ORIGINAL RESEARCH ARTICLE | UHD JOURNAL OF SCIENCE AND TECHNOLOGY

A Review of Database Security Concepts, Risks, and Problems

Ramyar Abdulrahman Teimoor*

Department of Computer, College of Science, University of Sulaimani, Sulaymaniyah, Iraq

ABSTRACT

Currently, data production is as quick as possible; however, databases are collections of well-organized data that can be accessed, maintained, and updated quickly. Database systems are critical to your company because they convey data about sales transactions, product inventories, customer profiles, and marketing activities. To accomplish data manipulation and maintenance activities the Database Management System considered. Databases differ because their conclusions based on countless rules about what an invulnerable database constitutes. As a result, database protection seekers encounter difficulties in terms of a fantastic figure selection to maintain their database security. The main goal of this study is to identify the risk and how we can secure databases, encrypt sensitive data, modify system databases, and update database systems, as well as to evaluate some of the methods to handle these problems in security databases. However, because information plays such an important role in any organization, understanding the security risk and preventing it from occurring in any database system require a high level of knowledge. As a result, through this paper, all necessary information for any organization has been explained; in addition, also a new technological tool that plays an essential role in database security was discussed.

Index Terms: Database security, Attack, Threats, Protection, Encryption, Database vulnerability

1. INTRODUCTION

Databases and database systems are an indispensable part of contemporary life; most of us engage in at least one database-related activity each day [1]. Simply, everyone can save data and information into a database in order to keep business apparatuses safe and protected. In the case of an emergency, technology has dramatically increased our odds of survival. In reality, technology has enhanced how we live, travel, communicate, study, and be treated medically, as well as how we conduct our lives. Technology employed in essential infrastructure that sustains our daily lives is becoming a necessity, and life would be unthinkable without it [2].

Today's databases and whole systems are often subjected to a variety of security risks. Many of these risks are prevalent in small businesses, but in large businesses and institutions, vulnerability is critical since they contain sensitive information that is utilized by many individuals and departments [3].

It is concerned with protecting databases against some form of unwanted access or danger at any stage. Server protection entails allowing or disallowing user behavior on the database and its properties. The security of their database has been sought by well-functioning organizations. They do not let the unlicensed user admittance their files or documents. They also state that their information is safe from any deceptive or unintended variations. The security priority is on data protection and privacy [4].

Access this article online

DOI:10.21928/uhdjst.v5n2y2021.pp38-46 | E-ISSN: 2521-4217 | P-ISSN: 2521-4209

Corresponding author's e-mail: Ramyar Abdulrahman Teimoor, Department of Computer, College of Science, University of Sulaimani, Sulaymaniyah, Iraq. ramyar.teimoor@univsul.edu.iq

Received: 17-07-2021 Accepted: 30-09-2021 Published: 10-10-2021

This study concentrates on the database security risks that the database forensics can mitigate, as it is becoming an increasingly important topic for investigation. The study aims at assisting organization to protect data by introducing the highest nine vulnerabilities found in database. Context information, being Up-to-date risk information for each threat, protection data and information user database safety gateway protections, and some other method has also been investigated [5].

What is every organization next issue, are data using database protected? Nowadays, security is one of the most critical and difficult tasks people encounter. It is difficult to maintain databases. Practitioners of database protection do not comprehend the assaults as well as associated to database protection issues. companies are unaware of the sensitive data contained within databases, tables, and columns, as per IT experts and Database Administrator (Admin), since either they are managing inherited presentations or taking no records or maintain the data model documentations. If you know the database properties, the databases are more difficult to be secured due to their specific implementation and procedures. We can describe the database protection as the tool for implementing a wide scale controlling data security, protecting databases internally and externally, as well as compromising database privacy, truthfulness, and accessibility, such as technological, managerial, and bodily controls, are used to ensure security [6].

The following is a breakdown of how this study is structured. In Section 2 a further overview of related works is presented. Section 3 describes type of attack in any system. In section 4, threat and prevention that may be used against any database system has been explained. In section 5 describe some methods for protecting information in the database, as well as several brand of new technologies that have a positive impact on database security, have been introduced. Finally, the study's conclusion has been described in section 6.

2. LITERATURE REVIEW

In this section, significant amount of work presented. It enabled us to check and use the following sources accordingly.

