International Journal of Management Information Systems and Data Science, 2024;1(04): 80-95
ISSN: 2997-9560
Doi: 10.62304/ijmisds.v1i04.202

ARTIFICIAL INTELLIGENCE ENHANCED IDENTITY AND ACCESS MANAGEMENT PREVENTING UNAUTHORIZED ACCESS IN MODERN ENTERPRISES

Md Takbir Hossen Sarker[1], Md Sanaur Rahman[2], Mohammed Mahi Uddin[3], Nur Alam Farhad Shakil[4]

[1]Master of Science in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA
Email: takbir.student@wust.edu
https://orcid.org/0009-0000-9667-6571

2Master of Science in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA
Email: msrahman.student@wust.edu
https://orcid.org/0009-0001-6959-9467

[3]Master of Science in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA
Email: mmahi.student@wust.edu
https://orcid.org/0009-0008-0085-0255

[4]Master of Science in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA
Email: nshakil.student@wust.edu
https://orcid.org/0009-0005-8217-3371

Keywords

AI-Enhanced Identity Management
Unauthorized Access Prevention
Cybersecurity
Enterprise IAM
Machine Learning
Authentication
Access Control
Adaptive Security

***Received**: 02nd August, 2024*
***Accepted**: 15th September,2024*
***Published**: 18th September,2024*

ABSTRACT

As enterprises increasingly migrate to digital platforms, securing systems from unauthorized access becomes crucial to safeguarding sensitive data. Identity and Access Management (IAM) systems have traditionally been implemented to manage user access and authenticate identities. However, with growing threats of sophisticated cyber-attacks, traditional IAM methods are proving inadequate. Artificial Intelligence (AI) has emerged as a transformative force in enhancing IAM systems by providing adaptive, intelligent solutions to prevent unauthorized access. This paper explores the role of AI-enhanced IAM in modern enterprises, emphasizing its ability to predict, detect, and respond to potential security breaches. Through a detailed examination of current AI applications in IAM, this study demonstrates how AI-enabled tools can increase security resilience, reduce false positives, and automate responses to evolving threats, thus offering enterprises a proactive defense against unauthorized access.

International Journal of Management Information Systems and Data Science, 2024;1(04): 80-95
Doi: 10.62304/ijmisds.v1i04.202

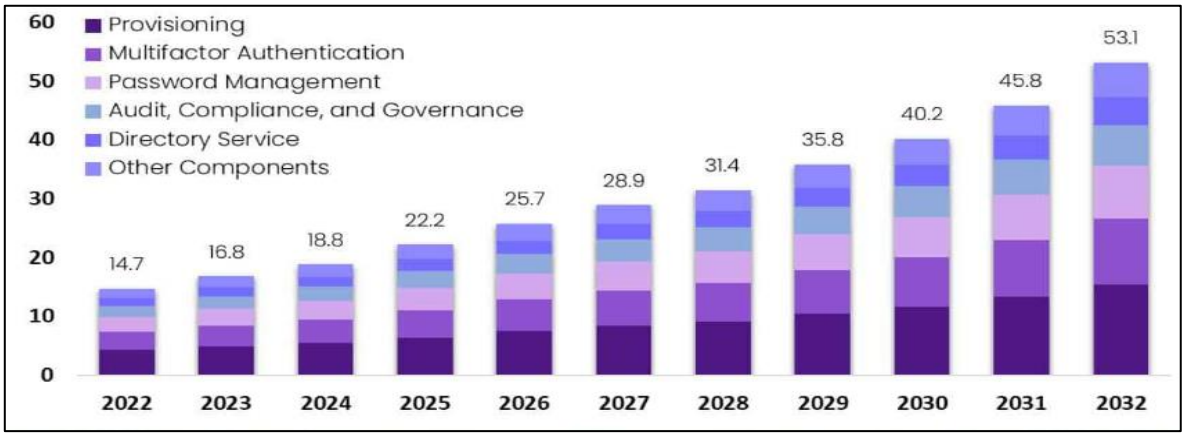
1 Introduction

In the era of digital transformation, modern enterprises are increasingly dependent on interconnected systems and vast digital infrastructures (Lee & Li, 2023). While these advancements have enabled organizations to enhance productivity and operational efficiency, they have also exposed enterprises to significant security threats, particularly unauthorized access to sensitive information. Unauthorized access, which can be caused by both internal actors (insider threats) and external attackers (hackers), is one of the most prevalent forms of security breach, leading to substantial financial, reputational, and operational damage (Li et al., 2024). Traditional Identity and Access Management (IAM) systems have long been the backbone of organizational cybersecurity, tasked with the critical role of managing user identities, granting permissions, and ensuring that only authorized users gain access to the organization's digital assets (Mansfield-Devine, 2022). However, these traditional systems are becoming increasingly inadequate as the complexity and frequency of cyberattacks rise, coupled with the challenges introduced by remote working environments and cloud-based infrastructures (Lee, 2009; Mazar et al., 2008).

IAM systems, in their conventional form, often rely on static authentication mechanisms, such as passwords or two-factor authentication, which can be easily compromised by sophisticated attackers (Ma, 2022). Furthermore, the increasing adoption of cloud computing and bring-your-own-device (BYOD) policies has expanded the attack surface, making it difficult for static IAM solutions to effectively secure enterprise networks (Melián-González et al., 2019). As these challenges mount, cybercriminals have begun deploying more advanced strategies, including phishing, credential stuffing, and advanced persistent threats (APT), to bypass traditional IAM defenses (Mikuletič et al., 2024). These methods target the inherent vulnerabilities within static access control systems, demonstrating the urgent need for more dynamic, intelligent, and adaptive security solutions. The integration of Artificial Intelligence (AI) in IAM systems has emerged as a revolutionary approach to address these security gaps, providing enterprises with the tools to not only detect but also predict and prevent unauthorized access attempts (Mohammadi et al., 2019).

AI-enhanced IAM systems differ from their traditional counterparts in that they leverage machine learning (ML) algorithms to analyze vast amounts of user data, detect behavioral patterns, and identify anomalies in real time (Moody et al., 2018). Machine learning algorithms, in particular, enable IAM systems to learn from historical data, allowing for continuous

Figure 1: Global Identity and Access Management Market (USD Billion)



Source: market.us (2024)

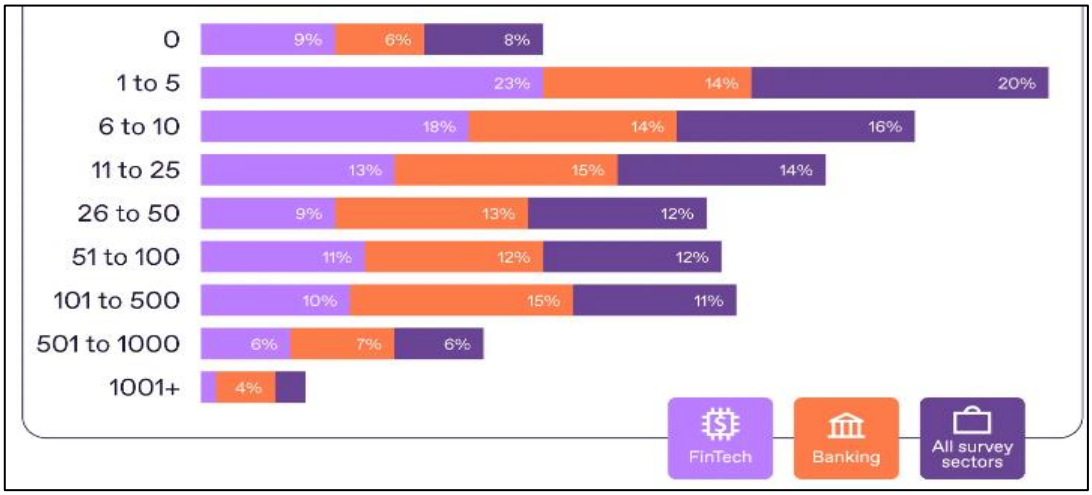
Doi: 10.62304/ijmisds.v1i04.202

Correspondence: ***Md Takbir Hossen Sarker***
Master of Science in Information Technology, Washington University of Science and Technology, Alexandria, Virginia, USA
Email: takbir.student@wust.edu

authentication that evolves with the user's behavior (Nasir et al., 2022). For instance, AI can analyze how a user typically interacts with an organization's systems—such as login times, access locations, and commonly used applications—and flag any deviations from these patterns as potential security threats (Pandey et al., 2024). This continuous monitoring process provides a dynamic layer of security that is not reliant on static credentials, making it more difficult for unauthorized users to exploit known vulnerabilities. As a result, AI-enhanced IAM systems are increasingly being adopted to mitigate the risk of insider threats and external attacks (Nasir et al., 2022) (See figure 1).

