Database Security Audits: Identifying and Fixing Vulnerabilities before Breaches

Baljeet Singh
Technical Lead, Wipro Limited, India.

Abstract: In today's data-driven environment, the security of databases has become a critical concern for organizations across all sectors. With increasing incidents of cyber-attacks, data breaches, and insider threats, there is an urgent need for systematic and proactive approaches to safeguard sensitive information. Database security audits serve as a vital mechanism to identify, assess, and mitigate vulnerabilities before they can be exploited by malicious actors. This paper presents an in-depth study on the role and methodology of security audits in enhancing database security, with a special focus on vulnerability detection and prevention. The audit process involves a structured assessment of database configurations, access controls, user privileges, logging mechanisms, and patch management strategies. By employing advanced auditing tools and techniques, organizations can uncover hidden threats, non-compliant practices, and configuration weaknesses that could potentially lead to security breaches. Moreover, periodic audits enable compliance with regulatory standards such as GDPR, HIPAA, and PCI DSS, ensuring both legal and operational security. The paper includes a comprehensive literature survey that explores existing research, tools, and frameworks used in database security audits. It also discusses core working principles, including automated scanning, anomaly detection, and real-time monitoring. Case studies and comparative analyses demonstrate the effectiveness of various audit practices in both Oracle and open-source database systems. The study emphasizes the need for continuous enhancement in audit methodologies through artificial intelligence and machine learning. These emerging technologies have the potential to revolutionize audit efficiency and threat prediction. The findings underscore the importance of incorporating proactive security audits as an integral component of database security strategy to prevent breaches before they occur.

Keywords -Database Security, Security Audit, Vulnerability Assessment, Data Breach Prevention, Access Control, Oracle Security, Compliance Monitoring, Audit Trail, Threat Detection, Patch Management, Risk Mitigation, Real-Time Monitoring, Insider Threats, Security Best Practices, Database Hardening

I. INTRODUCTION

In an increasingly digitized world, data has become one of the most valuable assets for organizations. From personal information and financial records to intellectual property and operational data, the integrity and confidentiality of stored data are paramount. As organizations rely heavily on databases to manage this critical information, the need for robust database security measures has grown significantly. However, with the rise in sophisticated cyber-attacks and the increasing complexity of IT infrastructures, databases have become prime targets for malicious activities.

Database breaches can lead to severe consequences, including financial losses, reputational damage, legal penalties, and the loss of customer trust. Many of these breaches stem from vulnerabilities that go unnoticed until exploited. This highlights the urgent need for proactive security mechanisms, one of the most effective being database security audits. These audits provide a systematic process to examine and evaluate database systems for weaknesses, misconfigurations, unauthorized access, and non-compliance with security policies. Security audits are not merely reactive tools but play a preventative role in identifying potential threats before they materialize. By regularly auditing database activities, user roles, access permissions, and system configurations, organizations can strengthen their security posture and ensure compliance with standards such as GDPR, HIPAA, and PCI DSS. This paper explores the importance of database security audits as a proactive defense strategy. It provides a detailed analysis of audit methodologies, tools, and best practices used to detect and mitigate vulnerabilities. The study also includes a review of existing literature, working principles behind effective auditing systems, and practical insights into implementing audits in real-world scenarios. With the growing threat landscape, integrating intelligent and automated auditing processes is essential to maintaining secure and resilient database systems.

1.1The Importance of Database Security in the Digital Age

As businesses, governments, and individuals generate vast amounts of data, databases have become critical repositories for storing sensitive information. From financial records to personal data and intellectual property, databases house the backbone of operations in nearly every sector. In the digital age, where data is often considered the new currency, the security of these databases is paramount. A single breach or vulnerability can compromise the integrity, confidentiality, and availability of information, leading to devastating consequences. As such, organizations must recognize that ensuring the security of their databases is not just a technical requirement but a strategic imperative. The increasing sophistication of cyber-attacks, alongside the rise of more complex database environments (cloud-based, hybrid systems, etc.), further underscores the need for robust and dynamic security measures.

