ISSN 2347 - 3983
Volume 11. No.2, February 2023
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter041122023.pdf
https://doi.org/10.30534/ijeter/2023/041122023

Mitigation of Database Security Threats in Transaction Processing System

[1]Wumi Ajayi, [2]Efe L. Omoghene, [3]Obumneme K. Ukandu, [4]Olayinka Adelola
[1]Department of Software Engineering, Babcock University, Ogun State, Nigeria, ajayiw@babcock.edu.ng
[2]Department of Computer Science Babcock University, Ogun State, Nigeria, omoghene0092@pg.babcock.edu.ng
[3]Department of Computer Science Babcock University, Ogun State, Nigeria, ukandu0183@pg.babcock.edu.ng
[4]Department of Computer Science Babcock University, Ogun State, Nigeria, adelola0346@pg.babcock.edu.ng

Received Date: January 04, 2023 Accepted Date: January 24, 2023 Published Date : February 07, 2023

ABSTRACT
The main function of the transaction processing system (TPS) in the business world is to handle data transactions. Hence, it is crucial to secure the database, we discuss the problem of database threats in a transaction processing system in this article. A transaction process system (TPS) refers to an information processing system for business transactions that collects, modifies, and retrieves all transaction data. Database security denotes the safeguarding of database management systems using a variety of strategies against malicious cyberattacks, unlicensed access, and illegitimate use. The elements that need to be protected by database security systems include the data that has to be stored, the database where it is stored, and the database management system used to administer the data. It involves safeguarding the system from harm, infiltration, and exploitation. Additionally, it safeguards any database-related applications. The aim of this study is to explore possible database security threats in a TPS, along with some security challenges, and mitigation techniques to these threats.

Key words: Mitigation, Transaction Processing, Database Security, Web Application, Malware, Database Management, Access Control

1. INTRODUCTION

Prior to the advent of the internet, every business, from the banking sector (which is on a large scale) to the transportation sector, such as the airline, train, and bus industries, and even down to hotels, fitness centers, parks, and recreation centers, had a process in place for handling transactions. This method was analog and would have been viewed as taxing by business owners as well as by clients or those looking for services. The requirement for physical presence to conduct a transaction, the limited-service clientele, and the lengthy customer waiting times which may practically be the length of a train were just a few of the obstacles this process faced.

Data security and management are also significant constraints in this analog system. In order to keep the organization from becoming overburdened or losing its momentum, it is crucial that the information received in transactions be processed in a database system) [1]. Nevertheless, the advent of the internet led to the development of Transaction Process Systems (TPS), which aids users in processing data transactions within a database system and tracking transaction programs. The process of buying products and services by an organization is kept stable and under control by TPS. Using this technology, TPS is in charge of monitoring transactions from payment accounts, whether or not they are physically present, processing payroll, and permitting a financial delay between the time a product is purchased and the time it is sold [2].
Despite the fact that TPS is mostly composed of people, software, and hardware, there are four primary parts: input, processing system, storage device, and output.

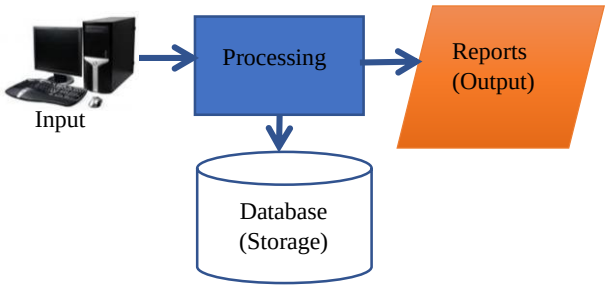

Figure 1: Pictorial view of TPS components. Source: [3].

Because memory has a tendency to be volatile in some situations and because the data being processed is delicate, a transaction process needs to be secured in order to be effective. Therefore, the database management system needs to be properly protected. Because of the sensitive information they store, databases are regarded as the lifeblood of any

organization. It would be worth noting that TPS's databases are vulnerable to failure, which could be caused by a variety of security threats.

