RESEARCH ARTICLE OPEN ACCESS

Password authentication in cloud

Indal Singh[1] Rajesh Rai[2] Sachin Murarkar[3]
M.Tech Scholar NRI Institute of Information Science & Technology Bhopal (M.P)-462021, India

Abstract
Cloud computing is an Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers [1]. Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services. Authentication is one the most important security primitive [6]. Password authentication is most widely used authentication mechanism. Password provides security mechanism for authentication and protection services against unwanted access to resource. In this paper, we applied a technique to preserve our password using graphical authentication.

Keywords- Cloud computing, Sender, Receiver, Data security.

I. Introduction

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability [2].

When anyone wants to access the network, for security purposes every web application provides user authentication. From ancient day's secret data or code is used for hiding and giving security to information. In user authentication the process which we have to pass through is username and password. Authentication process divided into Token based authentication, Biometric based authentication and Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical password. In today's changing world when we are having number of networks and personal account some sort of easy authentication [3] schema need to be provided.

II. Basics models of Cloud Computing

Service Models of Cloud Computing: - According to NIST, the cloud model is composed of three service models:

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. 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 [4].

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, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment [4].

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) [4].

Deployment Models of Cloud Computing: - According to NIST, the cloud model is composed of four deployment models:

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 [4].

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 [4].

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 [4].

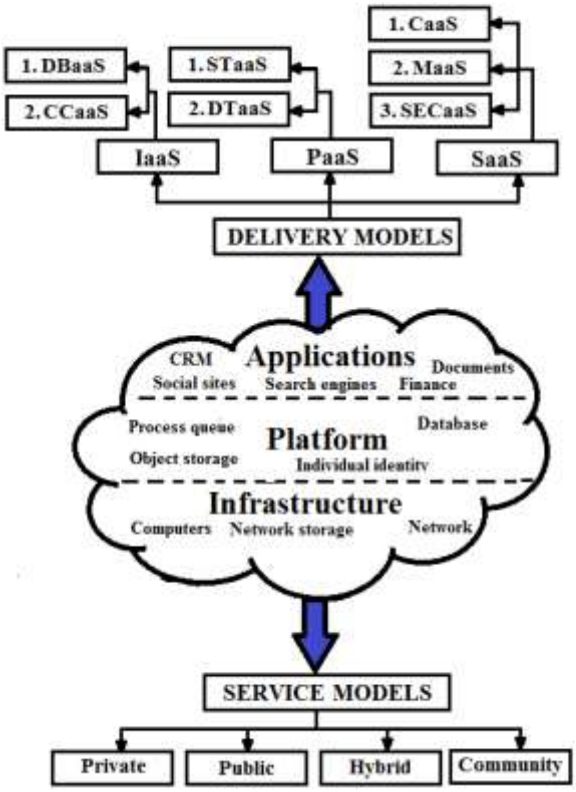

Figure 1 Service & delivery models in cloud

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) [4].

III. Classification of Authentication methods

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or simply an object running in a device. Authentication process assures the basic security goals, i.e. confidentiality and integrity. The first line of defense for protecting any resource is Authentication [8].

Authentication is a process of validating who you are to whom you claimed to be, or in other words a process of identifying an individual, usually based on a username and password. Currently what we have in the field, are the following set of techniques [9]:
Human Authentication Techniques are as follows:
1. Knowledge Base (What you know)
2. Token Based (What you have)
3. Biometrics (What you are)
4. Recognition Based (What you recognize)

Computer Authentication Techniques are as follows:
1. Textual Passwords
2. Graphical Passwords
3. Biometric schemes (fingerprints, voice recognition etc.)

