Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Bachelor Thesis

Network monitoring, implementation of security systems in the company

Abbas Badoudam

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Abbas Badoudam

Informatics

Thesis title

Network monitoring, implementation of security systems in the company

Objectives of thesis

The objective of this thesis is to analyze the effectiveness of database activity monitoring tools in detecting security threats and vulnerabilities in company database systems.

Methodology

This thesis will adopt a systematic review approach to analyze the existing literature on the effectiveness of database activity monitoring (DAM) tools in detecting security threats and vulnerabilities in company database systems. The following steps will be taken to conduct the systematic review: first, the research design will be a systematic review of the literature on database activity monitoring tools in detecting security threats and vulnerabilities. This approach will involve a structured process for searching, selecting, and analyzing relevant literature. Then, the search strategy will involve searching electronic databases such as Scopus, Web of Science, and IEEE Xplore. The following keywords will be used in the search: ”database activity monitoring,” ”database security,” ”vulnerability detection,” ”security threats,” and ”security breaches.” Inclusion criteria will be studies published in peer-reviewed journals and conference proceedings from 2015 to 2023 that evaluate the effectiveness of DAM tools in detecting security threats and vulnerabilities. The findings from the literature will be synthesized to develop a conceptual framework summarizing the key themes and trends related to the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems. By utilizing a systematic review approach, this study aims to provide an extensive analysis of the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems.

The proposed extent of the thesis

35-45p.

Keywords

Database activity monitoring; Security threats; Database security; Threat detection; Network monitoring

Recommended information sources

Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics, 6(1), 1-11.

Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), 3587-3608.

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1-48.

Sarmah, S. S. (2019). Database Security–Threats & Prevention. International Journal of Computer Trends and Technology, 67(5), 46-53.

Teymourlouei, H., & Harris, V. E. (2020, December). Effectiveness of Real-Time Network Monitoring For Identifying Hidden Vulnerabilities inside a System. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 43-48). IEEE.

Tsai, P. W., Tsai, C. W., Hsu, C. W., & Yang, C. S. (2018). Network monitoring in software-defined networking: A review. IEEE Systems Journal, 12(4), 3958-3969.

Expected date of thesis defence

2023/24 SS – PEF

The Bachelor Thesis Supervisor

Ing. Martin Havránek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 24. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 04. 03. 2024

Declaration

I declare that I have worked on my bachelor thesis titled " **Network monitoring, implementation of security systems in the company**" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 11.03.2024 ______________________________

Acknowledgement

I would like to seize this moment to convey my heartfelt gratitude to all the esteemed faculty members of the department for their unwavering assistance and support throughout the course of my study. Furthermore, I extend my sincerest appreciation and respect to my esteemed thesis supervisor, Ing. Martin Havránek, Ph.D., for his invaluable guidance and unwavering support, which were instrumental in the successful completion of my thesis. Lastly, I am deeply grateful to my wife, Zohreh, for her unwavering support and encouragement throughout this journey.

Network monitoring, implementation of security systems in the company

Abstract

The objective of this thesis is to analyse the effectiveness of database activity monitoring (DAM) tools in detecting security threats and vulnerabilities in company database systems. The thesis conducted a systematic review of literature from 2015 to 2023. The PRISMA guidelines were followed to ensure methodological transparency and rigor. The study identified 25 papers that met the inclusion criteria. The findings revealed that DAM tools can detect various security threats that compromise company database systems' confidentiality, integrity, and availability. These threats included unauthorized access and data breaches, SQL injection attacks. The study explored various DAM tools, focusing on IBM Guardium, Imperva's Secure Sphere, Oracle Audit Vault, and Database Firewall. These tools offered features like data protection and access control, real-time monitoring and alerting, security policy and compliance. Their real-time protection was crucial for immediate response to emerging security threats. The study concluded that DAM tools are effective in real-world security scenarios, providing valuable insights for organizations to strengthen their database systems against evolving threats.

Keywords: Database activity monitoring; Security threats; Database security; Threat detection; Network monitoring

Dohlédnutí nad sítí, implementace bezpečnostních systémů ve společnosti

Abstrakt

Cílem této práce je analyzovat účinnost nástrojů pro sledování aktivity databází (DAM) při detekci bezpečnostních hrozeb a zranitelností v databázových systémech společnosti. Práce provedla systematický přehled literatury z let 2015 až 2023. Byly dodrženy pokyny PRISMA, aby byla zajištěna metodologická transparentnost a rigoróznost. Studie identifikovala 25 článků, které splňovaly kritéria pro zařazení. Zjištění ukázala, že nástroje DAM mohou detekovat různé bezpečnostní hrozby, které ohrožují důvěrnost, integritu a dostupnost databázových systémů společnosti. Mezi tyto hrozby patřily neoprávněný přístup a úniky dat, útoky SQL injection. Studie prozkoumala různé nástroje DAM, zaměřila se na IBM Guardium, Secure Sphere od společnosti Imperva, Oracle Audit Vault a Database Firewall. Tyto nástroje nabízely funkce jako ochranu dat a kontrolu přístupu, monitorování a upozorňování v reálném čase, bezpečnostní politiku a dodržování předpisů. Jejich ochrana v reálném čase byla klíčová pro okamžitou reakci na vznikající bezpečnostní hrozby. Studie dospěla k závěru, že nástroje DAM jsou účinné v reálných bezpečnostních scénářích a poskytují cenné poznatky pro organizace, jak posílit své databázové systémy proti se vyvíjejícím hrozbám.

Klíčová slova: Sledování aktivity databází; Bezpečnostní hrozby; Bezpečnost databází; Detekce hrozeb; Sledování sítě

Table of content

1 Introduction

In today's digital landscape, businesses consider data the lifeblood of their operations, relying extensively on databases to store and manage sensitive information. The escalating pace of cyber threats necessitates robust measures to safeguard these databases (Ingole, 2023). Databases serve as the cornerstone of organizational IT infrastructure, and many organizations employ real-time database activity monitoring (DAM) systems for data security, privacy protection, and data leakage prevention. However, challenges, as highlighted in the multi-billion-dollar Google-Waymo vs. Uber case, reveal the limitations in processing vast amounts of data activity logs and the potential vulnerability of DAM policies to concept drifts (Grushka-Cohen et al. 2019). As a crucial organizational asset, data faces severe threats from insider cyber-attacks, where malicious insiders exploit their credentials to exfiltrate confidential information. Existing security tools, primarily designed for external threats, may prove less effective when insiders with proper credentials are involved in data exfiltration (Sallam et al. 2015). IT security, applied through various methods and techniques, is designed to minimize computer systems' susceptibility to unintentional and deliberate threats (Sarmah, 2019). The primary risks linked with database attacks include threats such as Structured query language (SQL) injection, overuse of privileges, and vulnerabilities like inadequate native audits and exposure of backup data (Sarmah, 2019). DAM has become an essential instrument for database security, ensuring data integrity, confidentiality, and availability. DAM tools, engineered for real-time monitoring, examination, and documentation of database operations, are pivotal in identifying and reducing security threats and vulnerabilities. As organizations aim to monitor and analyze database activity to pinpoint potential threats and vulnerabilities, DAM tools have become vital in implementing security measures (Brodsky, 2015).

The efficacy of DAM tools in real-time monitoring and alerting administrators to suspicious activities, such as unauthorized access attempts, underscores their importance in preventing data breaches and other security incidents (Abdiyeva-Aliyeva, Hematyar, 2022). As study by Sarmah (2019), database security threats include various attacks, such as privilege escalation, SQL injection, and unauthorized access. DAM tools play a significant role in detecting and thwarting these attacks by providing a proactive approach to monitor database activity and alert administrators to suspicious actions. Furthermore, DAM tools play a crucial role in helping companies comply with regulatory standards. For instance, the Data

Security Standard set by the Payment Card Industry mandates the surveillance and auditing of database activity to ensure the safety of credit card information. Monitoring database and file activity across different domains allows organizations to issue alerts when perilous events transpire. Security information and event management (SIEM) and DAM systems contribute to the detection of data misuse, leakage, impersonation, and database system attacks by auditing database activity and applying anomaly detection algorithms (Kaplan, Sharma, Weinberg, 2011). DAM systems generate alerts based on policy violations or anomalous activities, offering vital insights to security officers (Sallam et al. 2015). In the context of DAM, the primary objective is to distinguish standard actions and avert attacks from internal and external sources.

Moreover, DAM facilitates real-time monitoring; rule sets and policies, and the aggregation of database logs without exerting additional loads on the database (Çinar, 2015). This thesis will utilize a systematic review approach to meticulously examine the existing literature on the effectiveness of DAM tools in identifying security threats and vulnerabilities within company database systems. Through a systematic and structured review process, this approach intends to analyse the effectiveness of database activity monitoring tools in detecting security threats and vulnerabilities in company database systems. The structure of the thesis is outlined as follows:

Chapter 1 highlighted the significance of DAM in strengthening database security, Chapter 2 outlined the objectives and methodology, Chapter 3 presented a detailed literature review about database security threats, vulnerabilities, and DAM tools, Chapter 4, which was the practical part, provided an overview of recent studies on database activity monitoring tools. Chapter 5 presented the results and discussion, Chapter 6 concluded the study, and Chapter 7 presented references.

2 Objectives and Methodology

2.1 Objectives

The objective of this thesis is to analyse the effectiveness of database activity monitoring tools in detecting security threats and vulnerabilities in company database systems.

