Abstract

Sensitive database such as a banking application contains the bank account details of all customers in a particular bank. The necessity of this application is to keep data confidential which are managed by higher officials in bank. The static password method is used for providing security for e-transaction nowadays. This method leads to various attacks like Brute force attacks, Dictionary attack, Shoulder sniffing and guessing. To overcome the issues in static method, dynamic password method has been introduced, which changes the login password for every session. Since password changes dynamically, guessing of passwords avoided and if the intruder knows current session password it became invalid for next session. This proposed method has two level of authentication. In first phase it checks for user’s Id, password and random colour priority. In second phase Knuth-Morris-Pratt algorithm has been used which matches string pattern in generated random matrix for providing dynamic password in every session.

Key words: Static password, dynamic password, security, random color, grid, matrix.

1. Introduction

Sensitive database such as a banking application contains the bank account details of all customers in a particular bank. The necessity of this application is to keep data confidential which are managed by higher officials in bank. The static password method is used for providing security for e-transaction nowadays. This method leads to various attacks like Brute force attacks, Dictionary attack, Shoulder sniffing and guessing. To overcome the issues in static method, dynamic password method has been introduced, which changes the login password for every session. Since password changes dynamically, guessing of passwords are avoided and if the intruder knows current session password it doesn’t valid for next session. Enhanced database security with two level authentications, the proposed application contains two level
authentications for login. The first level makes use of colour code values and in second level using grid to generate dynamic password. The proposed methodology overcomes the drawbacks in the existing static password verification method. Enhanced database security with two level authentication incorporates following features: Creating account, Giving colour code, security, Getting new password from the grid, Viewing customer and staff details, Generating profit analysis, Amount Transfer and Closing account.

II. Literature Review

For every user pattern should be defined at first, this pattern stored in database along with user credentials. Server generate grid along with unique id and sends back to client. Then user enters his username, and password from the grid using pattern then it sends to the server. Then this credentials received by server for authentication. At this time server uses algorithm called checksum to verify password whether it matches with generated password in grid. If password match authentication success or else it fails. Based on size of server grids were generated. In case of low end server grids are generated and stored in database based on request from the user grids are used at random. A cron is run every one hour to check whether 20% of grids is unused if it goes below then new grids are generated automatically. In higher end server grids are created instance because of high bandwidth and processing supported by server. The user submits his username and password from the grid. The grid is retrieved from database by grid id followed by pattern to regenerate correct password. Once authentication is finished stored grid information is removed from memory.

A public key based dynamic password scheme uses public key concept for instead of generating an encryption to store in server. One way function (DES) uses cyphertext to encrypt the password store in tables. This concept cannot be fully accepted, they is possible of cracking password. So they introduced public key concept for password authentication schemes. This concept uses l.lamport dynamic password scheme where f^m-r (PW m) “PWM “is password and “f “ is automatic generation of password with respect to m times. If user logins for first time then f^m-1 (PW 1) and if second time f^m-2(PW 2) and if the value goes small the value of” m” becomes small. So “m” cannot be small since it has to login many times. Similarly time and user login id is need to be stored and used for generating unique id and password. This is possible by fabinscheme, it is similar to quadratic residue (used for generating password randomly for each time) and the m value problem is corrected in this scheme. And this uses public key that verify the user id and password each time the user enters this avoids instead of using encryption. Token based authentication using mobile phone, is a
concept of dynamic password or one time password mechanism. When the user send the request to the server, user send username, static password to server. The server generate dynamic password based on the static password. The dynamic password stores in the database. Server verifies the password and the client password. If the password is same as in the database, the server can allow the client to access the data. In Sim based dynamic password: First the client send the request to server. The server checks the user id, static password, sim IMSI number. During the registration time user provides his/her phone number. Based on the phone number, server collects the sim IMSI. Whenever the user wants to access the data, server should check user id, password, IMSI number. Server generates dynamic password based on the static password and send dynamic password to client via sms. Secure User Authentication in Cloud Computing proposes idea that VPN supported firewall is placed between the cloud host and client. All traffic is passed through this tunnel and it protects from insider and outer attacks. This model needs multiple channels. Due to tunneling sniffed data is considered as just garbage by intruder. In this model they used Cisco firewall pix 525 which have 330 mbps throughput for 280000 simultaneous sessions. And then create VPN users and assign IP to each user. Scalable User Authentication Scheme for Secure Accessing to Cloud-Based Environments (SUAS) has been proposed to increase the reliability and efficiency in cloud based environments. This concept has three major agents, first user authentication agent (UAA1), second user authentication agent (UAA2) and key major agent (KMA). UAA1 is based on modified Diffie-Hellman algorithm, which confirms user identity. The connection was established by UAA2 based on RSA small-e algorithm. UAA2 sends public key to client, password encrypted by public key using RSA small- e algorithm. Rate of security is increased by storing keys and exponents in different cloud server and also avoids various possible attacks. Intelligent agents are used to manage keys and exponents between UAA1 and UAA2.

