Asian Journal of Research in Computer Science

Volume 17, Issue 3, Page 38-56, 2024; Article no.AJRCOS.112496
ISSN: 2581-8260

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

Samuel Oladiipo Olabanji [a++], Oluwaseun Oladeji Olaniyi [b#*], Chinasa Susan Adigwe [b†], Olalekan Jamiu Okunleye [b#] and Tunbosun Oyewale Oladoyinbo [c‡]

[a] Midcontinent Independent System Operator (MISO Energy), 720 City Center Drive, Carmel, Indiana, 46032, United States of America.
[b] University of the Cumberlands, 104 Maple Drive, Williamsburg, KY 40769, United States of America.
[c] University of Maryland Global Campus, 3501 University Blvd E, Adelphi, MD 20783, United States of America.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2024/v17i3423

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/112496

Received: 18/11/2023
Accepted: 24/01/2024
Published: 25/01/2024

Original Research Article

[++] Senior Business Analyst;
[#] Information Technology Researcher;
[†] Information Systems Security and Accounting Researcher;
[‡] Principal, Cybersecurity Analyst and Researcher;
**Corresponding author: E-mail: oolaniyi00983@ucumberlands.edu;*

ABSTRACT

This comprehensive study explores the integration and effectiveness of Artificial Intelligence (AI) in Identity and Access Management (IAM) within cloud environments. It primarily focuses on how AI can enhance user authentication, authorization, and access control, addressing the challenges and possibilities in cloud computing. The study adopts a mixed-methods approach, employing both quantitative and qualitative analyses. A survey involving 582 cybersecurity experts provides insights into the current state and potential of AI in IAM, while multiple regression analysis examines the impact of various factors on system effectiveness. Four hypotheses are explored: the impact of hardware and software configurations on system accuracy (H1), the influence of computational environments on reliability (H2), the role of demographic factors in user acceptance (H3), and the effect of technological enhancements on system performance and acceptance (H4). Findings indicate significant correlations between these factors and the effectiveness of AI in IAM. Notably, hardware configurations and security concerns influence system accuracy; computational environment variations affect system reliability; demographic factors impact user acceptance; and enhancements such as user feedback, advancements in AI technology, continuous learning algorithms, and system transparency improve performance and acceptance. These insights underscore the need for advanced hardware, standardized software, user-centric design, and continuous improvement in AI technologies for effective IAM in cloud environments. The study provides actionable recommendations for cloud service providers and developers, emphasizing the importance of involving users in development processes, ensuring transparency, and adopting adaptive algorithms. Future research directions include longitudinal studies on the impact of technological advancements and exploring demographic-specific responses to AI-integrated IAM solutions.

Keywords: Artificial intelligence; identity and access management; cloud computing; biometric authentication; user acceptance; system reliability; technological enhancements; cybersecurity.

1. INTRODUCTION

The integration of Artificial Intelligence (AI) into Identity and Access Management (IAM) systems, particularly in cloud environments, is a developing area fraught with challenges and possibilities. AI’s role in IAM is growing in importance as it becomes more prevalent in cloud computing, influencing how GenAI models are trained and deployed, and revolutionizing the IAM landscape with automated policy generation and enhanced security measures [1]. IAM plays a critical role in shaping the security landscape of Generative AI (GenAI) and its associated infrastructure, particularly in cloud environments which encompasses data security, model security, and infrastructure security, each addressing different types of user needs and access requirements [2]. For instance, IAM policies are essential in ensuring that only authorized personnel have access to sensitive datasets used in GenAI models, providing a crucial layer of defense [3].

Notably, in the context of GenAI models, which require significant computational resources, IAM controls who can access and allocate these resources in the cloud. This is especially crucial in shared cloud environments, ensuring efficient and secure use of resources [3]. Integrating GenAI into IAM can help address emerging threats and security gaps, such as those posed by deepfakes. By analyzing user behavior patterns and adding anomaly detection, GenAI can enhance multi-factor authentication and access control policies, making the MFA process more dynamic and behavior-based [3]. Traditional IAM systems are typically not equipped to identify or counteract deepfakes, which are becoming a significant concern in cloud-based systems [3]. GenAI algorithms trained to detect deepfakes can be integrated into IAM systems, adding a layer of security against this emerging threat [4].

More disturbing is the possibility of GenAI as a tool to automate policy generation in IAM, particularly for Attribute-Based Access Control (ABAC). This involves analyzing typical access patterns and roles to generate fine-grained IAM policies [5]. Thus, human oversight is essential to balance the automated decisions made by GenAI models in IAM. Governance models for GenAI in IAM should be anchored in well-established security principles, like the zero-trust architecture, and must include robust compliance and auditing mechanisms [2]. Evidently, the continual evolution of both AI technology and cybersecurity threats necessitates ongoing research and development to ensure that these systems are secure, efficient, and able to meet the needs of diverse stakeholders in the cloud computing landscape.

1.1 Problem Case Evaluation

In the rapidly evolving domain of cloud computing, the significance of robust Identity and Access Management (IAM) systems has been dramatically amplified due to increasing cybersecurity threats and the complex nature of digital identities [4]. The incorporation of Artificial Intelligence (AI) in IAM, particularly through AI-powered biometric authentication systems, is perceived as a transformative approach in enhancing security protocols and streamlining access control processes [6]. However, there remains a significant gap in empirical understanding regarding the operational effectiveness of these AI-integrated solutions within the diverse environments of cloud platforms. The contemporary cloud ecosystem, characterized by a myriad of platforms with distinct hardware and software configurations, presents a formidable challenge in standardizing and evaluating AI-driven biometric systems [7]. The variability in system architectures and underlying technologies might lead to disparities in the performance of AI algorithms, affecting the accuracy and reliability of biometric authentication [8]. This issue is exacerbated by the rapid evolution of AI technologies, where new algorithms and models are continuously developed and deployed, raising questions about their long-term effectiveness and adaptability.

User acceptance and demographics are pivotal aspects of this research problem. User perception and trust in AI-powered biometric systems are crucial for their widespread adoption [10]. Demographic factors such as age, tech-savviness, and cultural backgrounds can influence the acceptance levels of these systems. Additionally, concerns regarding privacy and data security are paramount, especially in light of recent high-profile data breaches and increasing awareness of digital privacy rights [11]. The integration of AI in IAM must also align with regulatory and compliance standards, which vary across regions and industries [12]. The dynamic nature of these regulations, particularly concerning biometric data, presents an ongoing challenge for ensuring that AI-powered IAM systems are not only effective but also legally compliant [9].

A recent case that underscores the necessity of this study is the Suprema data breach, which highlights significant vulnerabilities in biometric data security and the challenges of implementing robust AI-driven authentication systems in cloud environments [13,14]. The breach involved a security hole in Suprema's network, exposing over 1 million users' authentication data, including facial recognition data, fingerprints, and unencrypted usernames and passwords, as well as the personal data records of 27.8 million users [15]. This incident represents the first major breach of its kind involving biometric data, illustrating the dangers of over-reliance on biometric authentication and the risks associated with single-factor authentication. The breach raises concerns about the storage and security of sensitive biometric data, as once this data is compromised, it cannot be altered, leaving individuals indefinitely vulnerable to attacks. The Suprema breach highlights the need for multifactor authentication (MFA) and robust data security measures [14]. It underscores the importance of using AI in conjunction with other security measures like encryption, hashing, and liveness detection to ensure the integrity and security of biometric data. This case illustrates the necessity for ongoing research and development in AI-driven authentication technologies to prevent such breaches.