2.2 Methodology

This thesis will adopt a systematic review approach to analyze the existing literature on the effectiveness of database activity monitoring (DAM) tools in detecting security threats and vulnerabilities in company database systems. The following steps will be taken to conduct the systematic review: first, the research design will be a systematic review of the literature on database activity monitoring tools in detecting security threats and vulnerabilities. This approach will involve a structured process for searching, selecting, and analyzing relevant literature. Then, the search strategy will involve searching electronic databases such as Scopus, Web of Science, and IEEE Xplore. The following keywords will be used in the search: "database activity monitoring," "database security," "vulnerability detection," "security threats," and "security breaches." Inclusion criteria will be studies published in peer-reviewed journals and conference proceedings from 2015 to 2023 that evaluate the effectiveness of DAM tools in detecting security threats and vulnerabilities. The findings from the literature will be synthesized to develop a conceptual framework summarizing the key themes and trends related to the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems. By utilizing a systematic review approach, this study aims to provide an extensive analysis of the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems.

3 Literature Review

3.1 Database security threats and vulnerabilities

A range of studies highlighted the significant threats and vulnerabilities facing database security as follows:

Deepika, Prasad, Balamurugan, Charanyaa (2015) conducted a study highlighting the growing concern around data security, evident in the rising number of reported cases involving the loss or exposure of sensitive data by unauthorized sources. Security, as a composite aspect, played a crucial role in safeguarding sensitive data and database management software from unauthorized users or malicious attacks. The paper's objective was to showcase a variety of prevalent data security methods, offering perspectives on tactics that could be employed to bolster and enhance database security against potential threats.

Safianu, Twum, Hayfron-Acquah (2016) conducted a study exploring the risks that end-users presented to system security, highlighting the importance of the human element in information security, even with the progression of technology. The research, which included surveys and experiments such as a simulated phishing system, demonstrated that relying solely on technical solutions did not ensure a secure environment. The results emphasized the need for a comprehensive security approach incorporating the human aspect to prevent information and data breaches effectively. This research provided a significant understanding of the complex nature of threats to database security.

Pevnev, Kapchynskyi (2018) addressed the escalating challenges in database security due to a surge in recorded events and the imperative to safeguard confidential data. The paper explored computer security principles, emphasizing the three structures of database security: data confidentiality, prevention of unauthorized access, and detection of hardware and software failures. Sub-topics included ransomware, weak security, inappropriate database setup, SQL injection, cross-request, and misuse of disproportionate rights. The authors also reviewed data management techniques for securing machine knowledge, offering valuable insights into core threats and preventive measures in database security.

Hashim (2018) highlighted the importance of secure database operations in institutions, emphasizing robust data management to ensure confidentiality, integrity, and continuity. The paper addressed security challenges, proposing solutions such as encryption, system adjustments, and regular updates. The study comprehensively reviewed the top ten database vulnerabilities, including excessive privilege abuse, legitimate privilege abuse, database platform vulnerabilities, SQL injection, weak authentication, denial of service (DOS), database communication protocol vulnerabilities, and backup data exposure. Organizations had to address these threats to meet regulated industries' compliance and risk mitigation requirements.

Mousa, Karabatak, Mustafa (2020) investigated various types of threats and challenges, along with their implications on sensitive data, and presented diverse safety models. The fundamental premise of this study rested on the idea that by comprehending the vulnerabilities, threats, and challenges encountered by databases, database administrators could subsequently formulate an effective security strategy to safeguard their databases. The identified issues encompassed instances of excessive privilege abuse, SQL injection vulnerabilities, inadequately robust audit trails, and weaknesses in authentication mechanisms.

Lawal, Adesoji, Adekunle (2022) emphasized the complexity of securing databases for companies, especially with the growing intricacy of databases, network connections, and internal user additions. The paper identified common threats and vulnerabilities in organizational databases, providing essential security control recommendations. The study defined vulnerabilities as the shortcomings in security measures and threats as the potential dangers to assets. It posited that gaining insights into these elements enabled database administrators to devise efficient security strategies for improved protection.

Gharpure, Rai (2022) underscored the centrality of databases in modern applications and identified vital threats, including SQL injection, weak audit trails, access management issues, and encryption vulnerabilities. The study proposed solutions such as leveraging encryption, primarily through Crypto DB, to protect against breaches. It advocated for enhanced access control norms and recommended preventive measures against SQL injection attacks, providing valuable insights for defending against these database security risks.

Ingole (2023) presented a methodology for bolstering database security, addressing challenges and potential attacks. Key steps included identifying threats, evaluating existing measures, enforcing the least privilege principle, regular updates, security audits, user training, data encryption, activity monitoring, incident response planning, and staying abreast of research. This proactive approach was designed to protect sensitive data amidst a constantly changing threat environment, focusing on the ongoing enhancement of security protocols.

Chakraborty et al. (2022) highlighted the significance of data security challenges in organizations, particularly databases. The study stressed the necessity for a collaborative approach to secure databases involving various organizational components beyond the purview of database administrators. Moreover, they sought to comprehensively examine information security threats, vulnerabilities, and challenges, investigating new technological tools for effective mitigation. Alongside layered security controls across the entire network, establishing appropriate controls and policies for database access was deemed essential for database security. These encompassed administrative controls that governed installation, change, and configuration management, preventive controls overseeing access, encryption, tokenization, and masking, and detective controls that monitored database activity and data loss prevention tools. These measures aided in identifying and alerting on anomalous or suspicious activities.

3.2 Database Activity Monitoring (DAM) Tools

Database Activity Monitoring (DAM) systems were pivotal in safeguarding organizational data, knowledge, and intellectual properties. However, current DAM systems face limitations in examining only a subset of activity due to high-velocity streams and operational costs. They primarily served two functions: monitoring and alerting to aberrant activity (Grushka-Cohen et al. 2020). These tools monitored application and database activity for auditing and generated security alerts based on policy violations. Based on the study by Giribabu et al. (2018), database security refers to the measures used to protect and secure a database from illegitimate use and malicious threats. It included processes, tools, and methodologies that ensured security within a database environment. Database security covered and enforced security on all aspects and components of the database, including data stores, database servers, and database management systems. Some of the ways database security was analyzed and implemented included database activity monitoring. Bašić, Udovičić, Orel et al. (2021) presented a security enhancement subsystem that ensured in-database auditing for enterprise applications. This subsystem aimed to enhance security remediation, compliance reporting, and real-time threat detection by providing comprehensive auditing capabilities directly within the database. The article delved into the subsystem's design, implementation, performance evaluation, and comparisons with existing auditing solutions.

Furthermore, DAM services could issue security alerts when dynamic query elements deviate from security policies. Akhil et al. (2022) scrutinized DAM tools, like IBM Guardium, which effectively identified security threats and vulnerabilities in company database systems, offering visibility, monitoring, and analytics capabilities. Moreover, Bandit algorithms, applied in recommendation systems, could address the challenge of limited sampling in database activity monitoring, ensuring broad population coverage without compromising event detection quality. Alves-Foss et al. (2015) applied DAM at the web application and database levels to help block attacks and detect attack behavior. DAM was implemented to prevent SQL injection attacks by implementing runtime security monitoring and creating behavior-based rule sets. However, the drawback was that these tools could be expensive and might require installation and setup beyond the skill set of the database owner. Korsakova (2016) focused on research assessing Oracle Database Vault compliance with PCI DSS, emphasizing its role in protecting data from internal threats. The study employed a case study method to explore Oracle Database Vault's compliance with PCI DSS and the phased approach to achieve desired results. It provided insights into the security features and methods of Oracle Database Vault, addressing gaps in internal security and controlling privileged user access. Matthew, Dudley (2015) explored how auditing methodologies could augment database activity monitoring. Auditing within a database could expedite identifying and resolving security issues, thereby bolstering the effectiveness of database activity monitoring. Database auditing entailed the surveillance of a database to stay informed about user actions, ensuring that unauthorized parties did not access data. Auditing could aid in identifying issues with authorization or access control implementation, thereby enhancing DAM. Auditing activities fostered accountability for present actions in the future, deterring users and intruders from engaging in inappropriate actions based on that accountability. Additionally, auditing assisted in probing suspicious activity and alerting auditors about actions by unauthorized users, thereby further improving database activity monitoring. The deployment of auditing facilities offered by the database management system (DBMS) was vital for recuperating from attacks and safeguarding the database system's security.

4 Practical part

We constructed and reviewed a database of scientific papers that employed state-of-the-art techniques database activity monitoring tools in detecting security threats and vulnerabilities. over the last 9 years. In the practical part of this study, we followed the PRISMA guidelines to ensure methodological transparency and rigor. Detailed-based software 'Covidence' was applied in this review to extract the relevant studies, following the steps outlined in the PRISMA flow diagram (Fig.1). The review initially identified 182 papers, but 58 were duplicates and were excluded from further consideration. The remaining 124 papers were reviewed in full text. Of these, 99 were excluded because they did not meet the specific inclusion criteria of the review, which focused on studies that evaluated the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems. Finally, 25 papers were included in the analysis of the review.

