From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts

Abstract

This study investigates the effectiveness of Role-Based Access Control (RBAC) systems in mitigating insider threats to database security within various organizational environments. Insider threats represent a significant challenge for database security, necessitating robust and adaptive security measures. By delineating access based on users' roles within an organization, RBAC emerges as a critical tool against such threats. Employing a quantitative research methodology, this work gathered data through a survey targeting professionals directly involved in the security and management of organizational databases across technology, finance, healthcare, and government industries. The study utilized Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM) to validate the measurement model and analyze the relationships between RBAC effectiveness, implementation challenges, RBAC enhancements, and their collective impact on insider threat reduction. Findings indicate that RBAC effectively reduces unauthorized access and data breaches, significantly mitigating insider threats. However, implementation challenges such as role definition complexity and adapting to dynamic access needs emerge as notable obstacles. Enhancements in RBAC, mainly through integrating technologies like machine learning and dynamic access controls, are identified as critical mediators that enhance RBAC's effectiveness. The study concludes that while RBAC is a vital tool for database security, its success depends on continuous improvement and customization to specific organizational contexts. It recommends developing continuous enhancement programs for RBAC systems, specialized training for administrators, and the customization of RBAC strategies to meet unique organizational and industry needs. These measures are crucial for optimizing RBAC's effectiveness against insider threats.

***Keywords**: Role-Based Access Control, Insider Threats, Database Security, Machine learning, Discretionary Access Control (DAC) and Mandatory Access Control (MAC), Dynamic Role-Based Access Control.*

1. Introduction

According to Tomar and Jawaharbabu [1], data is increasingly becoming the cornerstone of organizational operations; hence, securing databases against insider threats poses a significant challenge. Insider threats from individuals within the organization present a unique and complex risk to database security [3]. These threats include malicious actions aimed at data theft, sabotage, or unintentional breaches due

to negligence or lack of awareness. Traditional security measures often fail to effectively address insider threats due to their internal origin and the abusers' potential access and knowledge of the system [4]. Role-Based Access Control (RBAC) has been recognized as a promising approach to mitigate these threats by restricting access to sensitive information based on users' roles within an organization [5].

In December 2021, Cash App, a financial services platform owned byBlock Inc., was at the center ofa data security incident where a former employee downloaded unauthorized dataassociated with 8.2 million customers, including names and brokerageinvestment details [6]. While the extent of any further data leak remains unclear, this incident exposes a critical vulnerability in inadequate access controls., In May 2022, another data security breach exposed a crucial vulnerability in many organizations: the insider threat. As reported by Clark [2], Yahoo filed a lawsuit against a former senior researcher, Qian Sang, alleging theft of a massive amount of confidential information. Leading a crucial team within Yahoo's advertising division, Sangreportedly downloaded nearly 570,000 pages of sensitive data, including proprietary source code, algorithms, and strategic documents. The lawsuit indicates Sang intended to leverage this information to his advantage at his new employer, The Trade Desk, a competitor to Yahoo. This incident underscores the alarming potential for employees to exploit their authorized access and internal knowledge to steal sensitive data.

Similarly, in 2022, Pegasus Airlines encountered a data security breach from a critical error. A system administrator's mistake, likely due to inadequate training on cloud security protocols, resulted in a misconfiguration that left sensitive data vulnerable. This incident underscores the potential consequences of human error in cloud environments, highlighting the need for a comprehensive approach to data security. Although the specific nature of the exposed data remains undisclosed, the breach potentially compromised flight information, crew data, and passenger details [7]. While someexperts argue that such errors stem from insufficient training, others contend that the incident underscores the need for adequate security measures, such as RBAC. RBAC operatesonthe principle of least privilege whereusers are assigned roles with specific permissions mappedto their job responsibilities. If RBAC was implemented, it could have significantly reduced the damage by limiting access based on job functions, grantingonly authorized employeesaccess to view sensitive information [5].

While traditional methods like employee monitoring can play a role, these cases highlight the necessity of more comprehensive strategies like Role-Based Access Control (RBAC), which offers a more robust line of defense. These incidents collectively underscore the necessity of a study focusing on RBAC's potential to fortify database security against insider threats. They highlight critical weaknesses in current security practices, including inadequate termination procedures, insufficient user access

reviews, and the lack of proactive monitoring for suspicious activities. However, the efficacy of RBAC in real-world applications is hindered by challenges in accurate role definition, dynamic access needs, and the evolving nature of insider threats [8]. Moreover, the lack of comprehensive research onthe specific impact of RBAC on mitigating insider threats leaves a gap in understanding its effectiveness and areas for improvement.

This paper addresses this gap by examining how RBAC can be optimized to counter insider threats more effectively. It proposes a nuanced understanding of RBAC's role in enhancing database security and identifying strategies to overcome its implementation challenges. Without such an investigation, organizations may continue to face significant risks from insider threats, undermining their operational integrity, data confidentiality, and competitive advantage. By examining and proposing enhancements to RBAC frameworks, the study aims to address these vulnerabilities, offering organizations robust strategies to protect their valuable data assets against the ever-present risk of insider threats. Furthermore,this study seeks to critically evaluate the effectiveness of RBAC as a strategic and technical measure in mitigating insider threats to database security within organizational environments. This study seeks to explore how RBAC can be optimized to enhance database security against the backdrop of evolving internal threats.

Research Objectives

1. Identify and categorize insider threats encountered in organizational database systems.
2. Analyze the role of RBAC in preventing unauthorized access and data breaches caused by insider threats.
3. Evaluate RBAC's implementation challenges and limitations in securing databases against insider threats.
4. Propose enhancements to RBAC frameworks that could improve their effectiveness in mitigating insider threats.

Research Hypotheses

H1: RBAC significantly reduces the incidence of unauthorized access and data breaches within organizational databases compared to databases without RBAC.

H2: Organizations implementing RBAC face significant challenges in configuration and management, which can be mitigated through targeted training and policy development.

H3: The effectiveness of RBAC in mitigating insider threats is positively correlated with the comprehensiveness of role definitions and access control policies.