One of the key advantages of AI-enhanced IAM systems is their ability to reduce the frequency of false positives, a common issue with traditional IAM solutions that often leads to unnecessary access denials or disruptions to legitimate users (Jim et al., 2024; Abdur et al., 2024). Through AI's capacity to process large datasets and refine predictive models, these systems are better equipped to distinguish between legitimate user behavior and potential threats, improving the overall accuracy of access control decisions (Ahmed et al., 2024; Islam & Apu, 2024; Nahar et al., 2024). This improvement not only enhances security but also ensures a seamless user experience, as legitimate users can access the system without unnecessary interruptions. AI also allows for automated responses to potential threats, such as revoking access or requesting additional authentication in real time, thereby minimizing the window of opportunity for attackers to exploit vulnerabilities (Parsons et al., 2015). This adaptability makes AI-enhanced IAM a proactive security solution, capable of keeping pace with the rapidly evolving threat landscape (see figure 2).

Figure 2: Number of identity fraud incidents during 2022



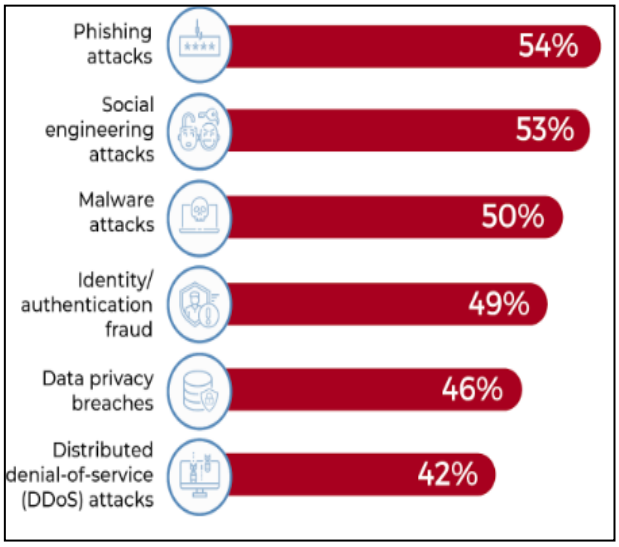
Despite these benefits, the implementation of AI in IAM is not without its challenges. One of the primary concerns involves the potential for algorithmic bias, where machine learning models may inadvertently favor or disadvantage certain groups based on the data used for training (Paul et al., 2023). This bias can lead to unfair access control decisions, particularly in organizations with diverse workforces. Additionally, AI-enhanced IAM systems require continuous updates and the integration of new data to remain effective, which can pose scalability challenges for large enterprises (Peng et al., 2023). Moreover, ensuring that AI-driven decisions are transparent and explainable is crucial for maintaining compliance with data protection regulations and building trust among users (Philip et al., 2023). As organizations continue to explore the integration of AI into their security frameworks, it is essential to balance the benefits of enhanced security with considerations of fairness, privacy, and transparency.

The primary objective of this study is to investigate the role of AI-enhanced Identity and Access Management (IAM) systems in preventing unauthorized access within modern enterprises. Specifically, the research aims to evaluate the effectiveness of AI in improving the accuracy, adaptability, and scalability of access

International Journal of Management Information Systems and Data Science, 2024;1(04): 80-95
Doi: 10.62304/ijmisds.v1i04.202

control systems by leveraging machine learning algorithms to detect anomalies, predict potential

Figure 3: Prevalence of Cybersecurity Threats in Enterprise Systems



security breaches, and respond autonomously to threats. Additionally, the study seeks to explore the practical challenges and ethical considerations involved in implementing AI-driven IAM solutions, such as algorithmic bias, data privacy, and transparency in decision-making. Ultimately, the research aims to provide actionable insights for organizations looking to integrate AI into their security frameworks to strengthen enterprise-wide cybersecurity (See Figure 3).

2 Literatre Review

The increasing complexity of enterprise networks and the rise of sophisticated cyber threats have exposed the limitations of traditional Identity and Access Management (IAM) systems. As organizations adopt cloud computing and remote work, static IAM methods, such as passwords and role-based access, are becoming inadequate for securing sensitive data. In response, Artificial Intelligence (AI) has emerged as a powerful tool to enhance IAM systems by providing real-time monitoring, adaptive authentication, and automated threat detection. This literature review explores the integration of AI in IAM, examining its benefits, challenges, and the current gaps in research related to preventing unauthorized access in modern enterprises.

2.1 Evolution of IAM in the Digital Age

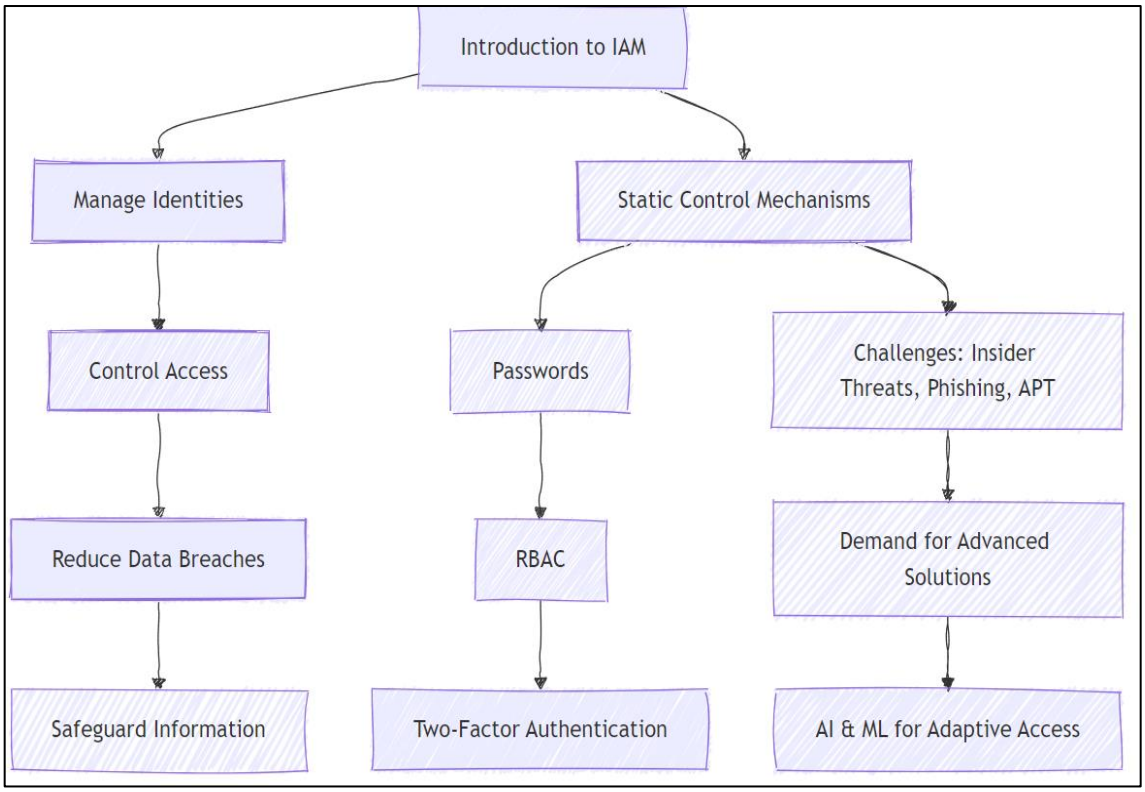
The rapid digital transformation of enterprises, driven by advancements in cloud computing and the rise of remote work, has significantly expanded the attack surface for organizations. Traditionally, IAM systems were designed to operate within controlled, on-premise environments, where security protocols could be tightly managed (Peng et al., 2023). However, as more organizations have adopted cloud services, employees are accessing enterprise systems from various devices and locations, introducing new vulnerabilities. The distributed nature of cloud infrastructures makes it challenging to secure user identities and access points, as traditional perimeter-based security models are no longer effective in safeguarding dispersed environments (Philip et al., 2023). Moreover, the COVID-19 pandemic accelerated the shift to remote work, further compounding the security challenges that IAM systems face. As employees access sensitive corporate data from home networks, often on personal devices, the risk of unauthorized access and data breaches increases (Pitardi et al., 2021). This evolution has created a pressing need for more robust IAM solutions capable of handling the complexity and scale of modern enterprise environments.

