IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 5 (Mar. - Apr. 2013), PP 85-89
www.iosrjournals.org

Analysis of Various Attributes to Have a Secure Database

Harpreet Saini[1], Dr.Kanwal Garg[2]

[1]*Research Scholor, M.Tech Department OfComputer Science And ApplicationKurukshetra University Kurukshetra, India*

[2]*Assistant Professor, Department OfComputer Science And ApplicationKurukshetra University Kurukshetra, India*

Abstract:*The premise of this paper is to analyze the various attributes by which the performance of database can be improved as well as for security of database. This paper provides an overview about how user, database administrator, system etc. affects the database security and also its performance. Author will try to analyze which of the attribute is better than the other one among various categories of attributes in terms of system performance and user authentication.*

Keywords:*Authentication, Database, Security*

I. Introduction:

As security is very important aspect in database so it is also important to know about those attributes which can affect the database and its performance also. Database system implies that the data is managed to some level of quality in terms of accuracy, usability etc. Ensuring the security of database is a complex issue as more complex the database, the more complex is the security measure that are to be applied. The presented paper comprises of six sections. The first section elaborates the introductory part. The second one is explaining the categories of attributes which are further subdivided into four parts i.e. user oriented, DBA oriented, system oriented and security policies. The third section analyse which method is better than other among various categories of attributes. The last two sections represent the conclusion and references.

II. Categories:

The categories of attributes are mainly divided in four sub-categories which are explained in detail below.

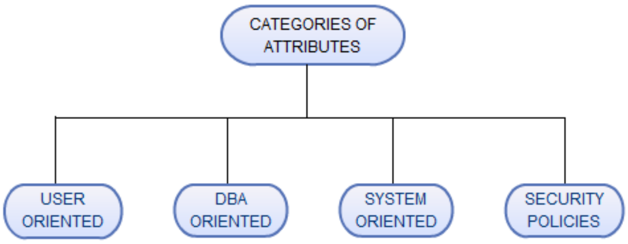

Fig.1-Categories of Attribute

2.1 USER ORIENTED:

In this section the main focus is given on authentication of the user. Authentication means user login which is the process during which user's identity is conformed. There are basically two strategies that can help to identify a user:

2.1.1 User id and password
2.1.2 Biometric identification

2.1.1 User id and Password:A fundamental security requirement is that you must know your users. You must recognize them before you can determine their privileges and access rights. Users can be authenticated in a number of different ways before they are admitting to create a database session. Passwords are one of the essential forms of authentication. A user must provide the correct password when starting a connection to avoidunauthorized use of the database. In this way, users tryingto connect to a database can be recognized by using information stored in that database. Passwords are assigned to the users when they are created. A user's password can be store by the database in the data dictionary in an encrypted form. At any time the users can change their passwords. Passwords must be kept secret at all times if database security systems are dependent on them but they are vulnerable to theft, forgery, and misuse. A number of steps can improve the basic password feature and provide greater control over database security out of which some are like : DBAs and security officers can control the password management policy through user profiles, the DBA can create standards for password complexity like minimum password length, password should be those words that cannot be found in the dictionary and also they should not consist of people's names or birthdates, after a certain amount of time passwords should be timed out or expiring.

2.1.2 Biometric Techniques:Biometric recognition refers to the use of different physiological characteristics like fingerprint recognition, face recognition, hand geometry recognition, iris recognition, retina recognition etc. and behavioural characteristics such as voice recognition, gait recognition, signature recognition etc. called biometric identifiers or biometrics. The main advantage that biometrics presents is that the information is unique for every individual and can identify the individual in spite of adaptation in the time which means it does not matter if the first biometric sample was taken year ago. The supports of e-learning security are: authentication, data confidentiality, access control, data integrity and non-repudiation. Biometric is a technique that can provide all these requirements with lots of reliability.

2.2 DBA ORIENTED:

Database administrators perform special operations like shutting down or starting up a database that should not be accomplished by normal database users.Database authentication includes the following category:

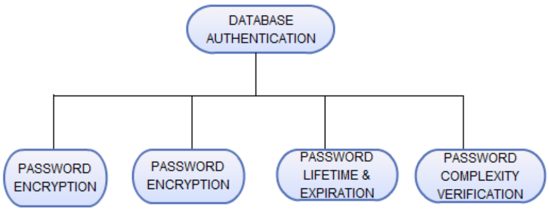
DATABASE AUTHENTICATION
PASSWORD ENCRYPTION
PASSWORD ENCRYPTION
PASSWORD LIFETIME & EXPIRATION
PASSWORD COMPLEXITY VERIFICATION

Fig.2- Types of Database Authentication

2.2.1 Password Encryption: To secure password confidentiality, password is always encrypted by the Oracle before sending them over the network. Oracle encrypts the passwords using a modified algorithm named as Advanced Encryption Standard (AES) algorithm.

