IJART- Vol-2, Issue-3, June, 2017 Available online at http://www.ijart.info/
DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

INTERNATIONAL JOURNAL OF APPLIED RESEARCH AND TECHNOLOGY
ISSN 2519-5115
RESEARCH ARTICLE

Study and Analysis of Different Database Threats and Basic Access Control Models

[1]Pramod Singh
[2]Bharat Mishra
[3]P. K. Rai

[1]Research Scholar MGCGV Chitrakoot
[2]Associate Professor MGCGV Chitrakoot
[3]Professor A.P.S. University, Rewa

Corresponding author:
Pramod Singh
singh.jobseek@gmail.com

Received: April 23, 2017
Revised: June 10, 2017
Published: June 30, 2017

ABSTRACT

Today's internet and communication technology growing rapidly and local business environment is now converted into global business environment. The database of private and public organizations is also increases rapidly. Hence the security of database became more important issue, the most common approach of database security is access control policy which is based on subject, object and their characteristics. The database security system has been developing a number of access control policies for assuring data confidentiality, integrity and availability. We review the key access control policies such as Mandatory Access Control policy (MAC), Discretionary Access Control Policy (DAC), and Role Based Access Control Policy (RBAC), we also perform a comparative analysis of these models which leads researchers in future to understand and enhance the basic access control models.

Keywords- Database, MAC, DAC and RBAC.

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

INTRODUCTION

The information is an important asset of today's global business environment. All organizations and government bodies are dependent on available information for taking right decision. This information's must be stored and get secured from unauthorized discloser. The information is stored and managed at different geographical environment and accessed from different places via different communication medium which can be subjected to be suspicious. Distributed environment requires a strong information management system to protect data and other resources form unauthorized discloser and improper modification at the same time system also confirms the higher availability of data and resources to legitimate users (Emil, 2009).

For enforcing protection requires an strong security system which supports only authorized accesses can take place and every access to a system and its resources must be controlled. The process used for controlling the misplaced of information is called access control and this access control needs the development of a strong access control system. the development of such system includes the three main concepts: Security policy, Security model and Security mechanism. Data security and privacy with integrity is necessary for every operation performed on the Internet. Whenever we discussed about security of data it is important to talk about the secure data transfer over the unreliable communication networks. But the data base security is also significantly important. A database contains important data that needs to be protected from various data attackers. Three pillars of database security are Confidentiality, Integrity, and Availability.

The Means of confidentiality is to the protection of data against unauthorized disclosure and it can be achieved by access control mechanism. It can be further enhanced by the use of encryption techniques is applied on data while stored into secondary storage or transmitted on a Network (Emil, 2009; Deepika & Soni, 2015 and Mohd et al., 2014). Integrity concept is used to Prevention of unauthorized accessing and improper data modification. It can be achieved by the combination of access control mechanism and semantic integrity constraints (Deepika & Soni, 2015 and Mohd et al., 2014). Availability make sure that data will always be available to the authorized user when the required (Deepika & Soni, 2015 and Mohd et al., 2014).

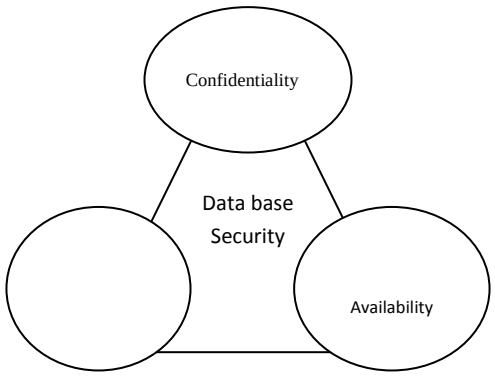

Figure-1: Security factor of database

Security threats to database

In rapidly changing environment the numbers of users are increases dramatically, so that the possibility of database security breaches is also increased. There are l various security vulnerabilities arise that can harm running database systems. An attacker will try to get administrative rights on database. Our goal is to try to protect database as much as we can. If presume that an attacker will try to execute malicious code from client application logging as guest, he/she will probably try to perform the following attacks.

