International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Cloud Identity Mastery: Overcoming Access Management Challenges in the Digital Ether

Shanmugavelan Ramakrishnan

SDG Corporation

Abstract: ***Identity and Access Management (IAM) in cloud environments is the focus of this in - depth analysis of AI's efficacy and integration. Addressing the opportunities and threats in cloud computing, it mainly focuses on how AI may improve user authentication, authorization, and access control. Utilising quantitative and qualitative analysis, the study takes a mixed - methods approach. Using multiple regression analysis, we look at how different aspects affect system efficacy, and a survey of 582 cybersecurity experts sheds light on where AI is today and where it could go in IAM. Here we test four hypotheses: first, that the configuration of hardware and software affects system accuracy; second, that computational environments affect reliability; third, that demographic factors play a role in user acceptance; and fourth, that technological improvements affect system performance and acceptance. The results show that these criteria are significantly correlated with AI's efficacy in IAM. System accuracy is affected by hardware configurations and security concerns; system reliability is affected by variations in the computational environment; user acceptance is affected by demographic factors; and improvements in performance and acceptance are brought about by enhancements such as user feedback, advances in artificial intelligence, continuous learning algorithms, and system transparency. For IAM to work in cloud settings, these findings highlight the importance of standardised software, user - centric design, cutting - edge hardware, and ongoing advancements in AI. Involving users in development processes, maintaining openness, and using adaptive algorithms are the three most important recommendations that the study offers to developers and cloud service providers.***

Keywords: Identity and Access Management (IAM), artificial intelligence (AI), Access management, Cloud

1. Introduction

The incorporation of artificial intelligence (AI) into identity and access management (IAM) systems, in particular those that are hosted in cloud environments, is an emerging field that is laden with both obstacles and opportunities. Increasingly common in cloud computing, artificial intelligence is having an impact on how GenAI models are trained and deployed, and it is revolutionising the IAM landscape with automated policy creation and increased security measures [1]. As a result, the role that AI plays in identity and access management (IAM) is becoming increasingly important. Especially in cloud environments, which encompass data security, model security, and infrastructure security, each of which addresses different types of user needs and access requirements, Identity and Access Management (IAM) plays a crucial role in shaping the security landscape of Generative Artificial Intelligence (GenAI) and its associated infrastructure. As an illustration, identity and access management policies are needed in order to guarantee that only authorised persons are able to access sensitive datasets that are utilised in GenAI models.

This serves as a vital layer of defence [3]. It is important to note that Identity and Access Management (IAM) governs who may access and assign the cloud - based resources that are necessary for GenAI models, which need a substantial amount of computational resources. When it comes to shared cloud environments, this is especially important because it guarantees the effective and safe utilisation of resources [3]. It is possible that integrating GenAI into IAM will assist in addressing new security vulnerabilities and threats, such as those that are posed by deepfakes. Generic artificial intelligence has the ability to improve multi - factor authentication and access control rules by analysing patterns of user behaviour and adding anomaly detection. This will result in the MFA process becoming more dynamic and behavior - based [3]. The majority of the time, traditional identity and access management (IAM) solutions are not suited to recognise or combat deepfakes, which are becoming an increasingly serious threat in cloud - based systems [3]. In order to add an additional layer of protection against this new type of threat, it is possible to incorporate GenAI algorithms that have been trained to identify deepfakes into IAM systems [4].

However, the idea of using GenAI as a tool to automate policy development in identity and access management (IAM), in particular for attribute - based access control (ABAC), is much more unsettling. In order to build fine - grained identity and access management policies, this requires investigating common access patterns and roles [5]. As a result, human oversight is necessary in order to maintain a balance between the automatic judgements that GenAI models in IAM make. Governance models for artificial intelligence in identity and access management (IAM) should be based on well - established security concepts, such as the zero - trust architecture, and they should have robust compliance and auditing methods [2]. It is abundantly clear that the ongoing development of artificial intelligence technology and the threats posed by cybersecurity calls for continuous research and development. This is necessary in order to guarantee that these systems are safe, effective, and able to cater to the requirements of a wide variety of stakeholders in the cloud computing landscape.

1.1 Problem Case Evaluation

In the realm of cloud computing, which is undergoing rapid development, the significance of dependable Identity and Access Management (IAM) systems has been drastically amplified due to the growing number of cybersecurity threats and the intricate structure of digital identities [4].

