Three Layer Security Model for Distributed Relational Database

Pramod Singh

Abstract: ***Today we are living in a digital world where we all are connected to an open access network to exchange information. This information is more valuable assets that need protection from unauthenticated access. There are many security models has been proposed to protect the data stored in database but still needs more protection from attacks. In this study we have a three layer security model for relational database. Proposed model builds a security architecture based on access control policy, cryptography techniques and stored procedure. These mechanisms and techniques are combined together to present an interactive three-layer security model for securing relational databases in distributed environment. This model provides a kind of security controlling both in rests of database and data in motion from malicious user and other attacks.***

Keywords- Database Security, stored procedure, Encryption, integrity, Confidentiality

I. INTRODUCTION

The rapid growth of network technology and information processing system led to the development of distributed database management system. In this type of system, data are stored in different computers scattered in different geographical sites connected via network [1, 2]. Distributed database includes number of functions like distributed transaction management, Distributed query processing, security and integrity. Distributed database security is an important issue which includes number of processes and procedures that protect a database from unplanned happenings. These activities can be considered as unconstitutional modification, authenticated exploitation and cruel attacks. [1, 2, 3].

Databases can be secured by many covers and types of facts safety, containing encryption, authentication, authorization and access control. The. Access control is a technique of certification to any entity to use of particular resource. Authentication is a process or action to confirming something or someone as authentic. Encryption is a technique to converting facts into incomprehensible form by using an algorithm. Multi-level security system of relational database is required for distributed environment [5, 6].

Access control becomes a mostly used technique today which is based on user roles with privileges on stored database objects.

Each object has a security level assigned and if the role belongs that level then he will be able to access the data these mechanism are very restricted and works very well in small and close environment but in open environment these access control model are not very expressive.

II. PROPOSED MODEL

The Developed model is a three layered security model which is shown in Figure 1.1. This model is a combination of many security approaches like database user's accounts, user information and privileges, stored procedures policy rules and crypto systems.

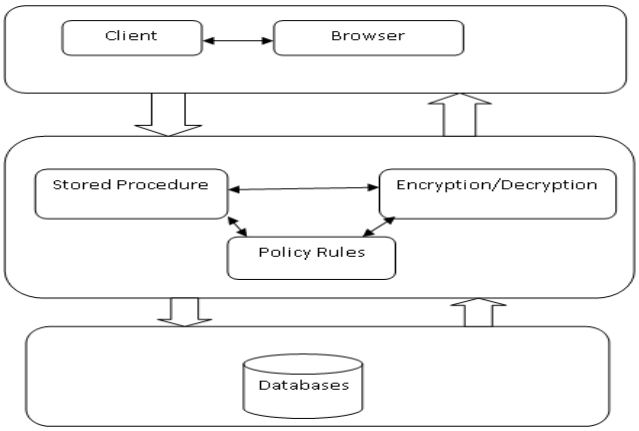

Figure 1.1: Three Layer Security Model

III. IMPLEMENTATION

The model has been developed by using the SQL server 2008. Top down design approach is used for the design of secure database. Proposed model is a three layer security model first layer is presentation layer which is responsible for the user interface. This layer takes user information and request from the user. After submitting the user information, a stored procedure will be called by passing the parameters like user name and password. Using DESENCRYPT () function user information are encrypted [8]. The encrypted values of user name and password are inserted into login table. This will prevent drop user login table attack.

The second layer contains the logical code and rules which is used to check the credentials of users in database. In this phase we classify our user in two roles admin and general user[6,7]. Admin has the authority to activate the roles and give the privileges to each user on database objects. First a set of roles has to be created by the following SQL command-

Create role admin
Grant Create session to dataadmin user;
Create role generaluser
Grant select to general user on table name;

When a role is granted to a user it becomes one of that user default roles and is enabled at login time. In data access layer, for each request a stored procedure is activated and after checking the credential requested information is send back to the user.

