Journal of Computer Science

Review

Security Threats to Databases in E-Commerce Systems: A Systematic Literature Review

Nurayn Mesfer Alqahtani

Department of Information Systems, King Saud University, Saudi Arabia

Article history
Received: 17-07-2024
Revised: 04-09-2024
Accepted: 11-10-2024

Email: norain.almosa@gmail.com

Abstract: Data is a primary by-product of each business. A typical business organization uses a database system to store and manage data. On the other hand, databases are the primary target of hackers and attackers. The existing literature shows that modern database systems are vulnerable to various data breaches, cyberattacks, or malware attacks. Modern business organizations and e-commerce owners look to protect their sensitive data by using secure database solutions that ensure restriction to unauthorized access, modification, or deletion of data. In the last decade, business organizations have also been relying on cloud-based storage solutions and these are also facing various security threats. Considering the sensitivity of database security, there is a need to investigate the existing security challenges to databases, existing well-known threats, and their possible solutions. A systematic literature review was conducted to explore the impact of well-known security threats such as SQL injection, Denial of Service (DoS) attacks, supply chain attacks, ransomware, unauthorized access, etc. on modern business and e-commerce systems and this study presents the import insights of the study, observations and findings of this review-based study. The findings are synthesized to define a set of guidelines for security analysts, database administrators, and researchers to understand and mitigate continually evolving security threats to databases.

Keywords: Database Security, Malware Attack, Supply Chain Attacks, Ransomware, SQL Injection, DoS Attack

Introduction

Modern companies are generating large volumes of data on a daily basis and this exponentially growing data is stored in a database for future usage. Relational databases have been a primary choice for storing and managing data for the last many decades. Additionally, historical data can be quite useful in providing significant intuition and assisting in decision-making in various aspects of an organization (Bertino, 2016). These days data is not only considered critically important for any business organization but also data is a source of innovation, future forecasting, and strategic planning of an organization. Modern businesses understand the power of data and they plan to harness the power of data with the help of data analysis and data mining techniques (Fleiner *et al*., 2022). However, in all this process, the database carries the role of central spot since it is a database system that ensures structured storage of data and timely accessibility and management of data. Following are the latest trends in threats and attacks to databases:

1. SQL Injection Attacks: SQL injection is a well-known vulnerability and a significant attack on databases (Yacono, 2022). Modern automated tools can make it quite simple to find and exploit weaknesses in modern e-commerce and web applications that are connected to various databases
2. Ransomware Attacks: A recent trend in ransomware attacks is a threat by the attackers to a user for not only encrypting the user's data but also leaking the user's sensitive information (Anciaux *et al*., 2019)
3. Supply Chain Attacks: These days breaches like the SolarWinds attack can lead to large-scale access to databases of multiple organizations
4. Insider Threats: The risk of insider threats has increased after the culture of remote work increased resulting in more accidental data exposures or deliberate disruption of data (Wilson, 1988)
5. Brute Force Attacks: Modern automated tools and bots have increased the frequency and scale of brute force attacks to target cloud databases and services with reused or weak passwords (Mousa *et al*., 2020)

6. Zero-Day Exploits: Recently, the investment in bug bounty programs has been increased and vulnerabilities have made zero-day a dangerous threat to database systems
7. Data Exfiltration Attacks: In the recent rise of "Exfiltration-as-a-service" models, attackers sell tools or access to naive attackers to extract data from databases

This study presents a review-based study that was primarily conducted to investigate the current security challenges and well-known threats to databases and their possible solutions. The study also aims to investigate the impact of well-known security threats such as SQL injection, Denial of Service (DoS) attacks, unauthorized access, etc. on modern business (Kothari *et al*., 2019). The observations and findings of this review-based study are finally synthesized to suggest and guide security analysts, database administrators, and researchers so that they can understand the severity of the threats and plan to mitigate the constantly evolving security threats to databases.

To understand the modern-day challenges to database security, experts recommend deploying the CIA triad. The net section explains the significance of the CIA triad.

Observing CIA Triad

The CIA triad or triangle defines the three most important pillars of database security that should be of prime importance. CIA stands for Confidentiality, Integrity, and Availability (CIA) as shown in Fig. (1). CIA is a multi-faceted but fundamental concept of database systems' security. Organizations have to establish a balance between the security of database systems and the integrity and availability of database systems. Organizations can use the CIA triad to assess the current security threats and risks in their database systems and also plan to address them (Wilson, 1988). Organizations can benefit from the CIA triad since it serves as an elementary structure to design and evaluate various security aspects, facets, and policies for databases (Mousa *et al*., 2020).