1.2 Challenges in Database Security

Despite advances in security technologies, databases remain vulnerable to a variety of cyber threats. Common challenges include the exploitation of weak access controls, outdated

software versions, and misconfigured security settings. Insider threats, whether intentional or unintentional, also pose significant risks, as unauthorized users may gain access to sensitive data. Additionally, as databases grow in size and complexity, managing their security becomes an increasingly difficult task. With cloud computing and the integration of third-party services, organizations face new security challenges related to data storage, access, and governance. These vulnerabilities are exacerbated by the rapid pace at which cybercriminals evolve their tactics, constantly seeking new weaknesses to exploit. Without effective security mechanisms in place, databases remain at risk of being compromised.

1.3 Role of Database Security Audits

To address these challenges, database security audits provide a systematic and proactive approach to identifying and mitigating potential vulnerabilities. Security audits involve a comprehensive review of the database's configuration, access controls, user privileges, data integrity, and compliance with established security policies. These audits are designed to uncover gaps in security measures before they can be exploited. By leveraging automated audit tools, security specialists can identify weaknesses such as excessive user privileges, poorly configured firewalls, or outdated patches that may leave databases exposed. Additionally, regular security audits help organizations stay aligned with industry standards and regulatory requirements, ensuring that they not only protect data but also avoid legal and financial penalties associated with non-compliance.

1.4 Impact of Data Breaches and Security Failures

The consequences of a database breach or security failure are far-reaching and multifaceted. Financially, the immediate costs can include expenses related to breach containment, recovery, and legal liabilities. For example, organizations may face significant fines for failing to comply with data protection regulations such as GDPR or HIPAA. Beyond direct financial impact, data breaches can severely damage an organization's reputation, eroding customer trust and loyalty. In an era where consumers are more aware of data privacy concerns, losing the confidence of customers can be detrimental to long-term business success. Moreover, security failures can have legal ramifications, especially if sensitive data is exposed or mishandled. Lawsuits, regulatory investigations, and damage to shareholder value can further compound the fallout from such incidents. As these risks continue to grow, preventing breaches through proactive database security measures becomes not just a necessity but a critical business function.

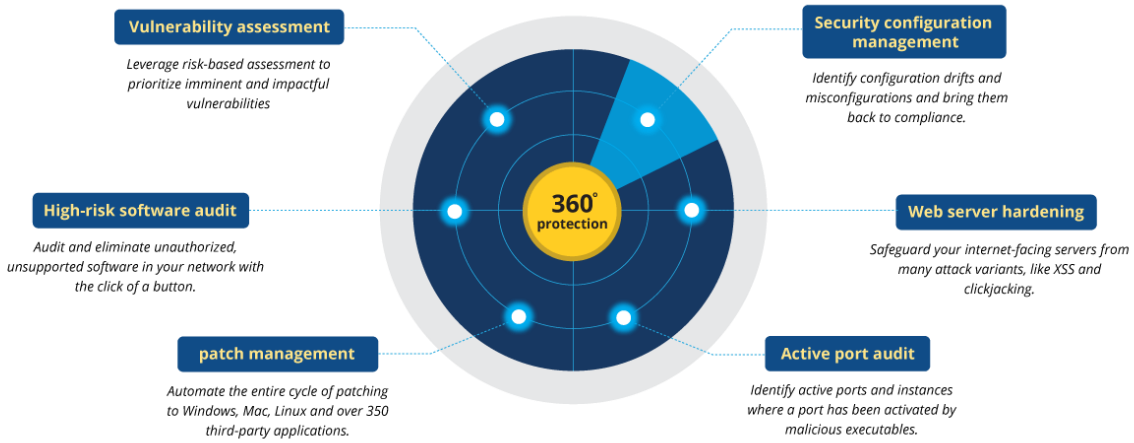

Figure1:Impact of Data Breaches and Security Failures

II. LITERATURE REVIEW

Database security has been a key focus of research for decades due to the increasing complexity of cyber threats targeting sensitive information. Early studies primarily concentrated on access control mechanisms, such as role-based access control (RBAC), and the encryption of data at rest and in transit to protect against unauthorized access. However, as database environments became more intricate, newer techniques emerged, focusing on real-time monitoring, anomaly detection, and database activity monitoring (DAM). These methods aim to identify and respond to threats dynamically. Significant progress has also been made in the development of automated database security audit tools, such as DB-SAT, which evaluate database configurations for vulnerabilities and provide recommendations for remediation. Many studies emphasize the importance of vulnerability management frameworks, where vulnerabilities are categorized and prioritized based on risk severity.