Revised Manuscript Received on February 15, 2020.

Dr. Pramod Singh, Assistant Professor, School of Studies Computer application Bastar University, Jagdalpur (CG),India.

The stored procedure provides the security to database from direct and SQL injection attacks.
Proposed model builds a security architecture based on access control policy, cryptography techniques and stored procedure. These mechanisms and techniques are combined together to present an interactive three-layer security model.

IV. EXPERIMENTAL RESULTS

Our experiment we are running several queries on database and measure the time of completion of the queries. We have two set of databases, fist one is unsecured database and another is secured database. These databases are filled with pretend data that we generated. There are four running environments, where all queries are running. The data is filled in database an student table is created and filled with 1000 records... In our database, we have used a primary key to uniquely identify the student records on database. Stored procedures and access policy rules are used for integrities. DES encryption is used for confidentiality. To compare the performance of queries between non-secure and secured databases we run four queries in four consecutive environments which are as follows-

Environment 1: in this environment we have considered only a non-secure database,

Environment 2: in this environment the data is not protected with integrity only encryption is applied for data protection

Environment 3: in this environment only stored procedure and access policy rules are applied for integrity.

Environment 4: in this environment both stored procedure and access policy rules are applied for integrity and encryption is applied for confidentiality.

We run a number of and types of queries on each environment many times to test the performance of the proposed model. This helps us to examine the performance of each environment and make aggregation of queries execution time.

A. Queries

The following four queries are executed during the experiment to understand the difference between secured and none secured query environment. In environment 1 we run our queries in none secure database, means there are no security parameters are applied. In environment 2 we are adding on encryption for confidentiality, in environment 3 we are adding stored procedures and policy rules for integrity and in environment 4 we have applied both confidentiality and integrity.

1. Display all student information from student table where Rollno. are as 1101, 1212, 1454, 1575, 1311 and 1648.

This query requests to display all records of students from all columns of the student table.

2. Display Rollno., name,F_name, gender, date of birth, Ph_no, class_name, marks, grad and result of student having Rollno. 1311.

In this query encrypted information is requested which contains sensitive data.

3. Display Rollno. of all students who got C grade.

In this query returns Rollno. of all students with C grade which does not contain any sensitive data.

4. Display the marks of all students.

This query is very expensive in execution at to in environments 2 and 3, where encryption and policy rules both are applied.in this query to extract the marks of all students checking of integrity and encryption decryption is required.

Our implementation there is two tables, login and student which are accessed remotely on the network. . To check the accuracy of the queries, we execute each query 10 times on each environment and get average execution time of each query in all environments. Execution of each query includes request sending to the database and fetching result from database and put it on the screen of users.

To avoid the performance issues related to queries result which may be very large. We have used filtering to show only timing statistics.to determine the scale our solution, we have splinted student table into three sub parts, each of which contains one third records of the student. We conduct our experiments with all students, 330 students and with 660 students.

A.1 Result of Query-1

Our first query was to: Display all student information having rollno.1101, 1212, 1454, 1575 and 1311 .

Figure 1.2 shows query first execution time in every environment on student table with all 1000 students. The execution time of query 1 in non-secure environment is very low, 0.05 millisecond that's why it is not shown in to the graph. Execution time of first query in second third and fourth environments are 50,150 and 300 milliseconds respectively.

