**Abstract**

In todays era, data is retrieved at a very fast speed, it is fetched and stored at the destination known as database. Database allows data to be stored and managed in a very efficient way. Data manipulation and maintenance are performed through the database management systems. Data is very important for any organization, so it is important to secure data stored in the database. Database security is the one that allows data to be protected from all possible database attacks. It is very important to develop security models to apply database security very effectively. There are different security models, as they deal with different aspects of security problems in the database systems. Security models may be different as they follow different rules, regulations and assumptions about what creates a secure database. It is very challenging for the database security personals to select appropriate or most relevant database models according to their organizations requirements. In the paper, we have reviewed about the database security attacks and their countermeasures and their relevant control methods. To plan an explicit and directive based database security, it is very critical to adopt approaches related to securing database. It is one of the most important or critical issues of any organization to secure their data stored in the database. There can be more complex security problems of database, as the data increases in the database along with its complexity.

**1. INTRODUCTION**

We can define database as a collection of data stored in computer’s hardware. Databases facilitated authenticated or authorized users to access, store and examine or analyze data efficiently and easily. Database is a collection of different tables. Each table has unique columns and rows. A user construct queries to fetched stored information according to the requirements in the form of views. Views are tables constructed through queries; they can have data from more then one table. The data in the database is stored in a way to effectively supports the process of information or data retrieval and storage. The repository in which the major chunk of data is stored in known as database. The user interface facilitate users to effectively manage data store in database by providing many functionalities. The user interface for databases is known as database management systems. Database management systems are applications software that allows authorized users, other applications to interact with the database and capture and analyze data. It assists companies to store and organize data for high quality performances and maintaining indices allows fast retrieval.

Database management systems provides the function of concurrency control. Data recovery operations are also provides by database management systems. In recent times, organizations require databases to save any type of data required. It is because of the fast retrieval of data and it is very affordable to create and maintained for any organization. Database is advantageous because it automates different business processes, it saves other resources and man hours required to do lot of manual or paper work. Without databases, users are required to manually track and verify various business transactions, that can be costly and prone to many human errors. But database management systems provides effective way to generate various reports. Entering warehouse stock information manually was time consuming and provides less accuracy, but hand held scanners can be used to store information directly in the database. It is concluded that database can provide speed and accuracy for the businesses processes. The other question arises that whether the data stored in the database is secured. In this era, security is most critical and challenging issue for any organization. Data is one of the most important asset of any organization. Databases can be complex and requires full understanding of security risks and issues by security professionals to secure database effectively.

After consulting many database experts and database administrators, many organization’s database administrators are now fully informed about which database, tables and columns have critical information. It is because they are working with legacy application and there are no proper database documentation and data models. Even if any expert have full database knowledge, it is difficult to protect database because of its unique implementation and database procedures. Database security can be implemented by using wide range of database security controls that can be implemented to secure database from various possible attacks, against database confidentiality compromises, against its integrity and availability. The security controls are technical, administrative and physical. Database security is protecting the data stored in a repository. In database environment, there are different security layers: database administrator, system administrator, security officer, developers and employee. Security can be compromise at any of these layers.

**2. LITERATURE REVIEW**

In this field, a significant amount of work has been done. Following references are used to review the work done by various authors to described the database security risks and threats and provide effective counter measures and their controls.

**Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin**

It is very obvious, that database acts as a backbone of any application. Database has organization’s critical and important data and there are lot of chances that it can be attacked. In this paper, authors have discussed various database attacks. In this paper, authors have reviewed important database security methods such as “access controls”,”methods against SQLIA”. The paper also has techniques such as encryption and data scrambling. This paper has also provides details about the furture research areas in the database security.

**Mr. Sohail Imran, Dr. Irfan Hyder**

Mr. Sohail Imran and Dr. Irfan hyder have discussed various database security problems and their related security models suitable for different database management systems. They have proposed various important and distinct security models to secure relational databases and object oriented databases. There are no proper standards or rules to design or develop these security models. Different security issues has been identified in this paper. Through this paper, one can construct and implement effective security policy in any organization.