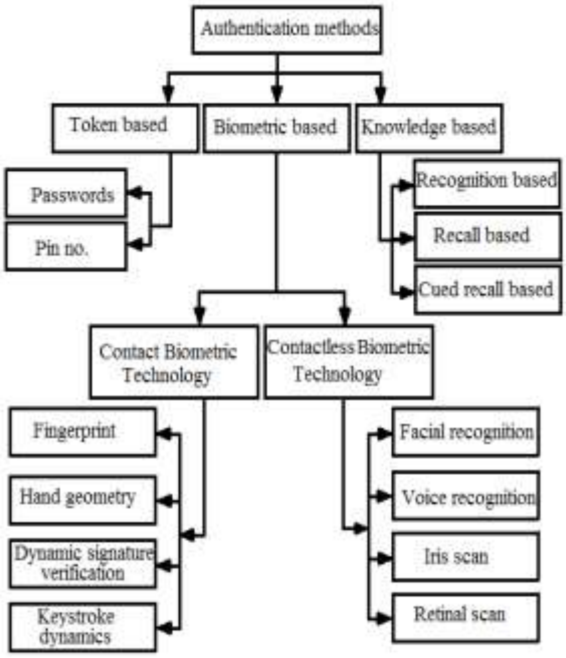

Figure 2 Classification of Authentication methods

IV. Problem Formulated

In this paper, we had proposed a method of password authentication by implementing double authentication technique. In the first step of authentication we apply the binary addition to our chosen username & in the second step we send the carry forward by OTP (One-Time Password) to the receiver, so as to decode the sent data.

V. Proposed Methodology

Assigning the values: - First of all, we created a tree diagram in which left arm (i.e. left sub-tree) is assigned the value as 0 & right arm is assigned as 1. On the basis of values so obtained, we obtained a table.

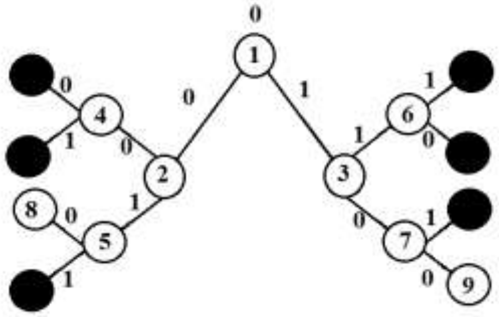

Figure 3 Tree diagram

1 = 0
2 = 00
3 = 01
4 = 000
5 = 001
6 = 011
7 = 010
8 = 0010
9 = 0100

Table1 Positions of numeric values

Username calculation: - Enter username not more than 6 characters.

Example

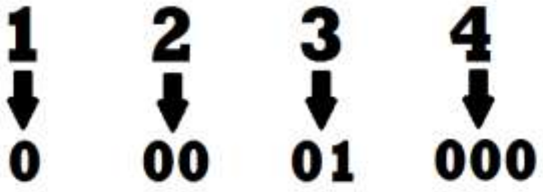

Figure 4 Binary values of positions 1234 according to tree diagram

For username 1234
1 2 3 4
0 00 01 000

Now, by adding the redundancy bits 1111 to the above generated bits, we get,

0 1111 00 1111 01 1111 000

Performing binary addition of the obtained binary value of the username:

carry 1111111111111111
0111100111011111000
+11111111111111111111
101111001111011110111

The obtained result is 101111001111011110111.

We will now the obtained bit to the receiver and send 1 of the first place of the data stream as OTP (One Time Password) to the mobile of the receiver for more secure authentication & the remaining 20 bits directly. When the user receives both the values, he knows what to do next.

The receiver then add the carry 1 to the 20-bit received values to obtain the desired value.

Here, 00000111(8-bit) and carry 1 will be added to get desired result.

111
01111001111011110111
+1
01111001111011111000

Thus, the decoded password is 01111001111011111000.

Now, by removing the redundancy bits the original data is found i.e. 0 00 01 000 = 1 2 3 4

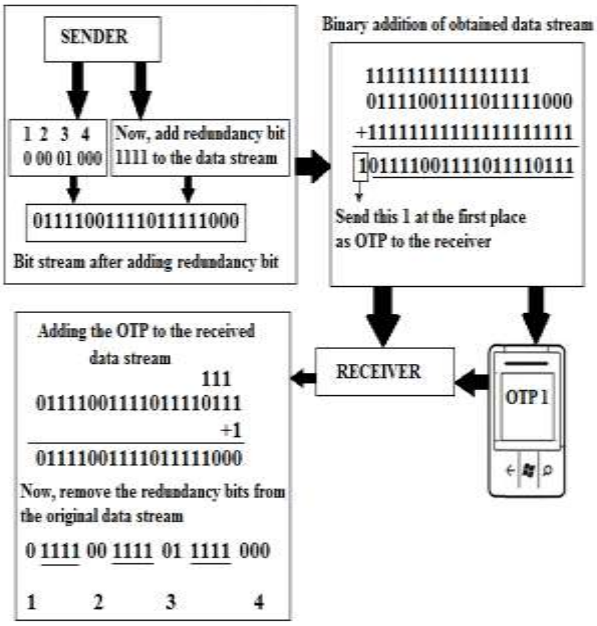
SENDER
1 2 3 4
0 00 01 000
Now, add redundancy bit 1111 to the data stream
01111001111011111000
Bit stream after adding redundancy bit
Binary addition of obtained data stream
1111111111111111
01111001111011111000
+11111111111111111111
101111001111011110111
Send this 1 at the first place as OTP to the receiver
RECEIVER
OTP 1
Adding the OTP to the received data stream
111
01111001111011110111
+1
01111001111011111000
Now, remove the redundancy bits from the original data stream
0 1111 00 1111 01 1111 000
1 2 3 4

