ABSTRACT

The objective of this paper is to propose a secure, user friendly and economical multi-level authentication scheme that uses multiple factors for gaining access to resource on insecure platforms and for financial transactions. The proposed study is based on a premise that when multiple levels and multiple factors are incorporated in an authentication scheme it not only becomes difficult to break but also resistant to different forms of attacks. This work purposes a scheme where authentication process is carried out in three levels using multiple factors and is called 3L-MFA. The scheme also uses Out of Band (OOB) authentication as one of the factors that offers credible security against man-in-the-middle (MIM) attack. The first level uses username password based on double encryption. Second level uses OTP verification based on Out of Band (OOB) authentication using email id and mobile number. Third level involves user’s interaction on graphical screen in terms of predetermined number of clicks on images, buttons and selection of predetermined number of menu items. The security of proposed system depends upon double encryption using SHA-1 and AES-128-CBC, out of band authentication using OTP and user interaction on a graphical screen that uses probability combination of various numbers.

Keywords: Cloud Computing, Multifactor Authentication, Double Encryption, Out of Band Authentication, Security, Graphical screen and Attacks.


http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=10&IType=1

1. INTRODUCTION

In the present era, cloud computing is one such technology that has evolved at a rapid pace. Two major computing giants IBM and Google introduced it to public in October 2007 [1]. It revolutionized the data world by providing on demand services such as software, servers,
networking, storage and database. The National Institute of Standards and Technology (NIST) defines cloud computing as “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” [2]. The cloud computing services [3] are categorized as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). In IaaS cloud providers lend infrastructure services such as servers, virtual machines, storage, networks, and operating systems to users. PaaS provides environment to the clients for developing, testing, delivering, and managing software applications. SaaS provides access to software applications but consumer never controls hardware, network or operating system. There are four different deployment models in cloud computing [4]:

- **Private Cloud**: The infrastructure of cloud is dedicated to a single organization that may consist of multiple consumers. It is not shared with other organizations. It is usually managed by the same organization or a third party. It is considered as most insecure but expensive choice.

- **Public Cloud**: The infrastructure is provided by the cloud service provider and is available for use by general public. The services are offered over the Internet. It is considered most insecure and is vulnerable to attacks.

- **Community Cloud**: The infrastructure is shared by organizations of same community. It may be owned and operated by the organization or by a cloud service provider.

- **Hybrid cloud**: It is a combination of private and public cloud.

In cloud, security and privacy are two major concerns. It becomes seriously important as data is distributed on different machines all across the globe [5]. In 2013, the Cloud Security Alliance (CSA) identified nine major threats to cloud “The Notorious Nine” [6]. These issues include data breaches, data loss, service traffic hijacking, denial of service, insecure interfaces and APIs, malicious insiders, cloud abuse, insufficient due diligence and above all shared technology. Apart from these issues, another threat to data stored on cloud is due to poor authentication methods and techniques used to access the resource [7]. Thus, in cloud security, authentication is an important factor as verifying the identity of user is one of the first steps to ensure security.

In this paper we have proposed a novel multifactor authentication scheme for cloud computing that operates in three different levels. The scheme is based on multiple factors such as encrypted password, OTP, email id, mobile number and count of mouse clicks on various graphical items on a screen.

### 2. AUTHENTICATION AND ITS TYPES

Authentication is a process of verifying the user’s identity. Authentication is defined as “mechanism that establishes the validity of the claimed identity of the individual” [8]. The various authentication types [9] are summarized in table 1:
A 3-Level Multifactor Authentication Scheme for Cloud Computing

Table 1 Types of authentication

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>TECHNIQUE</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge based</td>
<td>Numeric Password</td>
<td>A secret numeric password e.g. ATM PIN</td>
</tr>
<tr>
<td></td>
<td>Alphanumeric Password</td>
<td>Alphanumeric string of characters to be typed in by a user</td>
</tr>
<tr>
<td></td>
<td>Graphical Password</td>
<td>Recall based: User reproduces something chosen during registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pure recall-based: User reproduces password without any hint</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cued recall-based: User is given hint to recall password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recognition based: User chooses a set of preselected pictures</td>
</tr>
<tr>
<td>Possession based</td>
<td>Tokens</td>
<td>Static token: Device that store secret number, cryptographic keys, digital data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Synchronous dynamic token: OTPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Asynchronous tokens: User enters a challenge number on the token keypad to generate a response to this challenge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Challenge response token: Smart cards</td>
</tr>
<tr>
<td>Biometric based</td>
<td>Biological Features</td>
<td>User is authenticated on the basis of fingerprints, iris and retina, face, hand and ear geometry</td>
</tr>
<tr>
<td></td>
<td>Behavioral Characteristics</td>
<td>User is authenticated on the basis of voiceprint, keystroke dynamics and signature dynamics</td>
</tr>
</tbody>
</table>

Based on the number of factors used for authentication the schemes are further classified as [10]:

- Single factor authentication (SFA) uses only one factor for authenticating user. The most common example of SFA is the knowledge based username-password scheme.
- Multifactor authentication (MFA) uses two or more factor such as username-password with One Time Password (OTP), username-password with smart card or biometric.