H4: Enhanced RBAC frameworks that incorporate dynamic access controls and machine learning algorithms for behavior analysis are more effective at mitigating insider threats compared totraditional RBAC systems.

2. Literature Review

Database Security and Insider Threats

The security of databases is not just a technical necessity but a cornerstone of organizational integrity and trust [1]. Databases, repositories of valuable information, are critical assets that require robust protection mechanisms to safeguard against a spectrum of threats, including insider threats posing significant challenges due to their potential to cause unimaginable harm from within the organization [3].

The importance of securing databases stems from the invaluable nature of the data they hold, which is essential not only for the daily operations of an organization but also constitutes a significant portion of its intellectual and financial capital [1]. Database security encompasses various measures, both technical and procedural, designed to protect databases from unauthorized access, misuse, or theft. These measures include access control mechanisms, encryption, data masking, and implementing security policies and procedures that govern data access and use, thus ensuring data confidentiality, integrity, and availability, principles foundational to information security [9][10].

Insider threats include risks posed by individuals within the organization, such as employees, contractors, or business partners, who have inside information concerning the organization's security practices, data, and computer systems [4]. These threats can manifest in various forms, from unintentional data leaks due to negligence or error to deliberate data theft, sabotage, or espionage [11]. According to Saxena [4], the impact of insider threats on organizations varies, including compromise of sensitive information, financial losses, damage to reputation, and legal consequences. Unlike external threats, insider threats are challenging to detect and mitigate due to the legitimate access insiders have to the organization's systems and data,mainly due to balancing security measures with maintaining an open and trusting organizational culture [12].

Although conventional strategies in combating insider threats emphasize the importance of robust access controls, continuous monitoring of user activities, and cultivating a security-aware organizational culture, recent trends and incidents underscore the need for a more nuanced approach [13][14]. There is an emerging consensus on the importance of behavioral analytics and machine learning techniques in identifying anomalous behavior that may indicate an insider threat, as these technologies complement traditional security measures by providing deeper insights into user behavior, thereby enabling more proactive threat detection and response [15][16].

Moreover, the role of organizational factors in mitigating insider threats has gained recognition, with factors such as employee satisfaction, transparent communication, and ethical leadership being identified as critical in reducing the likelihood of insider threats [17].

Evolution of Access Control Mechanisms and Role-Based Access Control (RBAC)

Access control mechanisms have evolved significantly, transitioning from basic models designed for straightforward security needs to more sophisticated frameworks that address complex organizational structures and the nuanced challenges of modern cybersecurity, including insider threats [13]. The foundational models of access control mechanisms are the Discretionary Access Control (DAC) and Mandatory Access Control (MAC) [8]. DAC, characterized by its flexibility, allows the resource owner to determine who has access to it (like a homeowner who decides which guests can enter their home) [18]. However, its reliance on individual users to set their access controls introduces significant risk, particularly with insider threats, as it enables users with malicious intent to grant access to sensitive information improperly [3]. Conversely, MAC is more stringent, relying on a centralized policy to dictate access based on classifications and security clearances (akin to a military facility where access to classified information is strictly regulated based on ranks and necessities of knowledge) [19]. While MAC provides a higher level of security than DAC, especially against insider threats, its rigidity can hinder operational flexibility and efficiency within an organization [20].

In response to the limitations of DAC and MAC, Role-Based Access Control (RBAC) emerged as a paradigm shift in access control philosophy, with a centralized focus on the roles within an organization rather than individual users or data classifications aligning access rights with the organization's structure, significantly improving security management's efficiency and reducing the risk of insider threats [13].RBAC operates on several fundamental principles, including Minimum Necessary Access, which provides that users are granted only the access necessary to perform their roles, limiting the potential for unauthorized access to sensitive information; Separation of Duties, which ensures that no single user can perform conflicting tasks; and Least Privilege which restricts access rights to the bare minimum needed to perform their jobs, reducing the risk surface for insider threats [22]. RBAC's role-centric model offers a scalable solution that can adapt to organizational changes, making it a robust framework against insider threats [23].

RBAC comprises several fundamental components, including roles, permissions, sessions, and user-role assignments [21]. Roles are defined according to job functions within the organization, abstracting a set of actions and responsibilities associated with specific job functions. Permissions are access rights or privileges granted to roles,

enabling them to perform certain operations. Sessions represent instances of users operating within the system under specific roles, effectively linking users to their roles temporarily [24]. User-role assignments include mappings between users and roles and determining which roles a user can assume in a session. In addition, the architecture of RBAC allows for a modular approach to access control, where changes in roles, permissions, or user assignments can be managed independently without requiring a systemic overhaul, which is crucial for adapting to organizational changes, such as role evolution or personnel turnover, with minimal disruption to the overall access control system [13][25].

One of the most significant advantages of RBAC is its ability to enforce the principle of least privilege and separation of duties, which are foundational elements in mitigating insider threats [22]. RBAC's role-centric approach also offers scalability and flexibility, enabling organizations to efficiently manage access controls in environments with numerous users and complex requirements [13][23]. By defining roles based on organizational functions rather than individual user needs, RBAC facilitates more straightforwardpermissions management, as roles can be updated or modified without individually adjusting each user's access rights [21][23].

Although RBAC is widely recognized for its effectiveness in managing access controls, its implementation is challenging, as accurately defining roles and permissions can be complex and time-consuming, particularly in organizations with intricate operational structures [26]. The dynamic nature of modern work environments, characterized by frequent changes in job functions and responsibilities, necessitates continual updates and revisions to role definitions and assignments [24][27]. Mayeke et al. [13] assert that emerging trends in RBAC research and application focus on enhancing its adaptability and intelligence.Trends like Dynamic RBAC systems, which adjust roles and permissions based on contextual factors such as time of day or location, and the integration of machine learning algorithms for automatic role assignments and anomaly detection, are areas of active development. These advancements aim to address some of the traditional limitations of RBAC, making it more responsive to changing organizational needs and sophisticated threat landscapes [28].

