NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA SURATHKAL

Security Issues and Their Techniques in DBMS - A Novel Survey

STUDENT DETAILS-

NAME- SHUBHANGI

CLASS- 211CS153

SECTION- S1

PAPER DETAILS-

TITLE OF THE PAPER- Security Issues and Their Techniques in DBMS - A Novel Survey

AUTHOR NAMES- Mohd Muntjir, Sultan Aljahdali, Mohd Asadullah, Junedul Haq

CONFERENCE NAME- International Journal of Computer Applications

YEAR- 2014

ABSTRACT-

This document discusses the vulnerabilities, threats, and security methods of database management systems (DBMS). The paper emphasizes the need for security in DBMS due to the availability of company information on web pages connected to databases. The document provides an overview of recent trends in database protection and summarizes traditional approaches to securing databases. The three main requirements for data security are confidentiality, integrity, and availability (CIA). The paper discusses various security methods for DBMS, including role-based access control and content-based access control. The document also highlights the threat of SQL injection and suggests various intrusion detection systems to prevent it. The paper concludes that more research needs to be done to secure databases due to the vulnerabilities in internet connection and websites.

PROBLEMS ADDRESSED IN THIS PAPER-

This paper addresses the vulnerabilities, threats, and security methods of database management systems. The vulnerabilities include poor architecture, misconfigurations, vendor bugs, and incorrect usage. The threats include internal and external security breaches, such as incorrect data modification, unauthorized data observation, and data unavailability. The security methods discussed include access control mechanisms, encryption techniques, semantic integrity constraints, physical and logical data integrity protection, intrusion detection systems, and backup and recovery strategies. The paper also highlights the importance of confidentiality, integrity, and availability (CIA) in database management systems. The authors emphasize the need for security policies and procedures, secure initial configuration, and auditing to ensure database security. The paper concludes that while remarkable work has been done in this field, more research is needed to address the vulnerabilities in internet connection and website.

SOLUTIONS SUGGESTED –

The document discusses various security methods to prevent SQL injection attacks, including the use of Intrusion Detection Systems (IDS) such as Misuse Detection System for DBMS (DEMIDS), Detecting Intrusion in Databases through Fingerprinting Transactions (DIDAFIT), and real-time intrusion detection mechanisms based on user role profiles. The document also highlights the vulnerabilities in database management systems (VDBMS) such as poor architecture, misconfigurations, and vendor bugs, and suggests security methods such as access control, administration policies and procedures, secure initial configuration, auditing, and backup and recovery strategies. Additionally, the document mentions the importance of confidentiality, integrity, and availability (CIA) in database management systems and suggests techniques such as public key encryption (PKI), one-time passwords , and smart cards for authentication of users.

FUTURE WORK PROPOSED-

1. Privacy-Preserving Techniques: One area of future work involves exploring advanced privacy-preserving techniques for securing DBMS. This includes techniques such as differential privacy, secure multi-party computation, and homomorphic encryption. Further research is needed to assess the feasibility and effectiveness of these techniques in real-world DBMS environments, considering factors like performance overhead and data utility.

2. Scalability and Performance: As DBMS continue to handle large volumes of data and support high transaction rates, ensuring security without compromising scalability and performance becomes crucial. Future work should focus on developing efficient security mechanisms that can scale seamlessly with the growing demands of DBMS. This may involve exploring distributed security architectures, parallel processing, and optimizing security algorithms for improved performance.

3. Security in Cloud and Distributed Environments: With the widespread adoption of cloud computing and distributed database systems, securing DBMS in these environments poses unique challenges. Future research should investigate novel security approaches tailored specifically for cloud-based DBMS, including secure data migration, data isolation, and protection against cloud-specific threats such as shared resource vulnerabilities and insider attacks.

4. AI-Driven Security Solutions: Artificial intelligence (AI) techniques have shown promise in various domains, including security. Future work should explore the integration of AI-driven security solutions into DBMS to enhance threat detection, anomaly detection, and predictive security analytics. This involves developing intelligent algorithms that can continuously monitor DBMS activities, detect suspicious patterns, and adaptively respond to emerging threats.

5. Regulations and Compliance: Data protection regulations and compliance requirements continue to evolve, necessitating ongoing research on aligning DBMS security practices with these frameworks. Future work should focus on understanding the implications of regulations such as the General Data Protection Regulation (GDPR) and developing strategies to ensure compliance in DBMS environments. This includes techniques for data anonymization, consent management, and audit trails to demonstrate compliance.

6. User Education and Awareness: Despite robust security measures, human factors remain a significant vulnerability in DBMS security. Future work should emphasize user education and awareness programs to promote secure practices among database administrators,

developers, and end-users. This may include training programs, security guidelines, and awareness campaigns to mitigate the risk of social engineering attacks and unauthorized access.

The document mentions that despite the remarkable work done in the field of database security, more research needs to be done as there are vulnerabilities in internet connection and websites. Therefore, future work proposed would be to continue researching and developing intrusion detection systems and other security methods to prevent SQL injection and other threats to database management systems.