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

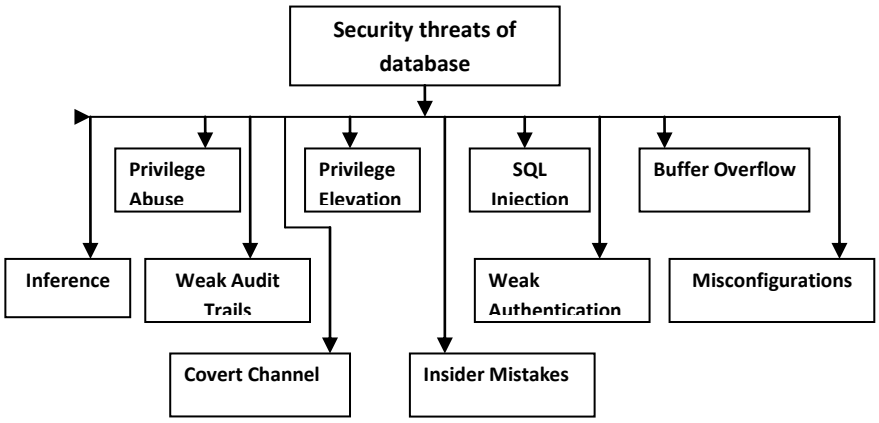

Figure-2: database security threats

Privilege Abuse

The information is a critical issue of today collaborative environment so there are many possibilities of privileged abuse i.e. the resources are illegally accessible by an unauthorized users or attackers (Rafiq, 2014 and Mohd et al., 2014).

Privilege Elevation

In distributed environment vulnerabilities in database software may be possible and attacker take advantage to convert access privileges of normal users to an administrator and change or misuse certain sensitive information stored in database (Rafiq, 2014 and Mohd et al., 2014).

Inference

Even we have a secure database it may be possible for users to draw inferences from the information stored in database. When a user can guess or have some prior knowledge about data stored in database then he could obtain an inference which leads security breaches. There are many cases which leads inferences in database (Malik & Patel, 2016; Rafiq, 2014 and Mohd et al., 2014).

SQL Injection

SQL injection is a technique for exploiting applications that use relational databases as their back end. In a SQL injection attack, an attacker tries to inserts unauthorized SQL statements into a weak SQL data channel. This is targeted to data channels include stored procedures and Web applications input parameters. These injected statements are then passed to the database where they are executed. (Deepika & Soni, 2015; Malik & Patel, 2016; Rafiq, 2014 and Mohd et al., 2014).

Misconfiguration

Database misconfiguration provides weak access points for hackers to bypass authentication methods and gain access to sensitive information. These flaws turn into the main targets for criminals to execute certain types of attacks. Default settings may not have been properly re-set, unencrypted files may be accessible to non-privileged users, and un-patched flaws may lead to unauthorized access of sensitive data (Rafiq, 2014 and Mohd et al., 2014).

Buffer Overflow

When a program or process tries to store more data in a buffer than it was projected to hold, this state is called buffer overflow. Since buffers contains only a finite amount of data, the extra data - which has to go anywhere - can overflow into contiguous locations, corrupting or overwriting the suitable data held in those locations. For example, a program is waiting for a user to enter his or her name. Rather than entering the name, the hacker would enter an executable command that exceeds the size of buffer. The command is usually

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

something short (Malik & Patel, 2016 and Rafiq, 2014).

Weak Audit

A database audit policy ensures automated, timely and proper recording of database transactions. This policy may be a part of the database security considerations from the time when all the sensitive database transactions have an automated record and the absence of this may arise a serious risk to the organization's databases (Deepika and Soni, 2015; Rafiq, 2014 and Mohd et al., 2014).

Covert Channel

A covert channel is an indirect resource of communication in a computer system which can be used to abate the system's security policy. A program running at an underground level is prevented from writing directly to unclassified data item. There are, however, other ways of communicating information to unclassified programs (Malik & Patel, 2016; Rafiq, 2014 and Kulkarni & Urolagin, 2012).