Comparative studies have highlighted the trade-offs between commercial tools like IBM Guardium and open-source solutions like Sqlmap, showing that the choice of tool often depends on the scale and complexity of the database environment. However, existing research often overlooks emerging technologies such as cloud databases, which present new challenges for traditional auditing techniques. Additionally, there is limited exploration into leveraging AI and machine learning to improve vulnerability detection and automate the auditing process, indicating a significant area for future research.

2.1 Overview of Existing Database Security Techniques

Database security techniques have evolved significantly in recent years to address the increasing sophistication of cyber

threats. Traditional methods of securing databases primarily focused on access control, encryption, and firewalls to protect against unauthorized access. Access control mechanisms, such as role-based access control (RBAC), have been fundamental in restricting user permissions and ensuring that individuals only have access to data necessary for their tasks. Additionally, encryption has been widely used to safeguard data both at rest and in transit, ensuring that even if attackers gain unauthorized access, the data remains unreadable. Firewalls and intrusion detection systems (IDS) are employed to monitor and prevent unauthorized database queries and attacks. However, as databases grow in complexity and scale, these traditional methods are increasingly complemented by more advanced security techniques, such as anomaly detection, machine learning-based threat detection, and continuous security monitoring. Additionally, with the rise of cloud computing and distributed databases, techniques such as multi-factor authentication (MFA) and database activity monitoring (DAM) have become integral components in safeguarding data. These methods aim to detect malicious activities in real-time and provide automated responses to mitigate potential threats.

2.2 Previous Work on Security Audits and Vulnerability Management

Security audits have long been recognized as essential tools for identifying and mitigating database vulnerabilities. A significant body of research has focused on developing automated and semi-automated auditing techniques to assess database security. Many studies have explored the use of automated security auditing tools, such as DB-SAT (Database Security Audit Tool), which can perform extensive scans of database configurations and identify potential vulnerabilities. Researchers have also investigated vulnerability management frameworks that provide a structured approach to identifying, classifying, and addressing security flaws. These frameworks typically follow a risk-based methodology, where vulnerabilities are prioritized based on their severity and potential impact. Furthermore, there has been significant work in understanding how security audits can be integrated with other IT governance and compliance frameworks, ensuring that organizations meet regulatory requirements such as GDPR, PCI DSS, and HIPAA. Despite advancements, challenges persist in ensuring the effectiveness and comprehensiveness of security audits, especially in large and dynamic database environments where manual audits can be time-consuming and error-prone.

2.3 Comparative Study of Security Tools and Methodologies

A comparative analysis of security tools and methodologies offers valuable insights into their strengths and weaknesses. Various security auditing tools have been developed, each with different features, capabilities, and suitability for specific database environments. For example, open-source tools like Sqlmap and commercial tools such as Oracle Database Vault and IBM Guardium are frequently compared in terms of their ability to detect vulnerabilities, their ease of integration with existing systems, and their scalability. Studies have shown that while commercial tools often provide robust features and support for complex environments, open-source tools can be more cost-effective and customizable for smaller organizations or specialized use cases. Additionally, methodologies for security audits can vary significantly. Some approaches focus on static analysis, which involves examining the database system configuration, while others emphasize dynamic analysis, such as real-time monitoring and behavior analysis. Comparative studies have found that combining both static and dynamic auditing techniques offers the best protection, as it provides both preventative and responsive security measures. However, the choice of tool or methodology often depends on the specific needs of the organization, including database size, complexity, budget, and compliance requirements.

Figure 2: Comparative Study of Security Tools and Methodologies

2.4 Gap Analysis in Current Research

While much progress has been made in the field of database security and auditing, several gaps in current research remain. A key challenge is the integration of security auditing with emerging technologies such as cloud databases, hybrid systems, and AI-driven environments. Many existing auditing tools and techniques were designed with traditional on-premise databases in mind and may not be fully effective in cloud or hybrid environments, where database instances are distributed and managed by third parties. Moreover, although security audits provide valuable insights into vulnerabilities, they still rely heavily on manual configurations and human interpretation, leading to the potential for missed vulnerabilities or false positives. There is also a need for more advanced techniques to assess the security of non-relational databases, such as NoSQL databases, which present unique challenges due to their schema-less nature and distributed architecture. Additionally, there is a lack of research on the integration of machine learning and artificial intelligence in security audits, especially for automating the detection of complex threats and predicting potential vulnerabilities before they are exploited. Lastly, while current research addresses known vulnerabilities, there is insufficient focus on emerging threats, such as zero-day exploits and

insider threats, which require innovative approaches to detection and prevention.