**Shelly Rohilla and Pradeep kumar Mittal**

As it contains the most important and critical assets of any organization i.e. Data. It is most favorite target of any attackers. Database can be compromised in different ways. This paper, discussed about various database security threats and risks from which database should be secured or well protected. This paper provides solutions to most of the security threats and problems, most of the solutions are very effective but some are ordinary.

**Shivandan Singh, Rakesh Kumar Rai**

Database is used by many applications. Without databases, these applications cannot work properly, hence database acting as backbone to these applications. Database are the main data storage for many organizations. Databases attacks are increasing as more organizations tends to store data in the database. These attacks, if successful can expose most important and critical data to the attackers. This paper includes the description and review of the most important database security techniques and methods such as “access control” techniques to prevent SQLIA. Data encryption and scrambling is also discussed in this paper. The paper also includes the future works related to the database security. This paper is useful to give more concrete database security solutions.

**3. DATABASE THREATS**

Today database systems are experiencing different types of attacks. It is important to review database attacks first , then discuss database security techniques.

**3.1 Excessive Privileges**

Authorization is the procedure that awards a client endorsement to make certain move in the assigned frameworks whether it is to see, adjust, share, or erase data. Authorization is worried about what the client is permitted to do.

The granularity of approval is just tantamount to the modernity of the framework which supports the entrance endorsement basic leadership procedure and requirement of affirmed get to.

The entrance endorsement procedure is intended to give access dependent on the client's job and occupation obligations which is alluded to the guideline of least benefit, which states clients, gadgets, projects, and procedures which are interconnected or should get to one another to impart and take certain activities, ought to be conceded simply enough consents to do their required capacities.

The danger of unreasonable and pointless access just as the danger of deficient access to play out a specific assignment to achieve an objective ought not be neglected. Extreme access rights past somebody's ordinary occupation capacities make an open door for blunders, mishaps, and endeavors which can influence the privacy, trustworthiness, and accessibility of data and frameworks. Inadequate access or access rights not gave in an auspicious way can likewise adversely influence business tasks.

A much extreme case is the point at which a client is conceded director or a root access to a framework with no support. The exceptionally special access ought to be constrained to only a couple of people in an association in such a case that the record is contaminated with malware or access accreditations are stolen, the interloper can cause a lot more noteworthy harm than with much restricted benefits.

At the point when somebody's entrance is past that individual's expected access to play out their activity obligations, at that point that entrance is viewed as past the standard of least benefit.

Indeed, get to rights might be heightened for certain people to achieve certain errands, for example, when supplanting someone else who has higher benefits, in any case, the raised access may must be specific and impermanent.

Countermeasures of privilege abuse includes the development of access control policy. It is very critical to provide unnecessary privileges to the user. Good audit trail can be a very effective to prevent legitimate privilege abuse.

**3.2 SQL INJECTION**

A portion of the client information sources may be utilized in confining SQL articulations that are then executed by the application on the database. It is workable for an application NOT to deal with the sources of info given by the client appropriately. If so, a malignant client could give surprising contributions to the application that are then used to outline and execute SQL explanations on the database. This is called SQL injection. The outcomes of such an activity could be disturbing.

SQL injection is a code injection strategy that endeavors the vulnerabilities in the interface between web applications and database servers. The defenselessness is available when client's sources of info are not effectively checked inside the web applications before being sent to the back-end database servers. Many web applications take contributions from clients, and after that utilization these contributions to build SQL inquiries, so the web applications can get data from the database. Web applications likewise use SQL questions to store data in the database. These are basic practices in the advancement of web applications. At the point when SQL questions are not deliberately developed, SQL injection vulnerabilities can happen. The SQL injection assault is one of the most widely recognized assaults on web applications.

Countermeasures for sql injection includes the usage of stored procedures instead of using direct queries. Implementing MVC architecture is another important factor in avoiding sql injection.

