Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Cyber security Risks in DBMS: Strategies to Mitigate Data Security Threats: A Systematic Review

M. Muzammal Farooq[1]
Department of Software Engineering, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
su92-mssew-s24-005@superior.edu.pk
Rana M. Faheem Younas[2]
Department of Software Engineering, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
mrfaheemrajpoot@gmail.com
Junaid Nasir Qureshi[3]
Bahria University Lahore. jnqureshi.bulc@bahria.edu.pk
Ali Haider[4]
DELL Secure Works, USA. digitaleyeali@yahoo.com
Fawad Nasim[5]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
fawad.nasim@superior.edu.pk
Hamayun Khan[6]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Abstract

Database systems have been prime targets for cyber-attacks and threats due to the critical nature of the data they store. Despite the increasing reliance on database management systems, this field continues to face numerous cyber-attacks. Databases are collections of well-organized data that can be accessed, maintained, and updated quickly. Database systems are critical to

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

your company because they convey data about sales transactions, product inventories, customer profiles, and marketing activities. The number of attacks against these repositories has also increased. Increasing internet consumption and constant technological development, specifically have led to an increasingly urgent need for cyber awareness. Database Management Systems (DBMS) are the backbone of modern organizations, enabling efficient storage and retrieval of sensitive information. However, as the digital landscape evolves, so do the cybersecurity risks targeting these systems. This paper critically reviews existing research to identify key cybersecurity threats to DBMS, including SQL injection, ransomware, insider threats, and denial-of-service attacks. The paper analyzes recent studies and explores advanced strategies for mitigating these threats, such as AI-driven anomaly detection, blockchain-based security models, and Zero Trust architectures. The objective is to provide a clear understanding of the risks and actionable insights into building robust, secure database systems. This study offers a comprehensive analysis aimed at helping researchers and practitioners develop effective data security measures, ensuring both resilience and adaptability in an increasingly hostile cyber environment.

Keywords: Cyber insurance, Cyber risk, Open data, Systematic review, DBMS, database security threat mitigation, Data protection strategies for DBMS, Cyber threats in database management, DBMS cybersecurity challenges

Introduction

In an age where data has become one of the most valuable resources, the security of Database Management Systems (DBMS) has emerged as a critical area of research. These systems are pivotal in managing, storing, and safeguarding sensitive information across industries, from finance and healthcare to education and government [1]. However, their increasing reliance has made them prime targets for sophisticated cyber threats,

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

which continue to evolve in complexity and impact. From SQL injection and ransomware to insider threats and denial-of-service attacks, DBMS faces a myriad of challenges that threaten data integrity, confidentiality, and availability. So, here are several Cybersecurity Threats in Database Management Systems (DBMS) [2, 3] Despite advancements in cybersecurity technologies, significant gaps remain in fully addressing the risks associated with DBMS. Current research often focuses on isolated threats or specific technologies, resulting in fragmented strategies [4]. Moreover, the dynamic nature of cyber threats and the lack of integrated solutions highlight the need for a holistic approach to database security. This review consolidates findings from multiple studies to bridge these gaps, providing a comprehensive understanding of the challenges and potential solutions [5, 6].

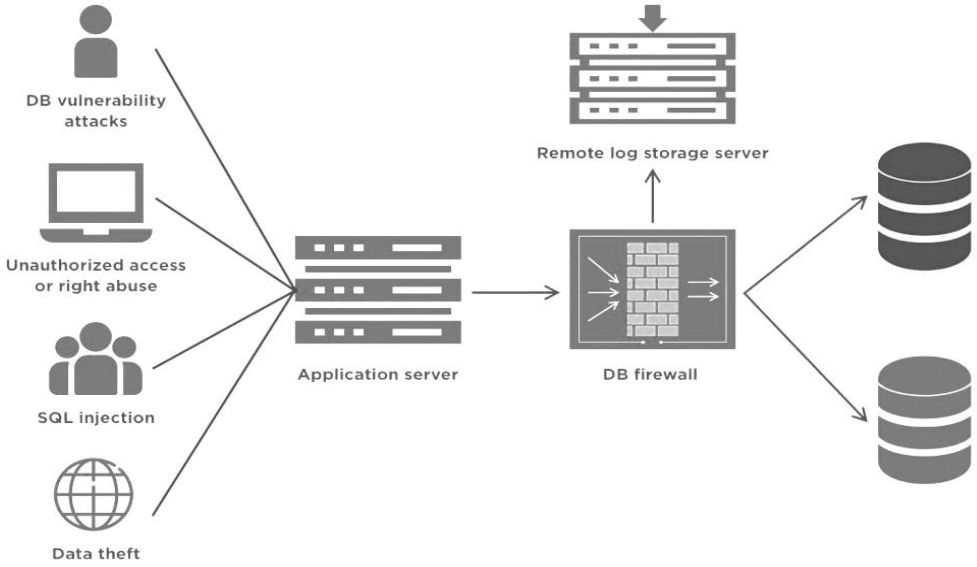

Figure 1: DBMS-Security system [7]

Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

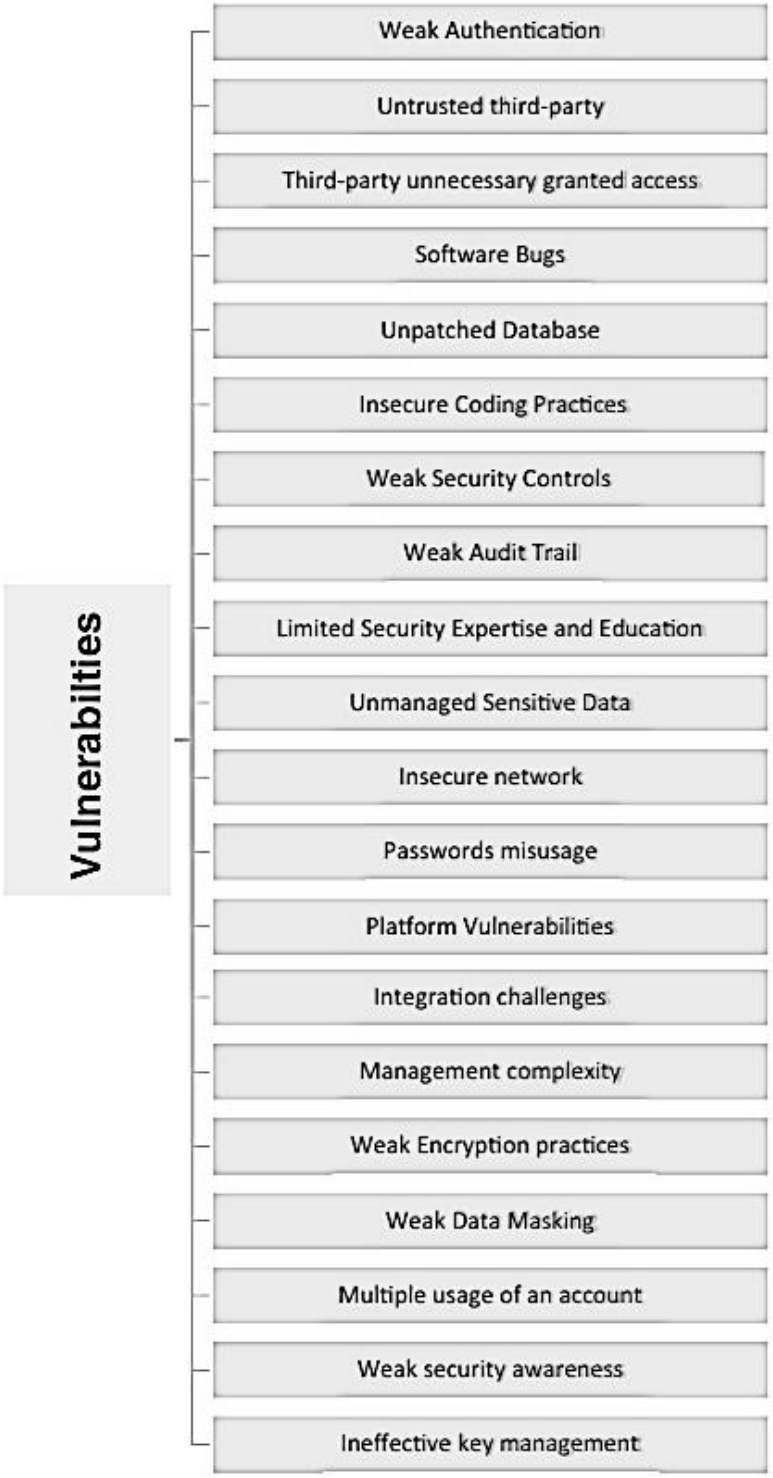

Figure 2: DBMS-Security vulnerabilities [8]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