2.1. Thilina [7]

This review has focused on the utilization of virtual resources in storing data for database users. It also includes information on the strategies used to address database security problems, as well as database attack and privacy risk mitigation measures. Organizations may store data and information in databases using an innovative business model that requires no initial investment. It also includes information on database security needs and assets. This review paper covers database security breaching risks, malware activities on such data, and how to address or mitigate those issues, as well as Oracle security database implementation.

2.2. Sharma [8]

This article discusses the security of relational database protection and security frameworks as an example of how internet application security for explicit database authorization may be designed and implemented. Because Relational Database securities are the most popular target for attackers, protection associations and substance are regarded as significant company resources that must be meticulously protected. This research was conducted to identify the problems and risks associated with relational database security, as well as the requirements for relational database set security and how Database Relations are used at different levels to provide security.

2.3. Albalawi [9]

They propose an intelligent system for hiding sensitive data when statistical searches are combined. To begin with, the framework is helpful for defining sensitive information in order for the Admin to make decisions and establish regulations. Second, in the event of rule discrimination based on attribute-orientation, the framework investigates the connection between sensitive and other characteristics, allowing for the selection of attributes that may be used to drive private data.

2.4. Juma and Makupi [10]

In their view, databases are the heart of Information Systems (IS), therefore it is critical to maintain database quality to ensure IS quality. Recently, determining what constitutes a good database model or architecture has proven to be difficult. As a result, they measured certain characteristics and aspects in a database implementation in their discussion. A measure of evaluation is created using the many elements and qualities inherent in a database.

2.5. Odirichukwu and Asagba [11]

They believe that the number of businesses putting their data online is growing every day, enabling people to engage with and manipulate data all around the world. More information on the internet.

As the number of websites on the internet grows, so does the number of database security risks.

Ensuring security in developed applications, owing to a combination of factors a lack of security incentives, a tight timeline, and a web deficit Training on application security testing a review of the literature is presented in this article on twenty database security risks that affect web applications. Control actions that might be taken to prevent this attacks were investigated to raise awareness about online security the general population, as well as application developers. The work expresses an opinion that developers should make every effort to incorporate all of the required features while developing apps, take security precautions. Involvement is also important. All developers should get security testing training. The task at hand despite ensuring sufficient security, the author finds that Admin should develop a method of maintaining a continuous backup of their database apps available online.

2.6. Paul and Aithal [3]

This article discusses the fundamentals of databases, such as their meaning, features, and roles, with an emphasis on various database security issues. Furthermore, this article emphasizes the fundamentals of security management, as well as relevant technologies. As a result, various aspects of database security have been briefly discussed in this article.

2.7. Mousa *et al*. [12]

According to the authors of this study, assaulters would rather attack the database because of the data sensitivity and value.

Databases compromised in many different ways. The database should be secured against different forms of attacks and threats. Most of the assaults identified in this study can be solved. Some of the assaults are real and some are not. In this article, they discuss various types of assaults.

2.8. Singh and Rai [13]

They concluded that databases are the foundation of modern applications. For businesses, they are the primary storage option. As a result, database attacks are on the rise, but crucially threatening. They give the intruder (InT) access to sensitive information. This study discusses a variety of database assaults. This study also includes a review of relevant database security strategies as well as potential study in the field of database protection. This study will result in a more concrete approach to the database security issue.

2.9. Tabrizchi and Rafsanjani [14]

The goal of this project is to examine the many components of cloud computing as well as the current security and privacy issues that these systems confront. Furthermore, this work introduces a new classification system for recent security solutions in this field. This study also addressed outstanding problems and suggested future approaches, as well as introducing different kinds of security risks that are affecting cloud computing services. This article will concentrate on and investigate the security issues that cloud organizations, such as cloud service providers, data owners, and cloud users, confront.

3. TYPE OF ATTACK

In a database, there are several protection layers. An InT will compromise protection at all of these levels, which include the database Admin, server Admin, security officer, developers, and employees [5].

Three types of attackers can be found [15]:

A. Intruder (InT)
InT is an unwanted user who attempts to obtain useful information from a computer device by manipulating it excessively.

B. Insider (InS)
InS is one of the members of trustworthy users who violates his or her permission and attempts to obtain knowledge outside his or her own allocation.

C. Administrator (Admin)
Admin is a user with authority to operate a computer system who, in violation of the organization's security policies, abuses his or her management rights by spying on database management systems (DBMS) activities and obtaining sensitive data.