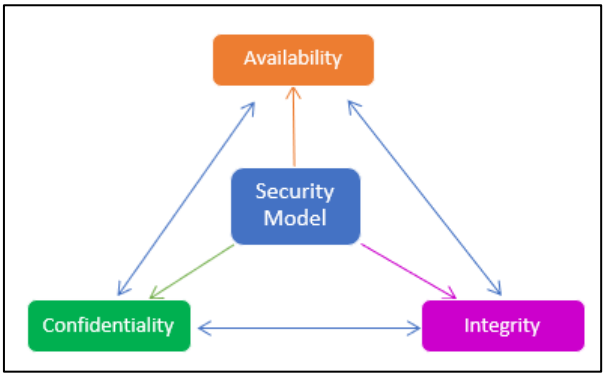

Fig. 1: CIA triad and its basic components

Following is the description of each pillar of the CIA triad.

Confidentiality

Confidentiality is a process that takes care of data privacy and secrecy. In terms of confidentiality, one must ensure illegal access to data to avoid any misuse of data. In implementing confidentiality in an organization modern techniques and practices like encryption can be helpful in improving the security of data. The databases storing data in encrypted format are more secure (such as MySQL) than the databases securing data in plain format. On the other hand, encryption can also be helpful in securely transmitting data.

Integrity

Integrity is a process that ensures fair and reliable use of data. Such reliability and fairness in data usage can be achieved by inhibiting fraudulent and unlawful access to data. In a modern database system, integrity can be implemented by ensuring only authorized and legitimate access to database systems.

Availability

Availability is a process that ensures the prevention of a database system from malicious attacks, threats, and software faults. Such attacks and faults can cause unavailability of data and inaccessibility of a database for a certain period. Whereas the mechanism of availability helps to successfully recover data and database after intended hardware and software faults. In the literature, it is reported that machine learning can be helpful in handling DoS attacks and ensuring the continuous availability of data (Kothari *et al*., 2019).

Modern database systems are exposed to various types of security threats and attacks as discussed above. Such threats include illegal access to data that can result in illegal and unauthorized modification or deletion of data. Other security-related challenges that a business is facing these days are privacy, integrity, security, and availability (Kothari *et al*., 2019). Typically, the security threats to a database are certain activities or steps that can put the security and privacy of data at risk. Hacking and cyberattacks can be the main source of security threats. Hacking and misuse of data can have serious impacts on a company such as damage to reputation, business loss, or some legal or financial charges. To avoid such financial, legal, or repute losses, an organization has to continually assess and update its database system and ensure the security aspect of its database system (Sarmah, 2019). Organizations also have to bear a huge cost to protect their data and database systems from threats (Paul and Aithal, 2019).

Literature Review Methodology

The literature review presented in this article is based on the methodology described by Brereton *et al*. (2007) The systematic review process is divided into three phases such as planning, conducting, and concluding. The devised protocol of SLR is shown in Fig. (2).

In the second phase of this protocol, the selection criteria of the studies are defined. The third phase of this protocol concludes the observations of the study and the findings of the whole review process.

Research Questions

After a detailed discussion with experts and researchers, a set of research questions was devised as given in Table (1). The main objective of these research questions is to identify potential threats and risks to database security reported in the literature. This review conducted in this study will also synthesize the possible solutions reported in the existing studies. The second major objective of this study was to find out the major publications forums and trends of the studies addressing the challenges in database security.

Conducting Search

In the second phase of the methodology, a search strategy was devised to find all the relevant studies in the area of database security. The strategy for searching the relevant studies is based on the three steps below:

1. Data sources selection
2. Detection of search terms
3. Short-listing of studies using inclusion/exclusion criteria

Fig. 2: Devised protocol for the Systematic Literature Review (SLR) study

Table 1: Intended RQs and their potential bases

No.	Research Questions (RQ)	Bases
RQ1	What are potential threats and risks to database security and what are its solutions?	The main objective of this question is to investigate the potential threats and risks to database security and find solutions
RQ2	What are the publication forums and trends of the intended studies in Database security?	The main objective of this research question is to identify forums and trends of publication of intended studies

Table 2: Identified research databases

Data Origins	Website URL
IEEEXplore Digital Library	http://ieeexplore.ieee.org/Xplore/
The ACM Digital Library	http://dl.acm.org/
SpringerLink	http://www.springerlink.com/
ScienceDirect	http://www.sciencedirect.com/

Identifying Research Databases

In this SLR, first of all, a set of five major data sources were identified to search for the relevant studies. All these research databases were thoroughly searched to find the relevant case studies. The databases used for searching studies are shown in Table (2).