So below we discuss existing studies to identify the cybersecurity risks in Database Management Systems (DBMS) and examine the strategies proposed or implemented to mitigate these data security threats. This discussion aims to provide a comprehensive understanding of the challenges and solutions within this domain [9, 10]. These papers aim to provide actionable insights into mitigating cybersecurity risks in DBMS by synthesizing existing research. It emphasizes innovative strategies, including AI-driven security solutions, Zero Trust architectures, and blockchain frameworks, to ensure organizations can protect their critical data assets effectively. By bridging the gap between research and practice, this review serves as a valuable resource for both academics and industry professionals [11, 12]. This study focuses on advanced measures to enhance the cybersecurity of database servers, addressing the growing sophistication of threats. The authors propose strategies that integrate innovative technologies and frameworks to mitigate potential vulnerabilities. Some of the key approaches discussed include:

Zero Trust Architecture: This framework assumes that no user or device is inherently trustworthy and implements strict access controls [13].

Multi-Factor Authentication (MFA): Ensures an additional layer of security by requiring multiple forms of verification before granting access [14].

Machine Learning for Anomaly Detection: Uses algorithms to detect unusual behavior or unauthorized access attempts in real-time [15].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

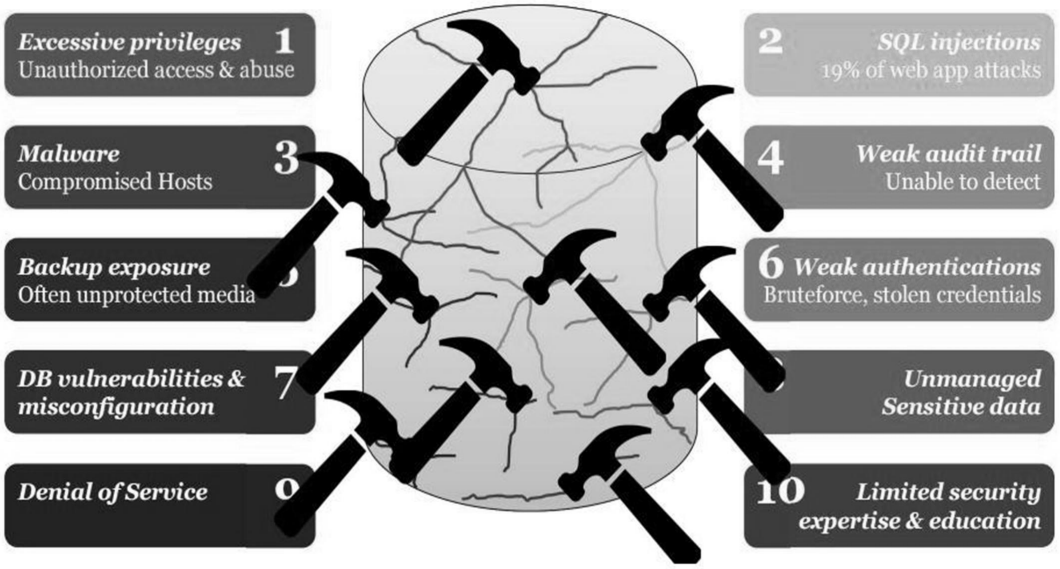

Figure 3: Possible DBMS Threats [16]

The paper also emphasizes the importance of adhering to regulatory frameworks such as GDPR and HIPAA to maintain data integrity and compliance. Overall, this study highlights a multi-layered approach that combines technology, policy, and user education to address modern database security challenges [17]. This paper examines the unique cybersecurity challenges faced by e-learning platforms and their associated databases. As e-learning systems grow in popularity, they have become prime targets for cybercriminals. The study identifies specific threats and proposes practical solutions, including:

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 1: Non-Technical Threats in DBMS [18]

Technical threats	Description of threats	Impact and example of threats
Human error	Human mistakes such as accidental disclosures of sensitive information, misdirected emails, and unintentional disclosure of login credentials.	Disclosures of sensitive information, misdirected emails, unintentional disclosure of login credentials
Insider threats	People who have access to sensitive data can intentionally misuse this data for malicious reasons. They are considered as threatening as the outsider threats. Insiders may be disgruntled employees, contractors and business partners. Some tactics that malicious users may use are copying files onto a Universal Serial Bus (USB) drive, emailing sensitive information to a personal account, sharing access credentials with unauthorized individuals, or even planting malware or other hacking tools to facilitate their activities. Insider threats can also be inadvertent negligence by individuals.	Internal threats from employees, lack of awareness and employee negligence
Third-party risks	Some organizations rely on third-party systems or services to manage their data, security vulnerabilities in these third-party systems, or services put enterprise data at risk.	Third-party risks

Unique Threats Identified

Denial-of-Service (DoS) Attacks: Overloading database servers to disrupt access [19].