Insider Mistakes

Some attacks are not planned, they just happen unknowingly, by mistake. This type of attack is called as "unintentional authorized user attack" or insider mistake. It may occur in two situations, when an authorized user accidentally accesses sensitive data and by mistake modifies or deletes the information and if when a user makes an unauthorized copy of sensitive information for the reason of backup or "taking work home." Although it is not a malicious act, but the organizational security policies are being violated (Malik & Patel, 2016 and Rafiq, 2014).

Weak Authentication

Weak authentication schemes allow attackers to assume the identity of genuine database users by thieving or otherwise obtaining login credentials. An attacker may take up any number of strategies to acquire credentials (Malik & Patel, 2016; Rafiq, 2014 and Mohd et al., 2014).

Security components of database

Security means protection of information and information system from unauthorized access, modification and misuse of information. The purpose of distributed database security is to deal with protecting data from people or, software having malicious intension. Distributed system has four main security components, security authentication, authorization, Encryption, and access control.

Authentication

Generally authentication is realized by password. A user must supply the correct password when establishing a connection to avoid unauthorized use of the database. Password are assigned when user are created. A database can store a user's password in the data dictionary in an encrypted format. User can change their password at any time (Deepika and Soni, 2015; Mohd et al., 2014 and Kulkarni & Urolagin, 2012).

Authorization

The purpose of authorization is to deliver one protected access point enabling the users to connect the network once and authorize them access to permitted resources (Deepika and Soni, 2015; Mohd et al., 2014 and Kulkarni & Urolagin, 2012).

Encryption

It is a method of encoding data that only authorized users can understand it. A number of encryption algorithms are available which are useful for the encryption and decryption of data on the server, RSA, DES, and PGP are most

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

popular algorithms (Malik & Patel, 2016; Mohd et al., 2014 and Kulkarni & Urolagin, 2012).

Access control

The policies which are used by the users to access data object are called access control policies. These access control policies or access control mechanisms are used for securing databases. In these policies whenever a user tries to access any data object, the access control mechanism checks the rights of the user against a set of pre-defined authorization. The access control policy is basically divided into three main access control policies, such as Discretionary Access Control Policy (DAC), Mandatory Access Control policy (MAC) and Role Based Access Control policy (RBAC).These policies are most popular access control policy and has been used for many applications (Elisa et al., 2005.

Discretionary access control

In DAC models, all the subjects and objects in a system are identified and the access authorization rules are specified for each subject and object in the system. Here the Subjects can be users, groups, or processes and objects can be user defined types or database items. the user (subject) has the authority to grant or revoke the access rights to another subject on a particular object at his discretion .this model is flexible and mostly used for distributed environment but it does not provide high security. For example this model allows one object to copy the data from another object; due to this the user who does not have access rights can access the original data, causes violation of security goals (Deepika and Soni, 2015).

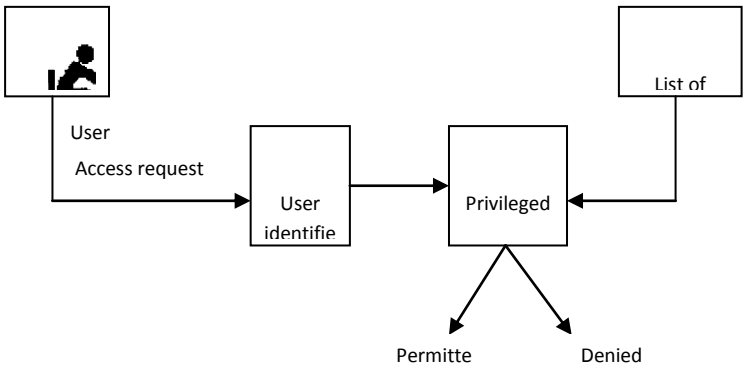

Figure-3: Architecture of DAC model

There are number of DAC model are introduced by the researcher the most popular one is the) access control matrix (ACM) model given by Harrison, Ruzzo and Ullman (Harrison and Ruzzo, 1976). The DAC model is based on three classes (S,O,A), i.e. the S for user, O for Object and A for action permitted. The access matrix model can be represented through the formula |S|*|O| matrix A. here the matrix represents different access rights to the subject on object, in HRU model Safety is general undecidable. The main problem of this model to decide the safe reachable state. In this model a particular subject has a particular access right that it did not previously possess (Garfinkel et al., 1997. Although the DAC is enforced

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

by many commercial DBMS products but it suffers from fallowing limitations.