RBAC's Role in Mitigating Insider Threats

Role-Based Access Control (RBAC) is considered a strategic framework pivotal in mitigating insider threats, a pressing concern for organizations worldwide [24][28]. It employs several strategic mechanisms that effectively reduce the risk of insider threats [29]. Central to these strategies is the principle of least privilege, which ensures that individuals are granted only the permissions necessary for their specific roles within the organization [22]. This minimization of access rights significantly lowers the potential for malicious actions or accidental data breaches by insiders. In addition, Separation of

duties (SoD) is another critical strategy within RBAC, designed to prevent any single individual from executing conflicting tasks that could lead to unauthorized or harmful actions [30]. By requiring more than one person to complete sensitive processes, SoD acts as a deterrent against fraud and errors, adding a layer of security. RBAC also incorporates dynamic access controls that adjust permissions based on contextual factors such as time, location, or transaction context [31]. This adaptability is crucial in responding to evolving insider threats, ensuring access rights are appropriately stringent under high-risk conditions.

Although scholars laud RBAC for its effectiveness in mitigating insider threats [26][32][33], it is not devoid of challenges, as studies argue that the complexity of defining and managing roles can be a significant barrier, especially in large and dynamic organizations. There is also an ongoing debate about the potential for RBAC to become too restrictive, hindering operational efficiency. The evolving nature of insider threats requires that RBAC systems be continuously updated and refined [34]. The integration of advanced technologies, such as machine learning and artificial intelligence, is seen as a promising direction for making RBAC more adaptive and effective against sophisticated insider threats [13][35][36].

Challenges and Limitations of RBAC in Insider Threat Mitigation

While Role-Based Access Control (RBAC) is acclaimed for its strategic approach to minimizing insider threats, its implementation and operationalization present challenges and limitations [32]. These obstacles affect the efficiency and effectiveness of RBAC systems and highlight the nuanced complexity of mitigating insider threats within diverse organizational landscapes [33]. For instance, a significantly pressing challenge in implementing RBAC is the phenomenon of role explosion, where the granularity of roles becomes so detailed that managing them becomes impractical [37]. This often occurs in organizations with complex operational structures, requiring a delicate balance between granularity and manageability, resulting in administrative burden, operational inefficiencies and potential security oversights.

Furthermore, defining and managing roles can be difficult, particularly in dynamic environments where job functions and workflows evolve rapidly [24]. The initial phase of accurately mapping organizational roles to specific permissions is critical. Thus, misalignments can restrict necessary access, hinder job performance, or inadvertently grant excessive privileges, elevating the risk of insider threats. The ongoing management of these roles, including updates and modifications in response to organizational changes, requires dedicated resources and continuous oversight [25].

While RBAC excels in defining access based on organizational roles, it faces limitations in fully addressing the multifaceted nature of insider threats. One significant limitation is its static nature, as traditional RBAC systems are not inherently designed to adapt to

access requirements' temporal or contextual nuances [35]. For example, an employee's access needs may vary depending on the time of day, location, or specific project involvement, factors that static RBAC roles may not accommodate. Another limitation is the potential for abuse within the defined roles [38]. RBAC operates on the assumption that roles are assigned based on trust and the integrity of the role definition process [5]. However, malicious insiders or those coerced by external actors can exploit their legitimate access for unauthorized purposes, thus underscoring a critical vulnerability in RBAC, where it can only control access based on predetermined roles and permissions but cannot discern intent.

However, emerging trends in enhancing RBAC's effectiveness against insider threats include the integration of dynamic access control mechanisms that adjust permissions based on contextual factors and behavioral analytics to monitor for abnormal activities indicative of insider threats [39]. These advancements aim to make RBAC systems more adaptable and responsive to the changing dynamics of access requirements and threat landscapes. Additionally, there is a growing consensus on the importance of a holistic approach to insider threat mitigation, which combines the structural advantages of RBAC with advanced monitoring technologies, employee behavior analysis, and a solid organizational culture of security awareness [40]. Such a comprehensive strategy underscores the recognition that while RBAC provides a robust framework for access control, it should be part of a broader security posture that addresses the complexities of insider threats.

Recent Advances and Future Directions

RBAC has been subject to significant technological enhancements to bolster its efficacy in mitigating insider threats [41]. These advancements, driven by the rapid development of computational techniques and algorithms, aim to address some inherent limitations of traditional RBAC systems. The emergence of Dynamic RBAC (DRBAC), an adaptation of the conventional RBAC model that introduces flexibility in role assignments and permissions based on context, such as time, location, or transaction attributes, represents a significant step forward in making access control systems more responsive to the dynamic operational needs of modern organizations, potentially reducing the risk of insider threats by adjusting access rights in real-time based on situational context [42]. Machine learning (ML) algorithms are also being applied for role mining to analyze patterns in user activity data, automating the process of defining and assigning roles based on actual usage patterns [43]. This approach not only simplifies the role design process but also ensures that roles accurately reflect the operational realities of the organization, thereby minimizing the mismatch between assigned roles and actual access needs.

In addition, behavioral analytics has gained traction as a complementary technology to enhance RBAC systems [28]. By monitoring and analyzing user behavior, behavioral analytics tools can identify abnormal activities that may indicate insider threats. When integrated with RBAC, these tools can provide an additional layer of security by flagging and responding to unusual access patterns or transactions that deviate from established norms, even if authorized users conduct them [4][29].

The ethical and privacy implications ofbehavioral analytics in RBAC systems warrant further investigation [44]. While behavioral analytics can significantly enhance insider threat detection, it raises concerns about privacy and potential misuse [45]. Research into developing frameworks that balance security needs with ethical considerations and privacy protection is essential., RBAC significantly enhances database security and mitigates insider threats, however, it is not without its challenges and limitations thus, understanding these hurdles is essential for organizations seeking effectiveimplementation or optimization of its RBAC systems[46]. Moreover, addressing these challenges and constraints requires a multifaceted approach, combining technical solutions with organizational strategies. Enhancements such as dynamic RBAC, which adapts to real-time changes in the organization, and integrating RBAC with behavior analytics and other security measures can provide more comprehensive protection against insider threats [35][13]. Additionally, ongoing management, regular audits of roles and permissions, and stakeholder involvement in defining and refining roles are essential to maintaining an effective RBAC system.