III. WORKING PRINCIPLES

The working principles behind database security audits are rooted in a structured and systematic approach to identifying and mitigating vulnerabilities within database systems. At its core, a database security audit involves several key processes: assessment, detection, analysis, and remediation. The first step in any security audit is the assessment of the database's configuration, including user roles, access permissions, encryption settings, and compliance with security standards. This phase aims to create a baseline understanding of the database's current security posture. Once the assessment is complete, detection mechanisms, such as automated vulnerability scanners and audit logs, are employed to identify potential security gaps. These tools search for common vulnerabilities, such as excessive user privileges, misconfigured access controls, and outdated patches, which are often entry points for cyber-attacks. Following detection, the analysis phase evaluates the impact and risk of identified vulnerabilities, prioritizing them based on severity. This is often supported by risk management frameworks that classify vulnerabilities into categories such as high, medium, or low risk, helping organizations allocate resources more effectively. Finally, remediation involves applying security patches, adjusting configurations, and strengthening access controls to eliminate vulnerabilities and prevent future threats. In more advanced systems, real-time monitoring and behavioral analysis are also integral principles. These principles enable continuous tracking of database activities, allowing for the detection of abnormal patterns that might indicate a security breach or unauthorized access. Furthermore, as databases become increasingly complex, integrating artificial intelligence and machine learning into auditing systems is becoming a common practice, enabling predictive threat detection and automated remediation.

3.1 Architecture of a Security Audit System

The architecture of a security audit system is designed to facilitate a comprehensive and continuous evaluation of database security. Typically, it consists of several key components: the data collection layer, the analysis layer, the reporting layer, and the remediation layer. The data collection layer gathers all relevant information, such as system logs, database configurations, user access patterns, and historical activities. This data can be sourced from database management systems (DBMS), operating systems, firewalls, and other network devices. Once the data is collected, the analysis layer applies various tools and algorithms to detect vulnerabilities and anomalous activities. This layer uses predefined security rules, pattern recognition, and sometimes machine learning to flag potential threats or non-compliance with best practices. The reporting layer processes the findings from the analysis layer, providing clear, actionable reports that highlight vulnerabilities, weaknesses, and security gaps, often with severity ratings. Finally, the remediation layer provides automated or manual actions to fix detected vulnerabilities. This might involve patching, configuration changes, or recommendations for improving database access controls. A well-integrated audit system is often capable of continuous real-time monitoring, offering insights and alerts on emerging threats while maintaining historical data for comprehensive long-term analysis.

3.2 Vulnerability Detection Techniques

Vulnerability detection is a critical component of database security audits. Various techniques are employed to identify potential security flaws within the database systems. One common method is static analysis, which involves reviewing the database configuration, schema, and access permissions without interacting with the live system. This method often uncovers issues such as overly permissive user privileges, weak password policies, or missing encryption settings. Dynamic analysis, on the other hand, involves actively testing the database while it's running to identify vulnerabilities in real time. This technique can detect issues such as SQL injection flaws, session hijacking risks, and misconfigured network settings. Another advanced technique gaining prominence is behavioral analysis, where patterns of database activity are monitored continuously to detect anomalous behavior that could indicate a breach. For example, if a user accesses sensitive data they don't typically interact with, it could signal an attack. Furthermore, vulnerability scanners, like Nessus or OpenVAS, can be used to scan for known vulnerabilities, cross-referencing them against databases of recognized exploits. Finally, machine learning algorithms are increasingly integrated into security audits, enabling systems to learn from historical data and predict potential vulnerabilities based on evolving patterns of attacks