These databases were selected since the databases cover all the journals, conferences, workshops, and symposiums that publish challenges in database security. Among the studies searched from these databases, only the complete, published, and peer-reviewed publications were selected. A set of research keywords were defined to thoroughly review the studies. Search terms like threats, risks, attacks, malware, database, security, privacy, etc., were used in the search. The logical operators AND and OR were also used to search different combinations of the keywords. After using the search terms a total of 483 studies were collected. Here, the duplicate studies were truncated to reduce the total to 254 studies.

Criteria for Study Selection

This section defines the criteria used for study selection in this SLR. The used criteria are divided into two phases. The initial selection of the studies and detailed selection of the studies. The initial criterion of selection is given below:

1. Select studies due to relevant titles
2. Select studies due to their relevance in the abstract

By using the initial criterion, a total of 91 studies were selected. To further rationalize the selection process and fine-tune the screening of studies inclusion/exclusion criteria were also defined. The studies were included based on the following points:

- Select the studies that address challenges/issues in database security
- Select the studies that are peer-reviewed
- Select the studies published from 2005-2024
- Select the studies written in the English language

Studies are rejected that met the following exclusion criteria:

DOI: 10.3844/jcssp.2025.25.33

- Exclude the studies that do not match the research questions
- Exclude the studies that have less than 5 pages

These inclusion and exclusion criteria were thoroughly applied to all 91 studies and finally, we left with 23 studies.

Results and Discussion

The key observations and findings of this review-based study are given in this section. The research questions given in Table (1) are discussed in this section. RQ1 investigates the key challenge in the area and RQ2 explores the publication forums and venues of the selected studies in this review.

RQ1. What are Potential Threats and Risks to Database Security and What are its Solutions?

The selected studies were examined in detail and all the key issues and challenges related to the security and privacy of databases were identified. The identified challenges are discussed in the following section, in detail.

Key Challenges

This section highlights the key factors and challenges intertwined with database security, including data, defense systems, and external influences. Table (3) highlights the major security threats and their relevant studies available in the literature.

Table (3) shows that the internal threats, SQL injection, Weak audit trial, and privilege of abuse are the most significantly addressed security attacks in the literature. However, Denial of Service, malware attacks, and platform vulnerability are the relatively less focused security threats or attacks in the literature. Security threats like ransomware attacks, supply chain attacks, insider threats, brute force attacks, zero-day exploits, and data exfiltration attacks are occasionally discussed in the literature or not discussed in the literature. The classification shown in Table (3) explains the focus of security experts especially in the domain of databases and e-commerce systems.

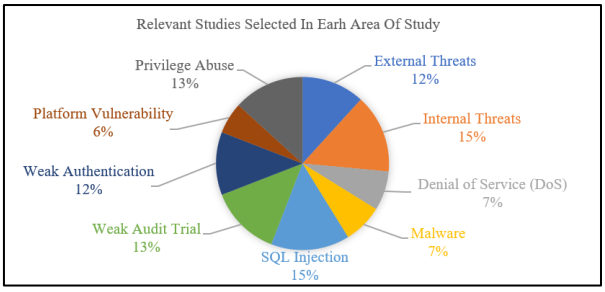

Fig. 3: The proportion of major security threats and attacks in selected studies

Figure (3) shows the proportion of the relevant studies on each type of potential security threat for database systems. SQL Injection and Internal Threats to databases lead with a 15% share each. On the other side, privilege abuse and weak audit trials keep a share of 13% each in the research studies. However, Weak authentication and external threats trail with 12% share each in the addressed studies. Denial of Service and Malware attacks on databases have a share of 7% each and platform vulnerability has a share of 6% in the literature. Four primary sources of threats as mentioned in Fig. (4) are: Weak protection of data, user misconduct, vulnerabilities, and external threats.