PROBLEMS RELATED WHICH ARE NOT ADDRESSED-

While the previous response outlined some future research directions, it's important to acknowledge that there may be several problems related to security in DBMS that are not adequately addressed. Here are a few additional issues that require further attention:

1. Zero-Day Exploits: Zero-day exploits refer to vulnerabilities that are unknown to software vendors and, therefore, lack patches or mitigations. DBMS may be susceptible to such exploits, putting sensitive data at risk. Future work should focus on developing proactive security measures that can detect and prevent zero-day attacks, such as anomaly detection algorithms and behavior-based monitoring systems.

2. Insider Threats: While insider threats were briefly mentioned earlier, they require more comprehensive research and mitigation strategies. This includes understanding different types of insider threats, such as malicious insiders, negligent employees, and compromised accounts, and developing techniques to detect, prevent, and respond to these threats effectively.

3. Advanced Persistent Threats (APTs): APTs are sophisticated, targeted attacks that aim to infiltrate and persistently exploit DBMS over extended periods. These attacks often involve multiple stages and evasion techniques, making them challenging to detect and mitigate. Future work should focus on developing advanced detection mechanisms, threat intelligence sharing frameworks, and incident response strategies to combat APTs effectively.

4. Supply Chain Security: DBMS security is not limited to the system itself but also extends to the entire supply chain involved in its development and deployment. Supply chain attacks can introduce backdoors or vulnerabilities into DBMS, compromising the security of the data. Future research should explore supply chain risk management strategies, secure development practices, and third-party assurance mechanisms to ensure the integrity and security of DBMS components.

5. Human Factors: While user education and awareness were mentioned in the previous response, human factors remain a significant challenge in DBMS security. This includes issues such as weak passwords, poor access control management, social engineering attacks, and user negligence. Future work should emphasize the design of user-friendly security interfaces, effective access control models, and comprehensive security training programs to mitigate these human-related vulnerabilities.

6. Integration with Emerging Technologies: DBMS are increasingly integrated with emerging technologies such as Internet of Things (IoT), edge computing, and artificial intelligence. The security implications of these integrations are not yet fully understood. Future research should focus on exploring the unique security challenges posed by these technologies, developing security frameworks, and best practices for secure integration and interoperability with DBMS.

Addressing these additional problems will contribute to a more comprehensive and robust security framework for DBMS, ensuring the protection of sensitive data and mitigating emerging threats effectively.

ISSUES IN THE PROPOSED SOLUTION-

While the proposed solutions and future research directions aim to address various security challenges in DBMS, there may be some potential issues or considerations that need to be taken into account. These include:

1. Performance Overhead: Implementing advanced security techniques and measures can introduce performance overhead in DBMS operations. For example, encryption and decryption processes may impact query response times. Future research should focus on optimizing and balancing security measures to minimize performance impact while maintaining adequate levels of protection.

2. Complexity and Manageability: Introducing novel security techniques and approaches may increase the complexity of managing and maintaining the security of DBMS. Administrators and users may require additional training and expertise to effectively deploy and configure these security measures. Future research should consider the usability and manageability aspects of the proposed solutions to ensure they are practical and feasible for real-world implementations.

3. Cost and Resource Constraints: Implementing advanced security measures in DBMS can incur additional costs in terms of hardware, software, and personnel. Organizations with limited resources may face challenges in adopting and maintaining these security solutions. Future research should explore cost-effective approaches and consider the resource constraints of different organizations to ensure that security measures are accessible and scalable.

4. Compatibility and Interoperability: As DBMS environments evolve and incorporate new technologies and components, ensuring compatibility and interoperability between different security solutions becomes crucial. Future research should address the integration challenges and potential conflicts that may arise when implementing multiple security techniques or when integrating DBMS with emerging technologies.

5. False Positives and Negatives: Intrusion detection and anomaly detection systems used in DBMS security can generate false positives (flagging benign activities as threats) or false negatives (failing to detect actual threats). Balancing the accuracy of detection with minimizing false alarms is essential. Future research should focus on improving the accuracy and effectiveness of security systems, utilizing machine learning algorithms and fine-tuning detection mechanisms.

6. Evolving Threat Landscape: The security landscape is constantly evolving, with new vulnerabilities, attack techniques, and threat actors emerging over time. Future research should consider the adaptability and agility of security solutions to address emerging threats and keep pace with evolving attack vectors. Continuous monitoring, threat intelligence sharing, and collaboration between researchers and industry practitioners are essential in staying ahead of the evolving threat landscape.

Addressing these issues and considerations will be vital to ensure the practicality, effectiveness, and long-term sustainability of the proposed security solutions in DBMS environments.

MY PROPOSED SOLUTION-

To address the potential issues related to the proposed solutions for security challenges in DBMS, the following approaches can be considered:

1. Performance Overhead:

- Conduct performance analysis and optimization to identify and address any bottlenecks or areas where the security measures may impact performance. This may involve optimizing

encryption algorithms, implementing parallel processing techniques, or utilizing hardware-accelerated encryption technologies to minimize performance impact.