Unauthorized Access: Exploiting weak authentication measures [20].

Cyber Espionage: Stealing sensitive government data [21].

Insider Threats: Malicious or negligent misuse by employees [22].

Electoral Data Manipulation: Tampering with votes in politically sensitive regions [23]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 2: Comparison of Measure for DBMS Security [24]

Database Security Measures	Authentication Methods	Access Control Models	Encryption Techniques	Auditing and Monitoring	Intrusion Detection Systems
Traditional Password-Based	Username/Password	Discretionary Access Control	Symmetric Encryption	Audit Trails	Signature-Based IDS
Authentication				Log Analysis	Anomaly-Based IDS
		Mandatory Access Control	Asymmetric Encryption	Event Correlation	
Biometrics	Fingerprint	Role-Based Access Control	Hashing	Real-Time Monitoring	
	Retina Scan			Security Information and Event Management	
	Facial Recognition				
				Systems (SIEM)	

Unique Threats

Cross-site scripting (XSS) attacks exploit web application vulnerabilities and SQL injection attacks targeting weak query structures. A method to secure data transfers by encrypting communications between users and servers.

IWAS Models: Real-time threat evaluation frameworks that assess risks and recommend mitigation strategies. By addressing these issues, the paper underscores the critical importance of implementing robust security measures in e-learning systems to ensure data privacy and system reliability [25, 26]. This paper systematically addresses cybersecurity risks in database management systems (DBMS) by creating a detailed classification of threats, weaknesses, and countermeasures. The authors emphasize that DBMS are frequent targets of cyberattacks due to the critical nature of the data they store.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 3: Comparison of DBMS-based Cyber Security Risk Management Tools [27]

Tool	Metric	Strategy	Integration mechanisms with
Nessus Home	CVSS2, CVSS3	Results based on the risk factor of the vulnerability (e.g., Low, Medium, High, Critical)	Kenna, ThreatConnect, Cisco ISE, ForeScout
Saint8	Business unit, Criticality, Business cost, CVSS	Prioritization and the application of resources to assets based on metrics of importance to the organization.	Cisco FireSIGHT Management Center
EyeRetina	Business impact, Core Impact, Metasploit, Exploit-db, CVSS	Real risk to critical assets and exploitability	Kenna, IBM QRadar SIEM, LogRhythm
GFILanguard	OVAL, CVE	Security issues are rated by their severity level and each computer is given a risk and vulnerability rating.	Core Security Technologies
nCircle® IP360	CVE, CVSS OVAL, SCAP	Prioritizes vulnerabilities, manages risk and improves security efficacy by combining business context with vulnerability intelligence.	Kenna, IBM QRadar, Bringa, LockPath, Trusted Integration

The literature review identifies various technical threats, such as SQL injection, denial-of-service (DoS), and ransomware, as well as non-technical threats like insider misuse and human errors [28]. The paper highlights key vulnerabilities, including weak authentication, unpatched software, and insecure coding practices, which attackers commonly exploit. To mitigate these risks, the authors propose a structured framework that involves identifying key components, Assessing threats, Identifying vulnerabilities and implementing countermeasures. These countermeasures include robust access control, data encryption, intrusion detection systems, and continuous monitoring of database activity. The authors' approach focuses on proactive risk management, encouraging organizations to classify risks by severity and address them with a multi-layered defense strategy [29, 30].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Table 4: Non-technical threats in DBMS [31]