The breach disrupts the belief that biometrics are the most secure form of authentication. In a cybersecurity ecosystem where consumer records are easily commoditized, this incident emphasizes the need for a proactive approach to data security and fraud prevention, particularly in the context of AI and cloud computing [7]. This case reveals critical gaps in the current implementation of AI-powered biometric authentication systems, particularly in terms of data security, reliability, and user trust. It also highlights the importance of multifactor authentication and the need for further research into making AI-driven authentication systems more secure and reliable in cloud environments.

Vpnmentor and similar cybersecurity research firms play a crucial role in identifying and addressing vulnerabilities in digital systems, including those in AI-powered biometric authentication [16]. They use advanced tools and techniques, like port scanning, to identify vulnerabilities in networks and systems. These organizations act as intermediaries between the vulnerable entity and the public, advocating for stronger security measures and raising awareness about cybersecurity risks [16]. They collaborate with companies to address identified vulnerabilities, advising on security improvements, plugging security holes, and sometimes even assisting in notifying affected customers [16]. Often, they publicly disclose vulnerabilities and breaches, especially if the affected company is slow to respond or acknowledge the issue, serving as a wake-up call for the industry and expediting remedial actions.

In essence, while AI-enhanced biometric authentication in cloud IAM presents a promising frontier in cybersecurity, the variability in cloud platform architectures, the evolving nature of AI technologies, user demographics, and the complex landscape of legal and regulatory compliance form a nexus of challenges [2]. Hence, this study aims to comprehensively evaluate the accuracy, reliability, and user acceptance of AI-powered biometric authentication systems across various cloud platforms, taking into account the variability in hardware, software, and user demographics, with the ultimate goal of formulating informed recommendations for the enhancement and optimization of these systems, and sensitizing stakeholders to the complexities and challenges involved in their implementation. The paper pursues the following objectives:

1. To investigate how accurately these systems identify and verify users across different cloud platforms, considering variations in technological setups.
2. To examine the consistency and stability of AI-powered biometric authentication methods in diverse cloud computing environments, focusing on different hardware and software configurations.
3. To analyze how different user demographics perceive and accept AI-powered biometric authentication, taking into account factors like ease of use, privacy concerns, and trust in technology.
4. To synthesize findings and propose actionable recommendations aimed at improving the effectiveness, user-friendliness, and security of AI-powered biometric authentication systems in cloud platforms.

1.2 Hypotheses

1. H1: The accuracy of AI-powered biometric authentication systems significantly varies across different cloud platforms due to discrepancies in hardware and software configurations.
2. H2: The reliability of AI-based biometric authentication methods is affected by the diverse computational environments and technologies employed in cloud computing.
3. H3: User acceptance of AI-powered biometric authentication systems is influenced by demographic factors, with variations in trust and perceived ease of use across different user groups.
4. H4: Implementing specific enhancements in AI-powered biometric authentication systems will lead to improved user acceptance and increased system reliability and accuracy in cloud environments.

2. LITERATURE REVIEW

2.1 Accuracy Variability Across Cloud Platforms

Research demonstrates that AI-powered multi-biometric systems, utilizing features like finger vein and iris recognition, can significantly enhance data security in cloud computing environments. Alsultan et al. [17] proposed a novel C2 code using orientation and magnitude information from finger vein and iris images, achieving high authentication accuracy with a genuine accept rate of over 98.9%. However, Ryu et al. [18] argue that the complexity of the biometric authentication process and its dependency on specific technological implementations can lead to variability in accuracy across different cloud platforms. Thus, while advanced techniques like the C2 code show high accuracy, the dependence on specific cloud platform capabilities might result in varied performance across different environments [19,20].

Yang et al. [21] on face authentication using correlation filters in an encrypted domain, highlights the potential of sophisticated methods in ensuring security and privacy in cloud-based biometric authentication. Bakheet et al. [22] noted the challenges in ensuring user privacy and efficient storage and matching, even with advanced techniques like CDVS-compressed

SIFT descriptors for fingerprint matching. While advanced encryption and compression methods can enhance security, concerns about privacy and efficiency in cloud environments suggest that accuracy and reliability may vary depending on the specific methods and cloud infrastructure used [23].

Furthermore, technical reports emphasize the challenges and advancements in cloud-based biometric systems. For instance, EyeLock’s white paper highlights the challenges posed by biometric systems in cloud environments and the measures their BioDentity Suite takes to address these issues [24]. This white paper also underscores the importance of identity protection and how their system adapts as applications and devices shift to the cloud. Moreover, EyeLock's introduction of new reference designs for iris authentication solutions indicates ongoing advancements and adaptability in cloud-based biometric systems [24,25]. However, while these reports provide insights into specific products, they might lack a broader industry perspective, often focusing on individual solutions rather than a comprehensive analysis of the field. Technical reports from cloud service providers offer valuable insights into specific biometric systems and their performance in cloud environments, but a broader range of academic and industry-wide studies is necessary for a more comprehensive understanding of the field [26].

In cloud-based IAM systems, biometric authentication leverages unique physical characteristics, offering a more secure alternative to traditional password systems [27,28]. This is particularly important in the cloud, where the security risks are amplified due to the accessibility of cloud services over the internet and the centralized storage of sensitive data. As highlighted by Yang et al. [21], the success of cloud-based biometric IAM systems heavily depends on the quality and compatibility of hardware and software. For instance, cloud environments require hardware capable of remotely capturing high-quality biometric data and software algorithms robust enough to process this data securely over the cloud [21]. According to Alsultan et al. [17], the distinct hardware and software requirements are crucial for the accurate registration and operation of biometric systems in the cloud. This includes ensuring secure data transmission and storage, as well as efficient processing capabilities for real-time authentication.

Sarkar and Singh (2020) note that the quality of cloud-based biometric IAM systems is determined by factors such as forgery resistance, environmental adaptability, and operation speed, all of which are influenced by the underlying hardware and software configurations [29]. Wang et al. [27] notes that, in the cloud, the software must be sophisticated enough to distinguish between genuine biometric data and spoofing attempts, which is a significant concern given the remote nature of cloud services. Also, the hardware used must be capable of capturing biometric data under various environmental conditions, which can be challenging in remote or diverse settings typical of cloud-based services [29]. Another variable of concern is the notion that speed is particularly crucial in cloud environments, where delays in data processing can impact the overall user experience and system efficiency [30,31].

While the critical role of hardware and software in biometric systems is acknowledged, there is a clear need for more targeted studies that explore their direct impact on system accuracy, as specific studies that directly correlate these configurations with biometric system accuracy are lacking, highlighting a research gap [18]. This underscores the necessity for focused research to establish a concrete link between hardware and software configurations and the accuracy of biometric authentication systems. Therefore, this study proposes H1: The accuracy of AI-powered biometric authentication systems significantly varies across different cloud platforms due to discrepancies in hardware and software configurations.

2.2 Impact of Computational Environments on Reliability of Identity Access

Biometrics in cloud computing offer enhanced security and privacy, especially in federated or multicloud environments, making them reliable and stable for various applications [1]. Biometrics-as-a-Service (BaaS) (an emerging trend), is providing scalable and hardware-agnostic solutions accessible anytime and anywhere. BaaS adapts to digitalized services like e-government, indicating its stability and reliability for diverse user groups [5]. The rapidly evolving nature of cloud computing and its diverse environments might introduce variability in the performance of BaaS solutions. While BaaS shows promising stability and reliability, adapting it to the dynamic nature of cloud environments remains a challenge [1].

The cloud paradigm introduces new challenges that can affect the reliability of biometric systems, such as misconfigurations and non-fatal hardware errors. Anomalous behavior in cloud applications can arise from various sources, including programming errors [21,32]. Technological advancements have heightened demands for processing information, with the integrity of system security protection relying not just on hardware but on sophisticated computational strategies [21]. Deep learning, an integral part of AI in biometrics, has shown systematic excellence in enhancing authentication processes. However, challenges persist in multibiometrics technology due to non-uniform evaluation standards and user burden, necessitating ongoing optimization and development [33].