The shift to cloud computing and remote work has highlighted the inadequacy of static IAM solutions in addressing modern cybersecurity threats. Traditional IAM systems, which primarily relied on fixed access policies and static authentication methods like passwords and multi-factor authentication, are unable to adapt to the fluid and dynamic nature of cloud environments (Price & Cohen, 2019). In these environments, user roles and access points are continuously changing, and static policies can quickly become outdated or irrelevant. As a result, organizations are increasingly vulnerable to sophisticated threats such as credential stuffing, phishing, and advanced persistent threats (APT), which exploit the weaknesses of traditional IAM systems (Rom et al., 2017). Cloud platforms, in particular, require more granular and adaptive IAM controls to ensure that access is limited to authorized users, based on real-time contextual information such as user behavior, device type, and location (Safa, 2017). This has driven the development of dynamic IAM solutions

that leverage AI and machine learning to continuously monitor and adapt to evolving threats.

Dynamic IAM systems, powered by AI, have emerged as a critical solution to the challenges posed by cloud computing and remote work. Unlike traditional IAM systems, which rely on predefined rules and manual updates, dynamic IAM systems use machine learning algorithms to analyze user behavior patterns in real-time and adjust access controls accordingly (Rotman et al., 2017). By continuously learning from historical data, these systems can predict potential security threats, detect anomalies, and respond to suspicious activities before they escalate into breaches (Scheier & Carver, 1985). For example, AI-enhanced IAM systems can implement adaptive multi-factor authentication (MFA), where additional authentication steps are required only when abnormal behavior is detected, improving both security and user experience (Seyal & Turner, 2013). This adaptability is crucial in cloud environments, where users frequently change roles or access locations, and traditional static IAM systems would otherwise struggle to keep up with these changes (Sharma & Aparicio, 2022) (See figure 4).

Figure 4: Key points in the IAM system overview



The evolution of IAM systems toward dynamic, AI-driven solutions represents a significant shift in enterprise security. As organizations continue to embrace digital transformation, the need for IAM systems that can handle the complexity of cloud infrastructures and remote work environments will only grow (Singh et al., 2014). AI-enhanced IAM systems not only improve security by continuously monitoring user behavior and detecting anomalies but also offer scalability and efficiency in managing large and complex environments (Shao et al., 2023). Furthermore, by automating many aspects of access control, these systems reduce the administrative burden on IT teams, allowing for more efficient resource allocation (Singh et al., 2014). As threats continue to evolve, the future of IAM will likely depend on the ability of organizations to integrate dynamic, AI-powered solutions that can adapt to changing security needs while maintaining robust protection of sensitive data.

2.2 AI in Cybersecurity

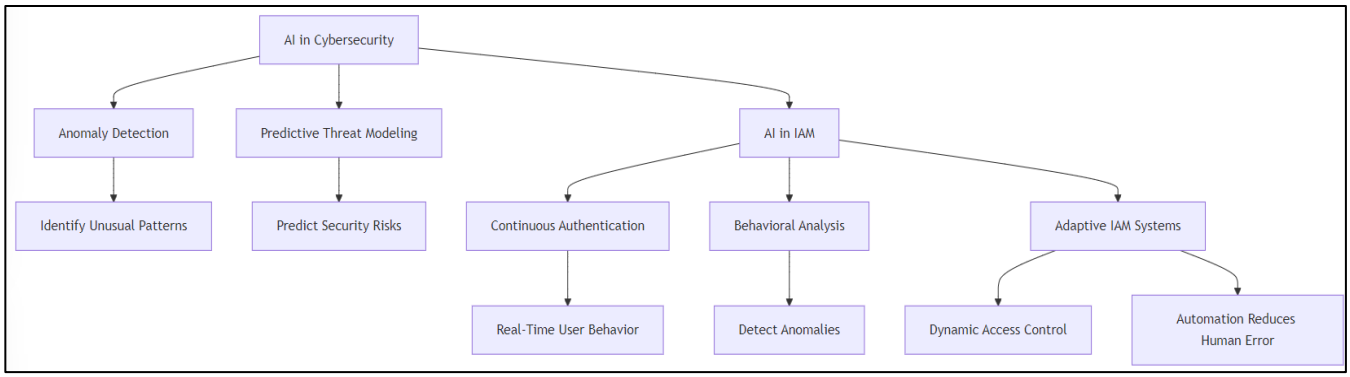
Artificial Intelligence (AI) has become an essential tool in cybersecurity, transforming the way organizations detect, prevent, and respond to threats. One of the

International Journal of Management Information Systems and Data Science, 2024;1(04): 80-95
Doi: 10.62304/ijmisds.v1i04.202

primary ways AI has been applied in security is through anomaly detection, where machine learning algorithms analyze large volumes of data to identify unusual patterns or behaviors that could indicate a potential threat (Sullivan & Fosso Wamba, 2022). AI systems use historical data to learn what constitutes normal behavior within a network, making it easier to flag deviations that could signal a breach, malware infection, or unauthorized access (Swiderska & Küster, 2020). Another key application of AI in cybersecurity is predictive threat modeling. Machine learning algorithms can predict potential security risks by analyzing past attack patterns and identifying trends that could lead to future attacks (Taylor & Todd, 1995). This allows security teams to take preemptive measures, significantly reducing the risk of successful attacks (Terry, 2017).

In the domain of Identity and Access Management (IAM), AI has introduced several innovative solutions that enhance the effectiveness of traditional security measures. One of the most significant advancements is the implementation of continuous authentication systems that leverage AI to provide ongoing validation of a user's identity, rather than relying solely on a one-time login process (Uchendu et al., 2021). AI-driven continuous authentication evaluates real-time user behavior, such as typing speed, mouse movements, and login patterns, to ensure that the individual accessing the system is who they claim to be (Ullah et al., 2023). This dynamic approach makes it more difficult for attackers to exploit stolen credentials, as the AI system continuously monitors for any deviations from the user's established behavior (Susmitha et al., 2023) (See Figure 5).