1.1 Problem Statement

Although it is generally understood that databases could be subject to security risks, there is still a great deal of ignorance or negligence regarding the ways for protecting databases of Transaction Processing Systems from security breaches that may occur from the outside or from within. So much sensitive information is transferred and stored during transactions in a transaction processing system, making it a target for security risks or attacks of any kind. The best course of action is to make protecting this database a top priority by putting in place safeguards that effectively counteract threats and streamline transaction processing to prevent more serious harm.

1.2 Aim

Based on the aforementioned problem statement, the aim of this work are as follows;

- ♠ Identify the characteristics of a transaction processing system
- ♠ Carryout an intelligent report on the various database security threats
- ♠ Consider the concerns of database security challenges
- ♠ Share measures that would assist in reducing database security threats in transaction processing system

1.3 Methodology

The purpose of this work is to address the issue raised previously by investigating database security risks in transaction processing systems and outlining countermeasures that could help institutions or businesses lower risks in their transaction processing system databases. The researchers conducted multiple analyses of a variety of literature to establish facts before drawing conclusions and making recommendations. Additionally, closely linked works were taken into consideration in order to develop a more sophisticated strategy for suggesting certain control measures for transaction processing system databases. The discussion covered transaction processing system characteristics, various database security concerns, and control approaches depending on the problems.

2. LITERATURE REVIEW

A transaction processing system (TPS) is a software program that processes the required online transactions for businesses such as train reservation systems, online money transfers, and airline ticket purchasing after receiving data from the customer as input [4]. Characteristics of a TPS include performance, reliability, controlled processing and consistency [5].

Performance: The need for prompt action and high productivity rate in a TPS cannot be overstated. It could be harmful for businesses if consumers or clients have to linger around for the TPS to take action. It should take no longer than a few seconds to complete the transaction from the moment the necessary data is inputted to the time the relevant result is produced.

Reliability: For enterprises, TPS dependability is crucial. A TPS fault could be detrimental to the organization because it might cause a halt to operations and, consequently, a loss of revenue because transactions cannot be completed. The backup and recovery processes in the cases of failure must also be quick and thorough.

Consistency: A TPS requires uniform processing of all transactions regardless of user or time. There would be far too many chances for irregular operations if it were inconsistent.

Controlled processing: Information storage and retrieval from a TPS must be done in an efficient and effective manner. The TPS must be accessible at all times for authorized employees. Authorized workers must have uncomplicated access to a TPS in order to retrieve data from it.

An effective and efficient method must be used for information storage and retrieval from a TPS. All authorized staff must have easy access to the TPS at all times in order to retrieve data from it. Ross Anderson, a security expert, coined the phrase "The Anderson Rule" [6]. The idea put forth is that there must be a balance between database security and usability. It states that “if a large system is designed for ease of access, it becomes insecure; if made watertight it becomes impossible to use”. The security mechanisms used for transaction processing systems have undergone more than a decade of development. There are numerous studies that outline the various ways in which these security measures impact the system's integrity. In order to secure a TPS, we will be outlining some of the countless lessons from literature in this section.

2.1 Existing Works

All transaction processing systems are ultimately comprised of the internal and external components. “Hardening”, or all-round security of databases involve ensuring that it is secure with respect to these two aspects.

[7] reviewed the security challenges attributed to transactional databases. In their paper, they noted that because different locations have different data usage standards, transactions such as mobile money transfer, which require third payment gateways coupled with user authentication creates distrust in users.

[8] highlighted that each aspect of a database has an assigned security constraint. They are internal and external constraints. Internal constraints deal with the security of the actual database, and external constraints deal with the database and actual operation it carries out with the outside world examples of which are transactions. These security constraints were categorized as local constraints. He suggested that for a more secured database, there should be more global constraints which will displace inconsistencies and conflicts created by local constraints.