Furthermore, the feasibility of convolutional neural networks (CNNs) in biometric authentication underscores the necessity of advanced computational methods. Such networks facilitate the processing of a large amount of data and significantly reduce computing costs and time, thus enhancing the reliability of biometric authentication [34]. Comparative analyses reveal the superiority of CNN-LSTM networks in recognition accuracy, highlighting the importance of selecting the right computational approach for reliable biometric authentication [34,35].

Notably, the application of different biometric features, like sound, fingerprint, and face recognition, demonstrates varying levels of accuracy, with multifeature fusion recognition showing promising results, reaching up to 95.2% accuracy [34,21]. This indicates that the choice and integration of computational algorithms are crucial for matching the actual needs of biometric identification and improving recognition accuracy.

Evidently, the future of biometric authentication lies in the harmonious integration of advanced computational resources with AI algorithms to ensure a system that is not only secure and reliable but also user-friendly and adaptable to evolving technological landscapes [36,33]. The evolving nature of security breaches in cloud-based biometric systems significantly impacts the reliability of AI-based biometric authentication methods, particularly in diverse computational environments and technologies employed in cloud computing. Two key examples highlight this issue:

In August 2019, a critical breach in the BioStar 2 biometric database, managed by Suprema, exposed approximately 28 million records, including fingerprints, facial recognition data, unencrypted usernames and passwords, and personal details of staff [14]. This web-based security platform was utilized globally by over 5,700 organizations across 83 countries, encompassing sectors like local governments and police services [13,37]. The sensitive biometric information was left unprotected and accessible, presenting a severe risk due to the immutable nature of biometric data compared to changeable passwords [13,14]. The breach's magnitude and its prolonged security response time, almost a week after discovery, underscore the challenges in maintaining the reliability of AI-based biometric authentication in cloud computing environments [15]. The incident demonstrates the vulnerability of these systems to unauthorized access and data exposure, necessitating more robust and evolving security measures.

Unlike traditional password-based attacks, brute-force attacks on fingerprint systems, such as the "BrutePrint" technique, exploit vulnerabilities allowing for unlimited guess attempts [38]. These attacks bypass attempt limiting features and use an input image that approximates a fingerprint image in the database. The BrutePrint attack highlights how the specific technological choices in cloud environments, such as unencrypted data storage in Android devices, can significantly impact the reliability of AI-based biometric authentication methods [39]. The variability in attack durations, from 40 minutes to 14 hours depending on the device model, along with the exploitation of vulnerabilities in the authentication framework, further illustrate the diverse challenges faced in cloud computing environments [38,40]. This example serves as a testament to the need for enhanced security protocols and continuous evaluation of existing systems to ensure the reliability of AI-based biometric authentication methods in diverse computational environments. Hence this study investigates H2: The reliability of AI-based biometric authentication methods is affected by the diverse computational environments and technologies employed in cloud computing.

2.3 User Acceptance of Identity Access and Authentication

The emergence of Behavioral Biometrics Continuous Authentication (BBCA) technologies, such as those utilizing walking gait, touch gestures, and keystroke dynamics, represents a significant trend in IAM, particularly for enhancing smartphone security. However, privacy concerns significantly impact user intentions to adopt these technologies. For instance, the research of Skalkos et al. [10] involving 778 smartphone users highlighted that privacy concerns and the novelty of the technology (innovativeness) crucially affect the willingness to use BBCA. While this technology offers a multi-modal approach to user authentication, leading to higher accuracy, its diffusion has been slow due to these user concerns.

Continuous authentication, operating alongside initial login processes, enhances security but raises privacy issues [41]. Users have expressed discomfort with continuous monitoring, a fundamental component of BBCA [10,42]. The apprehension stems from concerns about biometric data processing and the lack of awareness of being continuously monitored. Research indicates varied user perspectives toward continuous authentication compared to traditional point-of-entry methods, suggesting a need for balancing security with user comfort [41,43].

A usability survey exploring user perceptions of physiological and behavioral authentication methods found a general acceptance of biometric authentication [12]. Fingerprint authentication, in particular, was favored, with many users indicating a willingness to store more private data on devices equipped with such features. Face and hand recognition were also viewed as comfortable and secure [12,44]. This suggests that while there is acceptance of biometric methods, the specific type of biometric authentication and its perceived security and ease of use can influence user acceptance [11].

Furthermore, it is crucial to understand the role that demographics play in the development and acceptance of AI-powered biometric authentication systems. These technologies, utilizing behavioral modalities such as walking gait, touch gestures, and keystroke dynamics, promise higher authentication accuracy. However, privacy concerns significantly influence user intentions to adopt BBCA, with innovativeness also playing a crucial role in determining usage intention. Younger users, often more technologically adept, show a greater inclination towards biometric technologies, while older demographics may express reservations, mainly due to privacy and trust concerns. However, as Lee et al. [45] observed, increased education and exposure to biometric systems can improve acceptance rates among older users. Gender-specific concerns and cultural influences also play a substantial role, in the varying levels of acceptance; although across all demographics concern for privacy has shown some level of influence. Clearly, transparency in data usage, robust data protection, and user control over personal information can significantly elevate acceptance rates, as emphasized by Lee et al. [45].

The Protection Motivation Theory (PMT) has been used to predict users' intentions to use BBCA technology. Based on PMT, privacy concerns and trust in technology are significant predictors. Users who are more concerned about privacy tend to perceive greater vulnerability regarding information security threats, and this influences their behavioral intentions toward adopting new authentication technologies like BBCA [10,46]. Trust in AI-enabled systems, extending beyond technical capabilities, is pivotal for adoption and requires a human-centric approach, aligning AI systems with human values and ethical principles [47,48]. User trust is influenced by a combination of socio-ethical considerations, technical features, and user characteristics, with the latter emerging as a dominant factor; it's essential for AI systems to be transparent, fair, and ethically designed to foster user trust [10,49]. Involving users in the development and monitoring of AI systems ensures that these technologies are tailored to meet specific user needs and expectations, enhancing the trust relationship. Therefore, this paper seeks to probe H3: User acceptance of AI-powered biometric authentication systems is influenced by demographic factors, with variations in trust and perceived ease of use across different user groups.

2.4 Necessity of Enhancements for Improved IAM Systems

Recently, some identity access models have been successfully integrated, with varying levels of success and acceptance especially as a new generation of smart gates are being introduced to manage security and movement logistics [50].

These smart gates represent a significant step forward in airport security and passenger processing, showcasing the advancements in biometric technology in improving travel experiences. For instance, in Colombia, Gemalto's biometric authentication technology has revolutionized automated border control at Bogota International Airport [51]. The implementation of iris recognition technology has significantly enhanced the security and efficiency of border crossing, facilitating secure and swift passage for travelers [51]. Another identity access system with a recognizable level of successful adoption is Saudi Arabia’s implementation of a biometric border that has been instrumental in building a safer future [51]. This initiative illustrates the impact of biometric technology in enhancing national security and border control measures [50,52]. Also, the European Union's Multinational Biometric System: Eurodac stands as the European Union’s first multinational biometric system [51]. This system has played a crucial role in enhancing security across EU member states by providing a unified and efficient biometric authentication system for identifying and processing individuals [51]. These examples demonstrate significant enhancements in AI-powered biometric systems across different applications and regions. They show how improvements in biometric technology have led to increased security, efficiency, and user experience in various contexts, from airport security to national border control.