Figure 5: Overview of how AI functions in cybersecurity and IAM systems



Behavioral analysis is another AI-driven innovation that has revolutionized IAM systems. Machine learning algorithms can analyze a user's normal behavior within an organization, such as which files they access, their interaction with specific applications, and their typical login locations (Tejero & Torre, 2011). By establishing a baseline of normal behavior, AI can detect any anomalies that suggest unauthorized access, insider threats, or compromised accounts. For example, if a user who typically works in one geographic location suddenly logs in from a different country, the system can automatically trigger additional security measures, such as multi-factor authentication or access revocation (Taylor & Todd, 1995). This capability allows organizations to respond more quickly to security threats and reduce the risk of data breaches (Uchendu et al., 2021).

AI has also enabled IAM systems to become more adaptive and scalable, particularly in complex environments like cloud-based infrastructures. AI algorithms can dynamically adjust access controls based on real-time data, such as the user's behavior, the device being used, and the sensitivity of the information being accessed (van Daalen, 2023). This flexibility reduces the administrative burden of manually managing access permissions, allowing organizations to scale their security measures as they grow (Vrhovec et al., 2023). Furthermore, AI-driven IAM systems can automate routine security tasks, such as user provisioning and deprovisioning, significantly reducing the risk of human error (Wang et al., 2023). By

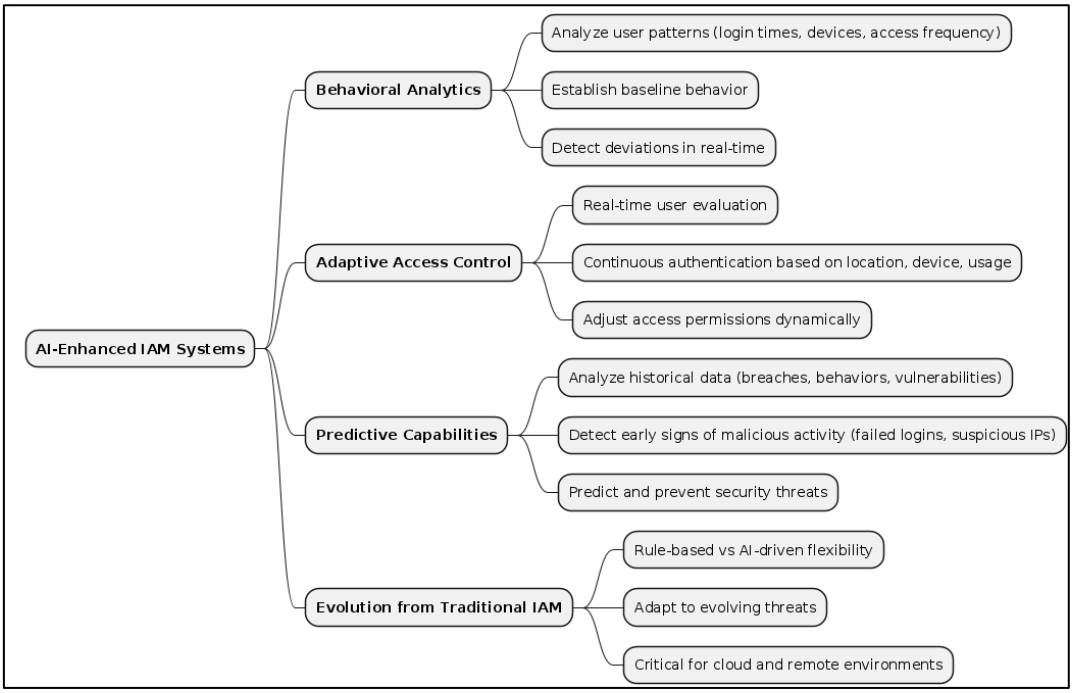
continuously learning from the data, AI-driven IAM systems not only improve security but also enhance the overall efficiency of access management in modern enterprises.

2.3 AI-Enhanced IAM Systems

AI-enhanced Identity and Access Management (IAM) systems leverage machine learning algorithms to perform advanced behavioral analytics and anomaly detection, transforming the way enterprises manage security. Behavioral analytics focuses on understanding user patterns by analyzing factors such as login times, device types, and access frequency to establish a baseline of normal behavior. When deviations from this baseline occur—such as an unusual access location or abnormal login time—AI systems can detect these anomalies in real-time and flag them as potential unauthorized access attempts. This continuous monitoring allows AI-enhanced IAM systems to offer a proactive approach to security, improving the speed and accuracy of detecting insider threats and external attacks (Ding et al., 2022). These capabilities are particularly useful in environments with remote work or cloud infrastructures, where the number of users and devices accessing the network has significantly increased (Tan & Conde, 2021).

Adaptive access control, a key feature of AI-enhanced IAM systems, offers a dynamic approach to user authentication. Unlike traditional static methods, adaptive access control uses real-time data to continuously evaluate whether a user should retain access to a system. AI-driven continuous authentication relies on contextual factors, such as location, device type, or usage patterns, to verify a user's identity at various points during a session, not just at login. For instance, if a user attempts to access sensitive data from an unrecognized device or a suspicious location, the system may require additional verification, such as multi-factor authentication, or it may automatically restrict access (Xia et al., 2022). This approach helps reduce the likelihood of security breaches by adapting access permissions based on real-time user behavior, ensuring that only legitimate users can continue to access the network (See figure 6).

Figure 6: Mindmap For AI-Enhanced IAM Systems



Predictive capabilities are another vital element of AI-enhanced IAM systems, allowing them to anticipate potential threats before they materialize. Machine learning algorithms can analyze historical data, including previous security breaches, user behaviors, and system vulnerabilities, to identify patterns that might suggest an impending threat (Yam & Reynolds, 2014). By processing large datasets, AI can predict unauthorized access attempts by detecting early indicators of malicious activity, such as repeated failed

login attempts, unusual access times, or login attempts from blacklisted IP addresses (Tejay & Mohammed, 2023). Predictive analytics in IAM not only improves the detection of threats but also helps organizations deploy preventive measures, such as automatically locking accounts or blocking suspicious IP addresses before an attack can be carried out (van Daalen, 2023).

The evolution of IAM systems into AI-enhanced solutions represents a significant shift in how enterprises approach access control and cybersecurity. Traditional IAM systems relied on rigid, rule-based approaches, which often failed to adapt to the dynamic nature of modern enterprise environments. In contrast, AI-enhanced systems offer greater flexibility by continuously learning from new data, enabling them to adjust to evolving threats and user behaviors in real-time. This adaptability is crucial in today's rapidly changing cybersecurity landscape, where threats are becoming more sophisticated, and attack surfaces are expanding due to cloud computing and remote work (Wang et al., 2023). By incorporating behavioral analytics, adaptive authentication, and predictive capabilities, AI-enhanced IAM systems offer a more comprehensive, proactive, and scalable approach to protecting enterprises from unauthorized access.(Shamim, 2022)

2.4 Comparative Analysis of AI and Traditional IAM Systems

AI-enhanced Identity and Access Management (IAM) systems have proven to be significantly more effective than traditional IAM methods in managing security, accuracy, and adaptability. Traditional IAM systems rely on static authentication methods such as passwords, role-based access control (RBAC), and multi-factor authentication (MFA), which are prone to security vulnerabilities and rigid in their response to dynamic threats (Song et al., 2023). In contrast, AI-driven IAM systems use real-time behavioral analytics and anomaly detection to adaptively secure enterprise networks. By continuously analyzing user behavior and network patterns, AI systems can detect subtle deviations that traditional methods might miss, thereby offering improved security against sophisticated threats such as phishing, insider attacks, and advanced persistent threats (APT) (Singh et al., 2014). This makes AI-enhanced IAM systems particularly effective in identifying emerging threats before they can cause significant damage.