The implementation of artificial intelligence (AI) in identity and access management (IAM), in particular through biometric authentication systems that are powered by AI, is regarded as a revolutionary strategy for improving security protocols and simplifying access control procedures [6]. This is despite the fact that there is still a major gap in empirical understanding regarding the operational effectiveness of these AI - integrated solutions inside the various contexts of cloud platforms. When it comes to standardising and testing AI - driven biometric systems, the contemporary cloud ecosystem, which is characterised by a multitude of platforms with diverse hardware and software configurations, poses a difficult obstacle [7].

It is possible that differences in the performance of artificial intelligence algorithms could be caused by the variety in system architectures and the technologies that lie beneath them [8]. This would have an impact on the accuracy and reliability of biometric authentication. This issue is made worse by the rapid evolution of artificial intelligence technologies, which are constantly being developed and implemented, resulting in the creation of new algorithms and models. This raises doubts about the usefulness and adaptability of these technologies over the long term. There are a number of important facets of this research problem, including user approval and demography. It is essential for the general adoption of AI - powered biometric systems that users have a positive opinion of them and trust in them [10].

Age, amount of technological expertise, and cultural background are all examples of demographic factors that can have an impact on the degree to which these systems are accepted. In addition, issues regarding privacy and data security are of the utmost importance, particularly in light of recent high - profile data breaches and the growing awareness of the rights associated with digital privacy [11]. Regulatory and compliance criteria, which differ from region to region and industry to industry, must also be aligned with the incorporation of AI in identity and access management [12].

A persistent obstacle that must be overcome in order to guarantee that AI - powered identity and access management systems are not only efficient but also in accordance with the law is the ever - changing nature of these regulations, particularly those that pertain to biometric data [9].