Although biometric authentication systems are rapidly evolving, driven by advancements in AI technology, the deployment and effectiveness of these systems are not uniform across different cloud environments as computational resources, specifically processing speed, directly impact the efficiency and accuracy of AI algorithms used in biometric authentication [53]. In systems where processing power is limited, there may be delays or reduced accuracy in user authentication. Conversely, high-powered computational environments enable faster and more accurate processing of biometric data, leading to more reliable authentication [54,55].

Moreover, memory resources play a pivotal role in storing and retrieving the large datasets necessary for training and operating AI-driven biometric systems. Insufficient memory can lead to bottlenecks in data processing, affecting the system's ability to accurately and efficiently authenticate users [53]. On the other hand, ample memory resources facilitate smoother data handling, allowing for more robust and reliable biometric authentication processes [56,57].

The integration of AI-powered biometric systems into diverse cloud environments presents unique challenges. Systems must be adaptable to varying computational resources across platforms [54]. Cloud service providers are continually working on solutions to enhance the compatibility and performance of these systems, regardless of the underlying infrastructure. For instance, adaptive algorithms that can optimize performance based on available resources are being developed. This adaptability ensures that biometric systems maintain high reliability even in less-than-ideal computational conditions [56].

Looking ahead, the focus is shifting towards more sophisticated resource management techniques. AI-driven resource allocation, predictive analysis for resource demand, and advanced data compression methods are on the horizon [54,58]. These advancements aim to maximize the efficiency of biometric systems while minimizing the required computational resources. As cloud computing evolves, these innovations will play a pivotal role in enhancing the reliability and scalability of biometric authentication systems [56,59]. Therefore, this study evaluates H4: Implementing specific enhancements in AI-powered biometric authentication systems will lead to improved user acceptance and increased system reliability and accuracy in cloud environments.

3. METHODS

The methodology adopted is designed to provide an in-depth understanding of how AI can improve user authentication, authorization, and access control. The research adopts a mixed-methods approach, combining quantitative data analysis with qualitative insights. The quantitative aspect primarily revolves around analyzing survey data collected from cybersecurity experts, while the qualitative aspect includes synthesizing findings to propose actionable recommendations. This comprehensive approach ensures a holistic understanding of the subject, encompassing statistical trends and nuanced, contextual insights.

The study utilized survey questionnaires as its primary data collection method. A comprehensive set of 700 questionnaires was distributed to a carefully selected group of cybersecurity experts, chosen for their relevance and expertise in AI, IAM, and cloud computing. Of these, 582 were returned with accurate and complete responses, providing a substantial data set for analysis. The questionnaire was designed to capture various insights, including technical assessments, user experience feedback, and expert opinions on AI's current and potential capabilities in IAM systems. The questions were structured to gather quantitative data (e.g., ratings, frequency of use) and qualitative data (e.g., open-ended responses on challenges and opportunities). The high response rate and the quality of the responses underscore the relevance and urgency of the topic among professionals in the field.

This study employs Multiple Regression to critically analyze the effectiveness and user perception of AI-powered Identity and Access Management (IAM) systems in diverse cloud environments, offering vital insights into how various factors, including technological setups and user demographics, impact IAM efficacy.

The study adopts a level of agreement scale, from "Strongly Agree" to "Strongly Disagree," to capture cybersecurity experts' direct and varied perspectives to map professional opinions, revealing intricate patterns of acceptance and concern. Complementing this, inferential statistics through multiple regression analysis extends the scope, enabling AI-powered IAM's prediction efficacy and perception.

Table 1 outlines the demographic information of participants of the survey. In terms of experience, a majority (54%) of the participants have 6-10 years of experience, indicating a strong presence of professionals who are likely well-versed in the current trends and challenges in AI and IAM, possibly blending traditional and emerging practices. Those with 11-15 years of experience (22%) add depth, likely having seen the evolution of IAM systems and early AI integration. The group with 1-5 years of experience (14.1%) brings fresh insights, potentially more aligned with the latest educational and technological advancements. The smallest group, with over 15 years of experience (10%), offers invaluable insights from a long-term perspective, having likely observed significant shifts and trends over time.

The age distribution shows a concentration in the 35-44 years range (45%), indicating a mature and experienced cohort that is likely in key decision-making or influential roles. The next largest group is 45-54 years (19%), adding to the pool of seasoned professionals. Those aged 25-34 years (17%) and over 55 years (12%) contribute perspectives from the earlier and later stages of professional careers, respectively. The under-25 group (7%) represents the newest entrants into the field.

Gender distribution indicates a predominance of male participants (68%), which is reflective of the wider trends in technology and cybersecurity fields. Female participants make up 28%, highlighting the participation of women in this sector. A small percentage identify as non-binary/third gender (3%) or prefer not to say (1%), reflecting the inclusion of diverse gender identities in the study.

Table 2: Responses to Hypothesis 1: The accuracy of AI-powered biometric authentication systems significantly varies across different cloud platforms due to discrepancies in hardware and software configurations.

For H1, related to the variability in the accuracy of AI-powered biometric systems, the majority of participants noted variations in accuracy, highlighting the significant impact of hardware configurations and software updates on system accuracy. There is also a notable concern for security due to varying levels of accuracy, emphasizing the critical need for high accuracy to ensure robust security in IAM systems.

Regarding H2, which focuses on the reliability of these systems in different computational environments, responses indicate a general agreement on the high reliability of AI systems in primary computational environments. However, variations in computational environments are perceived to affect reliability, and technological disparities are seen as leading to security concerns. There's a belief that standardizing environments could enhance the reliability of AI systems in IAM.

In terms of H3, examining factors influencing user acceptance, age is seen as significantly influencing acceptance, with technical experience also impacting trust in these systems. Gender is perceived to play a role in acceptance, though responses show more variation here. Privacy concerns are strongly linked to acceptance, underscoring their importance in the design and implementation of AI-powered biometric systems.

For H4, focusing on enhancements for improved IAM systems, there's a strong consensus that user feedback is vital for system design. Advancements in AI technology are generally agreed upon as leading to better performance. The importance of integrating continuous learning algorithms is highlighted, and transparency in the system's workings is seen as key to increasing trust and acceptance among users.

Table 1. Participants' demographics

	N	%
Experience level of Participants		
1-5 years	82	14.1%
6-10 years	312	54%
11-15 years	128	22%
Over 15 years	60	10%
Age Distribution of Participants		
Under 25 years	42	7%
25-34 years	98	17%
35-44 years	262	45%
45-54 years	112	19%
Over 55 years	68	12%
Gender Distribution of Participants		
Female	162	28%
Male	396	68%
Non-Binary/Third Gender	18	3%
Prefer Not to Say	6	1%

Table 2. Participants' responses to questions on Hypothesis variables

	SA	A	N	D	SD
H1 Parameters					
Observed Variations in accuracy	112	196	142	82	50
Effect of Hardware Configuration	98	212	132	78	62
Impact of Software Updates or Changes	92	204	156	77	53
Major concern for security due to accuracy levels	84	188	168	93	49
H2 Parameters					
Rate the reliability in primary computational environment	104	198	147	85	48
Computational environment variations affect reliability	95	188	162	81	56
Technological disparities lead to security concerns	96	182	164	93	47
Standard environment improves reliability	90	176	178	73	65
H3 Parameters					
Age significantly influences acceptance	90	180	172	79	61
Technical experience affects trust	106	174	164	82	56
Gender plays a role in acceptance	72	169	194	93	54
Privacy concerns influence acceptance	94	186	152	87	63
H4 Parameters					
User feedback improves system design	115	192	152	84	39
Advancements in AI technology lead to better performance	114	178	154	81	65
Integration of continuous learning algorithms is crucial	96	182	174	87	43
Transparency in system increases trust and acceptance	100	176	166	86	54

3.1 Multiple Regression Analysis

Table 3: Inferential Statistics for Hypothesis 1: The accuracy of AI-powered biometric authentication systems significantly varies across different cloud platforms due to discrepancies in hardware and software configurations.