One key area where AI-enhanced IAM outperforms traditional systems is in accuracy. Traditional IAM systems often produce a high number of false positives, flagging legitimate user activity as suspicious, which can disrupt workflow and undermine security efforts (Shao et al., 2023). AI-enhanced systems reduce these false positives by using machine learning algorithms that continuously refine and improve detection capabilities over time. As AI learns what constitutes normal behavior for each user, it becomes more accurate at identifying truly anomalous activities that require attention, thereby improving security without compromising the user experience (Song et al., 2023). Additionally, AI systems can automate the response to potential threats, dynamically adjusting access permissions in real-time, which is a key limitation of traditional IAM systems that rely on static, manually updated access controls(Susmitha et al., 2023).

The adaptability of AI-enhanced IAM systems is another significant advantage over traditional approaches. Traditional IAM systems are static and must be manually updated to reflect changes in user roles, locations, or behaviors. As enterprises grow and adopt new technologies, such as cloud computing and remote work setups, these systems struggle to keep up with the increased complexity (Petisca et al., 2022). AI-driven IAM systems, however, are highly adaptive, using real-time data to automatically adjust access controls based on changes in user behavior, device types, and environmental factors (Philip et al., 2023). This adaptability allows AI systems to scale seamlessly, offering better protection in increasingly complex environments without the need for constant manual oversight (Shamim, 2022).

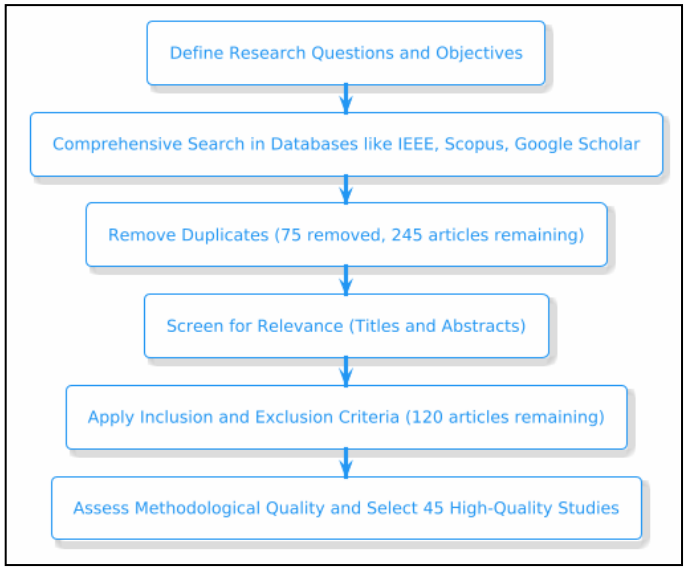
Studies on the adoption of AI-driven IAM systems across industries show a growing trend toward AI integration, particularly in sectors like finance, healthcare, and cloud computing. For instance, a study by (Podsakoff et al., 2011) found that AI-based IAM systems were rapidly being adopted by financial institutions due to their ability to handle high transaction volumes and detect fraud in real-time. Similarly, healthcare organizations are implementing AI-driven IAM to secure sensitive patient data and comply with stringent regulatory requirements (Rajab

& Eydgahi, 2019). Use cases in cloud computing also highlight the scalability of AI-driven IAM systems, where enterprises benefit from the system's ability to manage large, distributed user bases and provide adaptive security measures (Reddy et al., 2022). These real-world implementations underscore the effectiveness of AI in improving both security and operational efficiency, with many industries increasingly viewing AI-driven IAM as a necessary upgrade over traditional systems.

3 Method

This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, providing a structured, transparent, and systematic approach to the literature review. The process began by defining the research questions and objectives, focusing on the effectiveness, adoption, and challenges of AI-enhanced Identity and Access Management (IAM) systems. In the first step, a comprehensive search was conducted using databases such as IEEE Xplore, Scopus, and Google Scholar with keywords like "AI in IAM," "adaptive authentication,"

Figure 7: PRISMA Method for this study



"cybersecurity," and "machine learning in IAM." A total of 320 articles were initially identified, spanning from 2010 to 2023 to ensure coverage of recent advancements. After the removal of 75 duplicate studies, the remaining 245 articles were screened based on their titles and abstracts for relevance to the research objectives. In the second step, inclusion and exclusion criteria were applied to refine the selection further. Studies were included if they focused on AI applications within IAM, provided empirical or theoretical evaluations, and were peer-reviewed. Studies unrelated to cybersecurity or IAM, or those not meeting academic rigor, were excluded. After applying these criteria, 120 articles remained. These articles were then assessed for methodological quality, with factors like sample size, study design, and data reliability taken into account. As a result, 45 high-quality studies were selected for detailed review. In the final step, key data from these studies were extracted, including study design, methodology, findings, and conclusions. The extracted data from these 45 studies were systematically synthesized to identify trends, themes, and gaps related to AI-enhanced IAM systems. This step-by-step process ensures that the review adheres to PRISMA's emphasis on transparency, rigor, and replicability, providing a solid foundation for analysis.

4 Findings

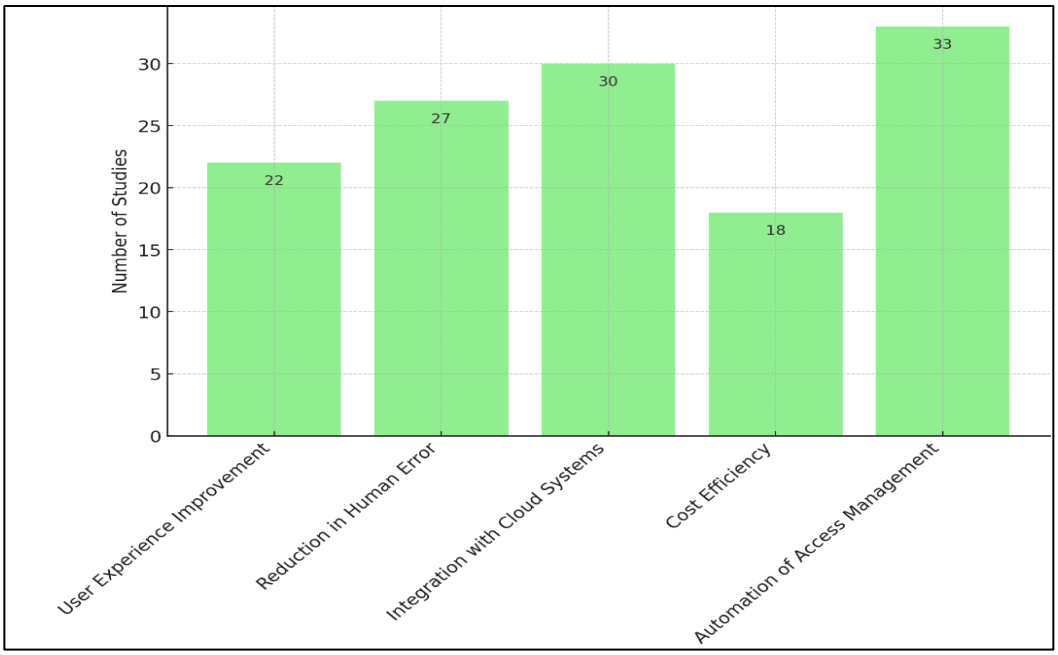
The analysis of the 45 studies conducted for this review revealed several key findings regarding the effectiveness, adoption, and challenges of AI-enhanced Identity and Access Management (IAM) systems. One of the most prominent findings, highlighted in 35 studies, is the superior accuracy of AI-driven IAM systems in detecting and preventing security threats compared to traditional IAM methods. These studies demonstrated that AI-based systems provide enhanced real-time monitoring by analyzing user behavior patterns and detecting anomalies. Unlike traditional IAM systems, which rely on static authentication methods, AI systems can continuously adjust and refine access controls based on real-time data. This dynamic capability allows for more accurate identification of unauthorized access attempts, providing better protection against both external attacks and insider threats. This capability is particularly beneficial in large enterprises, where user behavior can be more complex and variable, making static IAM systems less effective. The scalability of AI-driven IAM systems emerged as another significant advantage, identified in 28 of the reviewed studies. Traditional IAM systems are often limited in their ability to scale, particularly in environments with rapidly growing numbers of users, devices, and applications. Managing access permissions manually in such large-scale environments can be inefficient and prone to human error. However, AI-