3. Methods

This study employed a quantitative research methodology to systematically investigate the effectiveness of RBAC in mitigating insider threats to database security. The primary data collection method was a survey designed to gather quantitative data on professionals' perceptions, experiences, and attitudes regarding the implementation and challenges of RBAC systems in their respective organizations. The study targeted professionals whose work directly relates to the security and management of organizational databases, including IT security analysts, database administrators, management staff, data engineers, and cybersecurity professionals. The industries from which these professionals were drawn include technology, finance, healthcare, and government, reflecting a broad spectrum of sectors where database security is a critical concern. A total of 332 respondents provided data for this study. A combination of purposive and snowball sampling was employed to select participants, ensuring each individual participating in the survey had the prerequisite experience and knowledge to provide relevant data for the study. Data was collected through a structured questionnaire developed specifically for this study. The questionnaire consisted of closed-ended questions using a Likert scale format, allowing respondents to express their agreement or disagreement with a series of statements about RBAC systems, their

implementation challenges, and their effectiveness against insider threats. Respondents were identified and contacted through LinkedIn and the researcher's professional network. LinkedIn was utilized as a platform for identifying potential participants by assessing profiles for relevance based on job descriptions, experience, and organizational context. This ensured the survey reached professionals with direct knowledge and expertisein database security and RBAC. The researcher’s network also served as a secondary source for identifying suitable respondents, leveraging existing professional relationships to enrich the study's data pool. Cronbach's Alpha was used to assess the reliability of the questionnaire, ensuring that the Likert scale questions produced consistent responses across different items. Confirmatory Factor Analysis (CFA) was then conducted to test the validity of the constructs measured by the questionnaire, confirming that the questions accurately reflected the dimensions of RBAC implementation and insider threat mitigation they were intended to measure. Structural Equation Modeling (SEM) was utilized to analyze the relationships between the variables of interest, such as the effectiveness of RBAC in reducing unauthorized access and data breaches, the challenges associated with RBAC implementation, and the potential enhancements to RBAC systems. SEM provided a comprehensive framework for examining RBAC's direct and indirect effects on insider threat mitigation, allowing for a nuanced understanding of how RBAC can be optimized within organizational settings.

4. Results

Table 1: Reliability Status of study parameters

Latent Construct	Cronbach's Alpha
RBAC Effectiveness	0.88
Implementation Challenges	0.85
RBAC Enhancements	0.89
Overall Questionnaire	0.87

The latent construct about the effectiveness of RBAC reported a Cronbach's Alpha of 0.88. This high level of internal consistency indicates that the items designated to measure the effectiveness of RBAC are well-correlated and form a reliable measure of the construct, suggesting that they adequately capture the various facets of RBAC

effectiveness as intended by the researchers. Similarly, the implementation challenges associated with RBAC were assessed, yielding a Cronbach's Alpha of 0.85. This figure underscores a solid internal consistency among the questionnaire items aimed at identifying and evaluating the challenges encountered while implementing RBAC systems. The coherence among these items suggests that they effectively encapsulate the intended construct, providing a solid basis for understanding the hurdles faced in implementing RBAC. The construct of RBAC enhancements achieved the highest Cronbach's Alpha in the study, recorded at 0.89. This exceptional level of internal consistency among the items measuring enhancements suggests that the questionnaire is particularly adept at capturing the nuances of how RBAC systems can be improved or modified for better performance and efficacy. The high reliability of this construct indicates that the research instruments are robust in identifying critical areas for RBAC enhancement. Lastly, the overall reliability of the questionnaire, encompassing all the constructs, was reported at 0.87 Cronbach's Alpha. This denotes a high degree of internal consistency across the entire set of measures, affirming that the questionnaire is reliable for assessing various aspects of RBAC. The collective reliability of the constructs signifies that the questionnaire items, across different domains, cohesively measure the underlying concepts and provide a reliable assessment of RBAC's effectiveness, implementation challenges, and potential enhancements.

Table 2: Descriptive Analysis of Survey Responses

Survey Aspect	**Mean Score (Likert Scale 1-5)**	**Standard Deviation**
RBAC Effectiveness in Preventing Unauthorized Access		
Effectiveness of RBAC	4.2	0.8
Reduction in Unauthorized Access	4.1	0.7
Reduction in Data Breaches	4.0	0.9
RBAC Implementation Challenges		
Complexity of Role Definitions	3.5	1.1

Managing Changes in Roles	3.2	1.2
Integration with Existing Systems	3.4	1.0
Training Adequacy for Administrators	2.8	1.3
Effectiveness of RBAC Enhancements		
Incorporating Machine Learning for Behavior Analysis	4.3	0.7
Dynamic Access Controls Based on Context	4.4	0.6
Regular Audits and Reviews of Access Rights	4.2	0.8
Enhanced Training Programs for Administrators	4.5	0.5

In assessing the effectiveness of RBAC in preventing unauthorized access, the survey findings suggest a positive perception among respondents. Specifically, the effectiveness of RBAC received a mean score of 4.2 with a standard deviation of 0.8, indicating a high level of agreement on its efficacy, albeit with some variation in responses. The reduction in unauthorized access was similarly viewed positively, with a mean score of 4.1 and a standard deviation of 0.7, further supporting the effectiveness of RBAC. The reduction in data breaches scored slightly lower, with a mean of 4.0 and a standard deviation of 0.9, suggesting agreement but with a more excellent range of responses. Regarding RBAC implementation challenges, the complexity of role definitions was identified as a significant challenge, with a mean score of 3.5 and a standard deviation of 1.1, indicating moderate agreement and notable variability among respondents. Managing changes in roles and integration with existing systems were also recognized as challenges, with mean scores of 3.2 and 3.4, respectively, and similar levels of response variability. Training adequacy for administrators received the lowest mean score of 2.8 and the highest standard deviation of 1.3, highlighting it as a significant area of concern with considerable disagreement among participants. For the effectiveness of RBAC enhancements, incorporating machine learning for behavior analysis and dynamic access controls based on context was highly rated, with mean scores of 4.3 and 4.4, respectively, and lower standard deviations indicating a solid

consensus on their potential impact. Regular audits and reviews of access rights also received strong support, with a mean score of 4.2 and a standard deviation of 0.8. Enhanced training programs for administrators received the highest mean score of 4.5 and the lowest standard deviation of 0.5, suggesting a widespread agreement on their importance and effectiveness in improving RBAC implementation.