Countermeasures	Description
Data encryption	Encryption is the process of transforming data into a coded format to make it unreadable by intruders and difficult to decipher, whether it is during transmission or at rest. It can be applied to many data types, such as emails, files, databases, and other communication channels. Encryption can also prevent insider threats, as insiders who have access to the data will not be able to read it unless they have the required authorization. In addition, it helps organizations to ensure their confidentiality, integrity, and availability by adhering to several data protection regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Ensures the security of users by converting the data with the AES algorithm to the database management system, Message Digest (MD5), and Secure Hash Algorithm (SHA-256) to protect network data transmission. It is cost-effective; investing in the implementation of encryption technology is cheaper than dealing with the consequences of data breaches.
Access control	All DBMS use access control to create user accounts and passwords to prevent unauthorized people from entering the database system and obtaining confidential information. Granting and revoking privileges are methods of enforcing access control. The organization must set policies defined by access control that all contact with the databases must adhere to. It is suggested that web tripwire and login rituals be integrated using Multi-Factor Authentication (MFA). Access control allows organizations to do the following: - Access control allows organizations to implement a layered defense approach to security. - Helps organizations follow protection data regulations. - Prevents insider threats. - Allows organizations to detect and respond to security incidents. Access control systems consist of: - File permissions to create, read, edit, or delete files on the server. - Program permissions are the rights of executing an application program on the server. - Data rights, the rights of retrieving, or updating data in a database. Access control mechanisms: 1. Discretionary Access Control (DAC) 2. Mandatory Access Control (MAC) 3. Role-Based Access Control (RBAC)

The paper underscores the importance of understanding the interplay between threats and vulnerabilities to develop effective mitigation plans for securing DBMS. This aligns closely with your research title by providing a comprehensive strategy for addressing cybersecurity risks in databases [32]. This paper explores cybersecurity threats in public sector databases and presents advanced solutions to enhance security. The authors emphasize protecting sensitive public data, such as government and electoral records, from threats like data theft, unauthorized access, and insider misuse [33].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

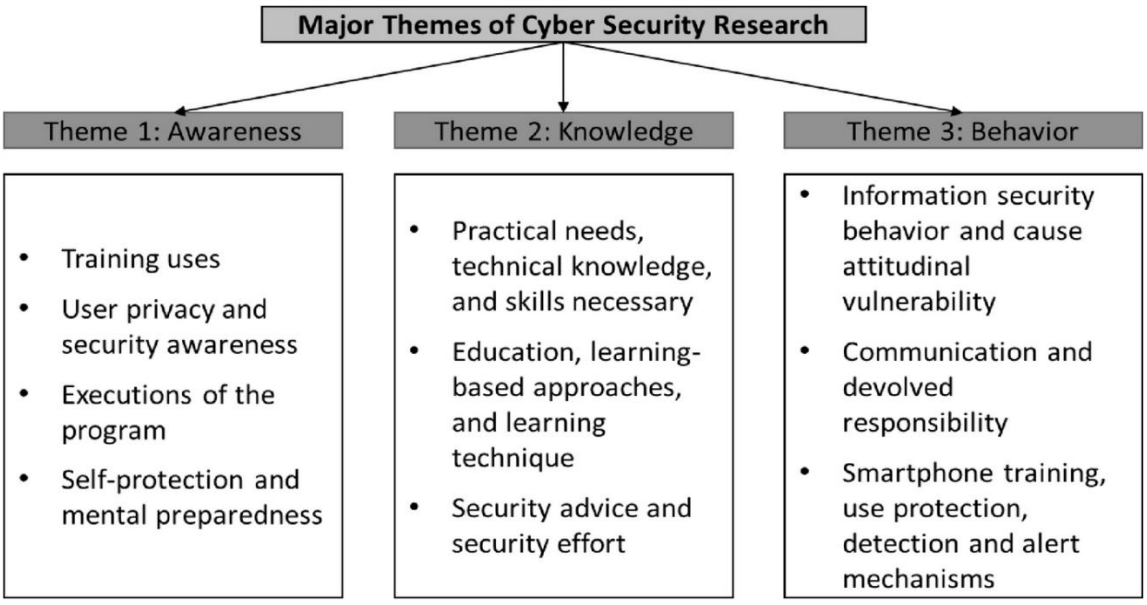

Figure 4: Cybersecurity Research areas [35]

Literature Review

How implementing prototypes, like blockchain-based algorithms and layered security architectures, can enhance resilience against cyber threats. By combining advanced technologies with best practices, the authors provide a practical roadmap for mitigating risks in DBMS. This paper complements your research focus by showcasing how emerging technologies like blockchain can address modern cybersecurity challenges in databases. The paper highlights how AI technologies like machine learning and deep learning strengthen database security by enabling real-time monitoring, anomaly detection, automated patching, and adaptive encryption. AI systems proactively identify threats, predict risks, and mitigate vulnerabilities while minimizing human error and manual oversight. Despite its benefits, challenges like AI misuse by attackers, ethical concerns, and computational demands are addressed [36].