2.2 Closely Related Works

[9] described various constituents involved in fortifying the database and also referencing information security within a company as very important and should be secured. The sole responsibility of an entire organization database, from the executives down to operations and information technology department, from system and safety to adherence, legal, and risk staff should be reviewed and new technological tools should be applied in exhuming the threats.
In their article from 2020, [10] discussed the alarming rise in database attacks. They stated that an object, a person, or a thing could endanger an asset by posing a likelihood of abuse or disorder of classified information.
In addition to identifying the security challenges in databases, [11] identified the importance of auditing. They noted that while not a security measure itself, auditing identifies the breach that occurred on a database, and exposes the vulnerabilities on it.
[12] classified database attacks into direct attacks and indirect attacks. While direct attacks are carried out directly on the database, indirect attacks are more subtle and instead infer the information on the database through database objects. They state that indirect attacks are more difficult to guard against. Furthermore, they classify database attacks into active and passive attacks and state that active attacks, which change the actual content of the database through spoofing, splicing ad replay are more dangerous and should be guarded against.
According to [13], a limited library of "transaction programs" that carry out particular tasks, such accessing and updating databases, are called upon by a user of a transaction-processing system to execute commands. Hence no arbitrary programs may be created by the user, assembled, or run. It was stated that the only programs that are permitted to operate in these systems are the certified transaction programs. Consequently, it is possible to enforce the access restrictions at the interface between machines and people.
These research articles have a slightly different focus because it is concerned with the database of transaction processing systems, threats and vulnerabilities to the database, and steps to mitigate them.

2.3 Gaps In Literature

[14], in his paper mentioned that in addition to other factors one reason for data breaches was that although the client server approach was used to replace the terminals, the majority of businesses did not yet permit external access. Due to the vulnerability of these workstations, the clients could not be completely trusted. The complexity of the environment, including cloud computing, clusters, grids, replication, IaaS/SOA, Web 2.0, etc., makes it much more difficult.
[15], in their paper, Security Issues in databases, observed that organizations adopt differing database security models in order to meet their organizational standards. They noted that these models have diverse functionalities as they were built to address different database security issues. Furthermore, the underlying assumptions for a secure database differ, and the models may conflict. Example of which are the differing access control methods used by relational database management systems and object-oriented database systems. By comparing discretionary and mandatory access control policies, they noted that both cases offer administrators and users access to the database, which may be beneficial or detrimental to the organization. He further noted that a these is still no standard for developing security models based on them.

3. DATABASE SECURITY THREATS

Security breaches may be caused by several software flaws, faulty setups, or recurring patterns of misuse or negligence.
Insider Threats: An insider or in-house threat is a breach in security that comes from within the organisation. It could be one of the factors listed below, each of which has authorized access to the database:

- - An official with nefarious motives
- A negligent staff of the company who predisposes the database to intrusion and attack by acting recklessly

- A third party who gains access to the database's credentials or acquires credentials using social engineering or another technique

Insider threats are one of the most prevalent causes of database security breaches, and they typically occur when several employees have been granted authorized access. [1].

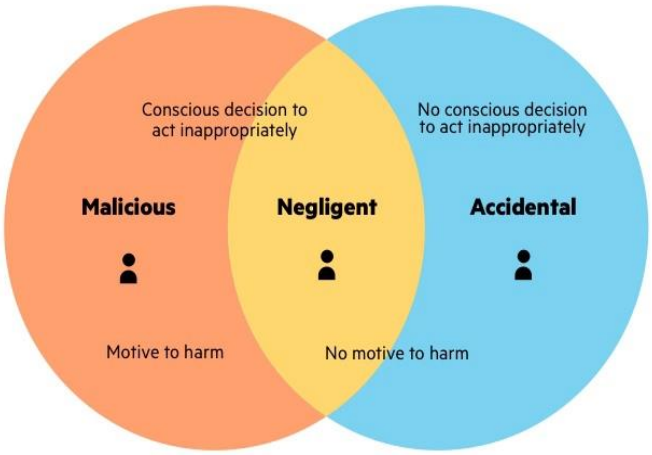

Figure 2: Three types of risky behaviour explained. Source: [1]