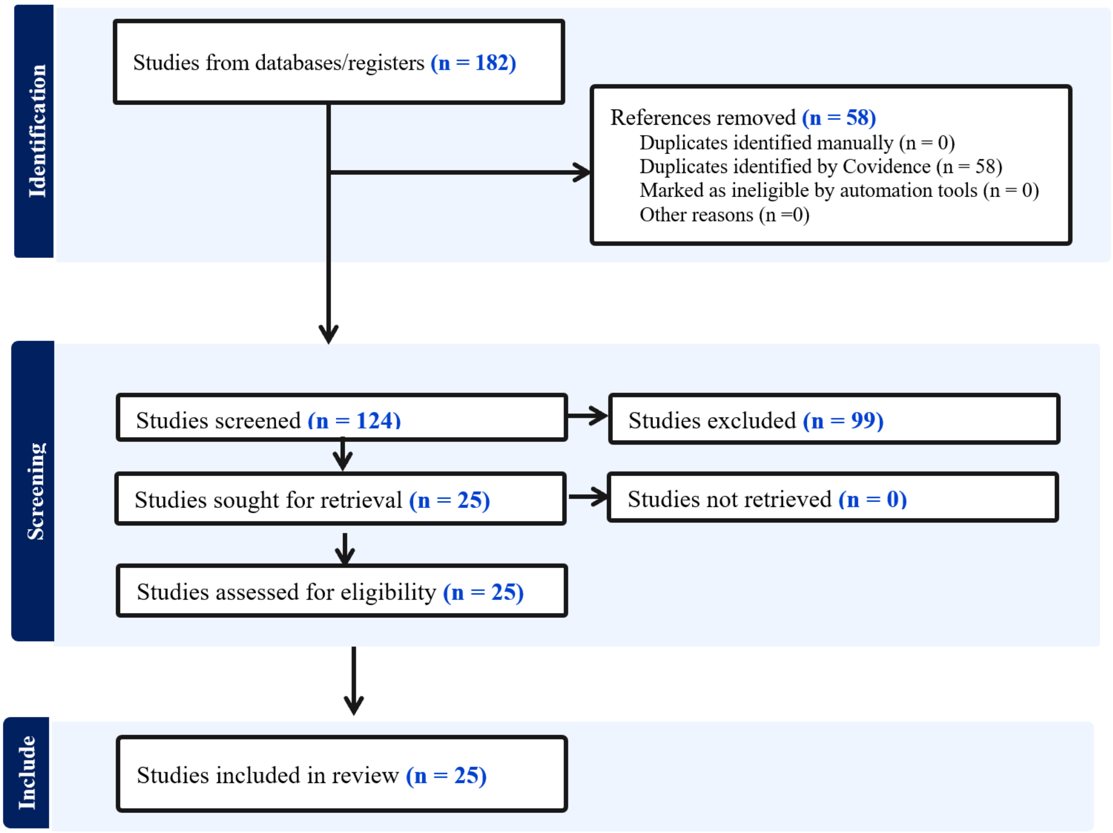
Identification
Studies from databases/registers (n = 182)
References removed (n = 58)
Duplicates identified manually (n = 0)
Duplicates identified by Covidence (n = 58)
Marked as ineligible by automation tools (n = 0)
Other reasons (n =0)
Screening
Studies screened (n = 124)
Studies excluded (n = 99)
Studies sought for retrieval (n = 25)
Studies not retrieved (n = 0)
Studies assessed for eligibility (n = 25)
Include
Studies included in review (n = 25)

Fig. 1 PRISMA-guided systematic review: a visual representation of descriptive steps (Covidence, 2023)

4.1 Capability Assessment and Evaluation of DAM Tools

The practical component of this study involved a detailed examination of DAM tools, aiming to assess their capabilities and evaluate key features critical for effective database security. A comprehensive Capability Assessment was conducted to evaluate the general functionalities of DAM tools. This assessment provided an overview of the features that these tools offer, setting the foundation for effective database security measures (Table 1).

Table 1. Overview of the recent DAM tools studies (2015-2023) (By author)

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
1	IBM Guardium– Database Activity Monitoring	Akhil et al. (2015)	IBM Guardium	- IBM Guardium protected data and monetized databases. - It counted the number of queries and restricted DDL and DML commands. - Sensitive data could be discovered using IBM Guardium and masking policy. - Guardium solution provided threat detection for database activity monitoring.	- Protected sensitive data such as Debit Card, Credit Card, Aadhar, PAN, Passport, Insurance Id's. - Restricted permissions to level 1 and level 2 employees. - Masked data with special characters and showed the last four digits. - Restricted DDL and DML commands in a database.
2	Security methods and how they are applied in oracle products	Korsakova (2015)	ORACLE Audit Vault Server and Database Firewall	- Oracle Database Vault implemented the separation of duties concept to prevent unauthorized administrative actions. - Oracle Database Vault complied with certain requirements of the PCI DSS. - The paper presented a list of requirements that Oracle Database Vault complied with.	- Monitored and analyzed in real-time. - Did not rely on native auditing or native logs. - Could perform continuous monitoring and alerting. - Could also block unauthorized activities.
3	Database security in private database clouds	Çinar (2015)	IBM Guardium IMPERVA Secure Sphere ORACLE Audit Vault Server and Database Firewall	- Two types of DAM solutions studied: SIEM tools and agent-based solutions. - Agent-based solutions collected logs from network logs and database listeners. - Agent-based solutions had disadvantages on host performance but do not interfere with database business process. - Encryption approach considered for effective and secure monitoring against internal and external attacks.	- Enabled the use of transactions on data transferring. - Collected logs from network logs and database listeners. - Ran separately from the database to avoid interfering with business processes. - Acted when a policy violation was detected.

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
4	Eagle: User Profile-based Anomaly Detection for Securing Hadoop Clusters	Gupta (2015)	IMPERVA Secure Sphere	- Imperva was a mature product that supported DAM by setting up rules and policies, but it lacked support for Hadoop. There was a need to develop a system for user activity monitoring that could detect anomalous user actions and protect the Hadoop cluster. - They developed Eagle, which was a highly scalable system capable of monitoring.	- Configurable thresholds for parameters were configured to raise alarms for specific activities. - Support was provided for monitoring and tracking user actions in the database. - An ability to detect anomalies in SQL queries and patterns used by users was present. - Integration with other security measures and access control policies was ensured.
5	DBSAFE—An Anomaly Detection System to Protect Databases from Exfiltration Attempts	Sallam et al. (2015)	IBM Guardium	- The proposed techniques were effective in detecting anomalies in database access. The system used these profiles to detect anomalous behavior that deviated from normality. - DBSAFE architecture provided a scalable system for learning patterns of behavior in database interactions. - The paper provided details on the formulation of the problem and techniques for using the classifiers.	- Ability to monitor different commercial RDBMSs and integrate with SIEM systems. - Good run-time performance to minimize impact on query processing times. - Ability to monitor different types of data access and variations in data access patterns.
6	Critical assessment of auditing contributions to effective and efficient security in database systems	Matthew, Dudley (2015)	N/A	- Outlines main auditing techniques and methods. - Highlighted the impacts of auditing on security and compliance with regulations. - Developing Database Audit and Protection (DAP) to provide better auditing and monitoring support than native logging in comparing DAM	- Auditing and monitoring

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
7	Database Security – Threats & Prevention	Sarmah (2019)	N/A	- Protocol validation technology can help detect vulnerabilities in database communication. - Prevention of Denial-of-Service attacks through various protections. - Regular application of security patches and security vulnerability checks. - Detecting security breaches including theft of hard disks and database backup tapes by different methods such as DAM are discussed.	- Real-time monitoring of database activity - Detection of unusual access behaviors and SQL injection attacks - Alerting for unauthorized changes to financial data and increased privilege levels - Application layer monitoring for fraud detection in multi-tiered applications
8	Diversifying Database Activity Monitoring with Bandits	Grushka-Cohen et al. (2020)	N/A	- Diversity in sampling activity enhances understanding of user behavior and anomaly detection. - C-Greedy sampling strategy outperformed all other strategies in terms of reward and recall metrics. - Random sampling consistently resulted in the poorest performance.	- Data security, privacy protection, and data leakage prevention. - Help implement security policies and detect attacks and data abuse. - Monitor database operations in real-time. - Use policies to decide which transactions to save based on rules and user activity groups. - Consider contextual information such as time of day, user activity profile, location, data sensitivity, and data volume
9	Database activity monitoring (dam): understanding and configuring basic network monitoring using Imperva's Secure Sphere	Brodsky (2015)	Imperva's Secure Sphere	- Implementation of network-based monitoring, particularly with tools like Imperva's Secure Sphere DAM, can lead to enhanced security for consolidated and sensitive databases. - Network-based monitoring allows for the real-time monitoring of user activity, facilitating the early detection of potential security threats or unauthorized access.	- Network-Based Monitoring - Importing Digital Certificates or Encryption Keys - Integrating with SIEM tools.

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
10	Database as a service: security and privacy issues, and appropriate controls	Akinde (2020)	Oracle Audit Vault Server and Database Firewall	- The identified security and privacy issues were discussed along with their consequences, and the impacts on security purposes were demonstrated. - Security controls provided by three vendors (Amazon, Microsoft Azure, and Oracle) were mapped with the identified issues to aid in the creation of security controls to mitigate risks.	- Real-time monitoring, anomaly detection, and alerting. - The capability to encrypt data. - User and Multifactor Access Control - Data masking
11	Review Paper on Dynamic Mechanisms of Data Leakage Detection and Prevention	Shivakumara, Patil, Muneshwara (2019)	IBM Guardium	- The development of automation solutions for self-defensive capabilities is proposed. - The risks of data loss and data leakage in organizations is highlighted. - DAM as a database security technology for monitoring and analyzing database activity that operates independently of the DBMS is discussed.	- Monitoring and analyzing database activity continuously and in real-time. - Generating real-time sensitive data alerts. - Helping detect and prevent unauthorized attempts to copy or send sensitive data.
12	Database security in private database clouds	Çinar et al. (2016)	Oracle Audit Vault Server and Database Firewall	- The paper presented a prototype implementation of a private database security cloud using InfoFence. - The proposed system had better performance results compared to Oracle Audit Vault Server. - The system supported multiple databases and languages.	- Real-time monitoring of database activities - Enhanced security measures for protecting database logs and information