3.3 Logging and Monitoring Mechanisms

Logging and monitoring mechanisms are fundamental to the detection and prevention of security breaches in database systems. Logging involves capturing and recording all user activities and system interactions with the database, such as login attempts, data modifications, and access to sensitive records. Logs provide a historical record that can be used for later analysis in case of suspicious activity. To ensure the integrity of logs, it is essential that they are securely stored and protected from tampering, often through mechanisms like cryptographic hashing or writing to immutable storage. On the other hand, monitoring mechanisms involve real-time observation of database activities. Tools such as Database Activity Monitoring (DAM) and Intrusion Detection Systems (IDS) continuously track queries, transactions, and system interactions to detect abnormal behavior. For example, if a user queries a large volume of sensitive data within a short time frame, or attempts actions outside of their usual activities, this could trigger an alert. Effective monitoring tools often include alerting systems, which notify administrators of suspicious activity, enabling rapid investigation and response. Monitoring can also be used to ensure compliance with regulatory standards, as real-time data feeds enable immediate visibility into unauthorized access or system failures.

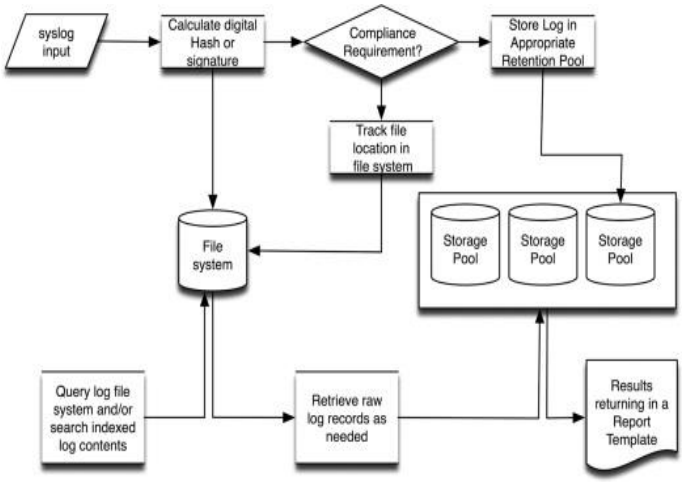

Figure 3: Logging and Monitoring Mechanism

3.4 Remediation and Patch Management Strategies

Remediation and patch management are essential processes for maintaining database security by addressing identified vulnerabilities and mitigating potential threats. Remediation typically refers to the actions taken to correct detected security weaknesses, such as altering database configurations, tightening user access controls, or deploying software patches. Automated remediation tools can assist in quickly addressing common issues, such as missing updates or insecure user privileges, by applying pre-defined actions based on audit findings. However, not all issues can be resolved automatically, so some remediation efforts may require manual intervention, such as reviewing complex security configurations or implementing customized fixes. Patch management focuses on ensuring that database systems and related software are regularly updated with the latest security patches. Many vulnerabilities, especially those exploited in high-profile attacks, arise due to unpatched software. Effective patch management involves maintaining a structured approach for testing, deploying, and validating patches to ensure they do not disrupt normal database operations. This process is often supported by tools like Windows Server Update Services (WSUS) or Red Hat Satellite, which automate the distribution of patches across systems. Patch management strategies also include planning for emergency patches in response to zero-day vulnerabilities, ensuring that critical patches are applied promptly to minimize exposure.

3.5 Integration with Compliance and Regulatory Standards

Integration with compliance and regulatory standards is a key aspect of a database security audit, ensuring that an organization meets legal and industry-specific requirements for data protection and privacy. Many organizations are subject to regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS), which mandate specific security controls for databases handling sensitive information. A security audit system integrates these standards by assessing whether a database is configured to comply with the rules outlined in each regulation. For example, GDPR requires databases to implement measures for data encryption, data access control, and audit trails for user activities. Security audit systems typically include pre-built compliance checklists and frameworks to automate the validation of regulatory compliance, helping organizations avoid costly fines and reputational damage. Integration with regulatory standards can also involve reporting mechanisms that provide clear evidence of compliance during audits or inspections by regulatory bodies. Moreover, these audits often generate reports that provide detailed explanations of where the system is compliant or where improvements are necessary. The evolving nature of regulations makes it essential to have a dynamic security audit system that can adapt to new legal requirements and ensure continuous compliance.