Unmanaged Sensitive Data: Organizations frequently store sensitive data in databases without performing a complete inventory of it. It could be challenging to maintain track of constantly changing, crucial data that is added to the database. Data management issues or negligence make it a hacker's prime target. Therefore, recently uploaded or inserted data may pose a threat to the database's security [16].
Excessive privileges can be considered a threat in situations when workers have been granted default database access that exceed the proposed requirements of their job task; this access may be abused eventually. Some businesses are not proactive enough to ensure that there is an update for employees who

change position or duties in the same organization or follow through removing access that was granted to employees who no longer associate with the organization.

Denial of Service (DoS/DDoS) Attacks: In a denial of service (DoS) attack, the cybercriminal floods the target service, in this case the database server, with a large number of fake requests. As a result of its inability to handle valid requests from actual users, the server regularly crashes or becomes unstable. Numerous machines that are controlled by the attacker's botnet and are a part of a distributed denial of service attack (DDoS) generate erroneous traffic. Without a highly scalable defensive architecture, it is difficult to stop them since the traffic volumes this generates are so huge. Cloud-based DDoS prevention services can ramp up vigorously to address very large DDoS attacks. [1].

Injection Attacks on SQL/NoSQL: According to [12] and [17], this kind of attack involves hostile or damaging code being inserted to the frontend (web) applications before being delivered to the backend database. The insertion of arbitrary non-SQL and SQL attack strings into database queries represents a threat peculiar to databases. They often take the form of HTTP requests or are created as web application form extensions. Any database system is vulnerable to these attacks if programmers do not adhere to secure coding principles and the firm does not routinely conduct vulnerability evaluations. SQL injections provide online criminals free access to all the information in a database. Such code attacks can be of two different types: SQL injections targeting conventional databases and NoSQL injections targeting enormous databases [17].

Overflow exploitation on databases with or without malware (malicious software): Sometimes a security breach's objective isn't to leak information, but rather to impede database performance, which compromises the performance of the application [18]. For example, it could be done on the e-commerce system at a peak time to prevent registration, money transfers, and check-ups. Hackers that run processes that are overloaded with data to cause buffer overflow, and this could be accomplished using malicious software or faulty devices. The block stops responding when it cannot handle the length of the request. Although the system can easily handle a few of these attacks, thousands of invalid requests cause it to crash. The outcome is a freeze in the software [18]. According to [19] report, the rate of internet users is on a trajectory projection as explained in the bar chart below.

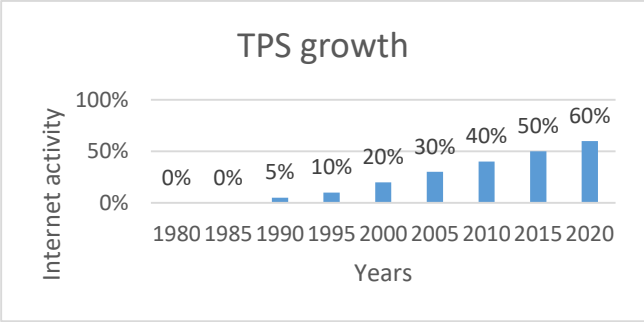

Figure 3: Bar Chart of Internet users over the years. Source: [19]

Backup attacks: Companies usually do not take sufficient precaution to safeguard their data backups. They usually use the same methods and security measures as the primary database. If the primary contents were already hacked, an attacker may easily compromise the backup. Another error is to either not safeguard the backup files at all or to lose track of where they are located. Businesses are more vulnerable to backup attacks if they have the following:

- Rapidly growing data masses: If an enterprise is scaling significantly, it is highly probable that the team is not focusing attention to the safety of backups.
- Branched infrastructures: Teams sometimes lose sight of where backups of databases are kept and how they are safeguarded when a system is vast and distributed.
- Lack of cybersecurity professionals: If a business doesn't have an internal department or professional security consultant, safety will gradually drop down the list of priorities [18].