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
13	Simulating User Activity for Assessing Effect of Sampling on DB Activity Monitoring Anomaly Detection	Grushka-Cohen et al. (2019)	IBM Guardium	- The results indicated that effective anomaly detection in database monitoring necessitates sampling policies that facilitate exploration, allowing security operators to extend their scrutiny beyond the initial suspects.	- Detecting attacks and data abuse. - Can issue alerts about policy violations and discover vulnerabilities. - Helping security officers detect data misuse and data leakage. - Automate aspects of the policy and policy calibration over time. - Monitoring big data streams
14	Hadoop-Based Healthcare Information System Design and Wireless Security Communication Implementation	Chen, Fu (2015)	IBM Guardium	- Hadoop-based healthcare architecture supported lightweight digital signature and big data storage. - Guardium provided DAM and auditing capabilities that enable users to integrate Hadoop data protection into existing enterprise data security strategies.	- Provides monitoring and auditing capabilities for database activities. - Enables integration of data protection into existing enterprise data security strategy. - Allows configuration and use of security policies and reports for Hadoop environments.
15	Securing large datasets involving fast-performing key bunch matrix block cipher	Karkarla (2019)	N/A	- The encrypted data shows a high level of security with minimal changes in the elements. - The performance of the key bunch block cipher with other symmetric key cryptosystems was compared. - The use of garbling to safeguard the databases and protect against data misuse during network transfers is discussed.	- Logs all accesses to the database by users. - Alerts during spurious accesses - Monitors and audits report for unauthentic activity - Reduces breaches by external attacks. - Grants access only to those with legitimate.
16	Role-task conditional-purpose policy model for privacy preserving data publishing	Elgendy et al. (2017)	N/A	- Privacy preserving data publishing model based on integration of multiple techniques. - Model meets requirements of workflow and non-workflow systems in enterprise environment.	- Real-time monitoring of database activity - Analysis of protocol traffic (SQL) over the network - Detection of known exploits or policy breaches

				- The model guarantees protection against insider threats such as database administrator.	- Identification of anomalous activity indicative of intrusion

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
17	Obtaining Value from Your Database Activity Monitoring (DAM) Solution	Miller (2015)	N/A	- Database activity monitoring tools help in capturing and monitoring database activities. - They assist in identifying policy violations and investigating users. - The tools may capture generic user information at the operating system and database level.	- Capture and monitor database activity in real-time. - Identify policy violations and unauthorized access attempts. - Provide detailed audit trails for compliance and security requirements. - Track and analyze user behavior and actions within the database. - Detect and alert on suspicious or abnormal database activity
18	Anomaly Detection in Large Databases using Behavioral Patterning	Mazzawi et al. (2017)	IBM Guardium	- The proposed algorithm detected malicious user activity in databases. - Algorithm relied on self-consistency and global-consistency components. - Experimental results showed low false positive rates and high accuracy. - An outlier detection engine based on the algorithm is included in IBM Guardium. - Algorithms can handle new actions and enhance accuracy.	- Centralized controls for real-time data security and monitoring. - Database vulnerability management. - Auto-discovery of sensitive data. - Complements rule-based security functions with unsupervised detection of anomalous behavior
19	Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks	Toapanta, Quimis, Gallegos, Arellano (2020)	N/A	- A taxonomy for workload management in database management systems is presented. - The paper provides a list of possible threats that a database may suffer. - The effectiveness of different simulation scenarios in the system is discussed. - the importance of security management in mitigating vulnerabilities is highlighted.	- Operating independently of the database management system. - Monitoring and analyzing database activity continuously and in real-time. - Generating real-time sensitive data alerts. - Detecting and preventing unauthorized attempts to copy or send sensitive data.

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
20	vulnerabilities of relational databases	Bašić, Udovičić, Orel (2023)	N/A	- Implementing strong access controls to prevent unauthorized access is implemented. - Using database activity monitoring tools to detect and prevent security breaches is discueed.	- Monitoring and tracking activities within a database. - Real-time alerts for suspicious or unauthorized activities. - Detecting and preventing SQL injection attacks. - Identifying and blocking unauthorized access attempts. - Track user activity and behavior patterns. - Offering auditing and reporting capabilities for compliance purposes. - Providing visibility into database activity and help identify vulnerabilities. - Integrating with other security systems for enhanced protection. - helping organizations identify and respond to security incidents in a timely manner.
21	Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment	Bann et al. (2015)	N/A	- The use of Mandatory Access Control (MAC) security policies for environment is proposed. - Guidelines for mitigating APT via spear phishing are discussed. - the mitigating APT attacks by monitoring database activity is discussed.	- Monitors access of sensitive data - Identifies unauthorized access attempts. - Triggers alerts and blocks unauthorized access. - Tracks inbound, outbound, and internal network traffic. -
22	cloud computing data security in cloud computing for banking	Tanvashi (2015)	N/A	- key security considerations and challenges in cloud computing is highlighted. - the affordability and flexibility of cloud computing is discussed. - the ability to monitor and control resource usage in the cloud is mentioned.	- Network monitoring or local agents - Alerting and blocking on policy violations.

Paper ID	Title	Study	DAM Tool Studied (if specified)	Results	DAM tools features and capabilities
23	Evaluating the Use of Security Tags in Security Policy Enforcement Mechanisms	Alves-Foss et al. (2015)	N/A	- Evaluating different classes of security policies and implementations of security tagging. - Developing a general understanding of appropriate uses, strengths, and limitations of security tagging technologies. - Identifying successful projects using hardware-based and software-based tagging.	- Block attacks and detect attack behavior. - Filtering attacks on the back end, especially for known SQL injection attacks. - Querying for typical SQL injections such as uneven numbers of quotes. - Supporting insertion, deletion, modification, and retrieval operations compliant with security policies.
24	Cybersecurity in WebGIS Environment	Giribabu et al. (2018)	N/A	- The architecture of WebGIS environment was presented. - The role of networking components in WebGIS security is discussed. - Various defense mechanisms for cybersecurity in WebGIS environment are portrayed.	- Auditing - Generating security alerts based on policy violations.
25	Database Forensics and Security Measures to Defend from Cyber Threats	Murthy, Nagalakshmi (2020)	N/A	- The importance of database forensics in identifying and analyzing cyber-attacks is Highlighted. - Provides remedies for protecting databases at various levels. - Mentions artifacts and sources for forensics analysis in MSSQL databases. Suitable monitoring and managing systems are required for large databases.	- Identifying anomalous activities in the database and its environment. - Monitoring and managing large database management systems

5 Results and Discussion

5.1 Detecting and Mitigating Threats with DAM Tools

This section discussed the different categories of security threats and the mechanisms used by DAM tools to detect and mitigate these threats. After providing a thorough summary of recent research on DAM tools in Table 1, the next step entailed a careful classification of the recognized security threats and their respective detection techniques. The classification, as depicted in Table 2, provided a detailed insight into the complex aspects of database security issues and the tactics utilized by DAM tools to combat these challenges.

Table 2. Classification of security threats and detection mechanisms in Database Activity Monitoring tools studies (By author)

Security Threat Category	Detection Mechanisms	Relevant Studies
Unauthorized Access and Data Breaches	Data Protection, Access Control, Data Masking, Real-time Monitoring, Block Unauthorized Activities	Akhil et al. (2015); Korsakova (2015); Çinar (2015); Gupta (2015); Sallam et al. (2015); Matthew, Dudley (2015); Sarmah (2020); Grushka-Cohen et al. (2019); Shivakumara, Patil, Muneshwara 2019; Çinar et al. (2016); Grushka-Cohen et al. (2020); Chen, Fu (2015); Karkarla (2019); Elgendy et al. (2017); Miller (2015); Mazzawi et al. (2017); Toapanta, Quimis, Gallegos, Arellano (2020); Bašić, Udovičić, Orel (2023); Bann et al. (2015); Tanvashi (2015); Alves-Foss et al. (2015); Giribabu et al. (2018); Murthy, Nagalakshmi (2020)
SQL Injection Attacks	Real-time Monitoring, Anomaly Detection, Blocking Unauthorized Access	Sarmah (2019); Alves-Foss et al. (2015); Bašić, Udovičić, Orel (2023)
Policy Violations	Configurable Thresholds, User Activity Monitoring, Alerting	Gupta (2015); Grushka-Cohen et al. (2019); Bašić, Udovičić, Orel (2023); Giribabu et al. (2018)
Network-Based Threats	Network-Based Monitoring, SIEM Integration, Alerting, Blocking	Brodsky (2015); Tanvashi (2015)
Anomalous Activity and Intrusions	Real-time Monitoring, Anomaly Detection, Automated Policy Calibration	Sarmah (2019); Grushka-Cohen et al. (2019); Miller (2015)
Data Privacy Violations	Data Masking, Encryption, Access Controls	Akhil et al. (2015); Akinde (2020)
Compliance and Audit Requirements	Auditing, Reporting, Compliance-focused Features	Miller (2015); Chen, Fu (2015)
Data Leakage and Misuse	Centralized Controls, Database Vulnerability Management, Auto-discovery of Sensitive Data, Anomaly Detection	Grushka-Cohen et al. (2019); Mazzawi et al. (2017)

Table 2 served as a structured taxonomy, organizing security threats into distinct categories and associating each with the specific detection mechanisms discussed in the literature. The categorization encompassed a spectrum of security concerns, ranging from unauthorized access and data breaches to specific threats such as SQL injection attacks, policy violations, network-based threats, anomalous activities, data privacy violations, compliance and audit requirements, and data leakage and misuse. For each security threat category, the table outlined the specific threats, the corresponding detection mechanisms, and referenced the studies that contributed to the classification. Some common security threats that these tools could detect included:

1. **Unauthorized Access and Data Breaches**

Unauthorized access and data breaches occurred when unauthorized users gained access to the database or when confidential data was leaked. DAM tools detected and prevented these threats by implementing data protection measures, controlling access to data, masking sensitive data, monitoring database activity in real-time, and blocking unauthorized activities. These measures ensured that only authorized users could access the data and any suspicious activity was quickly detected and stopped (Akhil et al. 2015; Korsakova, 2015; Çinar, 2015; Gupta, 2015; Sallam et al. 2015; Matthew, Dudley, 2015; Sarmah, 2019; Grushka-Cohen et al. 2020; Shivakumara, Patil, Muneshwara , 2019; Çinar et al. 2016; Chen and Fu, 2015; Karkarla, 2019; Elgendy et al. 2017; Miller, 2015; Mazzawi et al. 2017; Toapanta, Quimis, Gallegos, Arellano 2020; Bašić, Udovičić, Orel, 2023; Bann et al. 2015; Tanvashi, 2015; Alves-Foss et al. 2015; Giribabu et al. 2018; Murthy and Nagalakshmi, 2020).