Table 3: Major security threats and identified studies

Threat	Relevant studies
External threats	Chakraborty (2022); Rijah (2021); Gerić and Hutinski (2007)
Internal threats	Sallam and Bertin (2019); Chakraborty (2022); Rijah (2021); Bertino and Sandhu (2005); Zeb (2018)
Denial of Service (DoS)	Chakraborty (2022); Lawal *et al*. (2022); Pevnev and Kapchynskyi (2018)
Malware	Chakraborty (2022); Gerić and Hutinski (2007); Pevnev and Kapchynskyi (2018)
SQL injection	Chakraborty (2022); Rijah (2021); Lawal *et al*. (2022); Pevnev and Kapchynskyi (2018)
Weak audit trail	Chakraborty (2022); Khanuja and Adane (2011); Lawal *et al*. (2022); Stahlberg *et al*. (2007); Pevnev and Kapchynskyi (2018)
Weak authentication	Rijah (2021); Khanuja and Adane (2011); Lawal *et al*. (2022); Bertino and Sandhu (2005); Pevnev and Kapchynskyi (2018); Zeb (2018)
Platform vulnerability	Ghorbanzadeh *et al*. (2010); Lawal *et al*. (2022)
Privilege abuse	Lawal *et al*. (2022); Bertino and Sandhu (2005); Zeb (2018)

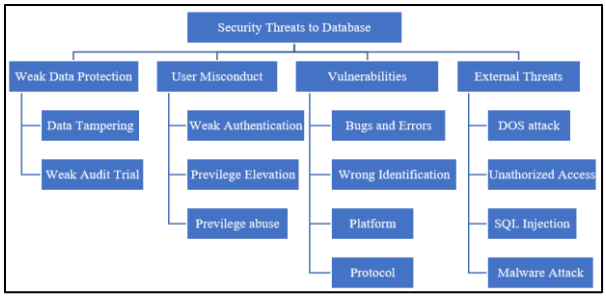

Fig. 4: Classification of database security threats and attacks

Weak data protection is further classified into data tampering and weak audit trials. User misconduct is further classified into weak authentication, privilege elevation, and privilege abuse. Vulnerabilities can also be of many sub-types such as bugs and errors, wrong identification, platform vulnerabilities, and protocol vulnerabilities. External threats may be categorized into DOS attacks, unauthorized access, SQL injection, malware, and other cyber-attacks (Wang *et al*., 2021). From the list of attacks discussed in Fig. (4), the most important threats and attacks are discussed below.

Illegal Act

An illegal act by a user refers to any activity that is performed by an authorized user that can cause any risk to the value of that organization. When an authorized user misuses data, services, or any facility of the system that he is not entitled to is known as an internal threat. Such internal threats can be the main source of a data breach or serious loss to an organization (Yaseen *et al*., 2019).

Excessive Privilege Abuse

An organization should not give excessive privileges to an employee. It is reported that around 80% of security attacks are caused by present or former employees. Secondly, assigning extra privileges or failing to revoke them promptly makes it overly easy for these individuals to engage in wrongful activities, some of which may even occur unintentionally or without the awareness that they are illegal (Malik and Patel, 2016). This abuse of lawful privileges can be viewed as a weakness because it creates a security vulnerability within the database.

Weak Audit Trail

Organizations need to implement strong audit policies and ensure the availability of adequate technology to cope with the various threats to databases. It is reported in the literature that various security threats occur due to non-compliance with an organization’s policies. An organization can face serious threats to its sensitive data if the organization has not properly recorded the audit information (Malik and Patel, 2016). On the other hand, an organization cannot meet certain regulatory requirements of the industry and government due to weak audit trials. To strengthen the security of a database system, an organization should improve its capabilities to audit.

SQL Injection

In this type of threat, known as SQL injection, a malicious attacker exploits vulnerabilities in a system to execute unauthorized SQL (Structured Query Language) statements. These SQL statements are "injected" into existing code or a data channel. Such injected code can be based on a set of input parameters and stored procedures. SQL injection can be very dangerous for database systems since it can help in gaining unauthorized access to a database. Such unauthorized access to a database can result in serious data breaches or data leaks (Deepika, 2015).

Denial K of Service (DoS/DDoS)

A Denial of Service (DoS) attack is used to make a database server stuck and ineffective. DoS attack is launched by sending fake network traffic in bulk to a database server to choke it. Cybercriminals generate such fake network traffic using multiple hacked computers or machines. The objective is to overwhelm the database server with this influx of fake requests, rendering it unable to process legitimate requests from actual users. As a result, the database server may either cash or become highly unstable, leading to disruptions in its normal operations (Singh *et al*., 2021).