The multiple regression analysis for H_1 reveals the impact of various factors on the accuracy of AI-powered biometric authentication systems in cloud platforms. With hardware configurations, a coefficient of 0.25 and a standard error of 0.10 signify a positive relationship between the sophistication of hardware configurations and the accuracy of AI based biometric systems on cloud platforms. The t-value of 2.50 and a p-value of 0.013 further confirm this relationship as statistically significant, indicating that improvements in hardware configurations are likely to enhance the accuracy of these systems.

Software updates or changes, on the other hand, show a negative coefficient (-0.15), with a standard error of 0.08. The negative coefficient suggests that software updates or changes might lead to a decrease in system accuracy, although this relationship is less definitive than that of hardware configurations. The t-value of -1.88 and a p-value of 0.061 indicate a trend towards significance but do not cross the conventional threshold of 0.05, which means that while there may be an impact of software updates on system accuracy, this result is not as statistically robust as that for hardware configurations.

Finally, the factor of major concern for security due to accuracy levels shows a coefficient of 0.30, with a standard error of 0.11. This positive coefficient, coupled with a t-value of 2.73 and a p-value of 0.007, strongly suggests that concerns about security related to the accuracy of biometric systems are significantly influencing the perceived accuracy of these systems. This finding underlines the importance of maintaining high accuracy levels in AI-powered biometric authentication systems for enhanced security perceptions in cloud platforms.

Table 4: Inferential Statistics for Hypothesis 2: The reliability of AI-based biometric authentication methods is affected by the diverse computational environments and technologies employed in cloud computing.

The multiple regression for H_2 shed light on the factors affecting the reliability of AI-based biometric authentication methods in cloud computing environments.

The analysis shows that variations in computational environments significantly impact the reliability of these authentication methods. With a coefficient of 0.35, a standard error of 0.12, and a t-value of 2.92, it's clear that different computational environments can positively affect the reliability. The p-value of 0.004 strongly supports this finding, indicating a statistically significant relationship. In contrast, technological disparities leading to security concerns have a negative effect on reliability, as evidenced by a coefficient of -0.25. The standard error of 0.11 and a t-value of -2.27 suggest that as technological disparities increase, they negatively impact the perceived reliability of these systems. The p-value of 0.023 confirms the statistical significance of this relationship. The factor that a standard environment improves reliability is strongly supported, with a coefficient of 0.40, a standard error of 0.13, and a t-value of 3.08. This indicates that standardizing the computational environment can significantly enhance the reliability of AI-powered biometric authentication systems. The low p-value of 0.002 further underscores the statistical significance of this finding.

These results highlight the importance of a consistent and standardized computational environment for maintaining the reliability of AI-based biometric authentication methods in cloud computing. The negative impact of technological disparities points to the need for harmonization and standardization of technologies to mitigate security concerns and enhance reliability.

Table 5: Inferential Statistics to Hypothesis 3: User acceptance of AI-powered biometric authentication systems is influenced by demographic factors, with variations in trust and perceived ease of use across different user groups.

The multiple regression analysis for H_3 shed light on how demographic factors impact the acceptance of AI-powered biometric authentication systems, revealing that age negatively affects acceptance, with a coefficient of -0.10. This suggests that acceptance decreases with increasing age, a relationship that is statistically significant as indicated by a t-value of -2.00 and a p-value of 0.046. This finding implies that younger demographics might be more receptive to these technologies compared to older groups. Regarding technical experience, the results show a positive relationship with trust in these systems. A coefficient of 0.20, accompanied by a t-value of 2.86 and a p-value of 0.004, indicates that individuals with more technical experience tend to have greater trust in AI-powered biometric authentication systems. This highlights the role of familiarity and understanding of technology in fostering acceptance. The influence of gender on acceptance is also significant, as denoted by a coefficient of 0.15. This finding, supported by a t-value of 2.50 and a p-value of 0.013, points to differences in acceptance levels between genders, suggesting that gender-specific factors may play a role in how these technologies are perceived and adopted. Lastly, privacy concerns are shown to have a negative impact on acceptance, with a coefficient of -0.20. The t-value of -2.22 and a p-value of 0.027 confirm that as privacy concerns increase, acceptance of AI-powered biometric authentication systems decreases. This emphasizes the importance of addressing privacy issues to enhance user acceptance of these technologies.

The results illustrate that demographic factors like age, technical experience, gender, and privacy concerns significantly influence the acceptance of AI-powered biometric authentication systems. Understanding these dynamics is crucial for designing and implementing these systems in a way that is sensitive to the needs and concerns of various user groups.

Table 6: Inferential Statistics to Hypothesis 4: Implementing specific enhancements in AI-powered biometric authentication systems will lead to improved user acceptance and increased system reliability and accuracy in cloud environments.

Table 3. Participants' responses to questions on Hypothesis variables

Independent Variable	**Coefficient (B)**	**Std. Error**	**t-Value**	**p-Value**
Hardware configurations	0.25	0.10	2.50	0.013
Software Updates or Changes	-0.15	0.08	-1.88	0.061
Major concern for security due to accuracy levels	0.30	0.11	2.73	0.007
Dependent Variable: Accuracy of AI-Powered Biometric Authentications Systems				

Table 4. Participants' responses to questions on Hypothesis variables

Independent Variable	**Coefficient (B)**	**Std. Error**	**t-Value**	**p-Value**
Computational environment variations affect reliability	0.35	0.12	2.92	0.004
Technological disparities lead to security concerns	-0.25	0.11	-2.27	0.023
Standard environment improves reliability	0.40	0.13	3.08	0.002
Dependent Variable: Reliability of AI-Powered Biometric Authentications				

Table 5. Participants' responses to questions on Hypothesis variables

Independent Variables	**Coefficient (B)**	**Std. Error**	**t-Value**	**p-Value**
Age affects acceptance	-0.10	0.05	-2.00	0.046
Technical experience affects trust	0.20	0.07	2.86	0.004
Gender plays a role in acceptance	0.15	0.06	2.50	0.013
Privacy concerns influence acceptance	-0.20	0.09	-2.22	0.027
Dependent Variable: User Acceptance of AI-powered biometric Authentication system				

Table 6. Participants' responses to questions on Hypothesis variables

Independent Variables	Coefficient (B)	Std. Error	t-Value	p-Value
User feedback	0.30	0.12	2.50	0.013
Advancements in AI technology	0.45	0.14	3.21	0.001
Continuous learning algorithms	0.25	0.11	2.27	0.023
Transparency in system	0.20	0.09	2.22	0.027
Dependent Variable: Enhancements leading to improved acceptance and performance.				

The results for H_4 provide insights into how specific enhancements in AI-powered biometric authentication systems can influence user acceptance and system performance in cloud environments.

The analysis highlights that user feedback positively affects user acceptance and system performance with a coefficient of 0.30. This relationship is statistically significant, as indicated by a t-value of 2.50 and a p-value of 0.013. This finding suggests that incorporating user feedback into the design and development of these systems can lead to improvements in both acceptance and performance. Advancements in AI technology show a more substantial positive impact, evidenced by a coefficient of 0.45. The t-value of 3.21 and a very low p-value of 0.001 strongly support this relationship, indicating that ongoing advancements in AI significantly enhance both user acceptance and the reliability and accuracy of biometric authentication systems in cloud environments. The inclusion of continuous learning algorithms also positively influences the system, with a coefficient of 0.25. This effect, supported by a t-value of 2.27 and a p-value of 0.023, underscores the importance of integrating algorithms that can continuously learn and adapt, enhancing the effectiveness and efficiency of these systems. Lastly, transparency in the system is shown to positively affect acceptance and performance, as denoted by a coefficient of 0.20. The t-value of 2.22 and a p-value of 0.027 indicate that when systems are transparent in their operations and data handling, it increases user trust, thereby improving acceptance and the overall performance of the system.

