IJERT
ISSN : 2278-0181
International Journal of Engineering Research & Technology

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 discretionaryAccess control policy and on the mandatory access control policy. In the area of discretionary access control models forrelational database systems, an important early contributionwas 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, aweakness in that they do not impose any control on howinformation is propagated and used once it has beenaccessed by subjects authorized to do so. This weaknessmakes discretionary access controls vulnerable to maliciousattacks, such as Trojan Horses embedded in applicationprograms [4] [5].

The objective of database security is to protectdatabase from accidental or intentional loss. Thesethreats increases the risk on the integrity of the data and itsreliability. Database security allows or refusesusers from performing actions on the database.Database managers in an organization are responsible to identify threatsand take necessary actions to mitigate any risks.These actions include controls using passwords andusername to identify users who access the databases.The system created is called database managementsecurity system which maintains user details log and allowsaccess 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 thedatabase to a safe mode after failure. There are varioustypes of security issues that are related to database.Physically security can be said to be security of thehardware associated with the system and where thedatabase is hosted or located. Some cause such asfloods andearthquakes can be a threat to that and theonly solution is to store databases back up. The othertypes of measure are the system issues or logicalsecurity. These are measures that resides in theoperating systems and usually far more difficult toachieve [7].

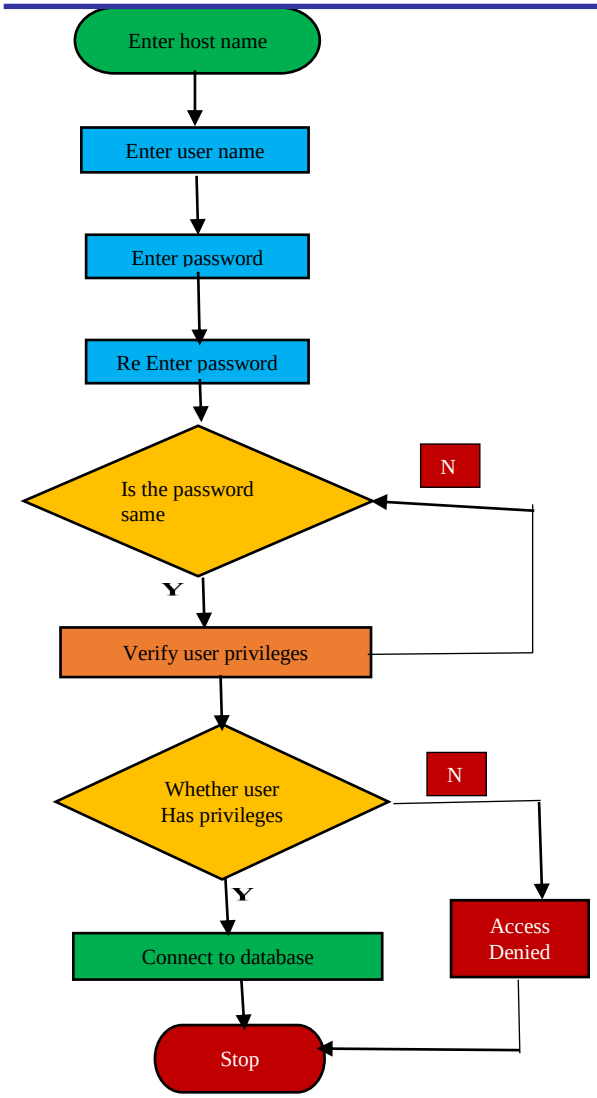

Fig 1: User authentication

Figure 1 describes the user login and verifies the privileges of the authenticated user to connect to the database. The privileged user can access the database and is authenticated to use that particular network within the organization.

Databaseinsecurity can also arise from weak system and procedures which cannot perform better authentication. Weak authentication can lead intruders to acquire legitimate rights of user andthen steal or change credentials. Some of the ways inwhich an attacker can hack in include use of socialengineering, where passwords are requested throughphone calls for maintenance purposes. Other includebrute force where the attacker does guess thepasswords. Strong authentication is therefore requiredto address these challenges. Besides that, there isbackup data exposure, where the storage media is left exposed leading to attacks[2].

III. PROPOSED SECHEME

Various attacks and Proposed Techniques to enhance security in organizations:

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.