2. **SQL Injection Attacks**

SQL injection attacks involve the insertion of malicious SQL code into a query. The real-time monitoring feature of DAM tools can detect unusual patterns in the SQL queries and block unauthorized access. Anomaly detection algorithms can identify patterns that deviate from the norm, indicating a potential SQL injection attack (Sarmah, 2019), (Alves-Foss et al. 2015), (Bašić, Udovičić, Orel, 2023).

3. **Policy Violations**

Policy violations occur when database activities violate the established policies. DAM tools can be configured to set thresholds for certain activities, monitor user activity, and send alerts when policies are violated. This helps in early detection and prevention of policy violations (Gupta, 2015), (Giribabu, 2018), (Grushka-Cohen et al. 2019), (Bašić, Udovičić, Orel, 2023).

4. Network-Based Threats

Network-based threats involve attacks that originate from the network, such as Denial of Service (DoS) attacks. DAM tools can monitor network activity, integrate with SIEM systems for a holistic view of security events, send alerts, and block threats (Brodsky, 2015), (Tanvashi, 2015).

5. Anomalous Activity and Intrusions

Anomalous activities are those that deviate from normal behavior. Intrusions refer to unauthorized access to the database. DAM tools can monitor database activity in real-time, detect anomalies using machine learning algorithms, and calibrate policies automatically based on the detected anomalies (Miller, 2015), (Sarmah, 2019), (Grushka-Cohen et al. 2019).

6. Data Privacy Violations

Data privacy violations occur when confidential data is accessed without authorization. DAM tools can mask sensitive data, encrypt data to protect it from unauthorized access, and control access to data (Akhil, 2015), (Akinde, 2020).

7. Compliance and Audit Requirements

Compliance and audit requirements are set by regulatory bodies. DAM tools can audit database activities, generate reports for audit purposes, and have features focused on compliance with various regulations (Miller, 2015), (Chen, Fu, 2015).

8. Data Leakage and Misuse

Data leakage and misuse involve the unauthorized access and use of data. DAM tools can control access to data, manage database vulnerabilities, discover sensitive data automatically, and detect anomalies in database activities (Grushka-Cohen et al. 2019), (Mazzawi, 2017).

Each of these categories represents a different aspect of database security, and DAM tools play a crucial role in protecting databases from these threats. By leveraging various features of DAM tools, organizations can ensure the security and integrity of their databases.

5.2 DAM tools features and capabilities

This section explored the advanced functionalities offered by select DAM tools. DAM tools have emerged as essential components of an organization's cybersecurity infrastructure, providing advanced features and capabilities to detect, prevent, and respond to various security threats. This discussion will delve into the key features and capabilities identified in the studies, shedding light on how these tools contribute to heightened security. Understanding these features is vital for assessing the sophistication and versatility of the tools.

1. Data Protection and Access Control

DAM tools, as demonstrated by Akhil et al. (2015) were instrumental in protecting confidential data, including details like credit card numbers and identification digits. They enforced access control policies by restricting permissions to specific employee levels, ensuring that only authorized individuals could interact with sensitive data. Additionally, these tools employed data masking techniques, enhancing privacy and limiting exposure while also restricting certain database commands and preventing potential security breaches. Korsakova (2015) introduced real-time monitoring and analysis, reducing reliance on native logs and allowing for continuous surveillance with prompt alerting capabilities. Çinar (2015) focused on transaction enablement, log collection, and responsive actions upon policy violations. Gupta (2015) integrated configurable thresholds, anomaly detection in SQL queries, and support for various security measures. Sallam et al. (2015) emphasized compatibility with different RDBMSs and integration with SIEM systems. Studies such as Shivakumara et al. (2019) and Grushka-Cohen et al. (2019) contributed to real-time monitoring, anomaly detection, and policy enforcement, incorporating contextual information into security policies. Akinde (2020) introduced encryption, user access control, and real-time monitoring, while Bašić, Udovičić, Orel (2023) presented a comprehensive suite of features ranging from real-time alerts to SQL injection attack prevention and integration with other security systems. These studies collectively illustrated a dynamic and evolving landscape where organizations could leverage a multitude of tools to fortify their data protection and access control mechanisms.

2. Real-time Monitoring and Alerting

Real-time monitoring, as highlighted by Korsakova (2015), Miller (2015), Çinar et al. (2016), Elgendy et al. (2017), Mazzawi et al. (2017), Sarmah (2019), Grushka-Cohen et al. (2019a, b), Shivakumara, Patil, Muneshwara, 2019, Akinde (2020), Toapanta, Quimis, Gallegos, Arellano (2020), and Bašić, Udovičić, Orel (2023) was a key feature of DAM tools. This capability enabled continuous analysis of database activities as they occurred, allowing for the immediate detection of security threats and vulnerabilities. The tools generated real-time alerts, notifying security personnel of unusual access behaviors, potential SQL injection attacks, or any unauthorized attempts to manipulate sensitive data, thus enhancing the system's ability to respond promptly to security incidents.

3. Security Policy and Compliance

Gupta (2015) and Grushka-Cohen et al. (2019) underscored the importance of security policy enforcement and compliance features. These tools facilitated the implementation of security policies, ensuring adherence to predefined rules and regulations. By offering configurable thresholds and integrating them with existing security measures, they enhanced the overall security posture of the company's database systems while maintaining compliance with industry standards and regulations. Grushka-Cohen et al. (2019) delved into various aspects of data security, emphasizing data security, privacy protection, and data leakage prevention. The authors proposed implementing security policies to detect attacks and data abuse, monitor database operations in real time, and make informed decisions on which transactions to save based on rules and user activity groups. Notably, the study highlighted the consideration of contextual information, including time of day, user activity profile, location, data sensitivity, and data volume, to ensure effective policy enforcement. The comprehensive approach presented in this study addresses the need for security policies and compliance measures within the realm of database security.

4. Anomaly Detection and Intrusion Prevention

Several studies in the provided information investigated and implemented features related to anomaly detection and intrusion prevention in the domain of database activity monitoring tools. Gupta (2015) configured thresholds, monitored user actions, and integrated anomaly detection into its capabilities. Sarmah (2019) focused on real-time monitoring, detected unusual access behaviors, and alerted for unauthorized changes. Grushka-Cohen et al. (2020) automated aspects of policy enforcement and monitored big data streams, aiding in the detection of attacks and data abuse. Chen, Fu (2015) provided auditing and monitoring capabilities, enabling integration into existing security strategies. Karkarla (2019) logged all database accesses, issued alerts during spurious accesses, and reduced breaches by allowing access only to legitimate users. Elgendy et al. (2017) conducted real-time monitoring, analyzed SQL protocol traffic, and identified anomalies indicative of intrusion. Miller (2015) captured and monitored real-time database activity, identified policy violations, and tracked user behavior. Mazzawi et al. (2017) centralized controls, performed vulnerability management, and complemented rule-based security with unsupervised anomaly detection. Toapanta, Quimis, Gallegos, Arellano (2020) operated independently of the database system, continuously monitored and analyzed activity, and generated real-time alerts. Bašić, Udovičić, Orel (2023) tracked activities, issued real-time alerts, prevented SQL injection attacks and integrated with other security systems. Murthy and Nagalakshmi (2020) identified anomalous activities within the database environment, contributing to the effective management of large database systems. Collectively, these studies demonstrated a dynamic and evolving landscape where organizations leveraged various tools to fortify their data protection and access control mechanisms, showcasing past contributions to the field of database activity monitoring tools.

5. Audit and Reporting

Several studies from the provided information explored and implemented features related to "Audit and Reporting" in the context of DAM tools. Matthew and Dudley (2015) emphasized auditing and monitoring as integral components of their database activity monitoring approach. Brodsky (2015) integrated network-based monitoring and emphasized the importance of integration with SIEM tools, indicating a focus on reporting capabilities. Chen, Fu (2015) explicitly mentioned monitoring and auditing capabilities for database activities, highlighting the comprehensive approach that includes data protection and audit functionalities. Karkarla (2019) prioritized logging all accesses to the database, implementing alerts for suspicious accesses, and auditing reports for unauthentic activity, showcasing a strong emphasis on audit features. Miller (2015) focused on capturing and monitoring real-time database activity, identifying policy violations, and providing detailed audit trails for compliance and security requirements. Mazzawi et al. (2017) designed centralized controls, incorporating database vulnerability management and auto-discovery of sensitive data, indicating a comprehensive approach to auditing and reporting. Bašić, Udovičić, Orel (2023) offered explicit auditing and reporting capabilities for compliance purposes, providing visibility into database activity and integrating with other security systems. Bann et al. (2015) monitored access to sensitive data, identified unauthorized access attempts, and triggered alerts, essential components of audit and reporting functionalities. Giribabu et al. (2018) concentrated on auditing and generating security alerts based on policy violations, emphasizing the reporting aspect. These studies collectively demonstrated a historical commitment to developing and implementing robust audit and reporting features within database activity monitoring tools, addressing the critical need for tracking, documenting, and reporting database activities for security and compliance purposes.