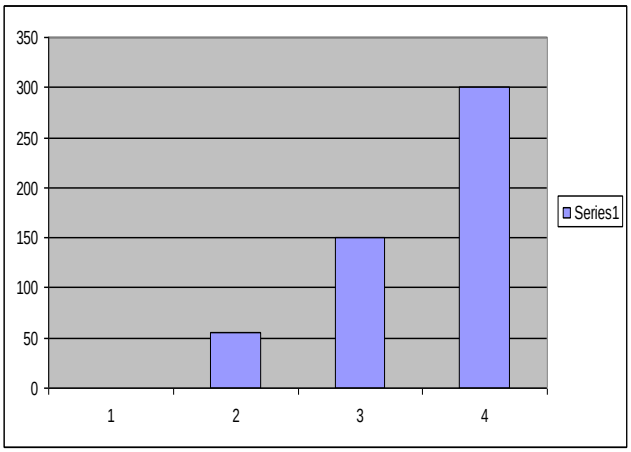

Figure 1.2: Time of execution of query 1 for all environments

The difference between performance of secured (4) and none secured (1) environment for displaying five students record from student table having 1000 records is 295. Means to display same information secured environment takes 300 ms while none secured environment takes 0.05 milliseconds. The performance of query is depends on encryption/decryption and integrity checking involve on the database.

A.2 Result of Query-2

To display the RollNo, Name, F_name, gender, date of birth, Ph_no, class_name, marks, grad and result of student having Rollno 1311 was the second query. This query is executed in all four running environments and the execution time is shown in Figure 1.3.

The execution time of this query in environment first takes 5 millisecond while in fourth environment it takes 65 milliseconds which is 60 times slower than first environment. This is similar for smallest dataset because all requested fields requires some verifications.

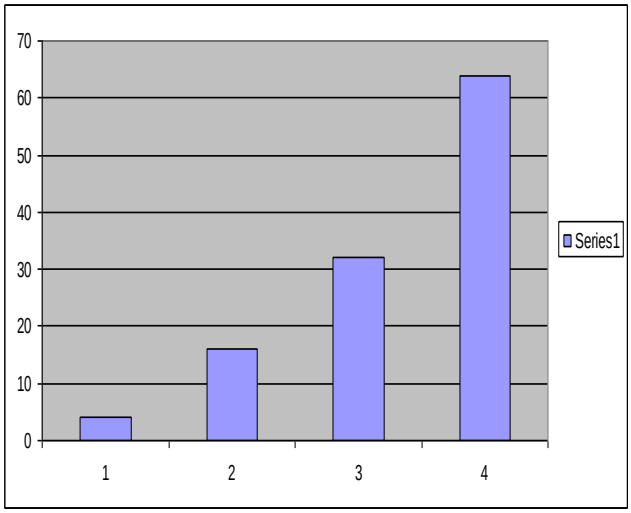

Figure 1.3: Time of execution of query 2 for all environments

A.3 Result of Query-3

Our third query was to display the RollNo. of all students who got C grade. Theoretically this query is very interesting and offers to see the scalability of
This query is interesting from a theoretical perspective, since it requests the Rollno of roughly a third of Students. It offers a way to see the scalability of execution and certifications on a big sub schema. The performance of execution of third query in all running environments on experimental dataset is shown in Figure 1.4.

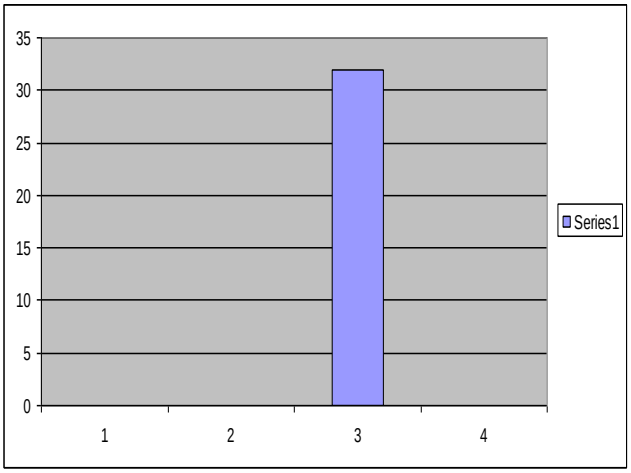

Figure 1.4: Time of execution of query 3 for all environments

From the above figure it is clear that the execution time of this query for environment first second and fourth is very low 0.5 which is not shown in figure but it takes long time to execute in environment three 32ms because it involves verification but not contain any encryption or decryption.