Privilege Elevation

The individuals with malicious intentions do target database platform software and can exploit weaknesses to get unauthorized access or to raise their privileges from a standard role to an admin role. The existing loopholes in database implementation and software include the integration of stored procedures, inherent capabilities, implementation of protocols, etc. For instance, an employee may contemplate exploiting a susceptible feature to get administrative privileges within a database system.

Once this malicious developer attains administrative privileges, they can carry out a range of harmful actions. These actions may encompass disabling audit mechanisms, creating fictitious data versions, initiating fund transfers, and acquiring additional administrative privileges (Teimoor, 2021).

Database Platform Vulnerabilities

A database may face a lot of threats, attacks, and risks due to weaknesses in the implementation of a system. One reason for such weaknesses can be the underlying platform. A platform is a combination of hardware and an operating system such as Windows or Linux. An attacker can use the inherent vulnerabilities of a platform and can get authorized access to the system or escalate his privileges. A common vulnerability exists in the Intel Wi-Fi driver and Intel pro set/wireless wi-fi software extension. The attackers can use this platform's vulnerability and can elevate the privileges of existing users (Yaseen *et al*., 2021). Attackers can further exploit this loophole to stop services and access sensitive information from a database a system.

Database Protocol Vulnerabilities

Besides certain platform vulnerabilities posed to a system, there can also be a few protocol vulnerabilities that can cause a serious threat to the database systems. Attackers use loopholes and weaknesses in

communication protocols to get unauthorized access to the database servers (Bajwa *et al*., 2016). Attackers exploit these vulnerabilities and can launch DoS attacks, data hacking, and other attacks.

Weak Authentication

Another major reason for data breaches and data leaks is the weak authentication process of a database. It is possible that the login credentials of the authorized users may be stolen and then misused to access a database (Teimoor, 2021). Usually, attackers use various methods and approaches to steal user's credentials. A few of these methods are below:

- Cryptanalytic attack
- Social engineering
- Direct credential theft

Malware

Malware is malicious software that is typically developed to exploit inherent weaknesses in a system, unlawfully excess its data, and damage it. Malware can be a direct threat to the privacy, security, or integrity of a database system (Singh *et al*., 2022). A typical malware is very much capable of infecting a database server and illegally accessing its data. It can also cause major security threats such as data breaches, data distortion, illegal access, and other serious security threats.

Solutions

The literature also suggests and recommends guidelines to counter various security threats and tacks to databases. A few of the solutions suggested in the literature are documented below:

- Use database firewalls such as packet filter firewalls, proxy server firewalls, and Stateful Packet Inspection (SPI) [S04]
- Strong audit trails and records can help to minimize threats and attacks to databases (Malik and Patel, 2016)
- SQL injection can be prevented by taking a few security measures like proper validation of input, using parameterized queries, and implementing proper access control (Deepika, 2015)
- Standardized hardware should be used to avoid platform vulnerabilities
- The communication protocol attacks can be countered using the "protocol validation" technique. This technique can assess, dissect, and compare database traffic. It can detect unusual patterns in data traffic and can warn about attacks in time (Bajwa *et al*., 2016)
- Strong authentication mechanisms should be implemented in database systems to avoid any possible hacking threats. Users need to be properly educated on the best practices of security. Furthermore, admins need to regularly monitor and audit access to protect against security threats (Teimoor, 2021)
- A database system can be protected against malware attacks by using proper anti-virus or anti-malware programs. To ensure the integrity and security of a database system, robust malware protection measures need to be implemented on a database server (Singh *et al*., 2022)

RQ2. What are the Publication forums and Trends of the Intended Studies in Database Security?

All 21 selected studies were analyzed to investigate their publication forums, venues, and year. Figure (5) shows that the selected studies were 48% published in journals and 52% were published in conferences.

Besides the publication forums, Further, the selected studies were investigated to find out the publication venues. It is shown in Fig. (6) that 33% of studies were published by IEEE and 10% of studies were published by ACM. However, 57% of studies were published by other publishers.

Besides the publications forums and venues, the selected studies are also analyzed to find out the year of the publication to understand the publication trends in the area of database security. Figure (7) shows that from the year 2005-2024, there were 21 studies published. The highest number of studies were published in 2019.