IV. CONCLUSION

In conclusion, database security is a critical aspect of protecting sensitive information in an increasingly complex digital landscape. As cyber threats evolve, organizations must adopt robust and proactive security measures to defend their databases against unauthorized access, breaches, and other malicious activities. Security audits play an essential role in identifying vulnerabilities before they can be exploited, ensuring that potential risks are mitigated and the integrity of data is maintained. Regular audits provide a comprehensive view of the database's security posture and help maintain compliance with industry regulations. By continually assessing database systems and updating security protocols, organizations can stay ahead of emerging threats and safeguard their data from unauthorized access. This paper examined the significance of database security audits, highlighting their essential role in detecting vulnerabilities, securing sensitive data, and maintaining compliance with regulatory standards. The findings revealed that database security is a multifaceted issue, with various detection techniques, such as static and dynamic analysis, behavior monitoring, and vulnerability scanning, being crucial for identifying risks. Additionally, the research emphasized that a well-structured security audit system, with components like real-time monitoring, logging, and automated remediation, is vital for ongoing protection. Another key takeaway is the necessity of patch management and the integration of security audits with regulatory compliance standards to ensure that database systems remain secure and meet legal requirements. The paper also identified gaps in current research, such as the need for more effective auditing methods for cloud-based and non-relational databases, and the potential for machine learning and AI to enhance threat detection and vulnerability management.

Regular security audits are indispensable for organizations seeking to protect their critical data and maintain a resilient security posture. As enterprises increasingly rely on databases for storing and processing vast amounts of sensitive information, regular audits help identify weaknesses before they can be exploited by cybercriminals. These audits are especially crucial in preventing data breaches, which can lead

to severe financial losses, legal consequences, and reputational damage. Security audits also help organizations stay compliant with industry regulations and standards, ensuring they avoid costly penalties. Furthermore, regular audits provide enterprises with a clear understanding of their database's security health, enabling proactive measures such as patching, configuration adjustments, and user access control updates. They also offer valuable insights for improving database architecture and developing more robust security policies. In an era of rapidly evolving cyber threats, adopting a continuous, audit-driven security strategy is essential to ensuring long-term protection.

For practitioners involved in database security, several key takeaways emerge from this study. First, the importance of integrating automated security auditing tools into database management practices cannot be overstated. Automation reduces the manual effort required for regular audits, ensures comprehensive coverage, and minimizes human error. Second, real-time monitoring and anomaly detection are essential in identifying potential threats before they escalate, allowing for quicker response times and mitigations. Practitioners should also be aware of the significance of patch management; ensuring that all software is up-to-date is a fundamental aspect of protecting against known vulnerabilities. Moreover, it is critical to integrate auditing tools with regulatory compliance frameworks, as this helps organizations meet the required standards and avoid penalties. Finally, continuous education and staying abreast of new technologies, such as AI and machine learning, are necessary for enhancing database security practices and improving the efficacy of security audits. Overall, practitioners must view database security audits as an ongoing process, not a one-time task, to ensure the protection of sensitive data and the resilience of their systems.

V. FUTURE ENHANCEMENT

As database environments continue to evolve and become more complex, the future of database security audits lies in integrating advanced technologies that can streamline and enhance the effectiveness of vulnerability detection, monitoring, and remediation. These innovations aim to address the growing scale and sophistication of security threats while making the audit process more efficient and proactive. The following sections outline potential future enhancements in the field of database security audits. Artificial intelligence (AI) is poised to transform the landscape of database security audits by enabling more efficient and accurate detection of vulnerabilities and threats. AI-driven security audits use advanced algorithms to analyze vast amounts of database activity data, identifying patterns and anomalies that may signal potential security risks. Unlike traditional auditing techniques that rely on predefined rules and signatures, AI can learn from historical data and adapt to new attack strategies in real time. Machine learning models can continuously improve as they process more data, enhancing the detection of both known and unknown vulnerabilities. These AI systems can also automatically prioritize the most critical vulnerabilities, helping security teams focus on the most pressing issues first. Additionally, AI can assist in automating the audit process, reducing the need for human intervention and ensuring faster responses to potential security threats. AI-driven security audits hold great promise for transforming the speed, accuracy, and scalability of database security assessments.