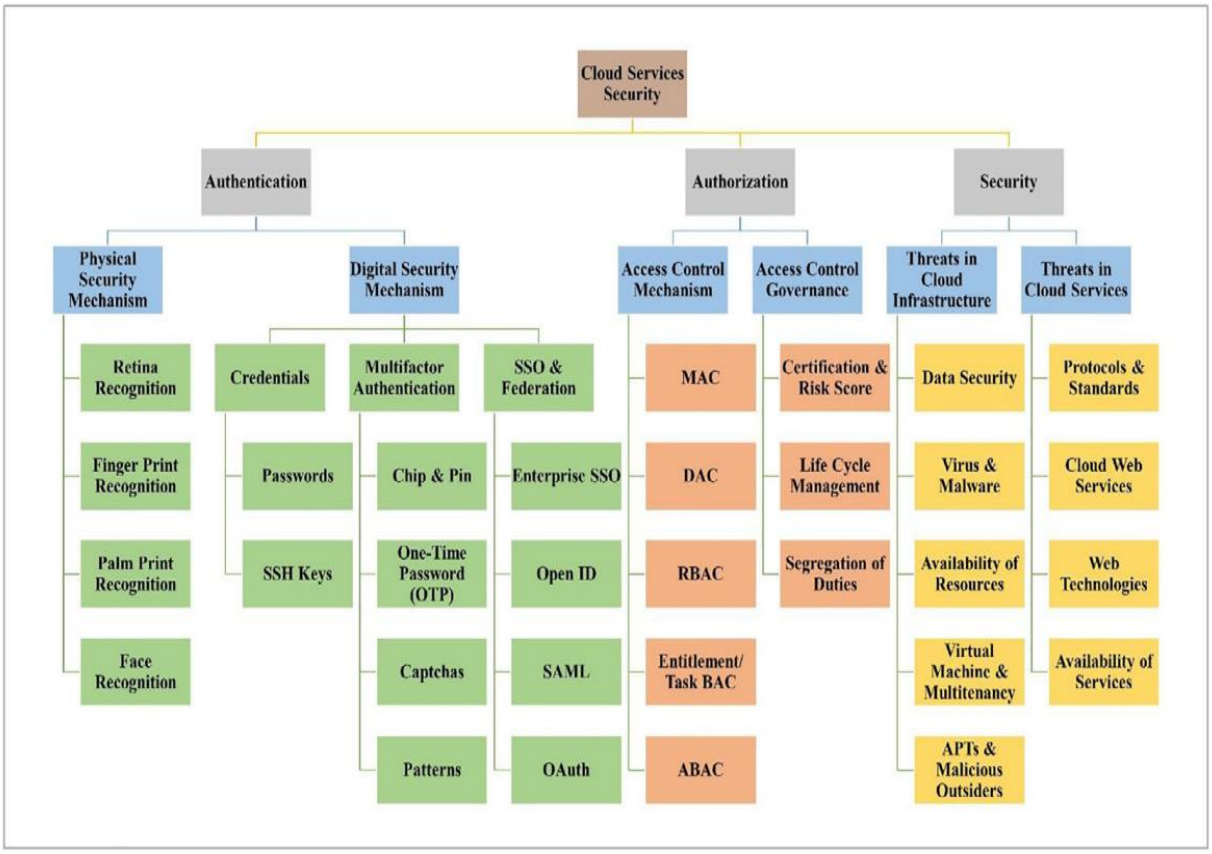

Figure 1: Taxonomy of cloud services security

In order to provide security in the cloud environment, IAM systems carry out a variety of operations. These operations include authentication, authorization, and the supply of storage and verification. The Identity and Access Management (IAM) system ensures that identities and attributes of cloud users are protected by guaranteeing that only authorised individuals are permitted to access cloud systems. Additionally, IAM systems assist in the management of access rights by determining whether or not the appropriate individual who possesses the appropriate privileges is accessing information that is stored in cloud - based systems. It is currently common practice for numerous organisations to use Identity and Access Management systems in order to enhance the level of protection afforded to sensitive data that is kept in a cloud - based environment. An example of a taxonomy of cloud service security is presented in Figure 1.

2. Literature Review

Access to digital resources and software programmes that is both straightforward and dependable for employees is one of the basic criteria for the running of many different types of organisations. Nevertheless, in actuality, it is challenging for IT managers and users to set up, maintain, and use this access, and it comes at a considerable cost. This is especially true when enterprises grow and their technological environment becomes increasingly heterogeneous. In addition, complexity is a factor that contributes to security incidents such as data breaches, which can lead to unanticipated expenditures for remediation and damage to the company's reputation (Enterprise Management Associates, Inc.2020), as well as customer turnover and heavy fines for breaking data protection regulation (Schlackl et al.2022).

The situation became even more dire during the COVID - 19 pandemic, when it was projected that seventy percent of workers were working from home (Sadler and Hancock 2020). According to Naidoo 2020, this coincided with an increase in the number of cyberattacks, the majority of which were phishing attempts. There have been a number of studies that have revealed that people who work from home experience increased levels of fatigue, lack of motivation, and distraction (for example, Velocity Smart Technology 2021). As a consequence of this, errors and a lack of attentiveness are more likely to occur (Irwin 2021), and the probability of employees divulging their passwords in response to a phishing attempt is increased.

Enterprises are provided with tools to assist them in managing and monitoring a growing number of identities beyond employees, such as external partners, customers, and – driven by the growing relevance of the Internet of Things (IOT) – smart devices (Haber 2020). Identity and access management (IAM) systems provide businesses with tools to support them in managing and monitoring, in addition to providing better password management for employees.

In order to reduce the risks associated with cybersecurity, 77% of businesses intend to raise their budget for identity and access management (IAM) (Globenewswire 2020). On the other hand, in 2017, only 38 percent of businesses utilised dedicated identity and access management software, which exemplifies the significant difficulties and expenses associated with the construction and upkeep of these systems. As a consequence of this, businesses also investigate novel methods, such as zero - trust architectures (Buck et al.2021), or they implement complementary strategies, such as increasing the level of cybersecurity awareness among their workforce and implementing anti - virus software (Deloitte 2020).

On the basis of the recommendations offered by the specialists regarding the make - up of the clusters, we applied the following modifications: "Privacy and Trust" was merged with "Control, " "Standardisation, Interoperability, and Simplicity" was merged with "Portability, " and "Availability" was added to "Manageability, Efficiency, Automation, and Cost. " It was a successful combination. Additionally, as a result of the discussion that was presented earlier, we came to the conclusion that the category "Simplicity" should be separated from Cluster 3 (which is comprised of "Standardisation, Interoperability, and Simplicity") and merged with the newly formed cluster labelled "Control, Privacy, and Trust. " This decision was made because all of these factors are strongly related to the position of the user. The "Effectiveness" element was added to the second new cluster in accordance with the suggestion made by Expert 8. In addition, we included the variable "Flexibility" in this cluster because it is related to the architecture of the system. By adhering to the recommendation of Expert 7, we provided the newly formed clusters with succinct labels in order to make them simpler to comprehend and to place the issues contained within the clusters in the appropriate context. Our modifications ultimately resulted in the formation of four distinct clusters, which are referred to as "Security & Compliance, " "Operability, " "Technology, " and "User" respectively. Figure 2 is an illustration of the final requirement structure for identity and access management.