Unique Threats Identified

Evolving Threats: Zero-day exploits, advanced persistent threats (APTs), and AI-driven attacks [37].

Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Internal Misconfigurations: Errors in firewall settings, patch delays, and weak data handling.

Sophisticated Data Breaches: Hackers bypassing traditional encryption methods [38].

Table 5: Comparison of DBMS- security threats, Solutions and damage [39]

First level threats	Second level threats	Damage	Solutions
Data not effectively protected	Data tampering	Data distortion or invalid	Tamper detection, User authentication, data encryption, Tamper proof material
	Data exposure	Illegal use User' data	User authentication, data encryption, Audit, Construct machine learning model
	Data monitored or collected	Privacy disclosure	Establishment of special system, data encryption
User exception	Illegal act	Break the role code of conduct	Intrusion detection, Establishment of special system, User behavior analysis
	Unauthorized access	Illegal processing of data	Access control
	Weak safety awareness	Create a breakthrough for attackers	Empirical research
Vulnerability of Defense system	Bug	Used to destroy the database	Safety assessment, Empirical framework
	Inaccurate identification	Reject normal users and accept illegal users	User authentication
External attack	Spam	Occupy a lot of storage space and commit fraud	Access control
	Malicious traffic	Server works abnormally	Audit, Intrusion detection
	SQL injection	Embedded trojan horse and illegal right raising	Access control, Access control, User behavior analysis, System risk prediction
	Illegal access	Break system authentication mechanism and obtain others data	User authentication, Establishment of special system, Intrusion detection
	Malicious software	Illegal access to user secret data	Data encryption, Malware detection, Intrusion detection
	DDoS attack	System functions not available	Intrusion detection, Access control
	Bypass and physical attack	Hardware Damage and less preventable	Intrusion detection, Tamper proof material

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

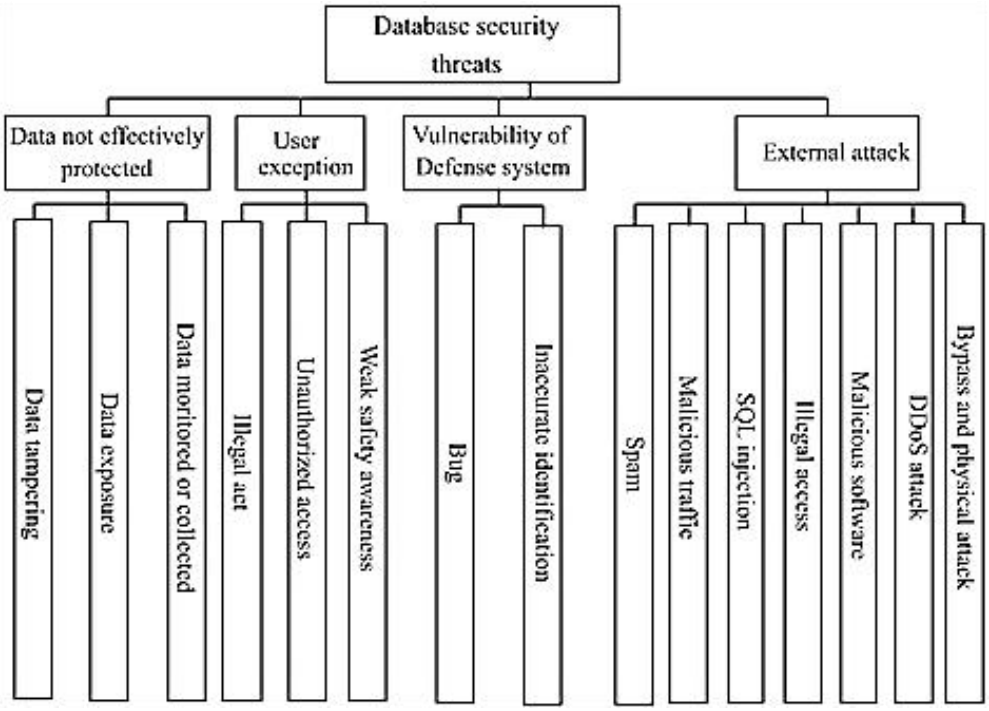

Figure 5: Data Security Threats for DBMS [40]

Proposed Solutions

AI transforms database security with adaptive and automated defenses. While offering robust solutions to mitigate modern threats, its implementation requires addressing ethical, computational, and misuse concerns. This research aligns with your focus on modernizing database cybersecurity strategies [41].