6. Attack Detection and Prevention

Numerous studies in the provided information focused on fortifying DAM tools with features cantered around attack detection and prevention. Korsakova (2015) pioneered real-time monitoring, disavowing reliance on native logs and introducing continuous surveillance with alerting and blocking functionalities. Sarmah (2019) proactively addressed real-time monitoring, detecting unusual access behaviours, and instituting measures against SQL injection attacks. Grushka-Cohen et al. (2019) significantly contributed to data security, privacy protection, and data leakage prevention by implementing policies that decide which transactions to save, thereby fortifying the system against attacks and data abuse. Akinde (2020) integrated real-time monitoring, anomaly detection, and alerting features, coupled with capabilities like encryption, user access control, and data masking for comprehensive attack prevention. Karkarla (2019) demonstrated the efficacy of logging, alerting, and reducing breaches by controlling access only to legitimate users. Elgendy et al. (2017) engaged in real-time monitoring, analysis of protocol traffic for known exploits, and identification of anomalous activities indicative of intrusion attempts. Miller (2015) advanced real-time capture and monitoring of database activity, detailed audit trail creation, and the detection and alerting of suspicious or abnormal database behaviour. Mazzawi et al. (2017) centralized controls for real-time security, managed database vulnerabilities, and complemented rule-based security with unsupervised detection of anomalous behaviour, enhancing overall attack detection and prevention capabilities. Toapanta, Quimis, Gallegos, Arellano (2020) operated independently of database systems, providing continuous monitoring, real-time alerting, and proactive measures against unauthorized attempts to access or transfer sensitive data. Bašić, Udovičić, Orel (2023) offered a comprehensive suite of features ranging from real-time alerts to SQL injection attack prevention, ensuring the detection and blocking of unauthorized access attempts and potential security incidents. Collectively, these studies showcased the evolution of database activity monitoring tools and their instrumental role in fortifying systems against a spectrum of attacks through advanced detection and prevention measures.

7. Network-Based Monitoring and Data Privacy

Several studies in the realm of database activity monitoring tools have addressed the crucial features of "Network-Based Monitoring" and "Data Privacy." Brodsky (2015) implemented network-based Monitoring, incorporated digital certificates, and amalgamated it with security information and event management (SIEM) tools to boost the comprehensive security framework. Toapanta, Quimis, Gallegos, Arellano (2020) operated independently of the database management system, employing continuous and real-time Monitoring, generating alerts for sensitive data, and actively preventing unauthorized attempts to copy or transmit such information. Tanvashi (2015) contributed by focusing on network monitoring and local agents, coupled with the capability to alert and block policy violations, thereby ensuring a robust network-based surveillance system for safeguarding sensitive data. These features are vital in company systems where the security and privacy of data are paramount concerns. Network-based Monitoring enables organizations to detect and respond to potential threats in real-time, while the emphasis on Data Privacy features ensures compliance with regulations and safeguards sensitive information. Together, these capabilities reflect past efforts to fortify security measures in company systems, acknowledging the critical role they play in maintaining the integrity, confidentiality, and security of sensitive data.

8. Comprehensive Security and Future Adaptability

Several studies in the realm of DAM, such as Grushka-Cohen et al. (2019), focused on delivering comprehensive security and future adaptability features. They placed a significant emphasis on safeguarding data through privacy protection, data leakage prevention, and the implementation of robust security policies. Notably, these studies incorporated real-time monitoring of database operations, utilizing policies to make decisions based on rules and user activity groups, and considering contextual information like time of day, user activity profile, location, data sensitivity, and volume. Akinde (2020) contributed to this landscape by integrating real-time monitoring, anomaly detection, and encryption capabilities, along with user and multifactor access control. Toapanta, Quimis, Gallegos, Arellano (2020) operated independently of the database management system, ensuring continuous real-time monitoring and analysis, generating alerts for sensitive data, and actively preventing unauthorized attempts to manipulate or transmit sensitive information. Bašić, Udovičić, Orel (2023) expanded on these functionalities by incorporating extensive monitoring, instantaneous alerting, proactive safeguards against SQL injection attacks, and seamless integration with other security systems. This approach equipped organizations with a holistic strategy for adeptly identifying and responding to security incidents. As a collective, these studies have played a crucial role in advancing the domain of database activity monitoring, guaranteeing not only comprehensive security measures but also the adaptability required to counter emerging threats effectively.

5.3 Exploring Various DAM Tools

5.3.1 IBM Guardium

IBM Guardium, as studied by Akhil et al. (2022), Çinar (2015), and Sallam et al. (2015), Shivakumara, Patil, Muneshwara (2019), is a comprehensive DAM tool developed by IBM. IBM Guardium focuses on maintaining, accessing, and protecting sensitive data, offering a robust solution for organizations seeking to safeguard their information. The DAM tool, developed by IBM, is tailored to manage, access, and protect sensitive customer data, including Debit Card, Credit Card, CVV, Expiry Date, Aadhar, PAN, Passport, and Insurance IDs. Presently, IBM InfoSphere Guardium has been implemented in numerous sizable enterprises (Çinar, 2015), (Sallam et al. 2015). BM InfoSphere Guardium offers monitoring and auditing features for database activity, allowing users to seamlessly incorporate Hadoop data protection into their current enterprise data security approach. Users have the flexibility to set up the system, leverage InfoSphere Guardium's security policies, and generate reports tailored for Hadoop environments. Notably, this process does not entail security communication through wireless sensor networks (Chen, Fu, 2015). As outlined in the study by Mazzawi et al. (2017), IBM InfoSphere Guardium products play a crucial role in ensuring the security, privacy, and integrity of information within a data center. These data security solutions boast a user base of over 1300 enterprise customers, spanning diverse sectors such as finance, healthcare, retail, and government institutions. Guardium is instrumental in implementing centralized controls for real-time data security and monitoring, managing database vulnerabilities, facilitating the automatic discovery of sensitive data, and performing other security-related functions. The technology mentioned in the paper acts as an improvement to the Guardium product, bolstering its rule-based security features by incorporating the unsupervised identification of unusual behavior.

5.3.2 Imperva’s Secure Sphere

Imperva stands out as a prominent DAM solution in the market, renowned for its robust database auditing features. Recognized strengths include real-time monitoring, protection of database transactions and functions, advanced privilege management, and effective policy administration (Çinar, 2015; Brodsky, 2015; Gupla, 2015). The Imperva DAM Solution provides a comprehensive suite of security advantages crucial for safeguarding sensitive data and preventing data breaches.

Through features such as real-time monitoring, analysis of user behavior, data access control, and threat detection, the DAM Solution empowers organizations to proactively manage security risks and uphold the integrity of their databases. Furthermore, the solution aids in regulatory compliance and adherence to data protection laws, ensuring that organizations meet stringent security standards. By embracing the Imperva DAM Solution, organizations can significantly bolster their cybersecurity stance and shield valuable data assets from both internal and external threats.

In recent years, numerous domestic and international companies have introduced diverse database security audit products, including IBM's InfoSphere Guardium, Imperva's SecureSphere in Israel, and ASI's DBProtect in the United States, as well as Venus Information Technology Co., Ltd's TianYue network security audit system. However, challenges arise due to the use of proprietary security communication protocols in isolation devices, making compatibility with independent security audit products difficult (Li, Zhang, Ma, Cheng, 2016).

5.3.3 Oracle Audit Vault and Database Firewall

In the systematic review, three notable papers underscored the importance of Oracle in the field of database activity monitoring. Oracle, a key player in the expansive world of big data and transaction databases, holds a significant position due to its extensive usage. Notably, the general agreement on Oracle Databases is that their activity monitoring solutions, as stated by Çinar (2015) and Çinar, Guncer, Yazici (2016), demonstrate exceptional stability and robust protective features. Oracle Audit Vault and Database Firewall embody this strength by flawlessly merging auditing and network-based monitoring functions. This powerful pair not only examines database traffic for threat detection and blocking but also aids compliance reporting by amalgamating audit data from databases, operating systems, and directories. The audit vault server, which contains an Oracle database with exhaustive auditing information, provides access to reporting tools through a dedicated data warehouse. A primary advantage is its compatibility with diverse databases, along with support for the latest versions of popular database management systems. Adding an extra layer of security, Oracle Database Vault is uniquely engineered to limit privileged database accounts from accessing confidential information while still allowing crucial operations like patching and backup. By utilizing sub-setting and data masking techniques, it enables users to extract complete or partial copies of application data. Moreover, Oracle's data cloud service includes fine-grain and unified auditing, similar to encryption, as explained by Akinde (2020).

5.4 Comparison between different DAM tools

In the systematic review, a single study was found that compared different DAM tools, underscoring the need for additional research to gain a more thorough understanding of how these tools compared in terms of effectiveness in practical applications. An extensive assessment was carried out based on the criteria set forth by Forrester Research (Çinar, 2015). Criteria such as “Database Auditing,” “User and App Auditing,” and “Audit Policies” were in direct alignment with the objective of comprehending the performance of these tools in monitoring and auditing database activities, inclusive of user and application interactions. Furthermore, the evaluation considered “Reporting and Analytics,” underscoring the importance of tools in offering robust reporting capabilities to assist in the detection of patterns and anomalies that could be indicative of potential security issues. The significance of “Real-time Protection” was paramount, as it directly pertained to the immediate response capabilities of DAM solutions to security threats as they emerged. These criteria, among others, contributed to a comprehensive understanding of the effectiveness of DAM tools in the context of real-world security scenarios, thereby providing invaluable insights for organizations aiming to bolster their database systems against evolving threats.