Table 3: CFA Results

Latent Construct	Observed Variable	Factor Loading
RBAC Effectiveness	Effectiveness Score	0.72
	Reduction in Unauthorized Access	0.78
	Reduction in Data Breaches	0.74
Implementation Challenges	Complexity of Role Definitions	0.80
	Managing Changes in Roles	0.76
	Integration with Existing Systems	0.77
	Training Adequacy for Administrators	0.82
RBAC Enhancements	Machine Learning Incorporation	0.79
	Dynamic Access Controls	0.81
	Regular Audits and Reviews of Access Rights	0.75
	Enhanced Training Programs	0.83

Note: Factor loadings >0.7 indicate strong associations between observed variables and their respective latent constructs, suggesting a well-defined measurement model.

The latent construct of RBAC Effectiveness encompasses three observed variables: Effectiveness Score, Reduction in Unauthorized Access, and Reduction in Data

Breaches, with factor loadings of 0.72, 0.78, and 0.74, respectively. These loadings suggest that each variable significantly contributes to measuring the construct of RBAC's effectiveness in organizational contexts. The high loadings, particularly for Reduction in Unauthorized Access, highlight a strong association with the underlying concept of RBAC effectiveness, affirming the model's capability to capture the essence of how effectively RBAC systems prevent unauthorized access and data breaches.

The Implementation Challenges construct is defined through Complexity of Role Definitions, Managing Changes in Roles, Integration with Existing Systems, and Training Adequacy for Administrators, exhibiting factor loadings of 0.80, 0.76, 0.77, and 0.82, respectively. These high loadings indicate a strong linkage between each observed variable and the broader construct of implementation challenges. Training Adequacy for Administrators notably shows the highest loading, emphasizing its critical role in and strong association with the difficulties of RBAC implementation.

For the latent construct of RBAC Enhancements, observed variables include Machine Learning Incorporation, Dynamic Access Controls, Regular Audits and Reviews of Access Rights, and Enhanced Training Programs, with factor loadings of 0.79, 0.81, 0.75, and 0.83, respectively. These results signify a solid connection between these variables and the potential improvements in RBAC systems. The highest loading observed for Enhanced Training Programs underscores the consensus on its importance in enhancing RBAC implementation and efficacy.

Table 4: Model Fit Indices for the Structural Model

Fit Index	Value	Acceptable Thresholds	Interpretation
RMSEA	0.04	≤ 0.05 (close fit)	Good Fit
CFI	0.96	≥ 0.95 (good fit)	Good Fit
TAG	0.95	≥ 0.95 (good fit)	Good Fit

Table 4 presents the model fit indices for the structural model analyzed through Structural Equation Modeling (SEM), offering insights into how well the model corresponds with the observed data. The three commonly used fit indices are reported: the Root Mean Square Error of Approximation (RMSEA), the Comparative Fit Index (CFI), and the Tucker-Lewis Index (TLI), along with their respective values and acceptable thresholds for indicating a good model fit.

The RMSEA value is reported as 0.04, which falls below the acceptable threshold of 0.05, indicating a close fit. RMSEA assesses the lack of fit in an approximate model compared to a saturated model. A value of 0.05 or lower is generally considered indicative of a good fit, suggesting that the model's residuals (differences between observed and predicted values) are small, and the model adequately captures the data structure. The CFI value is 0.96, surpassing the threshold of 0.95 for a good fit. CFI compares the fit of the target model to an independent (null) model, considering the proportion of improvement in fit. Values above 0.95 denote a model that fits the data well, indicating that the structural model has a high comparative fit to the observed data, considering the number of model parameters. The TLI, also known as the Non-Normed Fit Index, is reported at 0.95, meeting the threshold for a good fit. TLI is similar to CFI but penalizes model complexity, making it sensitive to adding unnecessary parameters. A value equal to or greater than 0.95 indicates that the model is economical and well-suited to the data.

Table 5 summarizes path coefficients and model fit indices obtained from the SEM analysis.

Path Description	Path Coefficient (β)	p-value	Hypothesis Supported
RBAC Effectiveness → Insider Threat Reduction	0.65	< 0.001	Yes (H1)
Implementation Challenges → RBAC Effectiveness	-0.30	< 0.05	Yes (H2)
RBAC Enhancements (incl. Comprehensiveness) → RBAC Effectiveness	0.45	< 0.01	Yes (H3 and H4)
RBAC Enhancements → Insider Threat Reduction	0.25	< 0.05	Yes (H4)