The future of database security auditing will see greater reliance on automation to streamline the vulnerability scanning process and provide continuous protection. Automated vulnerability scanning involves using advanced tools to continuously scan databases for potential weaknesses, such as outdated software versions, misconfigured access controls, or exposed sensitive data. Automation reduces the reliance on manual processes, significantly improving efficiency and ensuring that vulnerabilities are detected as soon as they arise. By integrating real-time vulnerability scanning with database monitoring systems, organizations can quickly identify and address security issues as they occur, rather than relying on periodic audits. This automated approach not only saves time and resources but also improves the accuracy of scans, as automated systems can detect subtle, hard-to-spot vulnerabilities that human auditors might overlook. Furthermore, real-time scanning can help organizations comply with evolving security standards by continuously monitoring the database's security posture and triggering alerts when deviations from security policies are detected.

As businesses increasingly move to cloud environments and adopt hybrid database models, ensuring security in these decentralized, distributed environments is becoming more challenging. Future security audit systems will need to offer enhanced integration with cloud and hybrid databases, ensuring that security policies and protocols are consistently applied across diverse infrastructure. Cloud-based databases, such as Amazon RDS or Google Cloud SQL, often involve third-party providers managing certain aspects of the security infrastructure, which can lead to gaps in visibility and control. Future advancements in security audits will focus on providing centralized, automated audit capabilities across cloud, on-premise, and hybrid environments. This integration will allow organizations to apply consistent security practices, such as access controls, encryption, and vulnerability assessments, regardless of where their databases are hosted. By creating unified security audit systems that can span cloud, hybrid, and on-premise architectures, organizations can ensure comprehensive protection across all their data assets and comply with industry standards more effectively.

One of the most promising advancements in database security audits is the integration of predictive threat analysis using machine learning (ML). While traditional security audits focus on identifying and mitigating existing vulnerabilities, predictive threat analysis leverages historical data and ML algorithms to anticipate future attacks and vulnerabilities before they occur. By analyzing trends in past database breaches, attack vectors, and system behaviors, machine learning models can detect patterns that indicate

emerging threats. For example, an ML model might recognize early warning signs of a SQL injection attack or insider threat, based on irregular database query patterns or anomalous user behaviors. These predictive models can help organizations proactively reinforce their security measures, patch vulnerabilities before they are exploited, and allocate resources more effectively. The use of ML in predictive threat analysis enables more proactive, rather than reactive, security, improving the overall resilience of database systems. As the technology matures, predictive analytics will play a key role in anticipating complex, sophisticated attacks and securing databases in an increasingly dynamic threat landscape.

REFERENCES

[1]. Bertino, E., Sandhu, R., & Sandhu, R. (2011). *Database Security: Concepts, Approaches, and Challenges*. *IEEE Transactions on Dependable and Secure Computing*, 8(4), 698–701. DOI: 10.1109/TDSC.2011.64

[2]. Kennesaw, J., & McLeod, D. (2012). *A Survey on Database Security and Auditing Techniques*. *International Journal of Computer Applications*, 42(9), 1–7. DOI: 10.5120/7170-0301

[3]. Gollmann, D. (2011). *Computer Security* (3rd ed.). Wiley-IEEE Press. ISBN: 978-1119942175

[4]. Jajodia, S., Bertino, E., Sandhu, R., & Wijesekera, D. (2002). *Database Security: Research and Practice*. Springer Science & Business Media. ISBN: 978-1461351604

[5]. Liu, L., & Sandhu, R. (2011). *Database Security: Challenges and Opportunities*. *International Journal of Information Security*, 10(3), 97–114. DOI: 10.1007/s10207-010-0100-3

[6]. Tuch, S., & Tesch, M. (2014). *Automated Database Security Auditing*. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (pp. 195–206). DOI: 10.1145/2556549.2556557

[7]. Maccari, A., & D'Alessandro, M. (2013). *Automated Database Security Auditing: A Review of Tools and Techniques*. *Journal of Computer Security*, 21(2), 171–208. DOI: 10.3233/JCS-130522

[8]. Bertino, E., Sandhu, R., & Sandhu, R. (2010). *Security and Privacy in Database Management Systems*. *Springer*, pp. 33–62. ISBN: 978-1441966871

[9]. Sharma, M., & Sharma, V. (2015). *Database Security Auditing Techniques: A Survey*. *International Journal of Computer Science and Network Security*, 15(5), 1–8.

[10]. Liu, H., & Zhang, H. (2014). *Security Audits and Their Impact on Database Vulnerabilities.* In *Proceedings of the 2014 International Conference on Information Security and Privacy* (pp. 256–263). DOI: 10.1109/ISP.2014.23