The paper comprehensively discusses the growing sophistication and frequency of cybersecurity threats, highlighting key types of attacks like malware, phishing, ransomware, and distributed denial-of-service (DDoS). It explores how these threats exploit vulnerabilities in systems, networks, and human behavior, causing financial loss and reputational damage. Advanced threats, such as state-sponsored attacks and hacktivism, are also analyzed for their broader societal and national implications [42, 43].

Anomaly Detection: AI identifies deviations in behavior to detect threats in real time.

Automated Patching: AI resolves vulnerabilities faster, reducing exposure to risks.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Adaptive Encryption: Dynamically adjusts encryption based on threat levels.

Real-Time Monitoring: Ensures immediate response to irregularities.

Predictive Risk Analysis: Anticipates threats using behavior trends. Automation: Reduces human error by handling routine tasks autonomously. The authors emphasize the importance of leveraging advanced technologies like Artificial Intelligence (AI) and machine learning to combat these threats. AI enhances Cybersecurity by enabling real-time threat detection, behavior analysis, and automated responses. However, the paper also raises concerns about the ethical use of AI, potential biases, and its reliance on high-quality data [44, 45].

Unique Threats Identified

Sophisticated Malware: Includes viruses, worms, trojans, and spyware designed to harm or steal data. Phishing and Social Engineering: Deceptive tactics to trick individuals into revealing sensitive information. Ransomware: Encrypted files held hostage until a ransom is paid [46]. DDoS Attacks: Overwhelming system resources to cause downtime. State-Sponsored Cyberwarfare: Targeting critical infrastructure for political or economic disruption [47].

Proposed Solutions

AI and Machine Learning: Enhances real-time monitoring, anomaly detection, and incident response.

User Education: Mitigates risks through awareness of phishing and social engineering tactics.

Advanced Encryption: Protects sensitive data from breaches.

Proactive Risk Management: Includes regular software updates and robust incident response plans.

Collaboration and Policy: Encourages organizations and governments to work together to address evolving threats.

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Figure 6: Strategies to Mitigate Data Security Threats [48]

Mitigating data security threats in DBMS requires a multi-layered approach that combines advanced technologies, robust policies, and user awareness. Insights from the analyzed studies suggest that organizations need to adopt both proactive and reactive strategies to address the evolving threat landscape effectively. These strategies ensure not only the prevention of attacks but also the timely detection and response to potential breaches. AI-Driven Anomaly Detection: Use machine learning algorithms to identify and respond to unusual database activity in real-time, reducing the risk of undetected breaches. Zero Trust Architectures: Implement strict access controls based on the principle of "never trust, always verify," ensuring that no user or device is inherently trusted. Encryption Techniques: Employ adaptive encryption methods to protect data both at rest and in transit, ensuring that sensitive information remains secure even if intercepted. Blockchain-Based Frameworks: Leverage blockchain for transparent and tamper-proof transaction records, enhancing data integrity and accountability. Regular Audits and Patch Management: Conduct frequent security assessments and ensure that software

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

vulnerabilities are promptly addressed through updates and patches. User Training and Awareness: Educate users on best practices for cybersecurity to minimize human errors, such as phishing attacks and weak passwords. Intrusion Detection Systems (IDS): Deploy systems that monitor network traffic and alert administrators of potential threats, enabling faster response times. By integrating these strategies, organizations can create a robust defense mechanism against modern cyber threats. The combination of innovative technology with well-defined policies and educated users ensures a secure and resilient database environment.

Conclusion

This article determined that awareness, knowledge, and behavior are important as cyber threats cause security issues. Some users take fitting action by pursuing cyber threat knowledge while others freely share cyber threat information and experiences also highlighting the dynamic and evolving nature of cybersecurity risks targeting DBMS. Key threats such as SQL injection, ransomware, insider misuse, and denial-of-service attacks pose significant challenges to organizations. However, innovative strategies, including AI-driven anomaly detection, blockchain-based frameworks, and Zero Trust architectures, offer promising solutions to these issues. The integration of advanced technologies with robust policies and user education is crucial to mitigating these risks effectively. This review consolidates findings from diverse studies, providing actionable insights into addressing the most pressing cybersecurity challenges. By adopting a proactive, multi-layered approach, organizations can safeguard their databases against evolving threats while maintaining operational resilience. The significance of this work lies not only in its contribution to academic research but also in its practical applications, equipping practitioners with tools to navigate the increasingly complex cybersecurity landscape.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Jawale, P. Warole, S. Bhandare, K. Bhat, and R. Chandre, "Jeevn-Net: Brain Tumor Segmentation using Cascaded U-Net & Overall Survival Prediction," Int. Res. J. Eng. Technol., pp. 56–62, 2020.