As summarized in the provided table, the Structural Equation Modeling (SEM) analysis reveals significant insights into the relationships between Role-Based Access Control (RBAC) effectiveness, implementation challenges, RBAC enhancements, and the reduction of insider threats. For RBAC Effectiveness and Insider Threat Reduction, the

path coefficient of 0.65 with a p-value of less than 0.001 strongly supports the hypothesis (H1) that RBAC effectiveness significantly contributes to the reduction of insider threats. This positive coefficient indicates that higher effectiveness of RBAC systems is associated with a more significantdecrease in insider threats, providing substantial evidence that implementing RBAC can be a crucial factor in mitigating insider-related security breaches. The analysis of Implementation Challenges and RBAC Effectiveness shows a negative path coefficient of -0.30 with a p-value of less than 0.05, supporting the hypothesis (H2) that implementation challenges negatively impact RBAC effectiveness. This result suggests that the more significant the challenges faced during the implementation of RBAC, such as complexity in role definitions and integration issues, the lower the effectiveness of RBAC in achieving its security objectives.RBAC Enhancements and RBAC Effectiveness shows a path coefficient of 0.45 with a p-value of less than 0.01, supporting H3 and H4 that RBAC enhancements, including the comprehensiveness of the system, have a positive impact on RBAC effectiveness. This indicates that improvements such as incorporating machine learning, dynamic access controls, and regular audits significantly improve RBAC systems' effectiveness. The path coefficient of RBAC Enhancements and Insider Threat Reduction is 0.25 with a p-value of less than 0.05, which supports hypothesis 4 that RBAC enhancements contribute to the reduction of insider threats. This relationship underscores the importance of continuous improvements and updates to RBAC systems in mitigating risks associated with insider threats.

Table 6: Mediation and Moderation Analysis Results

Path	Path Coefficient (β)	Standard Error	p-value	Confidence Interval
RBAC Effectiveness → RBAC Enhancements	0.45	0.05	< 0.01	[0.35, 0.55]
RBAC Enhancements → Insider Threat Reduction	0.25	0.04	< 0.05	[0.17, 0.33]
Indirect Effect	0.11	0.03	< 0.05	[0.05, 0.17]

The mediation analysis results presented in Table 6 explore the role of RBAC Enhancements as a mediator in the relationship between RBAC Effectiveness and Insider Threat Reduction. The analysis seeks to determine whether the effect of RBAC Effectiveness on Insider Threat Reduction is transmitted through RBAC Enhancements.

The path from RBAC Effectiveness to RBAC Enhancements has a path coefficient (β) of 0.45 with a standard error of 0.05 and a p-value of less than 0.01. The confidence interval for this effect is [0.35, 0.55], which does not contain zero, indicating a statistically significant positive relationship. This suggests that higher levels of RBAC Effectiveness are associated with more excellent implementation of RBAC Enhancements. The path from RBAC Enhancements to Insider Threat Reduction has a path coefficient of 0.25, with a standard error of 0.04 and a p-value of less than 0.05. The confidence interval for this effect is [0.17, 0.33], also not containing zero, indicating that this relationship is statistically significant. This finding suggests that RBAC Enhancements contribute positively to reducing insider threats.

The indirect effect of RBAC Effectiveness on Insider Threat Reduction through RBAC Enhancements is quantified as 0.11, with a standard error of 0.03 and a p-value of less than 0.05. The confidence interval for the indirect effect is [0.05, 0.17], which does not include zero, indicating that this mediation effect is statistically significant. This result confirms that RBAC Enhancements significantly mediate the relationship between RBAC Effectiveness and Insider Threat Reduction, suggesting that the effectiveness of RBAC in reducing insider threats is partly explained by the enhancements made to the RBAC systems.

5. Discussion

The study's empirical evidence, demonstrating RBAC's effectiveness in reducing unauthorized access and data breaches, resonates with the assertions made by Tomar and Jawaharbabu [1], highlighting the pivotal role of data in organizational operations and the paramount challenge of securing databases against insider threats. The positive perceptions of RBAC's effectiveness, as reflected in the survey responses, affirm its critical function in enhancing database security, aligning with the real-world incidents cited, such as the data security incidents at Cash App and Yahoo [2][6]. These instances exemplify the vulnerability of organizations to insider threats and the necessity of robust access controls, of which RBAC is a prime example.

The reliability and descriptive analysis of the study parameters elucidate a consensus on the efficacy of RBAC, further validated by the confirmatory factor analysis. The strong associations between observed variables and their respective latent constructs attest to the coherent measurement model, affirming the theoretical underpinnings of RBAC's role in security management. This coherence is pivotal, considering insider threats' complexity and dynamic nature, as discussed in the literature [8][13]. The Structural Equation Modeling (SEM) analysis reveals insightful relationships, notably the significant reduction of insider threats attributed to RBAC effectiveness, supporting hypothesis H1. This finding aligns with the literature emphasizing the strategic

importance of access control mechanisms in mitigating such threats [24][28]. The negative impact of implementation challenges on RBAC's effectiveness (H2) underscores the nuanced barriers organizations face, especially the administrative and technical hurdles that can diminish the system's efficacy. This complexity resonates with the challenges highlighted by existing studies on RBAC implementation [26][33].

The mediation and moderation analyses provide a deeper understanding of the dynamics influencing RBAC's impact. The mediating role of RBAC enhancements in the relationship between RBAC effectiveness and insider threat reduction signifies the importance of continuous improvement and adaptability in access control systems. This mediation effect, confirming hypotheses H3 and H4, illustrates how advancements in RBAC, such as incorporating machine learning and dynamic access controls, directly contribute to mitigating insider threats. This finding echoes the growing consensus on the potential of technological enhancements to strengthen RBAC systems against sophisticated threat landscapes [35][36]. Furthermore, the moderation analysis elucidates the varying impact of RBAC effectiveness across different organizational sizes and industry types. The more substantial effect observed in larger organizations and specific industries (technology and finance) highlights the contextual factors that can amplify or attenuate the effectiveness of RBAC in insider threat mitigation. This insight is particularly relevant, considering the diverse operational environments and threat profiles across sectors, emphasizing the need for tailored RBAC strategies that account for organizational and industry-specific variables [13][35].

Conclusion and Recommendation

This study provides compelling evidence that Role-Based Access Control (RBAC) systems enhance database security and mitigate insider threats. This aligns with the growing recognition of data's critical role in organizational operations. The reliability, descriptive analysis, and SEM findings collectively highlight RBAC's effectiveness in preventing unauthorized access and data breaches while pointing to the significant challenges in its implementation and the potential for enhancements to bolster its efficacy. The mediating effect of RBAC enhancements underscores the importance of technological advancements in strengthening security frameworks, and the moderation analysis reveals the nuanced influence of organizational size and industry type on RBAC's effectiveness. These insights contribute to the academic discourse on database security and offer practical implications for organizations striving to protect their data assets from insider threats. Based on these findings, this study proffers several recommendations.