2.2.2 Account Locking:A user’s account can be locked by the Oracle after a specified number of continuous failed log-in attempts. One can set up the account to unlock automatically after a specified time interval. The account can also be locked by DBA manually so that they must be unlocked explicitly by the database administrator.

2.2.3 Password Lifetime and Expiration: The database administrator can specify a period for passwords, after which they expire and must be changed before account login is again acceptable. A balanced period can be established during which each effort to login to the database account acquire a warning message to change the password. If it is not changed by the end of that duration then the account is locked and no more logins to that account are allowed without help by the database administrator. The database administrator can also set the password state to expired, causing the user's account status to change to expired [8]. Either the user or the database administrator must then change the password before the user can log in to the database.

2.2.4 Password Complexity Verification:Complexity verification checks that each password is complex enough to provide reasonable protection against intruders who try to break into the system by guessing passwords [8]. Each password must meet the following requirements according to the Oracle default password complexity verification routine checks such as the length of the password should be minimum of four characters, it should not equal to user id, it must include at least one numeric character, one punctuation mark and one alphabet character, it should be different from the previous password by at least three charactersand so on..

2.3 SYSTEM ORIENTED:

In this section the main focus is given on those attributes due to which the performance of the system can be affected and improved

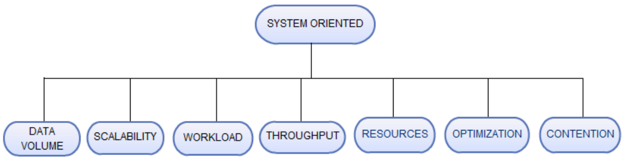

Fig.3-Types of System Oriented

2.3.1 Data Volume:The amount of data that the database has to manage for a specific period of time is known as Data volume. In terms of performance, the higher the data volume in the database, the less efficient the transactions executing against the database tend to be. As the volume of data extend, it adversely affects the database.

2.3.2 Scalability:System's capability to process more workload with a corresponding increase in system resource usage is known as scalability. In a scalable system, if the workload is doubled then the system would use twice as many system resources [3], but due to collision within the system, the resource usage might exceed twice the original workload.

2.3.3 Workload:The amount of work that the database can perform in a given period of time is known as Workload. It is a combination of operations containing data queries, batch jobs, data warehousing, online transactions and system commands that the database has to process. The complete workload can have a major impact on the performance of the database, so its effectiveness can be reduced when it has to perform many operations.

2.3.4 Throughput:Throughput is the quantity of data or information which is processed by a computer within a given duration of time. In terms of database performance, throughput defines the total capacity of the computer to process data. To assure that data are processed, computer capabilities, processor speed, the efficiency of the database management system software and the operating system are important which means that the performance of database can be reduced if processor speed is low, hard disk space is low and system software does not perform well.

2.3.5 Resources:Resources are the hardware or software tools that are important to perform database system functions. They involve the memory like allocated buffer pools or address spaces, the hard disk, micro cords, cache controllers and. A database can perform better if it has more resources at its disposal than one with fewer resources.

2.3.6 Optimization:Optimization includes the procedures which are used to make the database system to perform as effectively as possible. All types of database systems can be optimized; anyhow some of the optimization features may be internal or external to the DBMS and thus affecting the system performance.

2.3.7 Contention:The condition in which two components of the workload try to use a single resource to perform different roles is known as Contention. If the workload of the database for a particular resource is high then the contention happens. In that case, whenever the contention increases, the quantity of data processed in a given extent of time decreases.

2.4SECURITY POLICIES:

A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and users requirements change. Security policies discussed below are explaining about the security policies of system, data, user and password.