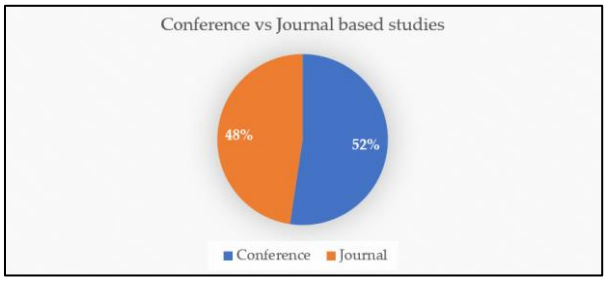

Fig. 5: The proportion of selected studies in each area of study

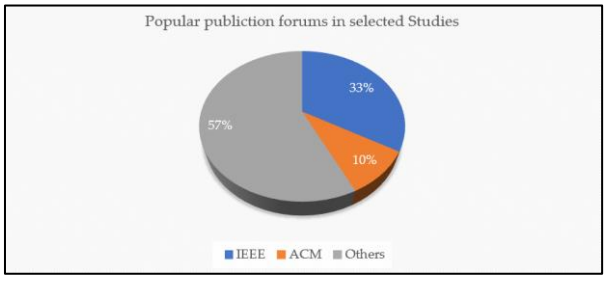

Fig. 6: The proportion of selected studies in each area of study

DOI: 10.3844/jcssp.2025.25.33

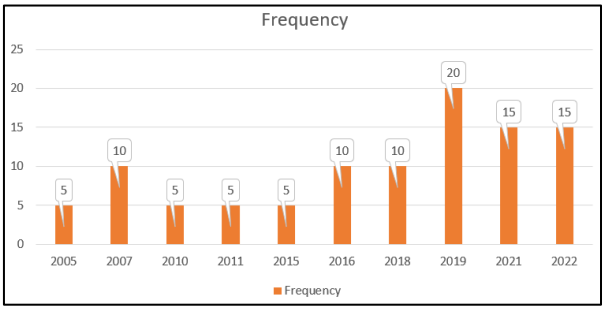

Fig. 7: The proportion of selected studies in each area of study

Figure (7) shows that from the year 2005-2022, There is a continuous rise in the publications in the area of database security.

Discussion

Modern database systems tend to be fragile against possible security risks and threats. Smaller organizations are frequently exposed to such risks and threats. However, mid and large-size organizations are more fragile and vulnerable to security attacks and threats since the larger organizations have to deal with a larger chunk of sensitive data (Brereton *et al*., 2007). A weak implementation of a database system that does not exhibit the international standards and guidelines of security tends to be more vulnerable to malicious attacks. Modern organizations can take necessary measures to minimize the vulnerabilities in database systems, use the latest and updated anti-virus systems, implement modern firewalls, and train their employees to remain safe from possible security threats and attacks.

Suggestions for Database Security

In the last two decades, the possible threats and attacks to databases have increased more largely. Due to the rise in potential risks and threats to databases, organizations also have to be very careful and take necessary measures to ensure the security and privacy of their database. In the field of Information Technology (IT), A dedicated field of security management provides a way of implementing a structured approach to protect database systems. An organization can adopt a particular methodology that consists of the following steps.

Identifying the Risk Analysis

For adopting a seamless security management system in an organization, the primary step is risk analysis. It is a critical phase in adopting a methodology of database security to perform risk analysis to identify potential risks and threats to security. Every company should evaluate and measure these risks based on their likelihood and potential impact. This assessment helps companies roughly estimate the risks and the associated costs. The concept of risk can be expressed as the product of harm and the probability of its occurrence.

Establishing Security Policies and Procedures

Establishing a security policy is the next step after conducting a risk analysis. This security policy serves several purposes, including defining the framework for information system resource utilization, specifying security techniques to be applied across organization departments in line with ISO 2000X standards, and educating users on IT security.

Developing Security Techniques

Implementing security techniques is essential to fulfill security requirements, such as ensuring information availability, integrity, confidentiality, and sometimes sustainability in information systems. These techniques encompass vulnerability audits, penetration tests (Pen-Tests), data security measures like encryption and access control, network security through tools like firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), security information monitoring, user education and the development of a business recovery plan (Bala *et al*., 2024). After discussing the significance of database security and the main aspects of data protection, the next section will discuss the recent threats targeting database security.