Limitations of Discretionary Access control

1. Enforcement of the security policy
2. Cascading authorization
3. Trojan Horse attacks
4. Update problems

Mandatory Access Control:

MAC policy is based on the classification of subject and object And control of data flow between them. This controlling is taking care by the central authority to govern the accessing of information according clearance of security levels of subjects on objects. The mandatory access control requires two rules, one is protection of Data from unauthorized disclosure, and the second is protects data from contamination. There are number of MAC models have been introduced, few popular from that are-Bell -lapadula, jajodia and sandhu, biba-multi level integrity model and etc. The multilevel security model is used to decrease the security risk of database by using multilevel security enforcement. The access control in multilevel security is based on the Bell–LaPadula model (Jajodia, 1996 and Tarai et al., 2013). In this model all subjects and objects are classified according to predefined sensitivity levels which can be used for taking decision for access rights Bertino and Sandhu, 2005). To assure confidentiality and integrity two rules: no read-up and no write-down is implemented.

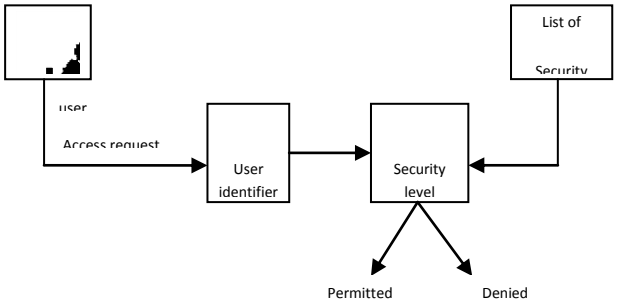

Figure-4: Architecture of MAC model

These rules ensure that the information cannot be flow from a higher sensitivity level to a lower sensitivity level (Bertino et al., 2000 and Sandhu, 1993).

Limitations of Mandatory Access control

1. Granularity of security object
2. Lack of automated security labeling technique
3. N-persons access rules

Role-based Access Control

A third approach for access control is represented by Role-Based Access Control (RBAC) model (Kulkarni et al., 2012). This policy is one of the important policies which is recently innovated and preferred by most of organizations. The role based access control policy is based on the activity of database users. In any organization each person has some responsibilities or it plays an important role and he has some rights.

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

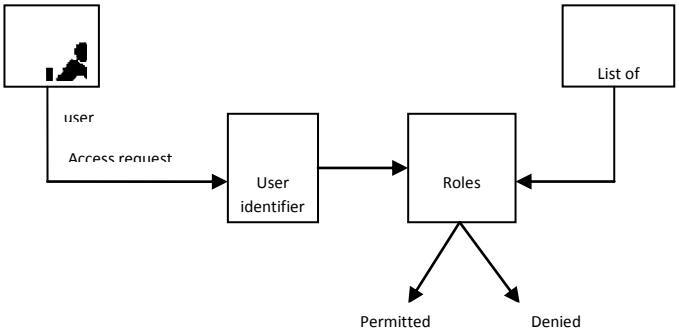

Figure-5: Architecture of RBAC model

The RBAC is based on these two concepts namely, role of user and rights of user on a particular subject (Tari et al., 1997 and Elisa et al., 2005). User of such system can play more than one roles, so a hierarchy of roles may exist which requires a proper management (Jajodia, 1996 and Tarai et al., 2013). Role and groups are two different things, a role is a Collection of privileges which can be activated and deactivated by users and a group is a collection of users. The membership in a group cannot be deactivated by users itself (Ferraiolo et al., 1999 and Bertino et al., 2005).