**3.3 MALWARE**

The size and unpredictability of the current working frameworks also, applications is persistently expanding and it isn't a simple assignment to guarantee the safe activity of such frameworks. Despite the fact that there are a few devices, for example, interruption location frameworks, nectar pots, and antivirus the dynamic nature of the assaults makes it hard to distinguish also, avoid assaults. Then again, it is straightforward undertaking for the aggressor to bargain such frameworks and produce various kinds of assaults. Subsequently we are seeing an expanding number of multi day assaults once a day. Multi day assaults are the assaults which are beforehand not known. So as to manage the malware the security apparatus merchants investigate the malware and create assault marks to manage the malware. In any case, in the vast majority of the cases the examination is done physically and this requires impressive time before a mark can be created for malware. What's more, mechanized devices, for example, ADMmutate empower the aggressor to naturally produce varieties to the malware for every contamination; making it very hard for the security experts to recognize and create appropriate assault marks.

Advanced attacks are conducted by cybercriminals, state-hired criminals and spies. They used different types of attacks includes spear phishing emails and malware to reach inside the organizations and get access to the critical data or information. Organizations are unaware about the malware attacks, authorized users are accessed by these cyber criminals to access organization’s networks and sensitive information or data.

Counter measures for malware can using firewalls and installing antivirus in the system.

**3.4 Weak audit trail**

Powerless Audit Trail is another risk for database security. Most review instruments have no consciousness of who the end client is on the grounds that all action is related with the web application record name. Plus, clients with managerial access to the database can mood killer local database examining to shroud their fake movement. A legitimate review trail should gather and file point by point records of the data put away inside your databases, especially those putting away touchy data like monetary or wellbeing records. The error that most associations make is expecting that their worked in review trails are adequate enough to enable them to remain agreeable and secure.

A large portion of the Organizations utilize local review instruments given by their database sellers or depend on impromptu and manual arrangements. Be that as it may, this procedure don't record subtleties important to help evaluating, assault recognition, and crime scene investigation. Aside from this, local database review instruments are amazingly infamous for expending high CPU throughput and plate assets driving numerous associations to quit evaluating. As per another whitepaper by Imperva, "most local review systems are exceptional to a database server stage. For instance, Oracle logs are not the same as MS-SQL, and MS-SQL logs are diverse structure DB2. For associations with heterogeneous database situations, this forces a noteworthy deterrent to executing uniform, adaptable review forms. At the point when clients get to the database through big business web applications, (for example, SAP, Oracle E-Business Suite, or PeopleSoft) it tends to challenge comprehend which database get to action identifies with a particular client." It is seen that review components have no attention to who the end client is on the grounds that solitary record name is related with the web applications. Moreover, local Database Auditing can be mood killer by the clients with Administrative Privilege to shroud any sorts of false action. To guarantee solid detachment of obligations approaches, the Audit capacities and duties must be isolated from both database directors and the database server stage.

Countermeasures for weak audit trail includes the usage of audit appliances related to network. These appliances should not affect database performances. These audit trail appliances should perform and operate independently and provides effective data or information collection.

**3.5 Backup Exposure**

The storage media used for backing up information is usually not protected from the unauthorized attacks. Due to this vulnerability, many information securities breaches has been experienced that involved backup storage media such as disks and tapes. Also, organizations do not focus on auditing and examine the activities of database administrators and who have access to the low-level data, this can result in the information stealing and misusing. It is very important for any organization to take care of their backup storage devices and also control and monitor the activities of database administrator, this is not only including in database security best practices but also it is one of the most important database security regulations.

Countermeasures for backup exposure includes the database encryption. The stored information should be encrypted , it will secures both production and backup duplicates of databases. Also audit the sensitive data control access and activities of database administrators.

**3.6 Weak Authentication**

Weak authentication refers to the authentication pattern that is weak and can be easily assumed or identify by the attackers. The weak authentication allows attackers to perform brute force attack, social engineering etc. It is very important to implement strong password patters or two factor authentication. The Authentication procedures should be linked with organizations user management infrastructures.

**3.7 Database vulnerabilities and Misconfigurations**

It is very usual to identify or detect vulnerable and unpatched databases.

Each Software Strive to be without blunder of bug free. Tragically, till date no one at any point prevailing to convey blunder free programming. Whatever might be the financial limit of the product, whatever might be the experience levels of the product improvement group, it's not possible for anyone to guarantee that the product they constructed is without bug! Bugs can be all over the place, regardless of whether its an Operating System (OS) or Database Management Systems (DBMS). Regardless of whether minor or major, These bug can have extreme effect on an Organization's System. In this way, database sellers discharge fixes occasionally to guarantee touchy data in databases is shielded from dangers. For example, Oracle gives a basic fix update (CPU) each quarter.

