, pp. 405-424.
9. Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18, 641-651.
10. Dhamija, R. and Perrig, A. (2000). Déjà Vu: User study using images for authentication. In Ninth Usenix Security Symposium.
11. Fitts, P.M. (1954). The information capacity of the human motor system in controlling amplitude of movement. Journal of Experimental Psychology, 47, 381-391.
12. Mandler, J.M. and Ritchey, G.H. (1977). Long-term memory for pictures. Journal of Experimental Psychology: Human Learning and Memory, 3, 386-396.
13. Morris, R. and Thompson, K. (1979). Password security: A case study. Communications of the ACM, 22, 594-597.
14. Norman, D.A. (1988). The Design of Everyday Things. Basic Books, New York.
15. Paivio, A., Rogers, T.B., and Smythe, P.C. (1976) Why are pictures easier to recall then words? Psychonomic Science, 11(4), 137-138.
16. Patrick, A. S., Long, A. C., and Flinn, S. (2003). HCI and security systems. In *Proc. CHI 2004*, ACM Press, 1056-1057.
17. Real User Corporation. (2001). The science behind Passfaces. http://www.realusers.com. Accessed: Dec. 2. 2002.
18. Rundus, D. J. (1971). Analysis of rehearsal processes in free recall.. Journal of Experimental Psychology, 89, 63-77.
19. Sasse, M. A., Brostoff, S. and Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technical Journal, 19, 122-131.