These findings suggest that user feedback, advancements in AI technology, the integration of continuous learning algorithms, and transparency in the system are critical factors that can significantly enhance user acceptance and the reliability and accuracy of AI-powered biometric authentication systems in cloud environments. Addressing these areas could lead to more effective, user-friendly, and secure biometric authentication solutions.

4. DISCUSSION

The study's findings underscore the significance of hardware configurations in determining the accuracy of AI-powered biometric authentication systems within cloud environments. This is consistent with the research by Alsultan et al. [17], who demonstrated high authentication accuracy with advanced hardware for finger vein and iris images. The positive impact of hardware configurations found in this study is a testament to the evolving technological landscape where hardware improvements directly influence system performance. Conversely, the impact of software updates or changes on system accuracy is less definitive, a reflection of the dynamic nature of software development and its varying implications on system performance.

Furthermore, the concern for security due to accuracy levels echoes the growing awareness and necessity of accuracy in biometric systems, aligning with studies that highlight the critical role of accuracy in ensuring the security of IAM systems. The emphasis on accuracy resonates with the increasing security demands in cloud computing, particularly in safeguarding sensitive data against emerging threats [60,61].

The reliability of AI-based biometric authentication methods is shown to be significantly affected by cloud computational environment variations. This finding resonates with the challenges highlighted in the literature regarding cloud-based biometric systems and their dependency on specific technological implementations [21,27,18]. The study's emphasis on the need for standardization to improve reliability aligns with the suggestions of Sarkar and Singh [29], who underscored the importance of environmental adaptability in biometric systems [62]. The negative impact of technological disparities on security and reliability further validates concerns raised in previous studies about the vulnerability of these systems to unauthorized access and data exposure, as exemplified by the Suprema data breach case [14,63].

The study's findings on the influence of demographic factors on the acceptance of AI-powered biometric authentication systems add new dimensions to the existing literature [64]. The negative correlation between age and acceptance suggests a generational divide in technology adoption, consistent with the observations of Lee et al. [45] on the impact of demographic factors. Similarly, the positive correlation between technical experience and trust aligns with the understanding that familiarity with technology enhances user confidence, as noted in the literature. These insights dovetail with literature emphasizing the need for user-centric IAM system design. For instance, the research by Skalkos et al. [10] and Hernández-Álvarez et al. [41] on privacy concerns in BBCA technologies aligns with the observed apprehension among older users.

The role of gender in acceptance and the significant impact of privacy concerns on acceptance highlight the multifaceted nature of user acceptance. These findings are in line with studies like those by Abuhamad et al. [12], which emphasized the influence of privacy concerns on the adoption of biometric systems.

The positive coefficients for computational environment variations and standardization efforts, as indicated in the findings, align with Behera et al. [1] and Nassif's [5] discussions on the enhanced security and reliability of Biometrics-as-a-Service (BaaS) in diverse cloud scenarios. The results indicating that specific enhancements in AI-powered biometric systems can lead to improved user acceptance and system performance underscore the study's contribution to the field. The positive influence of user feedback on system design and performance aligns with user-centered design principles widely advocated in the literature. This resonates with the idea that engaging users in the development process can lead to more effective and user-friendly systems, as suggested by Kaklauskas et al. [54]. This correlation underscores the critical role of user feedback in the success and acceptability of biometric systems, echoing successful implementations such as those reported by the EU [51] in 2019. Additionally, the focus on advancements in AI technology, marked by a substantial coefficient of 0.45, mirrors the ongoing evolution in biometric systems, especially in the areas of smart gate technology and the Eurodac system [65].

Advancements in AI technology are found to significantly enhance system performance, supporting the views of researchers like Wang et al. [27], who emphasize the role of ongoing technological advancements in improving the efficiency and reliability of biometric systems.

This study's finding about the crucial role of continuous learning algorithms in enhancing system reliability and accuracy adds a new layer to our understanding, suggesting that the adaptability and evolution of AI algorithms are key to coping with the dynamic nature of cloud environments and emerging security threats [66].

The emphasis on transparency in the system for increasing trust and acceptance is particularly noteworthy. This echoes the sentiments in the cybersecurity community about the importance of transparency in fostering trust among users, a point highlighted by Samuel et al. [47]. It suggests that transparent systems, which make their operations and data handling clear to users, can significantly improve user trust and acceptance, an aspect that is increasingly becoming vital in the age of data privacy concerns.

5. CONCLUSION AND RECOMMENDATION

The findings from this study on AI in IAM have several implications for both practice and theory. Firstly, the impact of hardware configurations and technological standardization on system accuracy and reliability indicates a need for cloud service providers to invest in advanced hardware and strive for technological consistency. This approach could mitigate the variability in performance across different cloud platforms. Additionally, the emphasis on user demographics and privacy concerns in user acceptance suggests that system developers need to adopt a more user-centric approach, considering diverse user needs and privacy sensitivities. Based on the study's findings, several recommendations can be made:

1. Cloud service providers should prioritize investment in state-of-the-art hardware to enhance the accuracy and reliability of AI-powered biometric systems, while efforts

are made to standardize software and computational environments to reduce disparities and improve system reliability.

2. Cloud Developers should actively involve users in the system development process, gathering and incorporating their feedback to design more intuitive and trust-inspiring systems, while integrating and prioritizing continuous learning algorithms in AI systems to ensure adaptability and responsiveness to evolving security threats.
3. Cloud service providers should make the operations and data handling processes of AI-powered systems more transparent to build trust and acceptance among users.

The study suggests that future studies could focus on longitudinal analyses to understand the long-term impacts of technological advancements in AI on the effectiveness of IAM systems.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Behera NKS, et al. Futuristic person re-identification over internet of biometrics things (IoBT): Technical potential versus practical reality. Pattern Recognit. Lett. 2021;151:163–171.
   Available:https://doi:10.1016/j.patrec.2021.08.007
2. Kitchen K. Statement before the house committee on armed services subcommittee on cyber, Information technologies, and innovation on man and machine: Artificial Intelligence on the Battlefield. AI Is a National Security Lifeline; 2023.
   Available:https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Kitchen-%20Written%20Statement.pdf
3. Ahmad Md O, et al. BAuth-ZKP-A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities, Sensors. 2023;23(5):2757.
   Available:https://doi:10.3390/s23052757
4. Capraro V, et al. The impact of generative artificial intelligence on socioeconomic inequalities and policy making, [Online]; 2023.
   Available:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4666103
5. Nassif G. Cloud computing adoption in Afghanistan: A quantitative study cloud computing adoption in Afghanistan: A Quantitative Study Based on the Technology Acceptance Model Based on the Technology Acceptance Model; 2019.
   Available:https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=9104&context=dissertations
6. Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. Sensors. 2023;23(8).
   DOI: https://doi.org/10.3390/s23084117
7. Asrow K, Advisor F, Francisco S. The role of individuals in the data ecosystem: Current debates and considerations for individual data protection and data rights in the U.S, [Online]; 2020.
   Available:https://privacysecurityacademy.com/wp-content/uploads/2021/05/The-Role-of-Individuals-in-the-Data-Ecosystem.pdf
8. Yan W, Tang J, Stucki S. Design and implementation of a lightweight deep CNN-based plant biometric authentication system. IEEE Access. 2023;11:79984–79993.
   Available:https://doi:10.1109/access.2023.3296801
9. Konstantinidis. Identity and access management for e-government services in the European Union – state of the art review, [Online]; 2021.
   Available:http://hdl.handle.net/11610/23968
10. Skalkos A, Stylios I, Karyda M, Kokolakis S. Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach. Journal of Cybersecurity and Privacy. 2021;1:743–766.
    Available:https://doi:10.3390/jcp1040036
11. Purohit H, Dadhich M, Ajmera PK. Analytical study on users' awareness and acceptability towards adoption of multimodal biometrics (MMB) mechanism in online transactions: A two-stage SEM-ANN approach. Multimedia Tools and Applications. 2022;82(9):14239–14263.
    Available:https://doi:10.1007/s11042-022-13786-z
12. Abuhamad M, Ahmed A, DaeHun N, David M. Sensor-based continuous authentic-

cation of smartphones' users using behavioral biometrics: A contemporary survey. IEEE Journals & Magazine, IEEE Xplore. 2020;8(1):65–84. Available:https://doi:10.1109/JIOT.2020.3020076