[2] B. Nagy et al., "Privacy-preserving Federated Learning and its application to natural language processing," Knowledge-Based Syst., vol. 268, p. 110475, 2023, doi: 10.1016/j.knosys.2023.110475.

[3] L. Campanile, S. Marrone, F. Marulli, and L. Verde, "Challenges and Trends in Federated Learning for Well-being andHealthcare," Procedia Comput. Sci., vol. 207, no. Kes, pp. 1144–1153, 2022, doi: 10.1016/j.procs.2022.09.170.

[4] [A. Velez-Estevez, P. Ducange, I. J. Perez, and M. J. Cobo, "Conceptual structure of federated learning research field,"Procedia Comput. Sci., vol. 214, no. C, pp. 1374–1381, 2022, doi: 10.1016/j.procs.2022.11.319.

[5] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi Yakoi, Muhammad Mansab, and Saleem Zubair. "Room Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7, no. 3 (2024).

[6] Imtiaz, Ahsan, Danish Shehzad, Fawad Nasim, Muhammad Afzaal, Muhammad Rehman, and Ali Imran. "Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems." In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), pp. 1-7. IEEE, 2023.

[7] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi Yakoi, Muhammad Mansab, and Saleem Zubair. "Room

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7, no. 3 (2024).

[8] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, ‘‘The security of big data in fog-enabled IoT applications including blockchain: A survey,’’ Sensors, vol. 19, no. 8, p. 1788, Apr. 2019.

[9] Nasim, Fawad, Sohail Masood, Arfan Jaffar, Usman Ahmad, and Muhammad Rashid. "Intelligent Sound-Based Early Fault Detection System for Vehicles." Computer Systems Science & Engineering 46, no. 3 (2023).

[10] Imtiaz, Ahsan, Danish Shehzad, Hussain Akbar, Muhammad Afzaal, Muhammad Zubair, and Fawad Nasim. "Blockchain Technology The Future of Cybersecurity." In 2023 24th International Arab Conference on Information Technology (ACIT), pp. 1-5. IEEE, 2023.

[11] Cellular IoT Connections Reached 3.4 Billion in 2023. Available online: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook

[12] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[13] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[14] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[15] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[16] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[17] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[18] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[19] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[20] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[21] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[22] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[23] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[24] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[25] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[26] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[27] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[28] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[29] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[30] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's)

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[31] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[32] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[33] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[34] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[35] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[36] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[37] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[38] S. K. M. et al., "Privacy-Preserving in Blockchain-based Federated Learning Systems," pp. 1–44, 2024, [Online].Available: http://arxiv.org/abs/2401.03552.
[39] J. Zhang, H. Zhu, F. Wang, J. Zhao, Q. Xu, and H. Li, "Security and Privacy Threats to Federated Learning: Issues,Methods, and Challenges," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/2886795.
[40] W. Si and C. Liu, "Privacy Preservation Learning with Deep Cooperative Method for Multimedia Data Analysis," Secur.Commun. Networks, vol. 2022, no. Iid, 2022, doi: 10.1155/2022/8449987.
[41] Q. Yang et al., "Federated Learning with Privacy-preserving and Model IP-right-protection," Mach. Intell. Res., vol. 20,no. 1, pp. 19–37, 2023, doi: 10.1007/s11633-022-1343-2.
[42] G. A. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, "Secure, privacy-preserving and federated machine learningin medical imaging," Nat. Mach. Intell., vol. 2, no. 6, pp. 305–311, 2020, doi: 10.1038/s42256-020-0186-

[43] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.
[44] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023
[45] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019
[46] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[47] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and Security in Federated Learning: A Survey," Appl. Sci., vol.12, no. 19, pp. 1–15, 2022, doi: 10.3390/app1219990

[48] T. Alam and R. Gupta, "Federated Learning and Its Role in the Privacy Preservation of IoT Devices," Futur. Internet, vol.14, no. 9, pp. 1–22, 2022, doi: 10.3390/fi14090246.