Figure 5 Working and flow of bits from sender to receiver

Algorithm for sender:

Step 1. Design tree for digit 1 to 9.
Step 2. Start from 1, assign left sub-tree as 0 and right sub-tree as 1.
Step 3. Repeat the procedure up to 9.
Step 4. Enter the username.
Step 5. Assign values to the digits in the username i.e. 1=0, 2=00, 3=01 etc.
Step 6. Insert redundancy bits between the values of the username.
Step 7. Now, perform the binary addition of the obtained data stream after adding redundancy bits.
Step 8. Send the 20-bits directly to the receiver and the digit at the first place as OTP to the receiver's mobile.

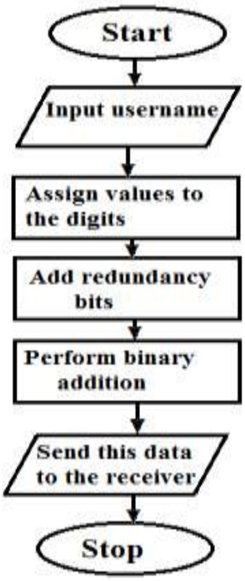

Figure 6 Flow chart for sender

Algorithm for receiver:

Step 1. Received data and OTP at receiver's side.

Step 2. Now, add this OTP bit to the received data stream of 20-bits.

Step 3. By performing addition of OTP to the 20-bit data stream, we get the data stream with added redundancy.

Step 4. Perform removal of redundancy bits from the original data.

Step 5. Now, assigns values to the obtained original data.

Step 6. Thus, the original data is found.

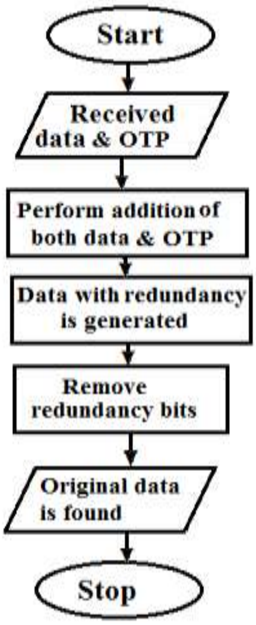

Figure 7 Flow chart for receiver

VI. CONCLUSION

Lack of privacy and security is the main hurdle in the wide adoption of cloud computing. We are almost at the beginning of the cloud era; it is hard to predict the impact of cloud computing on society. Cloud computing is not fully mature and needs to be explored [4].

This technique provides more secure password authentication than usual graphical password authentication techniques. Moreover, the extra bit from the result which is sent as OTP adds more security to password authentication technique.

References

[1] Mishra, R. ; Sch. of Comput. Eng., KIIT Univ., Bhubaneswar, India ; Dash, S.K. ; Mishra, D.P. ; Tripathy, A., *A privacy preserving repository for securing data across the cloud, 2011.*

[2] William Stallings and Lawrie Brown. *Computer Security: Principle and Practices. Pearson Education, 2008.*

[3] *Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice* Susan Wiedenbeck Jim Waters College of IST Drexel University Philadelphia.

[4] Peter Mell. (2011*) 'The NIST Definition of Cloud', Reports on Computer Systems Technology, sept., p. 7.*

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

[6] Virendra Singh Kushwah, Aradhana Saxena, *A Security approach for Data Migration in Cloud Computing, 2013.*

[7] http://www.thecloud.net.nz/go/what-is-cloud-computing

[8] Ishwarya M.V, K.Ramesh Kumar, *Secure Anonymization for Privacy Measure, 2013.*

[9] Grover Aman, Narang Winnie, *4-D Password: Strengthening the Authentication Scene, 2012*.

[10] Deepika Singh, Puran Gour, Rajeev Thakur, *User Security in Cloud Using Password Authentication, 2014.*