When an attacker breaks into the system, the two of the following attacked can be conducted [1]:

3.1.1. Direct Attacks

It refers to targeting the goal data first. These attacks are only possible and effective if the database has no security mechanism in place. If this attack is unsuccessful, the InT will move on to the next.

3.1.2. Indirect Attacks

It does not explicitly attack the goal, nonetheless data from or around the goal can be obtained by other in-between items, as the name suggests. Many of the variations of various questions are used and try to get through the authentication mechanism. It is difficult to keep track of these threats.

In general, database attacks are composed of two types [5] which are:

3.2.1. Passive Attack

In this case, the InT just inspects the data in the database and makes no changes. The following are few examples of passive attacks:

1. Static leakage: This attack obtains data about database plaintext content by analyzing a database snap taken at a given period.
2. Outflow of information: In this case, data about plaintext values can be accessed by connecting database values to the index location of mentioned values.
3. Dynamic leakage: Modifications made to a database over time may be detected and evaluated, as well as facts about plain text values.

3.2.2. Active Attack: Real database values are changed during an aggressive attack. These are more dangerous than passive attacks because they can lead to consumer confusion. For instance, a user can incorrectly capture information as a result of a query [5]. There are many methods for carrying out such an attack, which are mentioned below:

1. Spoofing – In this attack, a produced value is substituted for the cipher text value.
2. Splicing – This involves replacing a cipher text value with a new cipher text value.
3. Replay – This is an attack in which the cipher text value is replaced with an older version that has been changed or removed previously.

Because of the data they carry and their size, databases are the most popular target for cybercriminals [1]. A variety of database security risks and issues are addressed in this article.

4. THREAT AND PREVENTION

In this part, we'll go through nine of the most dangerous threats that may be utilized against databases, as well as how to avoid them form happening.

4.1. First Threat- Excessive Privilege Abuse

As soon as database access privileges given to users that go beyond what is required by their procedure, those privileges can be exploited for malicious purposes. A university Admin with the ability to alter student contact details can also use unnecessary database updating privileges to change grades, which is built-in.

Since Admin cannot identify and replace granularly, databases get admission to privilege management processes for each user, and a user eventually ends up with unnecessary privileges. Consequently, user(s) are given ordinary nonpayment access to privileges that go beyond the requirements of certain tasks [16].

Prevented by: Query-Level Access Control – Excessive Privilege Abuse Prevention

Accessing the question-level for regulation can be the solution of disproportionate rights. A process known as question-degree gets admission to control limits database rights to the bare minimum of SQL operations (select, update, and so on) and facts. The granularity of accessible data manipulations should develop outside the table to include the table rows and columns. A granular query-stage mechanism of accessible control could permit the previously mentioned college Admin updating the contact records while raising certain alarm if trying to change grades. Accessible control of query-stage can be valuable for detecting malicious workers who misuse their privileges but also for detecting unnecessary privilege abuse, in general, as well as for preventing the maximum assaults identified.

Implementation of the database software applications include a certain level of question-diploma management (triggers, row-stage protection, so on so forth), but the directed design of those "built-in" features make them unreasonable for anything but the built-in integrated deployments, the process of manual determination of the question-level access control policy for all database customers. The rows, columns, and operations take much time, to make matters worse, as user functions change over time, we should update query policies to represent the changes! Maximum database Admin will struggle to define a useful question policy for a few customers at a single time, let alone a smaller group of users over time. Consequently, most organizations provide unlimited rights of access to users with special collection of the paintings for a wider range of users. Automated gears are necessary for real-time question-degree access management to become a reality [16].

4.2. Second Threat - Authentic Privilege Abuse

Users to perform unauthorized tasks can use valid database privileges. Consider a hypothetical villain healthcare worker who has access to patient details through an application as the custom web. Internet application architecture usually limits users from accessing the medical history of a single patient. It is not possible to display several facts at the same time; meanwhile, electronic copies are not permitted. The villain worker, on the other hand, can get around those obstacles using a different client, such as MS-Excel connecting the database. The worker can also retrieve and buy all patient records using MS-Excel and the correct login credentials.

Personal copies of medical record files are unlikely to adhere to any healthcare record security policies of organization's patient. We have to be aware of two risks.

1) The villain employee swap personal information for make cash.
2) A careless employee retrieves and saves significant quantities of data to their client computer for authentic work purposes. Once information stored on an endpoint device, it would expose for Trojan virus, PC theft, and other assaults.