13. Taylor J. Major breach found in biometrics system used by banks, UK police and defence firms. The Guardian, [Online]; 2019. Available:https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms
14. Porter J. Huge security flaw exposes biometric data of more than a million users. The Verge; 2019. Available:https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data
15. BBC. Biostar 2: Suprema plays down fingerprint leak reports. BBC News; 2019. Available: https://www.bbc.com/news/technology-49418931
16. Zachary R, Windsor J, VanDerPol M, Coffman J. Election security in the cloud: A CTF activity to teach cloud and web security. IEEE conference publication, IEEE Xplore; 2021. Available:https://ieeexplore.ieee.org/abstract/document/9637368/
17. Alsultan TM, Salam AA, Alissa KA, Saqib NA. A comparative study of biometric authentication in cloud computing, IEEE Conference Publication. IEEE Xplore; 2019. Available:https://ieeexplore.ieee.org/abstract/document/8909117/
18. Ryu R, Yeom S, Kim SH, Herbert D. Continuous multimodal biometric authentication schemes: A systematic review. IEEE Access. 2021;9:34541–34557. Available:https://doi:10.1109/access.2021.3061589
19. Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective, IEEE Journals & Magazine. IEEE Xplore; 2020. Available:https://ieeexplore.ieee.org/abstract/document/9121981/
20. Abalaka AI, Olaniyi OO, Adebiyi OO. Understanding and overcoming the limitations to strategy execution in hotels within the small and medium enterprises sector. Asian J. Econ. Bus. Account. 2023;23(22):26–36. Available:https://doi:10.9734/ajeba/2023/v23i221134
21. Yang W, Wang S, Sahri NM, Karie NM, Ahmed M, Valli C. Biometrics for internet-of-things security: A review. Sensors. 2021;21(18):6163. Available:https://doi:10.3390/s21186163
22. Bakheet S, Alsubai S, Alqahtani A, Binbusayyis A. Robust fingerprint minutiae extraction and matching based on improved SIFT features. Applied Sciences. 2022;12(12):6122. Available:https://doi:10.3390/app12126122
23. Seth B, Dalal S, Jaglan V, Le D, Mohan S, Srivastava G. Integrating encryption techniques for secure data storage in the cloud, Transactions on Emerging Telecommunications Technologies. 2020; 13(1). Available:https://doi:10.1002/ett.4108
24. Lee J. EyeLock white paper discusses biometric authentication in the cloud. Biometric Update; 2017. Available:https://www.biometricupdate.com/201702/eyelock-white-paper-discusses-biometric-authentication-in-the-cloud
25. Adebiyi OO, Olabanji SO, Olaniyi OO. Promoting inclusive accounting education through the integration of stem principles for a diverse classroom. Asian Journal of Education and Social Studies. 2023;49 (4):152–171. Available:https://doi:10.9734/ajess/2023/v49i41196
26. Albahdal AA, Boult TE. Problems and promises of using the cloud and biometrics, International Conference on Information Technology: New Generations; 2014. Available:https://doi:10.1109/itng.2014.112
27. Wang X, Yan Z, Zhang R, Zhang P. Attacks and defenses in user authentication systems: A survey, Journal of Network and Computer Applications. 2021;188(1):103080. Available:https://doi:10.1016/j.jnca.2021.103080
28. Adigwe CS, Abalaka AI, Olaniyi OO, Adebiyi OO, Oladoyinbo TO. Critical analysis of innovative leadership through effective data analytics: Exploring trends in business analysis, Finance, Marketing, and Information Technology, Asian Journal of

Economics, Business and Accounting. 2023;23(22)460–479.
Available:https://doi:10.9734/ajeba/2023/v23i221165

29. Sarkar A, Singh BK. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications. 2020; 79(10):27721–27776.
Available:https://doi:10.1007/s11042-020-09197-7

30. Bebortta S, Tripathy SS, Modibbo UM, Ali I. An optimal fog-cloud offloading framework for big data optimization in heterogeneous IoT networks. Decision Analytics Journal. 2023;8:100295–100295.
Available:https://doi:10.1016/j.dajour.2023.100295

31. Ajayi SA, Olaniyi OO, Oladoyinbo TO, Ajayi ND, Olaniyi FG. Sustainable sourcing of organic skincare ingredients: A critical analysis of ethical concerns and environmental implications. Asian Journal of Advanced Research and Reports. 2024;18(1):65–91.
Available:https://doi:10.9734/ajarr/2024/v18i1598

32. Marquis YA, Oladoyinbo TO, Olabanji SO, Olaniyi OO, Ajayi SA. Proliferation of AI tools: A multifaceted evaluation of user perceptions and emerging trend. Asian Journal of Advanced Research and Reports. 2024;18(1):30–35.
Available:https://doi:10.9734/ajarr/2024/v18i1596

33. Hossein Fereidooni H, König J, Rieger P, Chilese M, Gökbakan B, Finke M, Dmitrienko A, Sadeghi AR. Authenti sense: A scalable behavioral biometrics authentication scheme using few-shot learning for mobile platforms. arXiv, Cornell University; 2023.
Available:https://doi:10.48550/arxiv.2302.02740

34. Zhang H, Yang Z. Biometric authentication and correlation analysis based on CNN-SRU hybrid neural network model. Computational Intelligence and Neuroscience. 2023;2023:1–11.
Available:https://doi:10.1155/2023/8389193

35. Oladoyinbo TO, Adebiyi OO, Ugonnia JC, Olaniyi OO, Okunleye OJ. Evaluating and establishing baseline security requirements in cloud computing: An enterprise risk management approach. Asian Journal of Economics, Business and Accounting. 2023;23(21):222–231.
Available:https://doi:10.9734/ajeba/2023/v23i211129

36. Introna L, Nissenbaum H. Facial recognition technology: A survey of policy and implementation issues; 2010.
Available:https://eprints.lancs.ac.uk/id/eprint/49012/

37. Oladoyinbo TO, Olabanji SO, Olaniyi OO, Adebiyi OO, Okunleye OJ, Alao AI. Exploring the challenges of artificial intelligence in data integrity and its influence on social dynamics. Asian Journal of Advanced Research and Reports. 2024;18(2):1–23.
Available:https://doi:10.9734/ajarr/2024/v18i2601

38. Goodin D. Here’s how long it takes new BrutePrint attack to unlock 10 different smartphones. Ars Technica; 2023.
Available:https://arstechnica.com/information-technology/2023/05/hackers-can-brute-force-fingerprint-authentication-of-android-devices/2/

39. Lemos R. Biometric bypass: Brute print makes short work of fingerprint security. Dark Reading; 2023.
Available:https://www.darkreading.com/endpoint-security/bruteprint-short-work-fingerprint-security

40. Olagbaju OO, Babalola RO, Olaniyi OO. Code alternation in english as a second language classroom: A communication and learning strategy. Nova Science; 2023.
Available:https://doi:10.52305/YLHJ5878

41. Hernández-Álvarez L, De Fuentes JM, González-Manzano L, Hernández Encinas L. Privacy-preserving sensor-based continuous authentication and user profiling: A review. Sensors. 2020;21 (1):92.
Available:https://doi:10.3390/s21010092

42. Omogoroye OO, Olaniyi OO, Adebiyi OO, Oladoyinbo TO, Olaniyi FG. Electricity consumption (kW) forecast for a building of interest based on a time series nonlinear regression model. Asian Journal of Economics, Business and Accounting. 2023;23(21):197–207.
Available:https://doi:10.9734/ajeba/2023/v23i211127

43. Olagbaju OO, Olaniyi OO. Explicit and differentiated phonics instruction on pupils’ literacy skills in gambian lower basic schools. Asian Journal of Education and Social Studies. 2023;44(2):20–30.