Limitations of Role-Based Access control

1. While RBAC supports a mark-able access control policy but also has some problems like Administrative issues for large systems.
2. Maintaining consistent information of the roles becomes difficult as the number of Roles increase.

Table -1: Comparisons of popular access control models

Parameters	DAC	MAC	RBAC
Basic concept	Owners behavior	sensitivity level of subject on object	Specification of roles
Accessing methods	Through owner	Through rules	Through roles
flexibility	less flexible	less flexible	Highly flexible
Degree of security	Less	high	high
Support grid or distributed environment	No	No	Yes
Supports Multi level database	No	Yes	Yes

Table1.shows that the DAC model works on the owners behaviour concepts while MAC works on the concept of subject and object and RBAC works on the specification of roles of users. In DAC model accessing has been perform through

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

owners validations while in MAC it is performed on the basis of rules and in RBAC it is performed by the validation of specified user roles. From table1 it is clear that the DAC model is less flexible in implementation and doesn't support more security while the MAC is less flexible but supports much security compare to DAC.RBAC model is highly flexible and supports strong security for database as well as computing environment. DAC and MAC are not good for distributed environment while RBAC is very good for distributed environment. MAC and RBAC supports multilevel database while DAC doesn't support.

CONCLUSION

Database security is a serious problem in today global business environment. In this paper we conducted study of database security threats and the techniques for securing database from attackers. There are 10 database threats and three main pillars of database security have been discussed. These three securities can be met by different method like cryptography, access control, authentication and authorization. The main goals of database security are to protect from unauthorized access to data, protect from unauthorized modification of data and to make sure that data always available when needed. We have also performed a comparative study of basic access control models in terms of security and supporting distributed environment. The RBAC models are expected to provide a framework for addressing a wide range of security requirements for distributed database environment. However, existing RBAC models are needed several improvements to provide high security to working with distributed environment**.**

REFERENCES

1. Emil BURTESCU, (2009), "Database Security – Attacks and Control Methods", JAQM, 4(4).
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. Deepika and Nitasha Soni, (2015), "Database Security: Threats and Security Techniques", "International Journal of Advanced Research in Computer Science and Software Engineering", 5(5).
4. Mohammed Rafiq, (2014), "Database Security Threats and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, 4(2).
5. Mohd Muntjir et.al (2014), "Security Issues and Their Techniques in DBMS - ANovel Survey", International Journal of Computer Applications, 85(13).
6. Saurabh Kulkarni and Siddhaling Urolagin, (2012), "Review of Attacks On Databases and Database Security Techniques", International Journal of Emerging Technology and Advanced Engineering, 2(11).
7. Betrino Elisa et al (2005) "Database Security-Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, 2(1).
8. Harrison and M.H. Ruzzo (1976)," J.D. Protection in operating Systems", Commun. ACM, 19(8): 461–471.
9. Min-A Jeong et al, (2003), "A Flexible Database Security System Using Multiple Access Control Policies", IEEE Journals.

DOI: https://doi.org./10.24163/ijart/2017/2(3):181-189

10. Garfinkel et al, (1997), "Web Security and Commerce",O'Reilly and Associates, Sebastopol,CA.
11. Sushil Jajodia (1996), "Database security and Privacy", ACM Computing Surveys, 28(1).
12. T. Tarai et al. (2013), "Enhancing database access control policies "AIJRSTEM, 3(1), pp. 109-113.
13. Elisa Bertino and Ravi sandhu, (2005), "Database Security-Concepts, Approaches and Challenges", IEEE Transactions on Dependable and Secure Computing, 2(1).
14. Bertino et al, (2000), "Protecting information on the Web", ACM Communication, 43(11): 189–199.
15. Sandhu (1993), "Lattice-based access control models", IEEE Computer, 26(11).
16. Saurabh Kulkarni et al (2012), "Review of Attacks on databases and database security techniques", IJ ETAE, 2(11).
17. Tari, Z. et al, (1997), "A role-based access control for intranet security", IEEE Internet Computing, 24–34.
18. Ferraiolo et al (1999), "A role-based access control model and reference implementation within a corporate intranet", ACM Trans, 2(1): 34-64.