3.1 Database Security Challenges

Databases are more vulnerable to threats as a result of the developing IT environment. It falls to individual institutions and businesses to clearly point their unique database threats and challenges and provide procedures, apportion resources and institute guiding standards that must be strictly adhered to in an attempt to check the increase in the rates of database threats. Database security challenges include:

Intellectual Property Rights: [20] reveals that due to the extensive use of intranets and the internet, organizations are more focused on the legal and informational elements of data. To overcome these issues, relational data watermarking approaches have recently been developed. Digital watermarking primarily protects content against illegitimate replication and distribution by enabling ownership of the content to be established. Traditionally, it has relied on the presence of a big noise domain where the item can be altered while retaining its essential properties. Research is required to determine the efficacy of such approaches and consider different strategies for preventing the violation of intellectual property rights. [20].

Distributed Platforms: As businesses use hybrid or multi-cloud infrastructures for their workloads, network environments are growing more complicated, which makes it harder to implement, maintain, and choose security solutions.

Strict regulatory criteria: It is increasingly challenging to comply with all standards as the international regulatory compliance structure becomes more intricate [1].

Database Resilience: [20] further stated that even with limited capabilities, database systems must work and continue to do so in the face of disruptive events like information warfare strikes. Certain conditions are requisite for a DMBS to ensure that it is capable of preventing threats and attacks; and also identifying them if they occur. They include:

Confinement - That is the immediate removal of the attackers' access to the system and the isolation or confinement of the damage to prevent it from escalating.

Damage assessment - Determine the extent of the problem, taking into consideration any damaged data or malfunctioning systems.
Reconfiguration - Reconfigure to allow operation to continue while recovery is being done in a less-than-optimal way.
Repair - Restoring a system's functionality to normal, repairing corrupted or lost data, and repairing or replacing defective system components..
Fault treatment: As much as possible, pinpoint the flaw that the attacker exploited and take action to stop it from recurring again [20].

3.3 Database Security Control Measures

A number of measures are taken as part of data security to prevent data from being stolen, destroyed, or maliciously altered. When numerous users in a Registered Technology Transfer Professional (RTTP) system have access to the data, there is a higher danger. The first line of defence is to restrict access to only authorized users using passwords, personal items, and biometric devices. Some persons can get around these. Firewalls and encryption are further defences [21].
Access control - A DBMS's security system must have features that limit access to the database as a whole. Create user accounts and passwords to manage the DBMS's log-in procedure. This task is known as access control [20].
Encrypt backups and files: [22] highlights that encryption uses one or more mathematical methods known as cryptography to secure digital data. He went on to clarify that encryption is a crucial safeguard for both individuals and businesses to prevent hackers from accessing critical data. For instance, websites that transmit credit card and bank account numbers encrypt sensitive data to guard against fraud and identity theft. According to [1], no matter how strong a firm's security is, there is constantly a chance of a hacker gaining access into the system. Attackers, however, are not the database's only security concern. A risk could also come from employees. An organization is continually in danger of having a careless or malevolent insider access and view a file they are not supposed to.
Data encryption adds an additional layer of protection against unauthorized intrusion. This is due to the fact that encrypted data is unreadable by both staff and attackers. Important program files, data files, and backups should be encrypted because encrypted data cannot be read without the encryption key, protecting sensitive data from illegal access. [1].
Block Public Network Access: Companies maintain databases of applications. In the majority of real-world scenarios, the end user typically does not require direct access to the database. Therefore, all public network access to database servers should be forbidden, unless the company is a hosting provider. Ideally, a business should install gateway servers for remote administrators (VPN or SSH tunnels) [1].
Lock down accounts and privileges: The configuration of privileged accounts on a database server should include a strong, exclusive password. Additionally, accounts that are no longer needed should be locked. The remaining accounts must have access limited to the bare minimum. Each account should only have access to the tables and functions (like SELECT or INSERT) that the user actually needs. Full access to all the database tables should not be granted to user accounts.
Web Application and Database Firewall: [23] conveys that these database firewalls keep track of every connection that is made to the database engine, and many of them are capable of taking proactive measures when they notice SQL Injection, buffer overflow, or denial of service threats. He added that these database firewall applications can do a lot to thwart attacks because they keep an eye on every command sent to the database server, regardless of whether it is a DDL (Data Definition Language) statement that drops tables stuffed with data or a DML (Data Modification Language) statement that selects, deletes, or updates data. The database server is shielded from risks to database security by a firewall. In most cases, a firewall would automatically deny access to any traffic. Additionally, it prevents the database from generating outgoing connections unless it is absolutely necessary to do so.
A web application firewall (WAF) must be installed in addition to a firewall to protect the database. This is due to the possibility of using web application attacks, such as SQL injection, to obtain unauthorized access to the databases.
The bulk of web application threats will not be blocked by a database firewall since traditional firewalls function at the network layer whereas web application layers operate at the application layer (layer 7 of the OSI model). At layer 7, a WAF can identify malicious web application traffic, such as SQL injection attacks, and stop it before it can harm the database. [1].
Regularly Patch Database servers: Making sure that patches are updated is crucial. Effective database patch management is a critical security tactic because attackers are continually hunting for new database security flaws and because new viruses and worms are continuously being produced and developed. By promptly deploying the most recent database service packs, important security hotfixes, and cumulative upgrades, database performance will become more stable.