Fixing a Database takes a very long time to an association. During this time the Database stays powerless. Programmers are sufficient to misuse un-fixed Database that still have default records and arrangement parameters. The initial step to be performed for ensuring your database is deciding how the databases are as of now designed from a security viewpoint. Most sellers give fix reports on a genuinely normal premise. When they discharge the fix, the assailant promptly and its welcome from them to discover the powerlessness and assault for doing hurt. Their discharge and fix levels will be distinguished and contrasted with seller security fix disseminations. An examination of ought to be done at this phase to locate the degree of seriousness of the vulnerabilities. The sorts of vulnerabilities will extend the range, from powerless and default passwords to unpatched database programming shortcomings. So the following stage is that at whatever point these patches are discharged they ought to be fixed – at any rate the most basic vulnerabilities. In the event that it is left unpatched, assailants can figure out the fix and endeavor the vulnerabilities, leaving the DBMS considerably progressively helpless that before the fix was discharged. The greater part of the Organization postponement even year to actualize the fix to decide whether it influences the entire system. At this point the Database stays helpless.

Counter measures for unpatched and misconfigured databases includes some precautions such as no default accounts should be there, and every account should be created by using unique username and passwords.

**3.8 Unmanaged Sensitive Data**

Many organizations failed to maintain accurate database inventory and the sensitive information objects placed in them. Database that are forgotten may contain critical information. These forgotten database must not have any proper controls and permissions and may get in control of unauthorized access.

Countermeasures of unmanaged databases includes the encryption of sensitive data, that if any forgotten database exists, but information cannot be used by unauthorized user as the data is already encrypted. It is very important to implement needed controls and permissions to database systems.

**3.9 Denial of Service**

A denial of service assault is a security risk where aggressors shell a system (for the most part an online system) with phony solicitations for service thus deny access to approved clients. along these lines, the assault bargains the accessibility of the system.

The thought process in DoS assaults is once in a while an abhorrence of the association running the system at the same time, more normally, it is utilized as a methods for extortion. Destinations are compromised with a DoS assault, which will make them inaccessible, except if they make an installment to the criminal who is undermining them.

Denial of service assaults are moderately simple to identify and kill in the event that they originate from a solitary PC so the most usually utilized DoS assault currently is a purported Distributed Denial of Service assault where a system of PCs send a huge number of solicitations to the system that is being assaulted. These systems are typically people groups' PCs that have been tainted with malware.

Countermeasures for denial of service attacks include the stiffening of TCP/IP container by implementing the accurate settings to maximize the capacity of the TCP connection pool. Minimize the TCP connection time period. Implement dynamic and automated backlog methods to confirm that connection queue is not haulted.

**4. CONTROL METHODS FOR DATABASE THREATS**

To get rid of database security threats every organization should have developed security policy and it should be implemented. Authentication is very important in security policy, because if there is strong authentication procedure then there will be less likelihood of any kind of threat. Different rights have been granted to different users in database systems. Access control methods are used to deal with different access rights and controls of different users. It is one of the basic method or technique to protect data objects in the database. The control access methods is supported by many database management systems.

**4.1 Access Control**

It is one of the important and basic functionality that should be provides by any database management system. It is used to protect data from the unauthorized access and blocking the read and write operations. The access controls allows entire communication should be conducted within the mentioned limitations of security policies. Errors can create huge problems in organizations. By controlling the access rights, likelihood of risks are minimized that affects the database security on the main servers. For example, if any table is modified or deleted unintentionally then the changes can be roll back. The mistaken deletion of tables can be restricted by applying access controls.

Access controls includes File, program permissions and rights to fetch and modify information in the database.

**4.2 Inference Policy**

It is very important to secure data at particular level. This protection can be implemented when certain data is required as facts and it is needed to be prevented at a particular level of higher security. It assists in identifying and determining how to secure information from being released. The main goal of the inference policy is to restrict the disclosure of information indirectly. Unauthorized data disclosure can be achieved by three ways: Correlated data, missing data and statistical inference.