Prevented by: Legitimate Privilege Abuse Prevention

Database access management is the solution for legitimate privilege misuse that applies to queries but also to the context nearby database access. One can probably identify users abusing legitimate database access rights by enforcing a policy of patron packages, place, and time.

4.3. Third Threat - Privilege Elevation

Attackers of database platform software to adjust a regular user access privileges to those of an Admin can also use vulnerabilities. Stored procedures integration, built-in capabilities, implementations of protocols, and square statements may all be vulnerable. For instance, a financial institution software developer may consider taking advantage of a prone feature acquiring database administrative privilege.

The villain developer can disable audit mechanisms; build fictitious versions, transfer funds, and more administrative privileges [13].

Prevented By: Privilege Elevation Preventive – Institution Prevention Systems (IPS) and Query Level Access Control (QLAC)

Combination usage of traditional IPS and QLAC to manipulate, privilege elevate exploitation can be avoided (see excessive privileges above). IPS examines database site users for patterns that may lead to identified weaknesses. Once a characteristic identified as a prone, for instance, IPS most probably blocks the entire access to the prone method or, if likely, blocks the most successful processes with embedded attacks.

4.4. Fourth Threat - Platform Vulnerabilities

Unauthorized entry, data corruption, or service denial can result from flaws in underlying working frameworks (Windows 2000, UNIX, and so on so forth) and extra services installed on a database server. For instance, the blaster computer virus exploited a weakness in Windows 2000 causing a situation of Denial of Service (DoS) [13]. With the advancement of technology, security has improved as well, and as a result, many vulnerabilities have been solved in later versions of Windows or other platforms.

Prevented By: Avoiding Assaults, Updating the Software, and Preventing InTs

Protecting database property requires a mixture of protection programs and the IPS network security. Over-time, provisions of updates by the seller mitigated vulnerabilities discovered in the database platform. Unfortunately, businesses provide and enforce software upgrades regularly. Databases are not covered during the replacement periods. Furthermore, compatibility problems can often prevent software upgrades from happening. IPS must be introduced to address these problems. As mentioned before, IPS examines database visitors and detects assaults aiming recognized defenselessness.

4.5. Fifth Threat - SQL Injection

In certain cases, SQL injection assault, the perpetrator introduction (or "injection") unauthorized database reports into an inclined SQL channel. Saved approaches and web utility enter parameters are typical instances of oriented record channels. Then these injected reports sent to the database, where they are completed. Using SQL injections permits attackers may acquire unlimited access to all the database [13].

Prevented By: SQL Injection Prevention

IPS query-level gets proper access to governing (see disproportionate Privilege Abuse), and event correlation is three strategies that can be mixed to effectively fight rectangular SQL injection such as:

1. Input validation and Parametrized queries
2. Avoiding administrative privileges
3. Using Web application firewall

IPS can detect SQL injection strings or save strategies that are vulnerable to attacks. However, we believe that IPS is unreliable because square inoculation threads are disposed to incorrect positivity. Those managers of protection who exclusively consider IPS application are inundated by viable warnings of SQL injection. Nevertheless, considering the correlation of the SQL inoculation mark along any other breach, including enquiry-stage get-in-to-manipulate violation, it is possible to manipulate the violation, and a real assault can be pinpointed with extreme precision. During normal business operations, SQL inoculation mark as well as any infringement does not probably occur similarly in the submission.

4.6. Sixth Threat - Weak Audit Trail

The inspiration behind the implementation of any database must involve the automated documentation of all sensitive and/or irregular database transactions. In several ways, a shaky database audit policy poses a serious threat to the company.

- Regulatory danger
- Deterrence
- Detection and Recovery
- Lack of User Accountability
- Performance Degradation
- Separation of Duties
- Limited Granularity
- Proprietary.

Prevented by: Preventing Weak Audit

The majority of the vulnerabilities associated with local audit equipment are resolved by high-quality network-based audit home equipment.

- High performance
- Separation of Duties
- Cross-Platform Auditing.

4.7. Seven Threat - DoS

Another common form of cyber-attack is the DoS in which demonstrative consumers are denied access to network applications or data. Common techniques may be used to establish DoS conditions, in which many of them can be linked to the mentioned vulnerabilities.