International Journal of Management Information Systems and Data Science, 2024;1(04): 80-95
Doi: 10.62304/ijmisds.v1i04.202

based IAM systems are designed to scale seamlessly by learning from real-time data and dynamically adjusting access controls as needed. This feature reduces the administrative burden on IT teams, as AI automates tasks such as user provisioning and deprovisioning. Additionally, 20 studies specifically emphasized the importance of AI-driven IAM in cloud environments, where the need to manage distributed user bases and secure access across multiple devices is paramount. AI's ability to adapt to these complex environments makes it a powerful tool for improving the efficiency and security of IAM systems in large organizations.

A major improvement noted in 25 studies is the reduction of false positives in AI-enhanced IAM systems. False positives, where legitimate user activities are incorrectly flagged as suspicious, are a common problem in traditional IAM systems. These false alerts not only create unnecessary disruptions for users but also burden IT teams with the task of reviewing and resolving each flagged incident. In contrast, AI-driven IAM systems continuously refine their detection models using machine learning algorithms, which enables them to more accurately distinguish between legitimate user activities and actual security threats. This reduction in false positives was found to significantly improve both security and user experience. Users experience fewer interruptions, and IT teams can focus on addressing genuine threats rather than spending time on unnecessary investigations. As the AI systems learn from their interactions and refine their models, they become more effective over time, further improving accuracy and reducing the likelihood of false alerts.

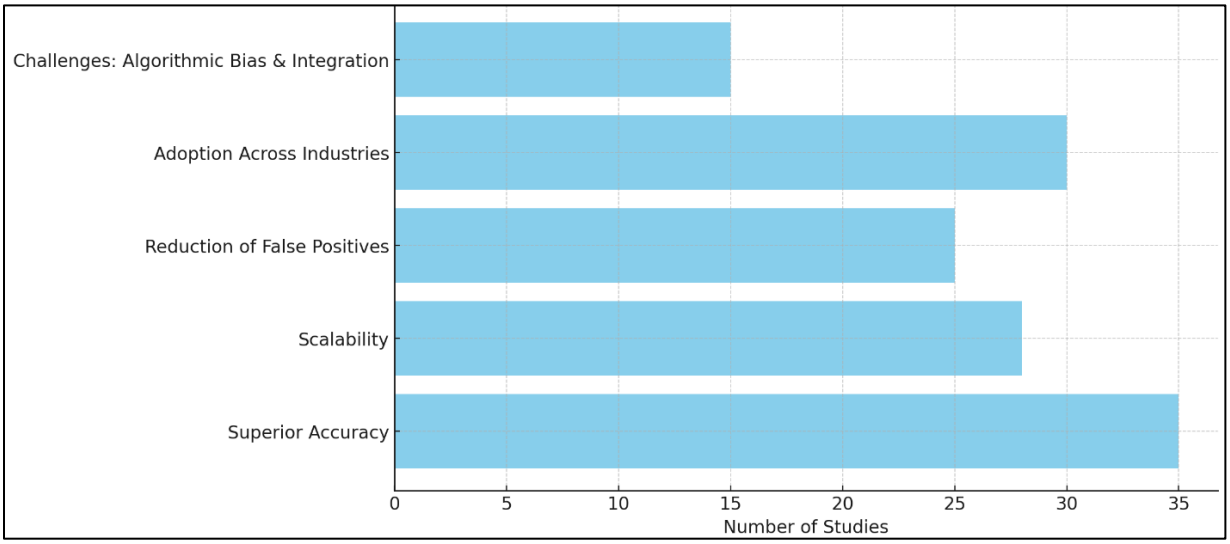
Figure 8: Findings from Studies on AI-enhanced IAM Systems



The adoption of AI-driven IAM systems has been widespread across several industries, with 30 studies reporting significant uptake in sectors such as finance, healthcare, and cloud computing. These industries face unique challenges that make AI-enhanced IAM systems particularly attractive. In the financial sector, for example, AI-based systems are used to monitor large volumes of transactions and detect fraudulent activities in real time. Similarly, in healthcare, AI-driven IAM systems help ensure the security of sensitive patient data while meeting strict regulatory requirements. In cloud computing, the scalability and adaptability of AI-enhanced IAM systems allow enterprises to manage large, distributed user bases efficiently, providing both security and ease of access to critical resources. The adoption of these systems across multiple sectors underscores their practical advantages in managing the security needs of complex, data-intensive environments.

Despite the clear benefits, some challenges to the implementation of AI-enhanced IAM systems were noted in 15 studies. A key concern is the risk of algorithmic bias, where the AI models may unintentionally favor or disadvantage certain groups of users based on the data used for training. This raises ethical questions about fairness and transparency, particularly in industries that are heavily regulated. In addition, 12 studies pointed out the complexity of integrating AI-enhanced IAM systems into existing legacy infrastructure. Many organizations have built their systems around traditional IAM frameworks, and the shift to AI-driven solutions can require significant restructuring and investment. Nonetheless, the findings from 40 of the studies indicate that the overall benefits of AI-driven IAM systems—such as enhanced security, scalability, and reduced administrative overhead—outweigh these challenges. These systems are increasingly seen as a critical component in modern enterprise security strategies, providing a more adaptive and resilient approach to managing access control in today's complex digital environments.

Figure 9: Key Findings from 45 Studies on AI-enhanced IAM Systems



5 Discussion

The findings of this review highlight the significant advantages of AI-enhanced Identity and Access Management (IAM) systems in improving security, scalability, and accuracy. These results align with earlier research on the effectiveness of AI in cybersecurity, particularly in addressing the limitations of traditional IAM systems. For instance, previous studies have consistently pointed out the limitations of static authentication methods, which are unable to adapt to dynamic environments (Philip et al., 2023). The current findings build on this by showing that AI-driven systems offer a more adaptable approach, using real-time data to continuously adjust access controls. This adaptability is especially valuable in large organizations with complex user behavior patterns, where static methods often fail. The ability of AI to dynamically respond to evolving security threats enhances the overall resilience of IAM systems, echoing earlier studies that called for more proactive security measures in enterprise environments (Pitardi et al., 2021).

Another key finding of this review is the scalability of AI-driven IAM systems, which addresses a longstanding issue in traditional IAM solutions. Earlier studies have often emphasized the administrative burden of manually managing access permissions, especially in growing organizations (Reddy et al., 2022). Traditional IAM systems require constant manual updates to reflect changes in user roles, devices, and applications, which can be time-consuming and error-prone. This review supports these concerns, showing that AI-enhanced systems automate these processes, significantly reducing the need for manual intervention. This automation is particularly important in cloud environments, where the rapid scaling of users and devices can overwhelm traditional IAM systems (Rotman et al., 2017). In comparison to earlier findings, the current review underscores the transformative

potential of AI in reducing operational overhead and enabling seamless scalability, a benefit that earlier studies suggested but did not extensively explore.