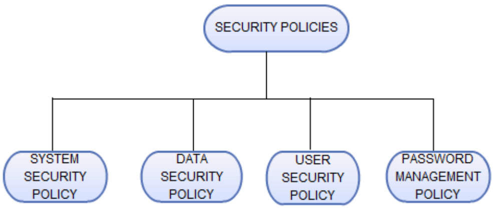

Fig.4-Types of Security Policies

2.4.1 System Security Policy: Each database has one or more administrators responsible for controlling all aspects of the security policy: the security administrators. If the database system is small then the database administrator might have the responsibilities of the security administrator. On the other hand if the database system is large then a special person or group of people might have responsibilities limited to those of a security administrator. A security policy must be build up for every database and should include several sub-policies like database user management, user authentication etc. as discussed below**.**

2.4.2 Data Security Policy: Data security involves working that control access to and use of the database at the object level. Data security policy decides which users have approach to a particular schema object, and the specific types of actions allowed for each user on the object. Total data security should be based on the sensitivity of data. If information is not sensitive, then the data security policy can be more inaccurate on the other hand if data is sensitive, then the security policy should be developed to maintain tight control over access to objects.

2.4.3 Use Security Policy: For user security policy there are certain levels of security like general user, end user, Administrator security etc. If user authentication is handled by the database, then security administrators should develop a password security policy to save the database access security. For example, database users must change their passwords at regular interval of time and by forcing a user to modify the passwords unauthorized database access can be reduced.

2.4.4 Password Management Policy: Database security systems which are dependent on passwords require that passwords must be kept secret at all the times but passwords are accessible to theft, falsification, cheat and misuse. To give permission for greater control over database security, Oracle's password management policy is controlled by DBAs and security officers through user profiles.

III. Analysis Of Attributes Of Various Categories:

In this section the author will discuss about the analysis of methods among various categories of attributes. The will try to find out which method is better than the other. In the first section i.e. user oriented section there are two parts one is user id & password and the other one is biometric techniques. Out of these two methods the author has given more importance to the biometric techniques because biometrics technologies are secure means of authentication as biometrics data are unique, cannot be shared, copied and lost. And also this technique required the person being authenticated to be present at the point of authentication[9].Thus biometric methods are most secure methods. In the second section the author has explain four sub-sections password encryption, account locking, password lifetime and expiration and password complexity verification. Out of these sub-sections password encryption is better than other methods as in case of account locking the account can be locked due to unauthorized person also if he failed to login that account in specified time interval, on the other hand password lifetime and complexity verification methods are also good but not better than password encryption as in this case the password is encrypted before sending over the network with the help of algorithm. In the third section author has discussed about the system performance and about various attributes due to which system performance can be improved or affected like data volume, scalability, work load, throughput etc. Out of these all attributes two attributes are better, the first one is resources as database can perform better if it has more resources at its disposal than one with fewer resources and other one is optimization as it includes the procedures which are used to make the database system to perform as effectively as possible. In the last section some security policies about system, data, user and password management are discussed. Out of these the author has considered the password management policy to be better than other because all other information are automatically be secured if the password is secured as database security systems are dependent on password so it must be kept secret.

IV. Conclusion:

In this paper the main focus is given on various categories of attributes by which the author has try to explore about the two things i.e. security and performance of database. From keeping in view the above explained categories of attributes the author has concluded that which method is better than the other out of each and every category in terms of system performance, user authentication.

References:

[1] http://www.agiledata.org/essays/accessControl.html#DatabaseImplementationStrategiesretrieved on 30-03-2013.

[2] http://docs.oracle.com/cd/B14117_01/network.101/b10777/authuser.htm retrieved on 30-03-2013

[3] http://www.ehow.com/info_12011201_factors-affecting-performance-database.html retrieved on 01-04-2013

[4] http://docs.oracle.com/cd/B28359_01/server.111/b28310/secure001.htm retrieved on 02-04-2013

[5] http://www.personal.psu.edu/glh10/ist110/topic/topic07/topic07_04.html retrieved on 02-04-2013

[6] http://www.oracle-base.com/articles/misc/os-authentication.php retrieved on 10-04-2013

[7] http://www.brighthub.com/computing/smb-security/articles/61400.aspxretrieved on 11-04-2013

[8] http://docs.oracle.com/cd/B19306_01/server.102/b14220/security.htm#i13527 retrieved on 11-04-2013

[9] ChanderkantVerma “Soft Biometric: An Asset for Personal Recognition” published in the proceeding of international journal of computer science & communication technologies, ISSN 0974-3375,Vol-1,PP. 160-163, Jan 2009.