- Select efficient security techniques that offer a balance between strong security and minimal performance overhead. This could involve choosing lightweight encryption algorithms or employing encryption techniques that operate at a granular level (e.g., column or row-level encryption) rather than encrypting the entire database.

2. Complexity and Manageability:

- Develop user-friendly interfaces and tools for managing security measures in DBMS. This includes intuitive graphical user interfaces, automated configuration wizards, and centralized management consoles that simplify the implementation and administration of security solutions.

- Provide comprehensive documentation and training resources to educate administrators and users on best practices for implementing and managing security measures in DBMS. Clear instructions and guidelines can help reduce complexity and ensure that security measures are correctly deployed and configured.

3. Cost and Resource Constraints:

- Prioritize security measures based on a thorough risk assessment. Identify the most critical security threats and allocate resources accordingly, focusing on addressing the highest priority risks first.

- Explore open-source security solutions and leverage community-driven efforts. Open-source solutions often provide cost-effective alternatives to proprietary software licenses, and they benefit from community contributions, offering continuous improvements and enhancements without significant financial investments.

4. Compatibility and Interoperability:

- Adhere to industry standards and best practices for security in DBMS to ensure compatibility and interoperability. This includes using standardized encryption algorithms, access control models, and protocols that facilitate integration with other systems and technologies.

- Develop well-defined APIs and interfaces that allow seamless integration with other security systems, technologies, or platforms. By ensuring compatibility at the interface level, organizations can enhance interoperability without sacrificing security.

5. False Positives and Negatives:

- Continuously fine-tune intrusion detection and anomaly detection systems by analyzing and adjusting detection thresholds based on real-world data and feedback. Incorporate machine learning algorithms to improve detection accuracy and reduce false positives and negatives over time.

- Establish feedback loops between security systems and administrators/users to gather information on false positives and negatives. This feedback can help refine detection algorithms and improve the accuracy of security measures.

6. Evolving Threat Landscape:

- Stay updated on the latest security threats and vulnerabilities through continuous monitoring and regular updates. This involves actively monitoring security communities, leveraging threat intelligence sources, and keeping abreast of industry updates. By promptly updating security measures and patching vulnerabilities, organizations can address emerging threats effectively.

- Foster collaboration and information sharing between researchers, security vendors, and industry practitioners to exchange knowledge, insights, and best practices. This collaboration helps ensure that security measures remain adaptive and capable of addressing the evolving threat landscape effectively.

By incorporating these approaches, organizations can mitigate potential issues related to the proposed solutions, enhancing the overall effectiveness and practicality of security measures in DBMS environments.

CONCLUSION-

The conclusion of the document states that while remarkable work has been done in the field of database security, the risk to databases has increased with the invention of internet technology. Many intrusion detection systems for databases have been devised, but more research needs to be done as there are vulnerabilities in internet connection and websites. The paper has identified the vulnerabilities, threats, and security methods of database management systems through a survey conducted on researches of database security. The vulnerabilities include poor architecture, misconfigurations, vendor bugs, and incorrect usage. The threats include people, malicious code, natural disasters, and technological disasters. The security methods include access control, auditing, backup and recovery strategies, and securing databases based on access control. The paper emphasizes the need for role-based access control and maintaining confidentiality, integrity, and availability (CIA) to avoid attacks due to network and SQL injection. The table provided in the document summarizes the vulnerabilities, threats, and security methods of database management systems.

REFERENCES-

1) Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow,IEEE, “Database Security—Concepts, Approaches and Challenges” in IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2,NO. 1, JANUARY-MARCH 2005

2) Andriy Furmanyuk , Mykola Karpinskyy, Bohdan Borowik, “Modern Approaches to the Database Protection” in IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications 6-8 September 2007,Dortmund, Germany

3) Marco Vieira, Henrique Madeira , “Detection of Malicious Transactions in DBMS”, 11th Pacific Rim International Symposium on Dependable Computing

4) Hassn A. Afyuoni, A Book, “Database security and auditing “

5) Aziah Asmawi , “System Architecture for SQL Injection and Insider Misuse Detection System for DBMS”, my -1-4244-2328 6/08/$25.00 © 2008 IEEE

5)Guoliang Zou, Jing Wang, Dongmei Huang, LiangJun Jiang, “Model Design of Role-Based Access Control and Methods of Data Security”, 2010 International Conference on Web Information Systems and Mining.

7) E.B. Fernandez,R.C. Summers and C.Wood, Database Security and Integrity. Addison-Wesley, Feb.1981.

9) Premchand B. Ambhore,B.B.Meshram,V.B.Waghmare,“A IMPLEMENTATION OF OBJECT ORIENTED DATABASE SECURITY” , Fifth International Conference on Software Engineering Research,Management and Applications.

9) Yu Chen and Wesley W. Chu, ”Protection of Database Security via Collaborative Inference Detection “, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 20, NO. 8, AUGUST 2008

THANK YOU.