Based on the fig .2 from the study by Çinar (2015), IBM Guardium, Imperva’s Secure Sphere, Oracle Audit Vault, and Database Firewall were all highly effective Database Activity Monitoring (DAM) tools, each with its own strengths. All scores were based on a scale of 0 (weak) to 5 (strong). IBM Guardium stood out with the highest overall score of 4.67, demonstrating exceptional performance in most categories, particularly in ‘User & App Auditing’ and ‘Auditing Repository.’ This suggested that IBM Guardium was highly effective in monitoring and auditing both user activities and applications, and it provided a robust repository for audit data. Imperva’s Secure Sphere, with an overall score of 4.38, also showed strong performance across the board. It was particularly notable in the ‘Audit Policies’ category, indicating its strength in providing comprehensive and customizable audit policies. Oracle Audit Vault and Database Firewall, while having varied scores across different categories, showed strength in the ‘Auditing Repository’ category. This suggested that they provided a reliable and efficient system for storing and managing audit data.

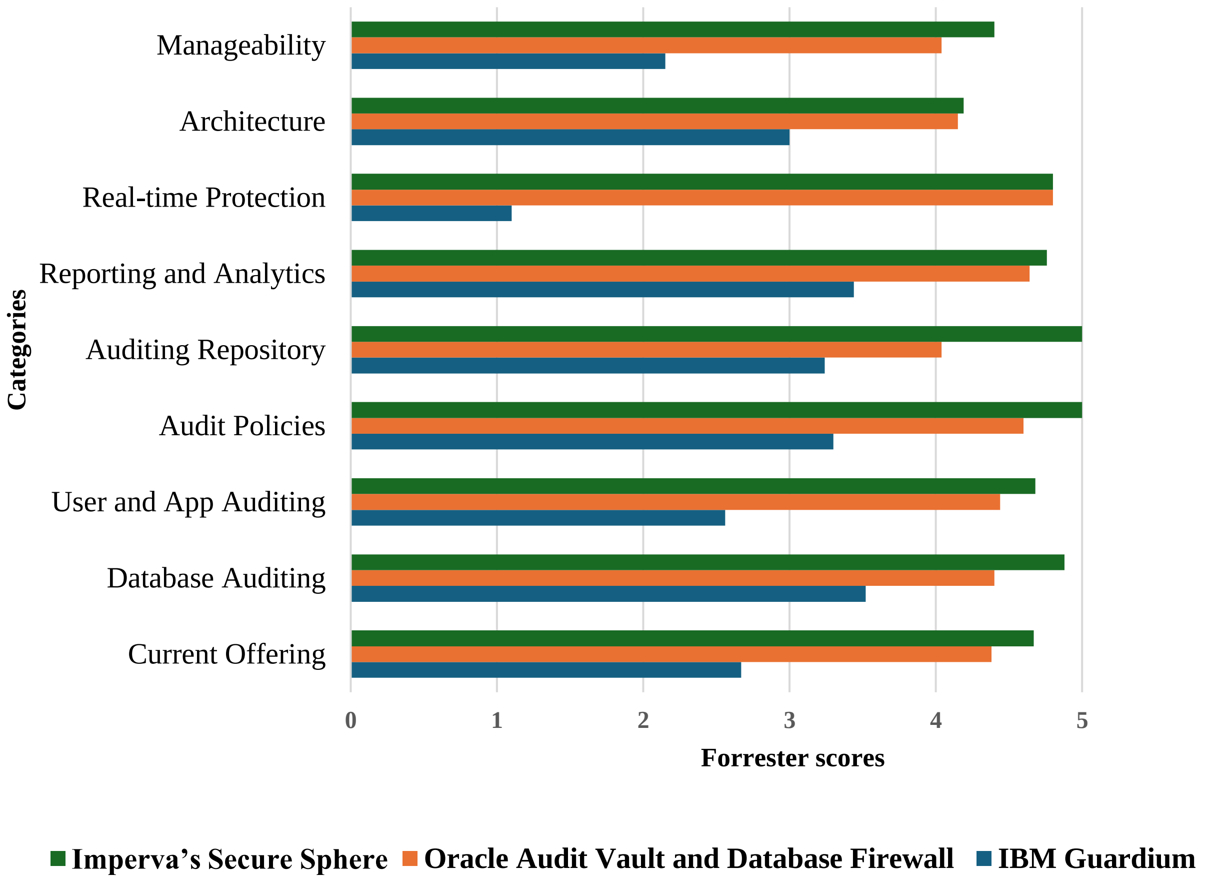

Fig. 2 Analysis of DAM Solutions by Forrester Research (Çinar, 2015)

5.5 Improvement of DAM tools

In the comprehensive review of 25 articles on DAM, improvements in DAM were the focus of 6 papers. Grushka-Cohen et al. (2020) significantly contributed to this field by proposing a novel algorithm that redefined the data sampling problem in DAM as a special case of the multi-armed bandit (MAB) problem. The algorithm, combining expert knowledge with random exploration, added diversity to the sampling process in DAM systems. Based on bandit algorithms, it optimized sampling using reward functions and ensured diversity in the recommended set. Evaluation of a simulated dataset demonstrated that adding diversity to the sampling improved coverage of user activity without compromising alert quality. The proposed algorithm outperformed other baseline approaches, emphasizing its potential to enhance DAM systems in detecting anomalies and protecting organizational data.

Çinar, Guncer, Yazici (2016) stood out for their discussion on DAM improvement through the development of a private database cloud. Their proposed solution utilized parallel threads and unique IDs as primary keys, facilitating efficient log transferring and ensuring data integrity. This enhancement enabled the simultaneous management of multiple databases. Incorporating a zipping algorithm minimized log file sizes, reducing network traffic and cost. Despite potential storage and performance issues, the proposed system, InfoFence, demonstrated superior performance compared to Oracle Audit Vault Server in a private cloud environment. The study's emphasis on network connection importance, bandwidth, and centralized security management provided valuable insights into DAM improvement possibilities.

Mazzawi et al. (2017) proposed a novel machine-learning algorithm for detecting malicious user activity in databases. The algorithm, relying on self-consistency and global consistency testing, examined the consistency of a user's activity and compared it with learned activity patterns. Considering the rarity, volume, and correlations among user actions, the algorithm improved DAM accuracy. Experimental results showcased the algorithm's ability to maintain low false positive rates while ensuring overall accuracy. The inclusion of these anomaly detection methods in the standard offering of IBM InfoSphere Guardium further validated their potential to enhance DAM.

Akhil et al. (2022) discussed the integration of DAM tools with SIEM systems, emphasizing the holistic view and centralized monitoring of security events. Chen and Fu (2015) explored IBM InfoSphere Guardium, providing DAM and auditing capabilities. The architecture supported lightweight digital signature, big data storage, and integration with Hadoop data protection, surpassing other works in terms of security.

Grushka-Cohen et al. (2019) concentrated on improving the efficiency of DAM systems in detecting and averting data breaches. They introduced an innovative simulation technique for user activity and evaluated the influence of sampling on anomaly detection algorithms. The Bayesian sampling policy, particularly the Gibbs sampling approach, significantly improved anomaly detection, highlighting the importance of data-driven sampling policies in improving DAM system efficiency, especially in monitoring large data streams.

6 Conclusion

This thesis aimed to analyse the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems. The methodology adopted involved a systematic review approach, encompassing an in-depth analysis of 25 papers and a practical investigation into state-of-the-art DAM tools.

The systematic review illuminated the diverse landscape of DAM tools, revealing their pivotal role in safeguarding company databases against various security threats. The literature synthesis, which culminated in a conceptual framework, provided a structured taxonomy of security threats and the corresponding mechanisms employed by DAM tools for detection and mitigation. The practical component, which focused on constructing and reviewing a database of scientific papers, delved into the capabilities of DAM tools, exemplified by IBM Guardium, Imperva's Secure Sphere, and Oracle Audit Vault and Database Firewall.

The results and discussions highlighted the multifaceted contributions of DAM tools in addressing security threats such as unauthorized access, SQL injection attacks, policy violations, network-based threats, anomalous activities, data privacy violations, compliance, and data leakage. A comprehensive examination of DAM tool features and capabilities showcased their pivotal role in fortifying database security. These features encompassed data protection and access control, real-time monitoring and alerting, security policy and compliance, anomaly detection, and intrusion prevention, audit and reporting, attack detection and prevention, network-based monitoring, and comprehensive security with future adaptability.

The exploration into various DAM tools, including IBM Guardium, Imperva's Secure Sphere, and Oracle Audit Vault and Database Firewall, provided a comparative analysis, highlighting their strengths and effectiveness based on criteria from Forrester Research. Each tool exhibited commendable performance, with IBM Guardium having the highest overall score.

The studies proposed innovative approaches for enhancing DAM effectiveness. Notable contributions included novel algorithms for data sampling, the development of private database clouds, machine learning algorithms for anomaly detection, integration with Security Information and Event Management (SIEM) systems, and simulation methods for user activity.

The thesis has significantly augmented the extant scholarly discourse by furnishing a comprehensive examination of the efficacy of DAM tools, coupled with a meticulous exploration of avenues for enhancement within this domain. The synthesis of literature and practical insights underscores the crucial role of DAM tools in fortifying company databases against evolving security threats.