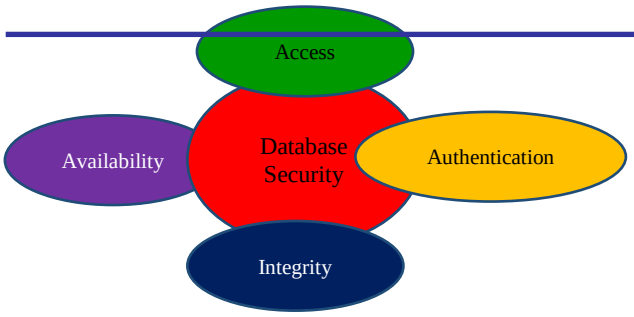

Fig.2Database Security

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 userregistration will be carried on.
Figure 4& Figure5 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
Exif from the sql prompt
end
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

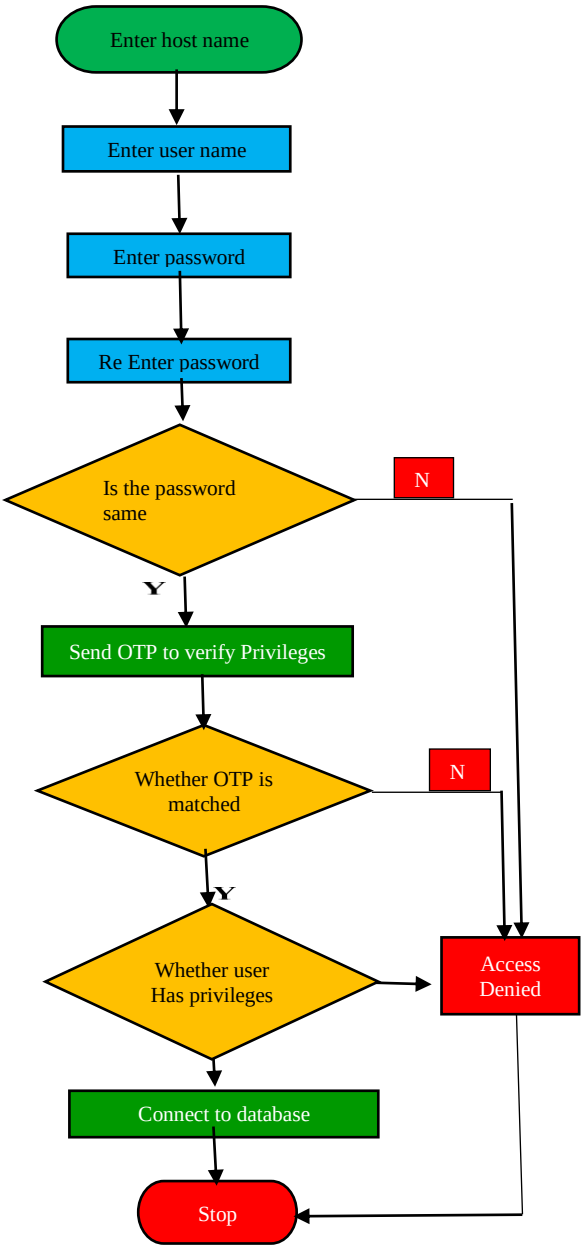

Fig 3: Proposed architecture to verify authentication using OTP

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.

Design Table 'userinfo' in 'SEO' on '(LOCAL)'

Column Name	Data Type	Length	Allow Nulls
username	varchar	20	✓
password	varchar	20	✓
email	varchar	50	✓
question	varchar	100	✓
answer	varchar	100	✓

Fig.4 Database design of User Information

Design Table 'uploadinfo' in 'SEO' on '(LOCAL)'

Column Name	Data Type	Length	Allow Nulls
keyword	varchar	20	✓
semantickeyword	varchar	20	✓
filepath	varchar	500	✓
owner	varchar	100	✓
rkey	varchar	100	✓
score	numeric	9	✓

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

[1] Mohammed Rafiq, “Database Security Threats and Its Techniques”, IJARCSSE, Volume 4, Issue 2, February 2014.
[2] P.G. Griffiths and B. Wade, “An Authorization Mechanism for aRelational Database,” ACM Trans. Database Systems, vol. 1, no. 3,pp. 242-255, 1976.
[3] R. Fagin, “On an Authorization Mechanism,” ACM Trans. Database Systems, vol. 3, no. 3, pp. 310-319, 1978.
[4] R. Sandhu and F. Chen, “The Multilevel Relational Data Model,”ACM Trans. Information and System Security, vol. 1, no. 1, pp. 93-132, 1998.
[5] S. Jajodia, R. Sandhu, and B. Blaustein, “Solutions to the Polyinstantiation Problem,” Information Security: An Integrated Collection of Essays, vol. 1, M.A. Abrams et al. eds., IEEE CS Press, pp. 493-529, 1994.
[6] S. Singh, Database systems: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
[7] S. Sumanthi, Fundamentals of relational databasemanagement systems Berlin: Springer, 2007.
[8] S. Singh, Database systems: Concepts, Design andapplications New Delhi: Pearson Education India,2010.
[9] Mr. Saurabh Kulkarni, Dr. SiddhalingUrolagin, “Review of Attacks on Databases and Database Security Techniques”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.
[10] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee,” Online Banking Authentication System using Mobile-OTP with QR-code”, Page(s): 644 – 648, Nov. 30 2010-Dec. 2 2010, E-ISBN : 978-89-88678-30-5. 2] IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005.