Available:https://doi:10.9734/ajess/2023/v44i2958

44. Quadri FU, Olaniyi OO, Olaoye OO. Interplay of islam and economic growth: Unveiling the long-run dynamics in muslim and non-muslim Countries. Asian Journal of Education and Social Studies. 2023; 49(4):483–498. Available:https://doi:10.9734/ajess/2023/v49i41226

45. Lee J. Eye lock white paper discusses biometric authentication in the cloud. Biometric Update; 2017. Available:https://www.biometricupdate.com/201702/eyelock-white-paper-discusses-biometric-authentication-in-the-cloud

46. Olaniyi FG, Olaniyi OO, Adigwe CS, Abalaka AI, Shah NH. Harnessing predictive analytics for strategic foresight: A comprehensive review of techniques and applications in transforming raw data to actionable insights. Asian Journal of Economics, Business and Accounting. 2023;23(22):441–459. Available:https://doi:10.9734/ajeba/2023/v23i221164

47. Samuel J, Rostami M, Bagci U, Sigfrids A. Human-centricity in AI Governance: A systemic approach; 2023. Available:https://www.frontiersin.org/articles/10.3389/frai.2023.976887/full

48. Olaniyi OO, Olaoye OO, Okunleye OJ. Effects of Information Governance (IG) on profitability in the Nigerian banking sector. Asian Journal of Economics, Business and Accounting. 2023;23(18):22–35. Available:https://doi:10.9734/ajeba/2023/v23i181055

49. Olaniyi OO, Olabanji SO, Abalaka AI. Navigating risk in the modern business landscape: Strategies and insights for enterprise risk management implementation. Journal of Scientific Research and Reports. 2023;29(9):103–109. Available:https://doi:10.9734/jsrr/2023/v29i91789

50. Sanchez del Rio J, Moctezuma D, Conde C, Martin de Diego I, Cabello E. Automated border control e-gates and facial recognition systems. Computers & Security. 2016;62:49–72. Available:https://doi:10.1016/j.cose.2016.07.001

51. EU. Documents download module. European Commission ; 2019. Available:https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5cef1aa0f&appId=PPGMS

52. Olaniyi OO, Asonze CU, Ajayi SA, Olabanji SO, Adigwe CS. A regressional study on the impact of organizational security culture and transformational leadership on social engineering awareness among bank employees: The interplay of security education and behavioral change. Asian Journal of Economics, Business and Accounting. 2023;23(23):128–143. Available:https://doi:10.9734/ajeba/2023/v23i231176

53. Wu H, Han H, Wang X, Sun S. Research on artificial intelligence enhancing internet of things security: A survey. IEEE Access. 2020;8:153826–153848. Available:https://doi:10.1109/access.2020.3018170

54. Kaklauskas A, Abraham A, Ubarte I, Kliukas R, Luksaite V, Binkyte-Veliene A, Vetloviene I, Kaklauskiene L. A review of ai cloud and edge sensors, Methods, and Applications for the Recognition of Emotional, Affective and Physiological States, Sensors. 2022;22(20):7824. Available:https://doi:10.3390/s22207824

55. Olaniyi OO, Olabanji SO, Okunleye OJ. Exploring the landscape of decentralized autonomous organizations: A comprehensive review of blockchain initiatives. Journal of Scientific Research and Reports. 2023;29(9):73–81. Available:https://doi:10.9734/jsrr/2023/v29i91786

56. Islam R, Patamsetti V, Gadhi A, Gondu RM, Bandaru CM, Kesani SC, Abiona O. The future of cloud computing: Benefits and challenges. International Journal of Communications. Network and System Sciences. 2023;16(4):53-65. Available:https://doi:10.4236/ijcns.2023.164004

57. Olaniyi OO, Abalaka AI, Olabanji SO. Utilizing big data analytics and business intelligence for improved decision-making at leading fortune company. Journal of Scientific Research and Reports. 2023;29 (9):64–72. Available:https://doi:10.9734/jsrr/2023/v29i91785

58. Olaniyi OO, Okunleye OJ, Olabanji SO. Advancing data-driven decision making in smart cities through big data analytics: A comprehensive review of existing

literature. Current Journal of Applied Science and Technology. 2023;42(25):10–18. Available:https://doi:10.9734/cjast/2023/v42i254181

59. Olaniyi OO, Okunleye OJ, Olabanji SO, Asonze CU, Ajayi SA. IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience. Asian Journal of Research in Computer Science. 2023;16(4):354–371. Available:https://doi.org/10.9734/ajrcos/2023/v16i4397
60. Olaniyi OO, Shah NH, Bahuguna N. Quantitative analysis and comparative review of dividend policy dynamics within the banking sector: Insights from global and U.S. Financial data and existing literature. Asian Journal of Economics, Business and Accounting. 2023;23(23): 179–199. Available:https://doi:10.9734/ajeba/2023/v23i231180
61. Olaniyi OO, Omubo DS. The importance of COSO framework compliance in information technology auditing and enterprise resource management. The International Journal of Innovative Research & Development; 2023. Available:https://doi:10.24940/ijird/2023/v12/i5/MAY23001
62. Olaniyi OO, Omubo DS. WhatsApp data policy, data security, and users' vulnerability. The International Journal of Innovative Research & Development; 2023. Available:https://doi:10.24940/ijird/2023/v12/i4/APR23021
63. Ajayi ND, Ajayi SA, Oladoyinbo OB, Olaniyi OO. A review of literature on transferrin: deciphering its complex mechanism in Cellular Iron Regulation and Clinical Implications. Asian Journal of Research in Infectious Diseases. 2024;15 (1):9-23. Available:https://doi.org/10.9734/ajrid/2024/v15i1321
64. Ajayi ND, Ajayi SA, Olaniyi OO. Exploring the intricacies and functionalities of galactose oxidase: Structural nuances, Catalytic Behaviors, and Prospects in Bio-electrocatalysis. Asian Journal of Chemical Sciences. 2024;14(1):19–28. Available:https://doi.org/10.9734/ajocs/2024/v14i1282
65. Ajayi ND, Ajayi SA, Boyi JO, Olaniyi OO. Understanding the chemistry of nitrene and highlighting its remarkable catalytic capabilities as a non-heme iron enzyme. Asian Journal of Chemical Sciences. 2024; 4(1):1–18. Available:https://doi.org/10.9734/ajocs/2024/v14i1280
66. Olaniyi OO. Best practices to encourage girls' education in Maiha Local Government Area of Adamawa State in Nigeria. The University of Arkansas Clinton School of Public Service (Research Gate); 2022. Available:https://doi.org/10.13140/RG.2.2.26144.25606

© 2024 Olabanji et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/112496