As the cybersecurity landscape undergoes continuous evolution, the insights gleaned from this study, alongside potential future research endeavours, will serve as instrumental pillars in fortifying the resilience of database environments against emergent threats and challenges.

By utilizing a systematic review approach, this study aims to provide an extensive analysis of the effectiveness of DAM tools in detecting security threats and vulnerabilities in company database systems.

7 References

ABDIYEVA-ALIYEVA, Gunay, HEMATYAR, Mehran, 2022. *Statistic Approached Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System's Database in NGN*. Journal of Advances in Information Technology. 13(5):524-529. https://doi.org/10.12720/jait.13.5.524-529

AKINADE, Sarat Kehinde, 2020. *Database as a service: Security and privacy issues, and appropriate controls*. https://doi.org/10.7939/r3-rq3n-1372

AKHIL, Bille, et al., 2022. *IBM Guardium–Database Activity Monitoring. International journal of engineering technology and management sciences*. 4(6):180-183. https://doi.org/10.46647/ijetms.2022.v06i04.0031

ALVES-FOSS, Jim, et al., 2015. *Evaluating the Use of Security Tags in Security Policy Enforcement Mechanisms.* 48th Hawaii International Conference on System Sciences (pp. 5201-5210). IEEE. https://doi.org/10.1109/HICSS.2015.614

BAŠIĆ, Bjanka, Udovičić, Petra, OREL, Ognjen, 2021. *In-database Auditing Subsystem for Security Enhancement.* 44th International Convention on Information, Communication and Electronic Technology (MIPRO), pp. 1642-1647. IEEE. https://doi.org/10.23919/MIPRO52101.2021.9596906

BRODSKY, Charles, 2015. *Database activity monitoring (dam): Understanding and configuring basic network monitoring using imperva's securesphere.* Sans Institute InfoSec Reading Room.

CHAKRABORTY, Ms Sushmita, 2022. *Database security threats and how to mitigate them.* In Empowering Smart Future Through Scientific Development and Technology Conference, USA. *https://doi.org/10.3390/mol2net-08-12642*

CHEN, H., FU, Z, 2015. *Hadoop-based healthcare information system design and wireless security communication implementation*. Mobile Information Systems. https://doi.org/10.1155/2015/852173

ÇINAR, Onur, 2015. *Database Security in Private Database Clouds* (master's thesis). Middle East Technical University, Graduate School of Informatics Institute, Turkey.

ÇINAR, Onur, R. GUNCER Haluk, YAZICI Adnan, 2016. *Database security in private database clouds*. International Conference on Information Science and Security (ICISS), pp. 1-5. IEEE. https://doi.org/10.1109/ICISSEC.2016.7885847

COVIDENCE, 2023. Covidence: Better systematic review management. Retrieved 2023, from https://www.covidence.org/

DEEPIKA, K., PRASAD, N. N., BALAMURUGAN, S., & CHARANYAA, S, 2015. *Survey on Security on Cloud Computing by Trusted Computer Strategy*. International Journal of

Innovative Research in Computer and Communication Engineering. 3(1):199-204. https://doi.org/10.15680/ijircce.2015.0301046

ELGENDY, Rana, et al., 2017. *Role-task conditional-purpose policy model for privacy preserving data publishing*. Alexandria Engineering Journal 56.4: 459-468. https://doi.org/10.1016/j.aej.2017.05.029

GHARPURE, Nisha, RAI, Aradhana, 2022. *Vulnerabilities and Threat Management in Relational Database Management Systems*. 5th International Conference on Advances in Science and Technology (ICAST) (pp. 369-374). IEEE. https://doi.org/10.1109/ICAST55766.2022.10039599

GIRIBABU, D, et al., 2018. *Cybersecurity in webgis environment*. Int. J. Comput. Internet Secur. 10(1): 11-34.

GRUSHKA-COHEN, Hagit, et al., 2019. *Simulating user activity for assessing effect of sampling on DB activity monitoring anomaly detection*. Policy-Based Autonomic Data Governance: pp: 82-90. https://doi.org/10.1007/978-3-030-17277-0_5

GRUSHKA-COHEN, Hagit, et al., 2020. *Using bandits for effective database activity monitoring*. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 701-713). Cham: Springer International Publishing. 12085: 701–713. https://doi.org/10.1007/978-3-030-47436-2_53

GUPTA, Chaitali, RANJAN, Sinha, ZHANG, Yong, 2015. *Eagle: User profile-based anomaly detection for securing Hadoop clusters*. International Conference on Big Data (Big Data) (pp. 1336-1343). IEEE. https://doi.org/10.1109/BigData.2015.7363892

Hashim, Hassan B, 2018. *Challenges and security vulnerabilities to impact on database systems*. Al-Mustansiriyah Journal of Science. 29(2): 117-125. https://doi.org/10.23851/mjs.v29i2.332

INGOLE, K., R, 2023. *Database Security*. International Journal For Science Technology And Engineering. 11(4):1568-1576. https://doi.org/10.22214/ijraset.2023.50415

KAKARLA, Shirisha, 2019. *Securing large datasets involving fast-performing key bunch matrix block cipher*. In Healthcare Data Analytics and Management (pp. 111-132). Academic Press. https://doi.org/10.1016/B978-0-12-815368-0.00004-X

KAPLAN, James, SHARMA, Shantnu, WEINBERG, Allen, 2011, *Meeting the cybersecurity challenge*. Digit. McKinsey.

KORSAKOVA, Maria, 2016. *Security methods and how they are applied in Oracle products* (Master's thesis, Itä-Suomen yliopisto).

LAWAL, Babatunde, ADESOJI, Adebesin, ADEKUNLE, Salami, 2022. *Contemporary Control Measures for Mitigating Threats and Vulnerabilities to organizational Databases.* Conference: iSTEAMS Research Nexus At: Ibadan

LI, Yong, ZHANG, Tao, MA, Yuan, ZHOU, Cheng, 2016. *Anomaly detection of user behavior for database security audit based on OCSVM*. In 2016 3rd International Conference on Information Science and Control Engineering (ICISCE) (pp. 214-219). IEEE. https://doi.org/10.1109/ICISCE.2016.55

MATTHEW, Olumuyiwa O, DUDLEY. Carl, 2015. *Critical Assessment of Auditing Contributions to Effective and Efficient Security in Database Systems*. In International Conference on Computer Science, Informatin Technology and Applications (CSITA-2015). AIRCC Publishing. https://doi.org/10.5121/csit.2015.50801

MAZZAWI, Hanna, et al., 2017. *Anomaly detection in large databases using behavioral patterning*. 33rd International Conference on Data Engineering (ICDE) (pp. 1140-1149). IEEE. https://doi.org/10.1109/ICDE.2017.158

MILLER, Mike; KOST, Stephen; REIMANN, Phil, 2015. *Obtaining Value from Your Database Activity Monitoring (DAM) Solution*. About Integrigy.

MURTHY, P. Srinivasa, NAGALAKSHMI, V, 2020. *Database forensics and security measures to defend cyber threats*. 3rd International Conference on Intelligent Sustainable Systems(ICISS) (pp. 1302-1307). IEEE. https://doi.org/10.1109/ICISS49785.2020.9316042

MOUSA, Abdulazeez, KARABATAK, Murat, MUSTAFA, Twana, 2020, *Database security threats and challenges*. 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE. https://doi.org/10.1109/ISDFS49300.2020.9116436

PEVNEV, Volodimir, KAPCHYNSKYI Serhii, 2018. *Database security: threats and preventive measures*. Advanced Information Systems. 2(1): 69–72. https://doi.org/10.20998/2522-9052.2018.1.13

SALLAM, Asmaa, et al., 2015. *DBSAFE—an anomaly detection system to protect databases from exfiltration attempts*. IEEE Systems Journal. 11(2): 483-493. https://doi.org/10.1109/JSYST.2015.2487221. k

SAFIANU, Omar, TWUM. Frimpong, HAYFRON-ACQUAH, J. B, 2016. *Information system security threats and vulnerabilities: Evaluating the human factor in data protection*. International Journal of Computer Applications. 143(5): 8-14. https://doi.org/10.5120/ijca2016910160

SARMAH, Simanta Shekhar, 2019. *Database security–threats & prevention*. International journal of computer trends and technology. 67(5): 46-53. https://doi.org/10.14445/22312803/IJCTT-V67I5P108

SHIVAKUMARA, T., PATIL, R. M., & MUNESHWARA, M. S, 2019. *Review Paper on Dynamic Mechanisms of Data Leakage Detection and Prevention.* 7(2): 349-358.https://doi.org/10.26438/ijcse/v7i2.349358

TANVASHI, Anand, SHRAVANI, B, 2015. *Cloud Computing Data Security in Cloud Computing for Banking*. Adarsh Journal of Information Technology.7(2): 50-61.

TOAPANTA, Segundo Moisés, QUIMIS, Alexander Escalante, GALLEGOS, Luis Enrique Mafla, ARELLANO, Ma Roció Maciel, 2020. *Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks*. IEEE Access, 8: 169367-169384. https://doi.org/10.1109/ACCESS.2020.3022746

8 List of pictures, tables, graphs and abbreviations

8.1 List of pictures

8.2 List of tables

8.3 List of graphs

8.4 List of abbreviations

IEE Xplore: Institute of Electrical and Electronics Engineers

SIEM: Security Information and Event Management

DAM: Database Activity Monitoring

SQL: Structured Query Language

DOS: Denial Of Service

PCI DSS: Payment Card Industry Data Security Standard

DBMS: Database Management System

DML: Data Manipulation Language

DDL: Data Definition Language