3. REVIEW OF VARIOUS MULTIFACTOR AUTHENTICATION SCHEMES

Multifactor authentication schemes go beyond traditional knowledge based username password authentication by adding various factors such as tokens (hardware or software), OTPs, mobile number, email id, Q R codes and biometrics to create two factor (2FA) or three factor (3FA) authentication schemes. These solutions lower the risks of data breaches by adding the extra layers of security that are difficult to crack [11].

3.1. Multifactor authentication schemes based on image

A graphical password based multifactor authentication scheme that is neither completely recognition nor recall-based [12] used cell phone as a second factor. A user has to click certain points in specific order on an image to get an access to a resource. A hint about the click point and their order is given to user by sending the same image in encrypted form to user’s cell phone or any other handheld device. Another Image Based Password MFA scheme [13] uses recognition based graphical password and Hash - MAC based OTP using SHA-1 algorithm. A 3-level password authentication scheme [14] uses image ordering, color pixels and OTP. In this scheme different hash functions such as SHA-1, MD5 are used for OTP generation.
In a two factor authentication scheme [15] digital image is used as second factor. This image is encrypted-decrypted using Cany's edge detection. The scheme supports mutual authentication, session key agreement and identity management. It also has lower transmission cost and has a capability to counter malicious attacks like insider attack, impersonate attack, dictionary, forgery, replay attack and reflection attack. A multistage authentication system [16] that has three stages used two different authentication methods: devices’ serial number and username and combination of patterns. In first stage user is authenticated using username and password and the system checks the device serial number. In second stage user highlights at least m right squares from a grid of n independent squares. In the final stage, the he has to select s images in a specific order.

A unique 3 Level Authentication and Authorization system [17] uses combination of recognition and recall based techniques. At first level user name and textual password is used and in second level, a grid of 16 images (4 x 4 matrix) is shown to the user. In this, user has to correctly identify the image that he had set his click points on during registration phase. In third level OTP is delivered on user’s registered number that is entered by the user in order to complete verification process.

3.2. Multifactor authentication schemes based on tokens

SofToken [18] a two factor authentication technique used basic username-password as first factor and a random number is generated by software on client-side as a second factor. A pseudo-random number called codeword is generated by the software on client computer that is entered by the user and verified by the server. A mutual authentication scheme [19] used username-password in first phase and a token generated by an application in second phase. This token is delivered to the registered mail-id of user. The proposed protocol resists many attacks such as replay attack and password stolen attack. Another token based authentication scheme [20] used Dual Factor Authentication Protocol (DFAP) along with mobile token. First password verifies the profile of a user and second password allows access to cloud resources. These passwords are sent securely by server using shared secret key and are provided by the user through his mobile phone using mobile token (UMT).

3.3. Multifactor authentication schemes based on biometrics

A biometric base authentication scheme [21] User Authentication Level System (UALS) with five levels that uses public key Infrastructure (PKI) with biometric in level 5. The scheme can be used for high-risk financial transactions or applications where a very high confidence is required in verifying the identity. A two factor authentication scheme combines human biometrics i.e. handwritten signatures and knowledge factor [22]. The handwritten signatures are matched using dynamic time warping (DTW) technique. Although the cost and resource requirements of the proposed system are low and does not depend on user end platform, it has been tested for small group of people only. A novel multifactor two-server authentication scheme called MTSAS [23] uses fingerprint pattern. In this scheme, server does not store fingerprint information and the user’s biometric characteristics cannot leave the user device. As a result, authentication is done by user’s device and not by the server.