Quality Threats

The studies selected in this review-based study are carefully selected. However, there is a possibility that the findings of this review-based study may be biased due to the following factors:

- There is a possibility that the selected studies may have shown bias in results and the same bias may be reflected in the results of this study
- A thorough survey was conducted using a set of search terms and it was ensured that all relevant studies were included in this study
- The election results and analysis results of this study were vetted by another expert, as well to ensure fairness and transparency in the results of this study

Conclusion

This study provides an overview of the major security threats and attacks to database systems. Database security threats can have significant and damaging consequences if they are successfully executed. However, this study has provided the current situation of security threats to databases and provided new insights into the implications of these threats to databases. It is also found that such database security threats can severely compromise the confidentiality, integrity, and availability of data within a

database system, leading to a wide range of negative outcomes. This study also states that the most common database security threats are insider threats, excessive privilege abuse, weak audit trail, SQL injection, Denial of Service (DoS/DDoS) attacks, privilege elevation, database platform vulnerabilities, database protocol vulnerabilities, weak authentication, and malware attacks. Modern business organizations and companies can take various steps to practically implement the proposed solutions such as identifying risk analysis, establishing security policies and procedures, developing appropriate security techniques, and deploying modern security tools.

Acknowledgment

I would like to express my deepest gratitude to King Saud University for providing me with the knowledge, resources, and opportunities to grow academically and professionally. I am also sincerely thankful to King Abdulaziz City for Science and Technology (KACST) for its invaluable support and contributions to advancing research and innovation. Their guidance and encouragement have been instrumental in the completion of this study.

Funding Information

The authors have no support or funding to report.

Ethics

This review paper is based on an analysis of publicly available literature, and no primary data collection involving human or animal subjects was conducted. Therefore, no ethical issues are anticipated.

Reference

Anciaux, N., Bouganim, L., Pucheral, P., Popa, lulian S., & Scerri, G. (2019). Personal Database Security and Trusted Execution Environments. *Proceedings of the VLDB Endowment*, *12*(12), 1994–1997. https://doi.org/10.14778/3352063.3352118

Bajwa, I. S., Razzaq, F., Bukhari, A. H., & Amin, R. (2016). Using Machine Learning to Generate SPARQL Queries from NL for NoSQL Database. *Sindh University Research Journal (Science Series*, *48*(2), 233–240.

Bertino, E., & Sandhu, R. (2005). Database Security - Concepts, Approaches and Challenges. *IEEE Transactions on Dependable and Secure Computing*, *2*(1), 2–19. https://doi.org/10.1109/tdsc.2005.9

Bertino, E. (2016). Data Security and Privacy: Concepts, Approaches and Research Directions. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 400–407. https://doi.org/10.1109/compsac.2016.89

Bala, I., Pindoo, I., Mijwil, M. M., Abotaleb, M., & Yundong, W. (2024). Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends and the Practical Applications of Artificial Intelligence. *Jordan Medical Journal*, *58*(3), 250–270. https://doi.org/10.35516/jmj.v58i2.2527

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from Applying the Systematic Literature Review Process within the Software Engineering Domain. *Journal of Systems and Software*, *80*(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

Chakraborty, S. (2022). Database Security Threats and How to Mitigate Them. *MOL2NET'22, Conference on Molecular, Biomed, Comput and Network Science and Engineering*. MOL2NET'22, Conference on Molecular, Biomed, Comput and Network Science and Engineering, Bayonne, France-Miami, USA, https://doi.org/10.3390/mol2net-08-12642

Deepika, N. S. (2015). Database Security: Threats and Security Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(5), 621–624.

Fleiner, R., Hubert, R., Banati, A., & Erdodi, L. (2022). Security Threats Based on Critical Database System Privileges. *2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC)*, 000117–000122. https://doi.org/10.1109/iccc202255925.2022.9922750

Gerić, S., & Hutinski, Ž. (2007). Information System Security Threats Classifications. *Journal of Information and Organizational Sciences*, *31*(1), 51–61.

Ghorbanzadeh, P., Shaddeli, A., Malekzadeh, R., & Jahanbakhsh, Z. (2010). A Survey of Mobile Database Security Threats and Solutions for it. *The 3rd International Conference on Information Sciences and Interaction Sciences*, 676–682. https://doi.org/10.1109/icicis.2010.5534685

Khanuja, H. K., & Adane, D. S. (2011). Database Security Threats and Challenges in Database Forensic: A Survey. *Proceedings of 2011 International Conference on Advancements in Information Technology (AIT 2011)*, 170–175.