DoS can be motivated by different factors. Ransom scams are often associated with DoS attacks linked to computer, in which a remote attacker constantly crashes computers before depositing money into a global bank account by the victim. A bug infection instead maybe blamed for DoS. Regardless of availability, the seriousness of the threat for most companies maybe posed by DoS [17].

Prevented By: DoS Preventive

DoS preventive necessitates several layers of protection. Protections at the network, software, and database levels are all critical. This study focuses on database-specific security. Recommendation focuses on link charge manipulations, query access control, IPS, and reaction timing controls the database-specific contexts.

4.8. Eighth Threat - Weak Authentication

By stealing or otherwise obtaining login credentials, attackers can predict the identity of legitimate database customers using vulnerable authentication schemes. To acquire credentials, an attacker can use various number of methods available [18].

- Cryptanalytic attack
- Social Engineering
- Direct Credential Theft.

Prevented By: Preventing Authentication Attacks

1- Strong authentication

It is crucial to use the most advanced realistic authentication technologies and rules. Where possible, two-factor (tokens, certificates, biometrics, etc.) authentication is preferred. Unfortunately, cost and ease of use, frequently furnish authentication impracticality. These situations necessitate the implementation of strict username and password policies (least possible duration, gender selection, as well as obscurity).

2- Directory integration

However, incorporation of strong authentication mechanisms with business enterprises catalogs the substructure for scalability and simplicity of use. The directory structure, among others, allows the user to consider using a particular login detail for numerous database and program. However, it increases the usefulness of double-factor authentication system. Moreover, it is easier for consumers remembering alternative passphrases on a regular basis.

4.9. Ninth Threat - Backup Data Exposure

Database backup in certain cases, storage media is completely unregulated. As a result, stealing backup disks and hard drives have been the focus of many high-profile security breaches.

Prevented by: Preventing Backup Data Exposure

Both backups of databases require encryption application. Indeed, certain carriers stated that the potential products of DBMS not necessarily support the unencrypted backup's usage. However, online produce of database statistics encryption advised frequently. Nevertheless, key management issues of presentation and cryptographic are frequently impractical, and granular privilege controls described above are in general considered as a weak substitute.

5. METHOD FOR PROTECTING DATABASE SYSTEM

In this section, two types of method have been explained, the first one is to eliminate security risks, any company must have a security policy in place that must be followed.

Authentication is crucial in security policy since proper authentication reduces the probability of attacks. On different database objects, different users have different access rights. The management of access rights is the responsibility of access control systems.

To safeguarding database statistic substances, besides the majority DBMS supports it is the greatest elementary practices [5]. The control methods concerning database protection depicted (See Fig. 1).

5.1. Access Controller

Is the most basic service, which any DBMS can offer? It has safeguarded data from unauthorized reads and writes. All contact to the database and objects of other systems must adhere to the policies defined by access control. Errors may be serious enough to cause issues in a company's operations. Admission rights controlling can aid mitigating dangers, which have a direct effect on the database protecting the main server. The access control is able to prevent the deletion or changing of a table made by accident. The access control can rollback, and prevent the deletion of particular files. access control systems consist of:

- File permissions to create, read, edit, or delete files on the server.
- Program permissions, the rights of executing an application program on the server.
- Data rights, the rights of retrieving, or updating data in a database.

5.2. Inference Strategy

Data protection at a particular level is critical. It is used once the processing of specific data in the form of facts should stop at a maximum level of protection. It helps the determination of how to keep knowledge from being posted. The inference control aims to prevent information from being revealed indirectly. Unauthorized data disclosure can ocur in one of three ways:

- Correlated data - a popular channel when visible data X and invisible data Y are semantically linked.
- Missing data - NULL values in the query masks a sensitive data. That way, existed data could be detected.
- Statistical inference - this is common in database, which contain a numerical data in regards to individuals.