4. PROPOSED MULTIFACTOR AUTHENTICATION SCHEME

The proposed three level multifactor authentication scheme (3L-MFA) is based on double encryption, out of band (OOB) authentication using one time Password (OTP) and graphical screen where user performs pre-registered clicks on graphical items such as images, menu items and buttons. The scheme has multiple levels and is based on premise that if one level is compromised, an attacker still has to cross other levels in order to access the resource.
The first level of authentication uses traditional username-password based on double encryption using SHA-1 and open SSL AES-128 bit ECB. The password submitted by user is first encrypted using SHA-1 encryption. The resulting password is further encrypted using open SSL and AES-128-ECB using a phrase or text provided by user as a key. The server does not store SHA-1 encrypted password rather it stores the password encrypted using AES-128 ECB and secret key given by the user i.e. the output of double encryption.

The second level of authentication uses a time based One Time Password (OTP) that a user has to submit to the server. The user is delivered this OTP on his registered e-mail id that is submitted by user via SMS to a number already provided to user thereby ensuring security using OOB authentication.

The third level of authentication presents a user with a graphical screen that contains various graphical items i.e. a set of images, menu items with multiple menu options and different shaped and colored buttons. In order to get authenticated at this level, a user has to click on specific number of buttons, images from a grid and select the certain number of menu items. The number of button and images to be clicked and numbers of menu items to be selected in a graphical screen are provided by the user at the time of registration.

4.1. Phases in Authentication Scheme

The scheme operates in three different phases: Registration, authentication and password change phase.

4.1.1. Registration Phase

In registration process, a user enrols oneself by providing certain details along with username, password such as e-mail id, mobile number. In addition, a user is asked to provide a phrase that will be used as a key for double encryption process using open SSL AES-128-ECB in the first level of authentication. User is also prompted to input the number of pictures to be clicked, number of buttons to be clicked and number of menu items to be selected on graphical screen during the third level of authentication. Figure 1 shows the details of registration form. In order to strengthen the authentication process user has to click a minimum of three pictures, three buttons and select a minimum of three menu items. All the details provided are stored in a database for the verification to be done at the time of authentication.

4.1.2. Authentication Phase

In order to gain access to the resource a user has to go through three different levels of authentication: double encryption-decryption with username-password, out of band authentication using time lived OTP and interaction on graphical screen using preregistered number of clicks on pictures, buttons and menu options.

In the first level, a screen is shown where a username and alphanumeric password is entered by the user. Figure 2 shows the first level login screen. Upon successful verification of this username and password from the database, server generates a random 6-digit OTP in the second level and sends it to the registered e-mail id of the user. Use has to send back this OTP to server via SMS from his registered mobile number. For this, a user has to access his e-mail id and SMS the code received in a threshold time of 5 minutes otherwise the login screen will expire and access will be denied as shown in figure 3. The received OTP is then checked by the server that not only validates the 6-digit OTP but also verifies that the OTP has been sent from the registered mobile number.

The successful verification of OTP takes the user to third level of authentication in which a user is presented with a graphical screen that contains a menu bar with multiple menu
options, specific number of buttons of different shapes and colors and a 6 x 5 grid of images as shown in figure 4. In order to cross this level of authentication, a user must click predetermined number of pictures in a grid along with predetermined number of buttons and has to select predetermined number of menu items. This number should match with the number decided by the user at the time of registration. For example, if at the time of registration user decided to click on three images, three buttons and select any three menu items from different menus then in order to pass this level he has to click on any three images from the grid, click on any three buttons and select any three menu items. It is mandatory that a user has to make correct combination of all three options. A mismatch in any of these three numbers would not let the user to login.

\[\text{Figure 1 Registration form}\]

4.1.3. Password Change Phase

In order to make authentication scheme user friendly a password change facility has been provided to the user. To reach this option a user has to undergo all three level of authentication. It means a user can change password only after successful login. The selection of password change option provides a user with a screen where a user can update all the information that was given by him at the time of registration. Here, a user can enter changed alphanumeric password, a new key phrase for encrypting SHA-1 password, update his email id or mobile number. User can also modify the number of images to be clicked, number of buttons to be clicked and number of menu items to be selected for third level of authentication in a graphical screen. Figure 5 shows the password change screen of proposed authentication scheme. Password change option enhances the usability of the authentication scheme.

\[\text{Figure 2 First level login}\]
A 3-Level Multifactor Authentication Scheme for Cloud Computing

**Figure 3** Second level OTP verification

**Figure 4** Graphical screen at third level of authentication

**Figure 5** Password change phase

4.2. **Working of proposed model**

The working of entire authentication scheme is summarized in following steps (figure 6):

**Step1:** User registers on the server and provides following information to the server: username, password, mobile number, e-mail id, key phrase, number of pictures to be clicked, number of buttons to be clicked and number of menu items to be selected.
Step 2: Clicking the login option on screen will prompt user for his username and password.

