Approach for Enhancement of Secure Access to Database Through One Time Password

S. Ch. Vijaya Bhaskar
Assistant Professor,
Department of Information Technology
MVSR Engineering College, Hyderabad

Dr. Anitha S
Professor,
Department of Electronics and Communication Engg
ACS College of Engineering, Bengaluru

Abstract—Database security restricts the user access to the database based on the privileges given by the administrators. As data is the most important and valuable asset, intruders target the database which can lead to misuse of data. This paper studies about providing security to access the database by generating a One Time Password (OTP), which will be sent to the primary credentials of the authorized user.

Index Terms: Authentication, Privileges, One Time Password, Security, Multi-level privileges.

I. INTRODUCTION

Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability.

Database security concerns with the ability to provide access to the authorized database users by giving valid credentials like user name and passwords with host name. The users in an organization working under same network can access the databases of the same network. The administrator provides the credentials to the users. The cross network database access where the vendor of one network tries to connect the other networks database the access is restricted, but restricting the database access within a single network is not possible.

This paper proposes a technique where the access to the database can be restricted by giving multi-level privileges to the users. The main threats in database security are Excessive Privilege Abuse, Legitimate Privilege Abuse, Privilege Elevation, Database Platform Vulnerabilities and Weak Authentication [1].

II. RELATED WORK

Early research in the areas of access control and authorization mainly focused on two models that are discretionary Access control policy and on the mandatory access control policy. In the area of discretionary access control models for relational database systems, an important early contribution was the development of the System access control model, which strongly influenced access control models of current commercial relational DBMSs [2] [3].

Discretionary access control models have, however, a weakness in that they do not impose any control on how information is propagated and used once it has been accessed by subjects authorized to do so. This weakness makes discretionary access controls vulnerable to malicious attacks, such as Trojan Horses embedded in application programs [4] [5].

The objective of database security is to protect database from accidental or intentional loss. These threats increases the risk on the integrity of the data and its reliability. Database security allows or refuses users from performing actions on the database. Database managers in an organization are responsible to identify threats and take necessary actions to mitigate any risks. These actions include controls using passwords and username to identify users who access the database. The system created is called database management security system which maintains user details log and allows access by providing with passwords and usernames [6].

Another threat to database security is that of privileges elevation. By using database platform software vulnerability a user can gain extra privileges to get permissions as database administrator [8].

Security of databases involves restoring the database to a safe mode after failure. There are various types of security issues that are related to databases. Physically security can be said to be security of the hardware associated with the system and where the database is hosted or located. Some cause such as floods and earthquakes can be a threat to that and the only solution is to store databases back up. The other types of measure are the system issues or logical security. These are measures that resides in the operating systems and usually far more difficult to achieve [7].
The authorization process establishes if a user can retrieve and manipulate specific data. There are two approaches: data access code can use authorization to determine whether or not to perform the requested operation, and the database can perform authorization to restrict the capabilities of the login used by Operating system.

With inadequate authorization, a user may be able to see the data of another user and an unauthorized user may be able to access restricted data. These threats can be addressed by using an OTP.

1. **Shared privileges to access the database:**
   Only the privileged users can be able to access the database which can be given by multi-level security. In the initial level all the users can connect to their own network and the privileges can be given by the username and passwords of that organization. In the next level of security the authorized users connect to the database by using shared username and passwords which can lead to the misuse of database where it will be difficult to identify the malicious users.

   This problem of malicious user can be overcome by providing an OTP generated by the database after verifying the multi-level credentials. The OTP will be forwarded only to the authorized users of the database [9][10].

2. **Unauthorized user privileges to access the database:**
   All the users of the same network will not be allowed to access the database. Privileges are given by the administrator to the database users. A malicious user in this case can be any user in the network who is not authorized to access the database but can intrude by using others credentials.

   This problem of intrusion can be overcome by providing OTP generated by the database which will be forwarded only to authorized database users. The intruder cannot be able to access the database without the OTP.

3. **Authorized user privileges to access the database:**
   All the database users of the same network will allowed to access the database with their own Privileges. A malicious user in this case can be any database user in the network who tries to connect to the database with others privileges to misuse the data.