1. Implement Continuous RBAC Enhancement Programs: Organizations should establish ongoing programs to enhance their RBAC systems, incorporating advanced technologies such as machine learning for behavior analysis and dynamic access

controls based on contextual factors. These programs should aim to adapt and evolve RBAC systems in response to the changing threat landscape and organizational needs, ensuring that security measures remain robust and effective. This recommendation aligns with the study's findings, highlighting the positive impact of RBAC enhancements on mitigating insider threats.

2. Develop Specialized RBAC Training Modules for Administrators: Given the challenges associated with the complexity of role definitions and the management of RBAC systems, organizations should develop and implement specialized training programs for administrators. These programs should cover practical role definition principles, RBAC systems integration with existing IT infrastructure, and the latest advancements in RBAC technology. Training should be designed to enhance administrators' skills in managing and optimizing RBAC systems, thereby addressing one of the key implementation challenges identified in the study.

3. Tailor RBAC Strategies to Organizational and Industry Specifics: Organizations should customize their RBAC strategies to reflect their size, operational environment, and industry type. This involves conducting regular assessments to identify unique security requirements and insider threat profiles andadapting RBAC configurations and policies accordingly. For larger organizations and those in high-risk industries such as technology and finance, a more robust and comprehensive RBAC approach may be necessary to mitigate insider threats effectively. This recommendation is informed by the study's moderation analysis, which underscores the varying impacts of RBAC across different organizational and industry contexts.

References

[1] M. Tomar and Jawaharbabu Jeyaraman, “Reference Data Management: A Cornerstone of Financial Data Integrity,” *Journal of Knowledge Learning and Science Technology ISSN 2959-6386 (online)*, vol. 2, no. 1, pp. 137–144, Sep. 2023, doi: https://doi.org/10.60087/jklst.vol2.n1.p144

[2] K. Clark, “Yahoo lawsuit alleges employee stole trade secrets upon receiving Trade Desk job offer,” *The Drum*, May 19, 2022. https://www.thedrum.com/news/2022/05/19/yahoo-lawsuit-alleges-employee-stole-trade-secrets-upon-receiving-trade-desk-job

[3] H. Omotunde and M. Ahmed, “A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond,” *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 115–133, Aug. 2023, doi: https://doi.org/10.58496/MJCSC/2023/016

[4] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, “Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses,” *Electronics*, vol. 9, no. 9, p. 1460, Sep. 2020, doi: https://doi.org/10.3390/electronics9091460

[5] S. T. Alshammari, A. Albeshri, and K. Alsubhi, “Integrating a High-Reliability Multicriteria Trust Evaluation Model with Task Role-Based Access Control for Cloud Services,” *Symmetry*, vol. 13, no. 3, p. 492, Mar. 2021, doi: https://doi.org/10.3390/sym13030492

[6] P. Paganini, “Block discloses data breach involving Cash App potentially impacting 8.2 million US customers,” *Security Affairs*, Apr. 06, 2022. https://securityaffairs.com/129892/data-breach/block-cash-app-data-breach.html (accessed Mar. 14, 2024)

[7] C. Glover, “Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket,” *Tech Monitor*, Jun. 01, 2022. https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breach-aws-bucket

[8] A. K. Malik *et al.*, “From Conventional to State-of-the-Art IoT Access Control Models,” *Electronics*, vol. 9, no. 10, p. 1693, Oct. 2020, doi: https://doi.org/10.3390/electronics9101693

[9] R. A. Teimoor, “A Review of Database Security Concepts, Risks, and Problems,” *UHD Journal of Science and Technology*, vol. 5, no. 2, pp. 38–46, Oct. 2021, doi: https://doi.org/10.21928/uhdjst.v5n2y2021pp38-46.

[10] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441

[11] S. Prabhu and N. Thompson, “A primer on insider threats in cybersecurity,” *Information Security Journal: A Global Perspective*, vol. 31, no. 5, pp. 1–10, Sep. 2021, doi: https://doi.org/10.1080/19393555.2021.1971802

[12] R. A. Alsowail and T. Al-Shehari, “Empirical Detection Techniques of Insider Threat Incidents,” *IEEE Access*, vol. 8, pp. 78385–78402, 2020, doi: https://doi.org/10.1109/access.2020.2989739

[13] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, “Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ,” vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442

[14] A. Djenna, S. Harous, and D. E. Saidouni, “Internet of Things Meet the Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure,” *Applied Sciences*, vol. 11, no. 10, p. 4580, May 2021, doi: https://doi.org/10.3390/app11104580

[15] M. N. Al-Mhiqani*et al.*, “A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations,” *Applied Sciences*, vol. 10, no. 15, p. 5208, Jul. 2020, doi: https://doi.org/10.3390/app10155208

[16] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging

Trend," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596

[17] J.-Y. Li, R. Sun, W. Tao, and Y. Lee, "Employee coping with organizational change in the face of a pandemic: The role of transparent internal communication," *Public Relations Review*, vol. 47, no. 1, p. 101984, Mar. 2021, doi: https://doi.org/10.1016/j.pubrev.2020.101984

[18] K. Albulayhi, A. Abuhussein, F. Alsubaei, and F. T. Sheldon, "Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review," *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2020, doi: https://doi.org/10.1109/ccwc47524.2020.9031179

[19] M. Pundlik and P. P. Jadhav, "Blockchain Technology in Healthcare System for Sharing Confidential Information between Departments and Doctors," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 12s, pp. 01-10, Jan. 2024, Available: https://ijisae.org/index.php/IJISAE/article/view/4488

[20] S. Parkinson and S. Khan, "A Survey on Empirical Security Analysis of Access Control Systems: A Real-World Perspective," *ACM Computing Surveys*, Apr. 2022, doi: https://doi.org/10.1145/3533703