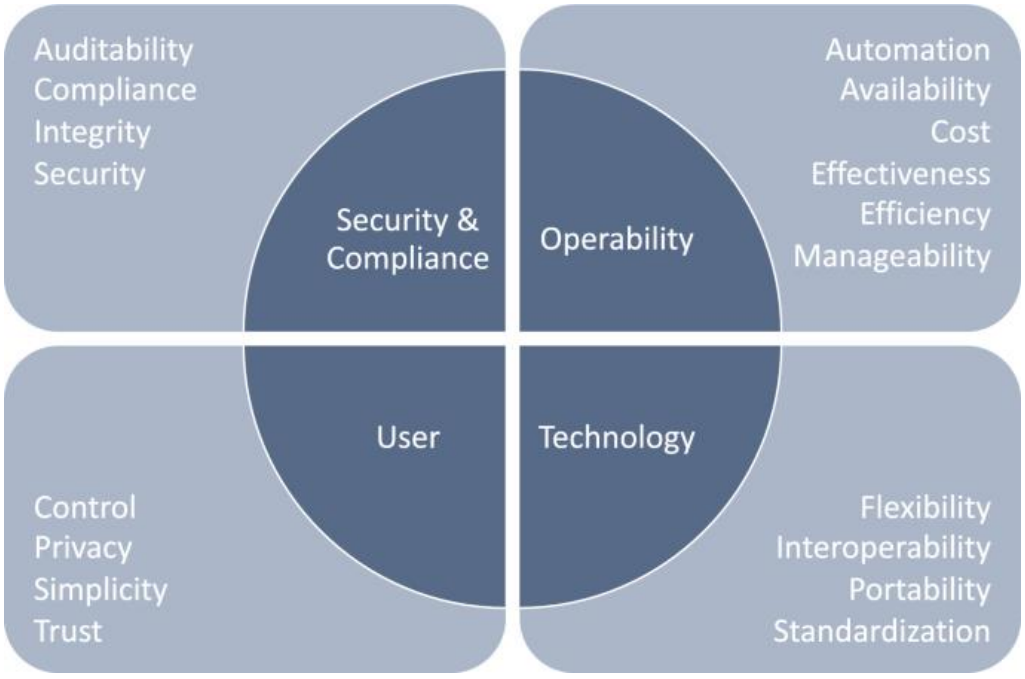

Figure 2: Requirements for an enterprise IAM system: consolidated results after the SLR and the evaluation with experts

There is no communication between the two ACA - Py agents that are responsible for the HR department and the intranet login in our prototype, and they do not make use of a common directory. (Schlatt et al.2022a; Sartor et al.2022) The employee uses a smartphone to run an SSI wallet application that has the capability to generate and use cryptographic keys, receive and manage virtual currency, and engage with verifiers in virtual private spaces. A portion of the capabilities offered by the ACA - Py can be considered to be included in the wallet application. As a result, the wallet also needs to have client capabilities for the Hyperledger Indy blockchain. Due to this, a user is now required to select the same blockchain that the other two agents are linked to within their digital wallet application.

3. Methodology

The methodology that was chosen is intended to achieve the goal of providing a comprehensive understanding of how artificial intelligence may enhance user authentication, authorization, and access control. The research makes use of a mixed - methods technique, which combines qualitative insights with quantitative data analysis. The quantitative part focuses primarily on the analysis of survey data collected from cybersecurity professionals, whilst the qualitative aspect involves the synthesis of findings in order to give recommendations that may be put into effect. Through the utilisation of this all - encompassing method, a comprehensive grasp of the topic is ensured, which includes both statistical trends and nuanced, contextual insights.

Questionnaires based on surveys were the primary way of data collecting that was utilised in this investigation. An exhaustive collection of seven hundred questionnaires was sent out to a carefully selected group of cybersecurity professionals. These individuals were picked for their experience in artificial intelligence, identity and access management, and cloud computing. There were 582 of these that were returned with responses that were correct and comprehensive, which provided a sizable data set for interpretation. An assortment of insights, such as technical evaluations, user experience feedback, and expert opinions on the capabilities of artificial intelligence (AI) in identity and access management (IAM) systems, were intended to be gathered through the use of the questionnaire. In order to collect both quantitative and qualitative data, the questions were designed to be constructed in such a way that they would collect ratings and frequency of usage, as well as open - ended replies on difficulties and opportunities. As a result of the high response rate and the quality of the responses, it is clear that the problem is becoming increasingly important and urgent among experts working in the sector.