4. CONCLUSION AND RECOMMENDATION

Database security is one of the central components of Transaction Processing Systems. It is crucial that we find the appropriate solutions to address the various database security issues in a transaction processing system. A database needs to be protected against any form of threat or attack. For safeguarding the databases, different control techniques like those listed above have been discovered and implemented. Despite the fact that some solutions offer long-term security, others are merely momentary. In this study, the various threats and challenges that a database is vulnerable to, as well as some control techniques, have been identified. Consequently, we may draw the conclusion that despite the astonishing advancement made in this area, the danger to databases has significantly increased since the development of internet technology. Since database security breaches are getting more frequent, it is apparent that having strong protection algorithms and a qualified safety staff is becoming much more important to businesses and users now.

REFERENCES

[1] Imperva. (2022, Oct. 15). *Relational Database Security* [Online]. Available: https://www.imperva.com/learn/data-security/database-security/

[2] G. Praiz. (2022). *Transaction Processing System: How it Works With Examples (Detailed Guide)* [Online]. Available: https://businessyield.com/business-services/transaction-processing-system/

[3] M. B. Amin, M. Alauddin, and D. M. M. Azad. (2022, May) " Business Transaction Processing System." *International Journal of Computer Information Systems* [Online]. Vol. 4, No. 5, 2012. Available: https://www.researchgate.net/publication/321070736_Business_Transaction_Processing_System

[4] Chegg. (2022, Nov. 15) *Learn About Transaction Processing System (TPS)* [Online]. Available: https://www.chegg.com/learn/computer-science/computer-technology/transaction-processing-system-tps-in-computer-technology#features-of-a-good-transaction-processing-system

[5] Uni Assignment Center. (2018. Nov) *Some Features Of Transaction Processing System Information Technology Essay* [Online]. Available: https://www.uniassignment.com/essay-samples/information-technology/some-features-of-transaction-processing-system-information-technology-essay.php

[6] Wikipedia Contributors. (2021. Nov, 30) *Anderson's rule* [Online]. Available: https://en.wikipedia.org/wiki/Anderson%27s_rule#:~:text=Anderson

[7] A. Sharma, V. Kansal, and R. P. S. Tomar. (2015, March). "Location Based Services in M-Commerce: Customer Trust and Transaction Security Issues," *Computer Science Journals* [Online]. Volume 9 issue 2. Available: https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-989

[8] R. Haraty. (2009, Jan) "Security Issues in Distributed Transaction Processing Systems Damage Assessment and Recovery from Malicious Attacks for Defensive Information Warfare View Project High-Performance and Accurate Mathematical Solvers in Hardware View project," *Encyclopedia of Information Science and Technology, Idea Group Publishing* [Online]. Available: https://www.researchgate.net/publication/243444402_Security_Issues_in_Distributed_Transaction_Processing_Systems

[9] S. Imran and I. Hyder. (2009, Dec) "Security Issues in Databases," *Second International Conference on Future Information Technology and Management Engineering* [Online]. Available: https://www.researchgate.net/publication/224099612_Security_Issues_in_Databases .