Step 3: Server verifies the username and password from the database by decrypting the SHA-1 password using the phrase given by the user as a key. This decryption is performed using open SSL and AES-128 CBC.

Step 4: If the username and password match is found in database, server generates a random 6-digit OTP that is delivered to the registered mail id of the user otherwise access is denied. At the same time server shows a screen that starts a back counter of 5 minutes.

Step 5: User retrieves this 6 digit OTP from his inbox and sends it to the server via a SMS from his registered mobile number.

Step 6: If this OTP is not sent within the time frame of 5 minutes the login time expires and access is denied. Upon receiving OTP from a user, server not only checks the correctness of 6-digit code but also ensures that the OTP has been sent through registered mobile number.

Step 7: If both the OTP and mobile number are correct, server displays a graphical screen that contains a 6 x 5 grid of images, a set of different shaped & colored buttons along with multiple menu items.

Step 8: User has to click on specific number of images in a grid, buttons and select menu items with the same count as was chosen at the time of registration.

Step 9: The correct number of all the three actions viz. picture clicks, button clicks and menu items selected will grant access to the user on the specific resource.

Figure 6 Working of Proposed Scheme
5. THREE LEVELS OF AUTHENTICATION SCHEME AND THEIR SECURITY MEASURES

The first level of authentication uses username password scheme based on double encryption/decryption principle. The users’ password is doubly encrypted using SHA1 and AES-128-CBC encryption. It is mandatory for a user to choose an alphanumeric password with minimum length of 8 characters. The password must contain uppercase, lowercase, numbers and special characters. This password is first encrypted using SHA-1 algorithm that produces 40 digit hexadecimal output. This 40 digit hexadecimal output i.e. encrypted password is further encrypted with open SSL AES-128-CBC using key phrase given by user during registration as encryption key. The unique feature with added security of proposed work is that the server’s database does not store the password as hashed form of SHA-1 encryption output rather it stores the result of double encryption i.e. the output of AES-128 encryption. In addition the phrase used as a key in AES encryption is stored in a separate table. As result, it is safe from insider attack. The attacker may get access to the table that contains doubly encrypted password but will not be able to decrypt this password without getting access to the phrase used as key to encrypt the SHA-1 encrypted password stored in second table.

During authentication phase, the server retrieves this doubly encrypted password from one table and the key from second table to decrypt the password which is then compared with the alphanumeric password entered by the user. If two passwords match user is taken to the second level of authentication. At this level our scheme offers higher security by performing double encryption and storing the key for second encryption in a separate table from the one that stores encrypted password. This level of authentication protects against insider attack and enhances security by using double encryption and decryption.

The second level of authentication uses out of band authentication (OOB) technique. Upon successful verification of username-password, the server generates a random 6-digit one time password (OTP) that is delivered to the user’s registered email id. At the same time a user is shown a screen which starts a timer that counts backwards. This timer is set for the limit of five minutes. Within this time frame user must access his registered mail id and retrieve the random code. This code is to be sent by the user to the server via SMS through his registered mobile number. If a user is not able to send SMS to server in a threshold time of five minutes the login screen will expire and the access will be denied. The 6-digit random code sent by the user will be matched with the code sent to the user in his registered email id. At the same time server will also ensure that the OTP has been sent from the registered number by verifying the same from database. If both the factors i.e. OTP and mobile number are found to be correct, user is directed to third level of authentication. This level of authentication in proposed schemes provides an extra layer of security in form of OOB authentication as the two separate and unconnected channels are used to send and receive the OTP. The use of OOB authentication protects the system from man-in-the-middle attack. The OTP used in the proposed scheme is time based hence forces an attacker to follow rigid time constraints in order to hack the communication. As the OTP has to be confirmed only from the registered mobile number it further makes it difficult for the attacker to gain access to users’ mail id and mobile phone at the same time.

The third level of authentication uses a graphical screen where a user has to interact with the items on screen using mouse. It is neither recognition based nor recall based graphical password scheme. Hence it does not put cognitive pressure on user’s memory. In our work, a screen with menu bar that contains multiple menu options, a set of different colored and shaped buttons and a grid of 6 x 5 images are loaded once the OTP has been confirmed. In order to get authenticated at this level, a user need to click on certain number of images and
buttons and has to select certain number of menu items from different menu options. The number of images and buttons clicked and number of menu options selected should match with the number chosen by the user at the time of registration. The correct combination of these three numbers authenticates the user. If any one number in the combination is incorrect the access is denied.