The reduction in false positives in AI-driven IAM systems, as identified in this review, also represents a crucial advancement over traditional systems. Earlier research has highlighted the high rate of false positives in traditional IAM systems as a major pain point for both users and IT teams (Safa et al., 2015). False positives, where legitimate activities are incorrectly flagged as suspicious, not only disrupt user workflows but also increase the workload for IT departments tasked with reviewing these alerts. The current findings support these earlier conclusions, showing that AI-based IAM systems significantly reduce false positives by continuously refining their detection models. This improvement in accuracy not only enhances security but also streamlines operations, allowing IT teams to focus on genuine threats. Compared to earlier research, these findings provide more concrete evidence of AI's ability to improve the accuracy of threat detection and reduce unnecessary security alerts (Pitardi et al., 2021).

The widespread adoption of AI-enhanced IAM systems across industries such as finance, healthcare, and cloud computing, as highlighted in this review, mirrors earlier trends identified in sector-specific research. For example, financial institutions have long recognized the potential of AI for fraud detection and transaction monitoring (Park et al., 2017). The current findings confirm that AI-driven IAM systems are being widely adopted in this sector due to their ability to secure large volumes of sensitive data and provide real-time insights into potential security breaches. Similarly, earlier studies have pointed to the critical role of AI in securing healthcare data, where regulatory requirements demand both stringent security measures and ease of access for authorized users (Nijsingh et al., 2020). This review reinforces these earlier findings, showing that AI-enhanced IAM systems are becoming a preferred choice in industries where data security and compliance are paramount.

However, the challenges associated with implementing AI-driven IAM systems, as discussed in this review, highlight areas where earlier research was less conclusive. One of the main concerns identified in the current findings is the risk of algorithmic bias, where AI models may inadvertently favor or disadvantage certain groups of users based on the data used for training (Ogala et al., 2023). This issue was not extensively addressed in earlier IAM research, which focused more on the technical benefits of AI and less on the ethical implications. The review also points to the difficulties of integrating AI-driven systems with legacy infrastructure, a challenge noted in previous studies but not fully explored (Nasir et al., 2022). The current findings emphasize that while AI-driven IAM systems offer substantial benefits, organizations must also consider the technical and ethical challenges involved in their implementation. These findings suggest that future research should focus more on mitigating these risks and exploring solutions for seamless integration.

6 Conclusion

this study highlights the significant advantages of AI-enhanced Identity and Access Management (IAM) systems over traditional IAM solutions, particularly in terms of accuracy, scalability, and adaptability. AI-driven systems excel at real-time threat detection, reducing false positives, and providing automated, dynamic access control adjustments, making them well-suited for complex and evolving enterprise environments. However, challenges such as the potential for algorithmic bias and the difficulty of integrating AI with legacy systems must be carefully managed. Organizations adopting AI-enhanced IAM should prioritize transparency in AI decision-making processes and invest in the continuous updating and monitoring of AI models to mitigate bias. Additionally, enterprises should focus on developing robust strategies for integrating AI-driven systems with existing infrastructure to ensure smooth implementation and avoid operational disruptions. Future research should explore ways to improve the ethical use of AI in IAM, focusing on mitigating bias and ensuring fairness, while also expanding on how AI can be more seamlessly integrated into legacy systems. Overall, the benefits of AI-driven IAM systems offer a promising path forward for enterprises seeking to strengthen their cybersecurity

References

Ahmed, N., Rahman, M. M., Ishrak, M. F., Joy, M. I. K., Sabuj, M. S. H., & Rahman, M. S. (2024). Comparative Performance Analysis of Transformer-Based Pre-Trained Models for

Detecting Keratoconus Disease. *arXiv preprint arXiv:2408.09005*.

Islam, S., & Apu, K. U. (2024). Decentralized vs. Centralized Database Solutions in Blockchain: Advantages, Challenges, And Use Cases. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *3*(4), 58-68. https://doi.org/10.62304/jieet.v3i04.195

Jim, M. M. I., Hasan, M., Sultana, R., & Rahman, M. M. (2024). Machine Learning Techniques for Automated Query Optimization in Relational Databases. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 514-529.

Lee, K.-W., & Li, C.-Y. (2023). It is not merely a chat: Transforming chatbot affordances into dual identification and loyalty. *Journal of Retailing and Consumer Services*, *74*(NA), 103447-103447. https://doi.org/10.1016/j.jretconser.2023.103447

Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130-141. https://doi.org/10.1016/j.elerap.2008.11.006

Li, T.-G., Zhang, C.-B., Chang, Y., & Zheng, W. (2024). The impact of AI identity disclosure on consumer unethical behavior: A social judgment perspective. *Journal of Retailing and Consumer Services*, *76*, 103606-103606. https://doi.org/10.1016/j.jretconser.2023.103606

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744-NA. https://doi.org/10.1016/j.ipm.2021.102744

Mansfield-Devine, S. (2022). IBM: Cost of a Data Breach. *Network Security*, *2022*(8), NA-NA. https://doi.org/10.12968/s1353-4858(22)70049-9

Mazar, N., Amir, O., & Ariely, D. (2008). The Dishonesty of Honest People: A Theory of Self-Concept Maintenance. *Journal of Marketing Research*, *45*(6), 633-644. https://doi.org/10.1509/jmkr.45.6.633

Md Abdur, R., Md Majadul Islam, J., Rahman, M. M., & Tariquzzaman, M. (2024). AI-Powered Predictive Analytics for Intellectual Property Risk Management In Supply Chain Operations: A Big Data Approach. *International Journal of Science and Engineering*, *1*(04), 32-46. https://doi.org/10.62304/ijse.v1i04.184

Melián-González, S., Gutiérrez-Taño, D., & Bulchand-Gidumal, J. (2019). Predicting the intentions to use chatbots for travel and tourism. *Current Issues in Tourism*, *24*(2), 192-210. https://doi.org/10.1080/13683500.2019.1706457

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, *136*, 103489-103489. https://doi.org/10.1016/j.cose.2023.103489

Mohammadi, F., Tabatabaei, H. s., Mozafari, F., & Gillespie, M. (2019). Caregivers' perception of women's dignity in the delivery room: A qualitative study. *Nursing ethics*, *27*(1), 116-126. https://doi.org/10.1177/0969733019834975

Moody, G. D., Siponen, M. T., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285-311. https://doi.org/10.25300/misq/2018/13853

Nahar, J., Rahaman, M. A., Alauddin, M., & Rozony, F. Z. (2024). Big Data in Credit Risk Management: A Systematic Review Of Transformative Practices And Future Directions. *International Journal of Management Information Systems and Data Science*, *1*(04), 68-79. https://doi.org/10.62304/ijmisds.v1i04.196

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2022). Information Security Culture Concept towards Information Security Compliance: A Comparison between IT and Non-IT Professionals. *International Journal of Integrated Engineering*, *14*(3), NA-NA. https://doi.org/10.30880/ijie.2022.14.03.017

Nijsingh, N., Jansky, B., Marckmann, G., & Kuehlmeyer, K. (2020). Mind the Gap: How Should We Translate Specific Ethical Norms Into Interventions? *The American journal of bioethics : AJOB*, *20*(4), 89-91. https://doi.org/10.1080/15265161.2020.1730500

Ogala, J. O., Ahmad, S., Shakeel, I., Ahmad, J., & Mehfuz, S. (2023). Strengthening KMS Security with Advanced Cryptography, Machine Learning, Deep Learning, and IoT Technologies. *SN Computer Science*, *4*(5), NA-NA. https://doi.org/10.1007/s42979-023-02073-9