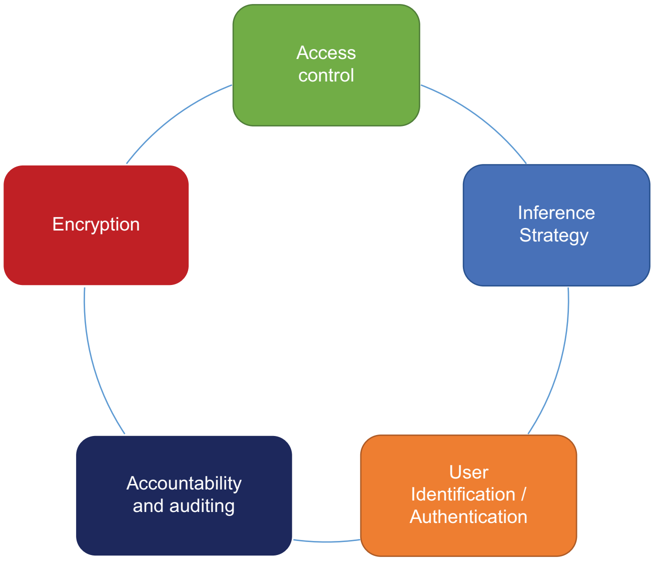
Access control
Inference Strategy
User Identification / Authentication
Accountability and auditing
Encryption

Fig. 1. Control methods for protecting database system.

5.3. Identification or Authentication of the User

It is better to know your users as a basic security requirement. After you've classified people, you'll need to determine what privileges and access permissions they have, as well as verifying their data that must use.

Until a user is allowed to construct a database, they should be authenticated in several ways. User identification and authentication are a part of database authentication, the OS or network service can perform an external authentication process. To establish user authentication Secure Sockets Layer (SSL), business parts, and middle-tier server authentication, also known as proxy authentication, can all be used. it is the most basic prerequisite for ensuring protection when considering the identification process which identifies a collection of people who are permitted to access the data. To ensure confidentiality, the authentication of identity initiates preventing unauthorized users from modifying sensitive data. Attackers make use of various methods such as bypass authentication, default password, privilege escalation, brute-force password guessing, and rainbow attack when attempting to breach a user identity and authentication [16].

5.4. Audit and Accountability

Database/non-database users audit and monitor a configured database behavior. Accountability refers to the method of keeping track of user activities on a device. To ensure the physical integrity of the data, auditing checks and accountability are required which necessitates a specific database access carried out with auditing and maintaining the resiliency of the data. If users' authentication accesses a resource successfully, the system will track all successful and unsuccessful attempts, and attempted accesses and their statuses will show in the audit trail files [16].

5.5. Encryption

It is a method of translating information into cipher or code that only those who have access to the cipher text key can make it ready. Encrypted data is the referral to cipher or encoded text. In a database, there are two states for data security. Data is in two statuses: at rest and in motion – data stored in a database, on a backup disk, or a hard drive. Once transiting through the network, it necessitates the use of various encryption solutions. Any of the problems of data at rest can be solved by encrypting it. Utilize solutions such as SSL/Transport Layer Security for Data in Transit [16].

In the second method any organization may make advantage of a using new technology tool that has a significant effect on database security such as:

1. Database Firewalls: Are a kind of Web Application Firewall that monitor databases to detect and defend against database-specific attacks, which are usually aimed at gaining access to sensitive data contained in the databases. Database Firewalls also allow you to monitor and audit every database access via the logs they keep. Specific compliance reports for laws like as PCI, SOX, and others may be generated by a Database Firewall [19].
   Herse some tool:
   - Cloudflare
   - Site Lock
   - Tufin Secure Track.
   - ManageEngine Firewall Analyzer.
   - FireMon.
   - AlgoSec.
2. Real Time Data Monitoring (RTDM): An Admin may examine, analyze, and change the addition, deletion, modification, and usage of data on software, a database, or a system using RTDM. Through graphical charts and bars on a single interface/dashboard, data managers may examine the general operations and functions done on the data in real time, or as they happen [20].
   Herse some tool:
   - Real-time Database profiler tool
   - Firebase console
   - Cloud Monitoring
3. Multi-factor database Authentication: Is a technique and technology for confirming a user's identification that requires two or more credential category kinds for the user to log into a system or complete a transaction. This technique requires the effective Answering of at least two separate credentials such as: Entering password, email verification, phone verification, or answering security question [21].
   Herse some tool:
   - LastPass
   - Duo Security
   - Ping Identity
   - RSA SecurID Access

6. CONCLUSION

The database security problems and research into various issues affecting the industry have frequently been listed in this survey. Organizations are now dependent on documents to make decisions about different business processes that will improve their bottom line. As a result, it is a smart idea to keep confidential details secure from prying eyes. Server security research papers have attempted to investigate the issues of potential assaults to database systems such as loss of confidentiality and honesty. Because of the knowledge and volume contained in databases, they are the most common and simple targets for attackers. There are many options to accommodate a database. Today, there are several forms of attacks and threats against which a database should be secured. This paper discusses the decisions that must be made in order to protect personal data from attackers. It also goes into depth about how a loss of privacy can lead to extortion and humiliation in the workplace. This survey also looked at strategies for dealing with any form of hazards. Views and authentication should be used in this case. Another method is to use an encryption strategy, which means the information is secured so that if an InT finds it, he or she is unable to use it, and the criteria for a reliable DBMS were also discussed.