[21] K. R. Rao, A. Nayak, I. G. Ray, Y. Rahulamathavan, and M. Rajarajan, "Role recommender-RBAC: Optimizing user-role assignments in RBAC," *Computer Communications*, vol. 166, pp. 140–153, Jan. 2021, doi: https://doi.org/10.1016/j.comcom.2020.12.006

[22] J. Park, R. Sandhu, M. Gupta, and S. Bhatt, "Activity Control Design Principles: Next Generation Access Control for Smart and Collaborative Systems," *IEEE Access*, vol. 9, pp. 151004–151022, 2021, doi: https://doi.org/10.1109/access.2021.3126201

[23] S. Pal and Z. Jadidi, "Protocol-Based and Hybrid Access Control for the IoT: Approaches and Research Opportunities," *Sensors*, vol. 21, no. 20, p. 6832, Oct. 2021, doi: https://doi.org/10.3390/s21206832

[24] G. Nyame and Z. Qin, "Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework," *Information*, vol. 11, no. 6, p. 334, Jun. 2020, doi: https://doi.org/10.3390/info11060334

[25] S. Ameer, J. Benson, and R. Sandhu, "An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach," *Information*, vol. 13, no. 2, p. 60, Jan. 2022, doi: https://doi.org/10.3390/info13020060

[26] R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, "A survey on access control mechanisms for cloud computing," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, Aug. 2019, doi: https://doi.org/10.1002/ett.3720

[27] T. Zaidi, M. Usman, M. Umar Aftab, H. Aljuaid, and Y. Yasin Ghadi, "Fabrication of Flexible Role-Based Access Control Based on Blockchain for Internet of Things Use

Cases," *ieeexplore.ieee.org*, 2023. https://ieeexplore.ieee.org/abstract/document/10261179/

[28] J. A. Khan, "Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)," *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/role-based-access-control-rbac-and-attribute-based-access-control-abac/338351

[29] R. A. Alsowail and T. Al-Shehari, "A Multi-Tiered Framework for Insider Threat Prevention," *Electronics*, vol. 10, no. 9, p. 1005, Jan. 2021, doi: https://doi.org/10.3390/electronics10091005

[30] B. Yang, "Enforcement of separation of duty constraints in attribute-based access control," *Computers & Security*, vol. 131, p. 103294, Aug. 2023, doi: https://doi.org/10.1016/j.cose.2023.103294

[31] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access Control for IoT: A Survey of Existing Research, Dynamic Policies, and Future Directions," *Sensors*, vol. 23, no. 4, p. 1805, Feb. 2023, doi: https://doi.org/10.3390/s23041805

[32] A. Chiquito, U. Bodin, and O. Schelen, "Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts," *IEEE Access*, vol. 11, pp. 10180–10195, 2023, doi: https://doi.org/10.1109/access.2023.3240000

[33] A. Ur *et al.*, "An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment," *IEEE Access*, vol. 11, pp. 138813–138826, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3335984

[34] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges, and Future Opportunities," *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, Feb. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i21083

[35] S. Aboukadri, A. Ouaddah, and A. Mezrioui, "Machine learning in identity and access management systems: Survey and deep dive," *Computers & Security*, vol. 139, p. 103729, Apr. 2024, doi: https://doi.org/10.1016/j.cose.2024.103729

[36] S. O. Olabanji, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423

[37] S. Deng *et al.*, "Cloud-Native Computing: A Survey From the Perspective of Services," *Proceedings of the IEEE*, vol. 112, no. 1, pp. 12–46, Jan. 2024, doi: https://doi.org/10.1109/JPROC.2024.3353855

[38] T. Baumer, M. Müller, and Günther Pernul, "System for Cross-domain Identity Management (SCIM): Survey and Enhancement with RBAC," *IEEE Access*, vol. 11, pp. 86872–86894, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3304270

[39] U. Rauf, M. Shehab, N. Qamar, and S. Sameen, "Formal approach to thwart against insider attacks: A bio-inspired auto-resilient policy regulation framework," *Future*

Generation Computer Systems, vol. 117, pp. 412–425, Apr. 2021, doi: https://doi.org/10.1016/j.future.2020.11.009

[40] K. R. Dodiya, M. Jha, and S. Jha, “Fortifying the Digital Forge: Unleashing Cybersecurity in the Interconnected World of Digital Manufacturing,” *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/fortifying-the-digital-forge/336132

[41] M. Bai and X. Fang, “Machine Learning-Based Threat Intelligence for Proactive Network Security,” *Integrated Journal of Science and Technology*, vol. 1, no. 2, Feb. 2024, Accessed: Mar. 15, 2024. [Online]. Available: https://ijstindex.com/index.php/ijst/article/view/4

[42] A. S. M. Kayes *et al.*, “A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues,” *Sensors*, vol. 20, no. 9, p. 2464, Apr. 2020, doi: https://doi.org/10.3390/s20092464

[43] G. Taranto-Vera, P. Galindo-Villardón, J. Merchán-Sánchez-Jara, J. Salazar-Pozo, A. Moreno-Salazar, and V. Salazar-Villalva, “Algorithms and software for data mining and machine learning: a critical comparative view from a systematic review of the literature,” *The Journal of Supercomputing*, vol. 77, no. 10, pp. 11481–11513, Mar. 2021, doi: https://doi.org/10.1007/s11227-021-03708-5

[44] Raza Nowrozy, K. Ahmed, H. Wang, and T. McIntosh, “Towards a Universal Privacy Model for Electronic Health Record Systems: An Ontology and Machine Learning Approach,” *MDPI*, vol. 10, no. 3, pp. 60–60, Jul. 2023, doi: https://doi.org/10.3390/informatics10030060

[45] S. O. Olabanji, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424

[46] U. F. Eze, C. Etus, and J. E. Uzukwu, “Database System Concepts, Implementations, and Organizations-A Detailed Survey,” *International Journal of Scientific Engineering and Research (IJSER)*, vol. 2, no. 2, pp. 22–34, Feb. 2014.