   This problem of intrusion can be overcome by providing OTP generated by the database which will be forwarded to primary level authentication of the user. The intruder cannot be able to access the database without giving the valid OTP.

   Figure 2 shows the system architecture of database security where the user is authenticated and the data will be made available to the user based on the privileges of the user.
Module Description

1. Authentication: The server is responsible for OTP generation. OTP is generated by considering username, password with OS user authentication. OTP is a 4 digit numeric format which is dynamically generated by the database. Based on the submission of valid OTP the user is connected to the database.

2. Availability: The data is uploaded into the database server. Once the user is given authentication by verifying the OTP the data in the database is made available to the user according to the permission given by the database administrator to read, execute or update the data.

3. Access: Admin wants registration and login through user name and password. Data owner and user registration will be carried on. Figure 4 & Figure 5 explains the accessible data that can be uploaded to a database.

4. Integrity: The data created or modified by the user adhere to a predefined set of rules. These rules are determined by the database administrator or application developer.

IV. DATABASE DESIGN

Algorithm: The database audit table stores the login credentials, mail id information, OS user information. The user provides the username, password to connect to the database. Once the login credentials are succeeded then proceed for the OTP generation. The server is responsible for random OTP generation. OTP is generated by considering username, password with OS user authentication. OTP is a 4 digit numeric format which is dynamically generated by the database. The database will generate the OTP by using dbms_random package. This package is called by the trigger which automatically fires once the user login is successful. Based on the submission of valid OTP the user is connected to the database.

Start
Create audit table
username,pwd,hostnumber
if username and password is valid then
  proceed for OTP generation
  <OTP generation>
else
  reenter username and password

if login credentials are succeeded then
  <OTP generation>
Else
  Exit from the sql prompt
end

OTP generation:

Fire trigger select round(dbms_random value(1000,9999))
from dual
Generate OTP and submit
In multi level check OTP entered by user
If (user input == true) then proceed with login else exit from the database.
Stop
Figure 3 describes the proposed architecture to verify the privileged user authentication by validating the OTP submitted by the user which is generated by database server.

<table>
<thead>
<tr>
<th>Column</th>
<th>Data Type</th>
<th>Length</th>
<th>Allow Null</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>varchar</td>
<td>20</td>
<td>✓</td>
</tr>
<tr>
<td>password</td>
<td>varchar</td>
<td>20</td>
<td>✓</td>
</tr>
<tr>
<td>email</td>
<td>varchar</td>
<td>50</td>
<td>✓</td>
</tr>
<tr>
<td>question</td>
<td>varchar</td>
<td>100</td>
<td>✓</td>
</tr>
<tr>
<td>answer</td>
<td>varchar</td>
<td>100</td>
<td>✓</td>
</tr>
</tbody>
</table>

Fig.4 Database design of User Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Data Type</th>
<th>Length</th>
<th>Allow Null</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>varchar</td>
<td>20</td>
<td>✓</td>
</tr>
<tr>
<td>filepath</td>
<td>varchar</td>
<td>500</td>
<td>✓</td>
</tr>
<tr>
<td>owner</td>
<td>varchar</td>
<td>100</td>
<td>✓</td>
</tr>
<tr>
<td>rkey</td>
<td>varchar</td>
<td>100</td>
<td>✓</td>
</tr>
<tr>
<td>score</td>
<td>number</td>
<td>9</td>
<td>✓</td>
</tr>
</tbody>
</table>

Fig.5 Database design of Uploaded Information

V. SECURITY IMPROVEMENT

Security in database provides control to data access by giving permissions to users. The sensitive data can be protected by giving access privileges to users. The OTP generated by the database provides multi-level security to data and it also helpful to identify the intruders.

VI. CONCLUSIONS

Motivating and solving the problem of securing database through multi-level authentication using OTP increases the protection of sensitive data. The performance of the system is improved by avoiding the intruders to avoid data loss. The security is provided to the data which has been uploaded in the database. The random OTP generation provides dynamic password which avoids the hacking and improves the security. The authentication from two different levels provides improved security for data retrieval. When multiple data owners are involved, the aspects of membership and data sharing need to be addressed. The proposed scheme provides privacy and complexity while handling the data sharing over database. Here the security is enhanced by means of Random OTP generation technique.

REFERENCES