Kothari, H., Suwalka, A. K., & Kumar, S. (2019). S. (2019). Various Database Attacks, Approaches and Countermeasures to Database Security. *International Journal of Advance Research in Computer Science and Management*, *5*(4), 357–362.

Lawal, B. O., I. B., M. C. B., Adesoji, A., & Salami, A. (2022). Contemporary Control Measures for Mitigating Threats and Vulnerabilities to Organizational Databases. *Conference: ISTEAMS Research Nexus*, 321–330.

Malik, M., & Patel, T. (2016). Database Security-Attacks and Control Methods. *International Journal of Information Sciences and Techniques*, *6*(1/2), 175–183. https://doi.org/10.5121/ijist.2016.6218

Mousa, A., Karabatak, M., & Mustafa, T. (2020). Database Security Threats and Challenges. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/isdfs49300.2020.9116436

Pevnev, V., & Kapchynskyi, S. (2018). Database Security: Threats and Preventive Measures. *Advanced Information Systems*, *2*(1), 69–72. https://doi.org/10.20998/2522-9052.2018.1.13

Paul, P. K., & Aithal, P. S. (2019). Database Security: An Overview and Analysis of Current Trend. *International Journal of Management, Technology and Social Sciences (IJMTS)*, *4*(2), 53–58. https://doi.org/10.47992/ijmts.2581.6012.0070

Rijah, M. (2021). Security Analysis, Threats and Challenges in Database. *International Journal Faculty of Arts and Culture, South Eastern University of Sri Lanka*, *14*(4), 40–47.

Sallam, A., & Bertino, E. (2019). Result-Based Detection of Insider Threats to Relational Databases. *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, 133–143. https://doi.org/10.1145/3292006.3300039

Sarmah, S. S. (2019). Database Security–Threats and Prevention. *International Journal of Computer Trends and Technology*, *67*(5), 46–53. https://doi.org/10.14445/22312803/ijctt-v67i5p108

Singh, D., Bhogawar, S., Nuthakki, S., & Ranganathan, N. (2021). Enhancing Patient-Centered Care in Oncology through Telehealth: Advanced Data Analytics and Personalized Strategies in Breast Cancer Treatment. *International Journal of Science and Research (IJSR)*, *10*(9), 1707–1715. https://doi.org/10.21275/sr24108012724

Stahlberg, P., Miklau, G., & Levine, B. N. (2007). Threats to Privacy in the Forensic Analysis of Database Systems. *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, 91–102. https://doi.org/10.1145/1247480.1247492

Singh, D., Nuthakki, S., Naik, A., Mullankandy, S., Singh, P. K., & Nuthakki, Y. (2022). Revolutionizing Remote Health: The Integral Role of Digital Health and Data Science in Modern Healthcare Delivery. *Cognizance Journal of Multidisciplinary Studies*, *2*(3), 20–30. https://doi.org/10.47760/cognizance.2022.v02i03.002

Teimoor, R. A. (2021). A Review of Database Security Concepts, Risks and Problems. *UHD Journal of Science and Technology*, *5*(2), 38–46. https://doi.org/10.21928/uhdjst.v5n2y2021.pp38-46

Wang, Y., Xi, J., & Cheng, T. (2021). The Overview of Database Security Threats' Solutions: Traditional and Machine Learning. *Journal of Information Security*, *12*(1), 34–55. https://doi.org/10.4236/jis.2021.121002

Wilson, J. (1988). Views as the Security Objects in a Multilevel Secure Relational Database Management System. *Proceedings. 1988 IEEE Symposium on Security and Privacy*, 70–84. https://doi.org/10.1109/secpri.1988.8099

Yacono, L. (2022). *How to Identify Database Security Threats in 5 Steps*. CIMCOR. https://www.cimcor.com/blog/identify-database-security-threats

Yaseen, M., Bahari, M., & Hammood, O. A. (2021). Blockchain Technology Applications, Concerns and Recommendations for Public Sector. *Mesopotamian Journal of Computer Science*, *2021*(2021), 1–5. https://doi.org/10.58496/mjcsc/2021/001

Yaseen, Q., Alabdulrazzaq, A., & Albalas, F. (2019). A Framework for Insider Collusion Threat Prediction and Mitigation in Relational Databases. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0721–0727. https://doi.org/10.1109/ccwc.2019.8666582

Zeb, A. (2018). *Security of Relational Database Management System: Threats and Security Techniques.*