III. Proposed System Overview

This proposed method has two level of authentication. In first phase it checks for user’s Id, password and random colour priority. In second phase Knuth–Morris–Pratt (KMP algorithm) has been used which generates random matrix for providing dynamic password in every session. In application part contains customers and staff details. Entering the password from grid will be time-consuming task because password searched in row and column wise in 6*6 matrix. Sequential process of the proposed approach is shown in figure 1.
Figure 1. Framework of the proposed system.

Detailed sequential steps to be adopted, the expected and the unexpected results of each phase description is tabulated in table.1.

Table 1. Expected and Unexpected results of the sequential steps.

<table>
<thead>
<tr>
<th>Sequence to be adopted</th>
<th>Predictable</th>
<th>Unpredictable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the code password</td>
<td>colour code value should match</td>
<td>password does not match the color</td>
</tr>
<tr>
<td>Enter the code password</td>
<td>colour code value should match</td>
<td>the password does match the color</td>
</tr>
<tr>
<td>Enter the dynamic password from grid</td>
<td>Enter the new generated password</td>
<td>the password doesn’t match DB</td>
</tr>
<tr>
<td>Enter the dynamic password from grid</td>
<td>Enter the new generated password</td>
<td>password match DB password</td>
</tr>
<tr>
<td>Enter the details in signup page</td>
<td>Fill the all text field</td>
<td>field is not filled</td>
</tr>
<tr>
<td>Enter the details in signup page</td>
<td>Fill the all text field</td>
<td>Field is filled</td>
</tr>
</tbody>
</table>

IV. Results and Discussion

End-user logs onto the system with his login credentials when entered without any discrepancy. New user is allowed to opt for the registration process, as shown in figure 2, by supplying all the required details.

Figure 2: Registration Phase.
Upon accurate matching of user credentials, the user can view the employees’ record as shown in figure 3, sanction loan amount to the regular customers and can terminate the account from the bank.

![Secure Auth](image)

**Figure 3: View staff details.**

By providing the security by two levels called colour code and grid, the shoulder suffering attack is been completely avoided and the advantage of using these application will be secured and cannot be hacked by hackers. These types of security can be useful in baking applications and for more confidential files. The gird in security level is scuffled at each time the login page opens and the colour code is also made scuffled each time the login is attempted. If any wrong is attempt is made using login this login is completely takes a reverse process and starts again from level 1 security.

V. Conclusion and Future Work

The application has been created and performed testing successfully. It overcomes various attacks in static method like Brute force attacks, Dictionary attack, Shoulder sniffing and guessing made by intruder. Hence sensitive database can be protected in this method. One of the disadvantage in this application is time – consuming processing process.

In future, the second level using grid to generate dynamic password that dynamic password can be used as password in session at first level security. Grid can be replaced by any other method because of time taking process.

References

1. Parekh Tanvi, Gawshinde Sonal, Sharma Mayank Kumar: Token Based Authentication using Mobile Phone 978-0-7695-4437-3/11 IEEE.
3. HaoZuo, Yongjun Shen, Shuxian Li, Huijun Shen: Two-way Real-time Authentication System based on Dynamic Password and Multi-biometric 978-0-7695-4719-0/12 IEEE.

6. Leinharn, Computer science telecommunications program: A Public key Based Dynamic Password Scheme 64110001439/14 IEEE.