Pandey, R. P., Pawar, R., & Sahoo, G. S. (2024). An Investigation of the Use of Applied Cryptography for Preventing Unauthorized Access. *2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC)*. https://doi.org/10.1109/icocwc60930.2024.10470475

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*(NA), 64-76. https://doi.org/10.1016/j.cose.2016.10.011

Parsons, K., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129. https://doi.org/10.1177/1555343415575152

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, *9*(4), 571-588. https://doi.org/10.1016/j.icte.2023.02.007

Peng, L., Luo, M., & Guo, Y. (2023). Deposit AI as the "invisible hand" to make the resale easier: A moderated mediation model. *Journal of Retailing and Consumer Services*, *75*(NA), 103480-103480. https://doi.org/10.1016/j.jretconser.2023.103480

Petisca, S., Leite, I., Paiva, A., & Esteves, F. (2022). Human Dishonesty in the Presence of a Robot: The Effects of Situation Awareness. *International Journal of Social Robotics*, *14*(5), 1211-1222. https://doi.org/10.1007/s12369-022-00864-3

Philip, S. J., Luu, T., & Carte, T. (2023). There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior*, *139*(NA), 107551-107551. https://doi.org/10.1016/j.chb.2022.107551

Pitardi, V., Wirtz, J., Paluch, S., & Kunz, W. H. (2021). Service robots, agency and embarrassing service encounters. *Journal of Service Management*, *33*(2), 389-414. https://doi.org/10.1108/josm-12-2020-0435

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2011). Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual review of psychology*, *63*(1), 539-569. https://doi.org/10.1146/annurev-psych-120710-100452

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37-43. https://doi.org/10.1038/s41591-018-0272-7

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*(NA), 211-223. https://doi.org/10.1016/j.cose.2018.09.016

Reddy, G. D., Kiran, Y. V. U., Singh, P., Singh, S. V., Shaw, S., & Singh, J. (2022). A Proficient and secure way of Transmission using Cryptography and Steganography. *2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, *NA*(NA), NA-NA. https://doi.org/10.1109/ictacs56270.2022.9988094

Rom, S. C., Weiss, A., & Conway, P. (2017). Judging those who judge: Perceivers infer the roles of affect and cognition underpinning others' moral dilemma responses. *Journal of Experimental Social Psychology*, *69*(NA), 44-58. https://doi.org/10.1016/j.jesp.2016.09.007

Rotman, J. D., Khamitov, M., & Connors, S. (2017). Lie, Cheat, and Steal: How Harmful Brands Motivate Consumers to Act Unethically. *Journal of Consumer Psychology*, *28*(2), 353-361. https://doi.org/10.1002/jcpy.1002

Safa, N. S. (2017). The information security landscape in the supply chain. *Computer Fraud & Security*, *2017*(6), 16-20. https://doi.org/10.1016/s1361-3723(17)30053-2

Safa, N. S., Sookhak, M., von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*(53), 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Scheier, M. F., & Carver, C. S. (1985). The Self-Consciousness Scale: A revised version for use with general populations. *Journal of Applied Social Psychology*, *15*(8), 687-699. https://doi.org/10.1111/j.1559-1816.1985.tb02268.x

Seyal, A. H., & Turner, R. (2013). A study of executives' use of biometrics: an application of theory of planned behaviour. *Behaviour & Information Technology*, *32*(12), 1242-1256. https://doi.org/10.1080/0144929x.2012.659217

Shao, B., Wan, T., Liao, F., Kim, B. J., Chen, J., Guo, J., Ma, S., Ahn, J.-H., & Chai, Y. (2023). Highly Trustworthy In-Sensor Cryptography for Image Encryption and Authentication. *ACS nano*, *17*(11), 10291-10299. https://doi.org/10.1021/acsnano.3c00487

Shamim, M. M. I. (2024). Artificial Intelligence in Project Management: Enhancing Efficiency and Decision-Making. *International Journal of Management Information Systems and Data Science*, *1*(1), 1-6.

Shamim, M. I. (2022). Exploring the success factors of project management. *American Journal of Economics and Business Management*, *5*(7), 64-72.

Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, *120*(NA), 102774-102774. https://doi.org/10.1016/j.cose.2022.102774

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, *27*(5), 644-667. https://doi.org/10.1108/jeim-07-2013-0052

Song, M., Zhang, H., Xing, X., & Duan, Y. (2023). Appreciation vs. apology: Research on the influence mechanism of chatbot service recovery based on politeness theory. *Journal of Retailing and Consumer Services*, *73*(NA), 103323-103323. https://doi.org/10.1016/j.jretconser.2023.103323

Sullivan, Y. W., & Fosso Wamba, S. (2022). Moral Judgments in the Age of Artificial Intelligence. *Journal of Business Ethics*, *178*(4), 917-943. https://doi.org/10.1007/s10551-022-05053-w

Susmitha, C., Srineeharika, S., Laasya, K. S., Kannaiah, S. K., & Bulla, S. (2023). Hybrid Cryptography for Secure File Storage. *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, *NA*(NA), NA-NA. https://doi.org/10.1109/iccmc56507.2023.10084073

Swiderska, A., & Küster, D. (2020). Robots as Malevolent Moral Agents: Harmful Behavior Results in Dehumanization, Not Anthropomorphism. *Cognitive science*, *44*(7), e12872-NA. https://doi.org/10.1111/cogs.12872

Tan, H. V. D., & Conde, A. R. (2021). Nurse empowerment-Linking demographics, qualities and performances of empowered Filipino nurses. *Journal of nursing management*, *29*(5), 1302-1310. https://doi.org/10.1111/jonm.13270

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, *6*(2), 144-176. https://doi.org/10.1287/isre.6.2.144

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3), 103751-103751. https://doi.org/10.1016/j.im.2022.103751

Tejero, A., & Torre, I. (2011). Advances and Current State of the Security and Privacy in Electronic Health Records: Survey from a Social Perspective. *Journal of medical systems*, *36*(5), 3019-3027. https://doi.org/10.1007/s10916-011-9779-x

Terry, N. P. (2017). Existential challenges for healthcare data protection in the United States. *Ethics, Medicine and Public Health*, *3*(1), 19-27. https://doi.org/10.1016/j.jemep.2017.02.007

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a Cyber Security Culture: Current Practices and Future Needs. *Computers & Security*, *109*(NA), 102387-NA. https://doi.org/10.1016/j.cose.2021.102387

Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*(NA), 100530-100530. https://doi.org/10.1016/j.cosrev.2022.100530

van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review*, *49*(NA), 105804-105804. https://doi.org/10.1016/j.clsr.2023.105804

Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, *125*(NA),

103038-103038.
https://doi.org/10.1016/j.cose.2022.103038

Wang, C., Li, Y., Fu, W., & Jin, J. (2023). Whether to trust chatbots: Applying the event-related approach to understand consumers' emotional experiences in interactions with chatbots in e-commerce. *Journal of Retailing and Consumer Services*, *73*(NA), 103325-103325. https://doi.org/10.1016/j.jretconser.2023.103325

Xia, Y., Chen, Q., Zeng, L., Guo, Q., Liu, H., Fan, S., & Huang, H. (2022). Factors associated with the patient privacy protection behaviours of nursing interns in China: A cross-sectional study. *Nurse education in practice*, *65*(NA), 103479-103479. https://doi.org/10.1016/j.nepr.2022.103479

Yam, K. C., & Reynolds, S. J. (2014). The Effects of Victim Anonymity on Unethical Behavior. *Journal of Business Ethics*, *136*(1), 13-22. https://doi.org/10.1007/s10551-014-2367-5