The proposed scheme makes it mandatory for a user to opt minimum of three clicks on buttons and images and select three menu items from various menus. To confuse the hacker and to enhance the security the images in the 6 x 5 grid change randomly every time user logs in. Also the labels, color, position/location of buttons are different on every login. The various menu options are also variable every time even for same user. Another feature of this level of authentication is that same image, button and menu item cannot be selected or clicked twice. The security of this level of authentication is calculated on the basis of probability model. In our proposed work, user need to interact with graphical screen on the basis of three factors viz. number of menu items selected, number of button clicked and number of images clicked in a grid. Therefore, the probability of third level of authentication being secure is given by the formula:

\[ S_{third \ level} = 1 - (p1 \times p2 \times p3) \]

Where \( S_{third \ level} \) is the probability of security of third level, \( p1 \) is the probability of guessing number of menu items selected, \( p2 \) is the probability of guessing number of button clicks and \( p3 \) is the probability of guessing number of image clicks. For example, if \( p1 = 1 \), \( p2 = 0.6 \) and \( p3 = 0.5 \) then the probability of this level being secure is 70%. Also only one attempt is provided to the user to select correct combination. To further enhance the security of system other types of graphical items such as radio buttons, checkboxes, and sliders can be added to include more clicks. This will increase the probability of system being more secure.

6. SECURITY ANALYSIS OF PROPOSED MODEL

6.1. Password space analysis

The proposed scheme offers large password space at third level of authentication. The size of key space increases with the combination of number of interactive items i.e. buttons, menu option and images on screen and number of items selected. If \( q \) images are to be clicked from \( p \), \( s \) buttons are to be clicked from \( r \) and \( u \) menu items are to be selected from total of \( t \) then the password space produced using these three combinations is

\[ ^pC_q + ^rC_s + ^tC_u \]

6.2. Security against attacks

INSIDER ATTACK: The user’s password is stored in hashed form based on double encryption using SHA-1 and AES. The database stores the encrypted form of SHA-1 encrypted password. Moreover the key used for second encryption and doubly encrypted password are stored in two different table. Even if an attacker gets access to password table key used for encryption is inaccessible.

DICTIONARY AND BRUTE FORCE ATTACK: The scheme resists both these attack as scheme is based on multiple factors. Even if the intruder is able to get the alphanumeric password, he still needs to have access to mobile number and email id of user.

MAN IN THE MIDDLE ATTACK: The scheme withstands MIM attack as it uses Out of Band authentication. OTP is delivered to registered email id and is verified through SMS from registered mobile number thereby using two separate channels for communication.
STOLEN VERIFIER ATTACK AND UNAUTHORISED ACCESS ATTACK: The authentication scheme is based on number of parameters such as doubly encrypted password, mobile number, email id, and user’s interaction on graphical screen. If one parameter is stolen or lost the authentication scheme does not fail as three levels based on different factors are to be crossed. Loss of mobile phone or unauthorized access to email id will not make scheme ineffective. User can update the lost credential through password change facility.

PASSWORD CHANGE: The scheme enables the user to update his alphanumeric password and key for second encryption. Moreover user can also update the number of clicks on buttons, images and menu items to be selected at third level of authentication. The password change facility makes our scheme flexible, user friendly and stronger in comparison with static password schemes.

REPLAY ATTACK: User has to SMS the OTP delivered on his email id in a time frame of five minutes through his registered mobile number to the server. The code is short lived and random every time. Hence it provides strong resistance to replay attack.

PASSWORD GUESSING ATTACK: The hashed output of SHA-1 algorithm is again encrypted using AES algorithm. The double encryption process makes password guessing extremely difficult.

6. CONCLUSION AND FUTURE WORK
This paper proposed a three level multifactor authentication scheme for cloud computing that includes double encryption, out of band authentication and user’s interaction on graphical screen at first, second and third level respectively. The proposed scheme is based on open source technologies and can be used to authenticate users for secure online transactions. The scheme withstands various security attacks such as MIM attack, insider attack, stolen credentials attack, password guessing and dictionary attack. The scheme has less cognitive load in comparison to recognition and recall based graphical password schemes as user has to remember certain numbers of clicks and not the image types and their order of clicks at the third level of authentication.

An empirical study of proposed model needs to be conducted to evaluate usability and to check the robustness of the system against different types of attack. Future scope of this work includes measuring trade-off between user login time and security, countering the shoulder surfing attack and checking whether the proposed scheme is feasible for all sorts of cloud applications. Further studies need to check the usage feasibility of proposed scheme for touch based screen.

REFERENCES