[10] N. A. Al-Sayid and D. Aldlaeen. (2013, March) "Database security threats: A survey study," *5th International Conference on Computer Science and Information Technology* [Online]. Available: https://www.researchgate.net/publication/261452732_Database_security_threats_A_survey_study

[11] I. Somtoochukwu and U. Chibueze. (2019, May) "Core Threats And Prevention In Database Security Core Threats And Prevention In Database Security," *World Journal of Engineering Research and Technology* [Online]. Vol. 5, Issue 3, 535-551. Available: https://www.researchgate.net/publication/335894304_Database_Security_-Threats_Prevention

[12] S. Gahlot, B. Verma, and A. Dayanand. (2020, March) "Database Security: Attacks, Threats and Control Methods," International Journal of Engineering Research and Technology [Online]. Vol. 5, Issue 10. Available: https://www.ijert.org/research/database-security-attacks-threats-and-control-methods-IJERTCONV5IS10011.pdf

[13] D. E. Denning and P. J. Denning. (1979, Sept) "Data Security," *ACM Computing Surveys (CSUR)* [Online]. vol. 11, Issue no. 3, pp. 227–249. Available: https://dl.acm.org/doi/10.1145/356778.356782

[14] S. Chakraborty. (2022, May) "Database Security Threats and How to Mitigate Them," *Research Gate* [Online]. Available: https://www.researchgate.net/publication/361909351_Database_Security_Threats_and_How_to_Mitigate_Them

[15] A. Mousa, M. Karabatak, and T. Mustafa. (2020, June) "Database Security Threats and Challenges," *8th International Symposium on Digital Forensics and Security (ISDFS)* [Online]. Available: https://www.semanticscholar.org/paper/Database-Security-Threats-and-Challenges-Mousa-Karabatak/e0c459c3417d303fb7d42f44d95cd8cefe9bd5dd

[16] M. Murray. (2010, Jan) "Innovations in Practice Editor: Anthony Scime Database Security: What Students Need to Know Executive Summary," *Journal of Information Technology Education* [Online]. vol 9. Available: https://www.jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf

[17] A. Mousa, M. Karabatak, and T. Mustafa. (2020, June) "Database Security Threats and Challenges," *8th International Symposium on Digital Forensics and Security (ISDFS)* [Online] Available: https://www.researchgate.net/publication/342189418_Database_Security_Threats_and_Challenges

[18] V. Ilyukha. (2022). *What Is Database Security: Standards, Threats, Protection* [Online]. Available: https://jelvix.com/blog/database-security

[19] World Bank. (2022, Dec). *Individuals Using the Internet (% of population) | Data* [Online]. Available: https://data.worldbank.org/indicator/IT.NET.USER.ZS

[20] Collegelib. (2022, Oct. 14). *Database security issues, challenges, and Control Measures* [Online]. Available: https://www.collegelib.com/database-security-issues-and-challenges/

[21] Wikibooks. (2020. Sept. 05). *HSC Information Processing and Technology/Transaction Processing Systems - Wikibooks, open books for an open world*

[Online]. Available: https://en.wikibooks.org/wiki/HSC_Information_Processing_and_Technology/Transaction_Processing_Systems#Data_Security

[22] J. Chen. (2022). *What Is Encryption? How It Works, Types, and Benefits* [Online]. Available: https://www.investopedia.com/terms/e/encryption.asp

[23] D. Cherry. (2015). *Securing SQL Server: Database Firewall - an overview* [Online]. Available: www.sciencedirect.com, 2013. https://www.sciencedirect.com/topics/computer-science/database-firewall