REFERENCES

[1] M. Malik and T. Patel. "Database security attacks and control methods". *International Journal of Information Technology*, vol. 6, no. 1/2, pp. 175-183, 2016.

[2] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker. "Security threats to critical infrastructure: The human factor". *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4986-5002, 2018.

[3] P. K. Paul and P. S. Aithal. "Database security: An overview and analysis of current trend". *International Journal in Management and Social Science*, vol. 4, no. 2, pp. 53-58, 2019.

[4] S. B. Sadkhan. "Related Papers". *Over Rim*, pp. 191-199, 2017.

[5] H. Kothari, A. Suwalka and S. Kumar. "Various database attacks, approaches and countermeasures to database security". *International Journal of Advance Research in Computer Science and Management Studies*, vol. 5, no. 5, pp. 357-362, 2019.

[6] J. C. Ogbonna, F. O. Nwokoma and A. Ejem. "Database security issues: A review". *International Journal of Engineering Inventions*, vol. 6, no. 8, pp. 1812-1816, 2017.

[7] T. Dharmakeerthi. "A Study on Security Concerns and Resolutions". *Researchgate. Net*, No. May, 2020.

[8] E. Technology and V. Sharma. "An analytical disparity of harbor tools erection for database system". *International Research Journal of Modernization in Engineering Technology and Science*, vol. 3, no. 2, pp. 501-510, 2021.

[9] U. Albalawi. "Countermeasure of Statistical Inference in Database Security". *Proceeding 2018 IEEE International Conference Big Data, Big Data 2018*, pp. 2044-2047, 2019.

[10] J. Juma and D. Makupi. "*Understanding Database Security Metrics: A Review*". Vol. 1. Mara International Journal of Social Sciences Research Publications, pp. 40-47, 2017.

[11] J. C. Odirichukwu and P. O. Asagba. "Security Concept in Web Database Development and Administration a Review Perspective. *2017 IEEE 3rd International Conference Electro-Technology National Development NIGERCON 2017*, vol. 2018-Janua, pp. 383-391, 2018.

[12] A. Mousa, M. Karabatak and T. Mustafa. "Database Security Threats and Challenges". *8th International Symposium Digital Forensics Secur. ISDFS 2020*, vol. 3, no. 5, pp. 810-813, 2020.

[13] S. Singh and R. K. Rai. "A Review Report on Security Threats on Database". *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 3215-3219, 2014.

[14] H. Tabrizchi and M. K. Rafsanjani. "*A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions*". Vol. 76. Springer, United States, 2020.

[15] P. Sharma. "Database Security: Attacks and Techniques". *International Journal of Scientific and Engineering Research*, vol. 7, no. 12, pp. 313-319, 2016.

[16] S. S. Sarmah. "Database Security Threats and Prevention". *International Journal of Computer Trends and Technology*, vol. 67, no. 5, pp. 46-53, 2019.

[17] T. Mahjabin, Y. Xiao, G. Sun and W. Jiang. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques". *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, 2017.

[18] H. B. Hashim. "Challenges and security vulnerabilities to impact on database systems". *Al-Mustansiriyah Journal of Science*, vol. 29, no. 2, p. 117, 2018.

[19] W. Lee. "*Lecture Notes in Electrical Engineering 461 Proceedings of the 7th International Conference on Emerging Databases*", 2019.

[20] I. Kotsiuba, M. Nesterov, Y. Yanovich, I. Skarga-Bandurova, T. Biloborodova and V. Zhygulin. "Multi-Database Monitoring Tool for the E-Health Services. *Proceeding 2018 IEEE International Conference Big Data, Big Data 2018*, pp. 2442-2448, 2019.

[21] C. Hamilton and A. Olmstead. "Database Multi-factor Authentication Via Pluggable Authentication Modules". *2017 12th International Conference Internet Internet Technology and Secured Transactions ICITST 2017*, pp. 367-368, 2018.