**4.3 User Identification/Authentication**

The most important and basic security requirement includes that one must know about their own users. Users should be identified before privileges and rights have been assigned. It is important so that organization can audit about the users actions and data activities.

Before users can create any database, there are various ways through which users can be authenticated. Database systems provides facility to authenticate and identify users. Operating system can perform the external authentication. Secure socket layer is also responsible for identification of users through middle tier servers. This type of authentication is known as proxy authentication.

It is very important requirement of database security as identification of users shows the type of users that are allowed to interact with the database systems. To confirm the security, users are identified and authenticated, and sensitive and critical data is stored by using encryption techniques preventing from being modified by unauthorized access.

**4.4 Accountability and auditing**

Auditing includes the monitoring and recording the database activities performed by both database users and non database users. Accounting is a process that allows to maintain the audit trail of users activities on the system. To confirm and ensure physical integrity of data, accounting and auditing is very important. If the user has logged in the system successfully and if he tries to access resource, the system should be able to monitor and record successful and unsuccessful attempts. The activity and its status should be recorded and stored in the audit trail.

**4.5 Encryption**

Encryption is a process to convert valuable information into a form that is not readable by a person. The information can be converted in the readable form to only those authorized people who have a key of encrypted cipher text. The data in the form of cipher text is known as encrypted data. There many encryption methods and techniques available to protect data from unauthorized access.

**5. CONCLUSION**

 Access security is a way that allows who can access data and what kind of data attackers are trying to access the database. There are many methods and techniques to improve the database security. This paper includes the review of the work done by various authors in the database security field. It includes various mandatory and discrete security models to secure the relational as well as object oriented database. The paper includes the information that can be used to develop effective database security policies. The paper focused more about the recent database threats and countermeasures and their control methods.

**6. REFERENCES**

Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin. (2012). Review of Attacks on Databases and Database Security Techniques. Facility International Journal of Engineering Technology and Database Security Techniques Research.

Sohail IMRAN, Dr Irfan Hyder, Security Issues in Database. (2009). Second International Conference on Future Information Technology and Management Engineering.

Shelly Rohilla, Pradeep Kumar Mittal.(2013). Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering.

Shivnandan Singh, Rakesh Kumar Rai. (2014). A Review Report on Security Threats on Database, International Journal of Computer Science and Information Technologies.

Debasish Das, Utpal Sharma, D.K. Bhattacharyya.(2010). An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications.

Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: principles and practice* (pp. 978 0). Upper Saddle River (NJ: Pearson Education.

Shulman, A., & Co-founder, C. T. O. (2006). Top ten database security threats. *How to Mitigate the Most Significant Database Vulnerabilities*.

Khanuja, H. K., & Adane, D. S. (2011). Database security threats and challenges in database forensic: A survey. In *Proceedings of 2011 International Conference on Advancements in Information Technology (AIT 2011), available at http://www. ipcsit. com/vol20/33-ICAIT2011-A4072. pdf*.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*(2-3), 203-225.

Denning, D. E. R. (1999). *Information warfare and security*(Vol. 4). Reading, MA: Addison-Wesley.

Ghorbanzadeh, P., Shaddeli, A., Malekzadeh, R., & Jahanbakhsh, Z. (2010, June). A survey of mobile database security threats and solutions for it. In *the 3rd International Conference on Information Sciences and Interaction Sciences*(pp. 676-682). IEEE.

Sharma, R. K., & Rawat, D. B. (2014). Advances on security threats and countermeasures for cognitive radio networks: A survey. *IEEE Communications Surveys & Tutorials*, *17*(2), 1023-1043.

Crites, J. G., Tor, D., & Gickler, C. (2006). *U.S. Patent No. 7,085,359*. Washington, DC: U.S. Patent and Trademark Office.

Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and secure computing*, (1), 2-19.

Rawat, D. B., & Bajracharya, C. (2015, April). Cyber security for smart grid systems: Status, challenges and perspectives. In *SoutheastCon 2015* (pp. 1-6). IEEE.