A.4 Result of Query-4

Our last query was to display the marks of all students. In this query encryption decryption is involved because it contains sensitive data and it also involves verification and validations according to the requirements of selected environments. In figure 1.5 we can see the execution time of the running query in all environments. Because environment one and three does not contain any encryption and decryption, so the execution time of this query in these environment is too short.

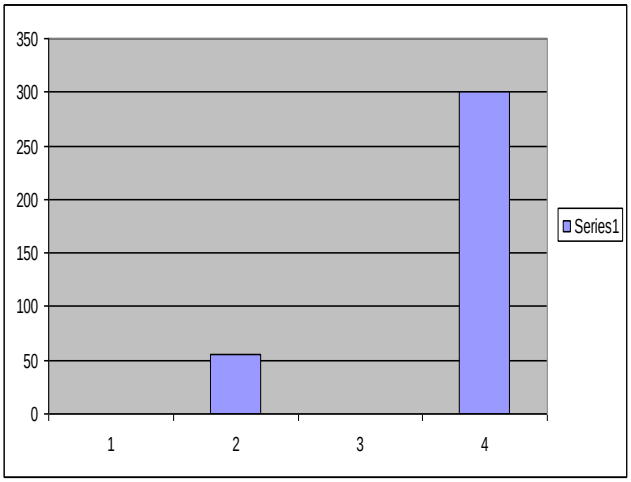

Figure 1.5: Time of execution of query 4 for all environments

From the above graph it is clear that execution time of this query in environment four is almost 295.9 times slower than the Environment first.
Experimental result shows that, when we run our queries in none secure environment it takes very minimum time approximate 25% faster to display the result of applied queries whereas in secure environment it takes more time to display the result. In queries that contains sensitive data which are protected by confidentiality and integrity takes time to check the validation of queries.

V. CONCLUSION

The developed model is tested in four different environments with four queries. In first environment we are not applied any security parameters. In second environment only encryption is applied for confidentiality, in third environment only stored procedures and policy rules are applied for integrity. Encryption stored procedures and policy rules are applied in fourth environment for confidentiality and integrity. Experimental result shows that this model is best for small database. if the database is large and contains sensitive data and multiple validation then this model takes more time to execute the queries.

REFERENCES

1. Mohd Muntjir (2014), “Security Issues and Their Techniques in DBMS - ANovel Survey”, International Journal of Computer Applications, 85(13).
2. Mubina Malik and Trisha Patel (2016),” Database Security – Attacks and Control Methods, International Journal of Information Sciences and Techniques (IJIST), 6(1/2).
3. Mohammed Rafiq, (2014), “Database Security Threats and Its Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, 4(2).

4. Osborn S. (2000),"Configuring role-based access control to enforce mandatory and discretionary access control policies",ACM Transactions on Information and System Security (TISSEC),3(2), 85–106.
5. Thuraisingham B.(1991), “Multilevel security Issues in Distributed Database Management System-II”,Elsevier Science Publication Ltd. Computer and Security,10(8),727-747.
6. Thuraisingham B. and Runinovitz H.(1993), “Multilevel Security Issues in Distributed Database Management System-III, Computer and Security,11(7),661-674.
7. Kaur A. and Kumari S.(2014),"Secure Database Encryption in Web Applications", International Journal of Advanced Research in Computer and Communication Engineering,3(7),7606-8
8. Srivastava S. and Tripathi R.R.K.(2012),"Attacks Due to SQL Injection & Their Prevention Method for Web-Application", International Journal of Computer Science and Information Technologies,3(2),3615-3618.

AUTHORS PROFILE

Dr. Pramod Singh, Assistant Professor School of Studies computer application Bastar University, Jagdalpur(CG) Mob-9691078337
Email-pramodsinghbvv@gmail.com
Qualification- MCA + Ph.D Area of research- Database Security