The purpose of this study is to critically analyse the effectiveness and user perception of AI - powered Identity and Access Management (IAM) systems in a variety of cloud environments. The study makes use of Multiple Regression to accomplish this, and it provides essential insights into the ways in which various factors, such as technological setups and user demographics, influence the effectiveness of IAM.

A level of agreement scale, ranging from "Strongly Agree" to "Strongly Disagree, " is utilised in the research project in order to capture the direct and various perspectives of cybersecurity specialists. This allows for the mapping of professional opinions, which in turn reveals nuanced patterns of acceptance and worry. In addition to this, the application of inferential statistics through multiple regression analysis broadens the scope, which enables the prediction accuracy and perception of AI - powered identity and access management.

A summary of the demographic information of those who took part in the survey is presented in Table 1. When it comes to experience, the bulk of the participants (54%) have between six and ten years of experience. This indicates that

there is a significant presence of professionals who are likely well - versed in the current trends and difficulties in artificial intelligence and identity and access management, possibly mixing these techniques with traditional ones. Those who have 11 - 15 years of experience (22%) bring dimension to the conversation because they have most likely witnessed the development of IAM systems and the early integration of AI.14.1 percent of the group has between one and five years of experience, which brings with it new perspectives that may be more in line with the most recent developments in educational and technological improvements. The smallest group, which accounts for ten percent of the total, has over fifteen years of experience and provides precious insights from a long - term perspective. They have most certainly witnessed important movements and trends over the course of time.

According to the age distribution, there is a significant concentration in the age range of 35 to 44 years (45%), which indicates a mature and experienced cohort that is most likely in influential jobs or critical decision - making positions. In addition to the pool of experienced professionals, the next largest category is those between the ages of 45 and 54 (19%). The opinions of individuals who are over 55 years old (12%) and those who are between the ages of 25 and 34 years old (17%) come from the earlier and later periods of their professional lives, respectively. Seven percent of the entire population is comprised of individuals who are under the age of 25.

By looking at the gender distribution, it is clear that the majority of participants are male (68%), which is reflective of the larger trends that are occurring in the sectors of technology and cybersecurity. The presence of women in this industry is highlighted by the fact that female participants make up 28% of the total. As a result of the inclusion of a wide range of gender identities in the research, a tiny percentage of respondents either identify as non - binary or third gender (three percent) or choose not to say (one percent).

Table2 ResponsestoHypothesis1: The accuracy of biometric authentication systems that are powered by artificial intelligence varies greatly across different cloud platforms due to differences in the configurations of the computer's hardware and software.

Regarding Hypothesis 1, which is concerned with the varying degrees of accuracy that may be achieved by AI - powered biometric systems, the majority of participants reported experiencing changes in accuracy. This highlights the important influence that hardware settings and software upgrades have on the results of the system. There is also a significant issue regarding security as a result of varied levels of accuracy, which highlights the essential requirement for high accuracy in order to guarantee robust security in identity and access management systems.

Regarding Hypothesis 2, which is concerned with the dependability of these systems in various computing contexts, the responses indicate that there is a general consensus regarding the high reliability of AI systems in primary computational environments. Variations in computational environments, on the other hand, are seen to have an impact on reliability, and technological differences are thought to be the cause of security concerns. It is a widely held view that the quality of AI systems in identity and access management could be improved by standardising surroundings.

Age is considered as a crucial component that influences user acceptance, and technical experience is also seen as having an impact on trust in these systems. This is in reference to Hypothesis 3, which examines the factors that influence user acceptance. Even if there is more variance in responses regarding this topic, it is believed that gender has a factor in acceptance. Privacy concerns are intimately linked to acceptability, which highlights the significance of these concerns in the design and deployment of biometric systems that are powered by artificial intelligence.

When it comes to H4, which is centred on improvements for enhanced IAM systems, there is a great deal of agreement that user feedback is quite important for the design of the system. Improvements in artificial intelligence technologies are generally acknowledged to be responsible for improved performance. There is an emphasis placed on the significance of incorporating algorithms for continuous learning, and it is believed that transparency in the functioning of the system is essential to facilitating an increase in confidence and acceptance among users.

4. Results and Study

t - Value=

$$t_{\widehat{\beta}} = \frac{\widehat{\beta} - \beta_0}{\mathrm{SE}(\widehat{\beta})}$$

p - value = P (TS ts | H_0 is true) = 1 - cdf (ts)

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%
Over15 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 Notto Say	6	1%

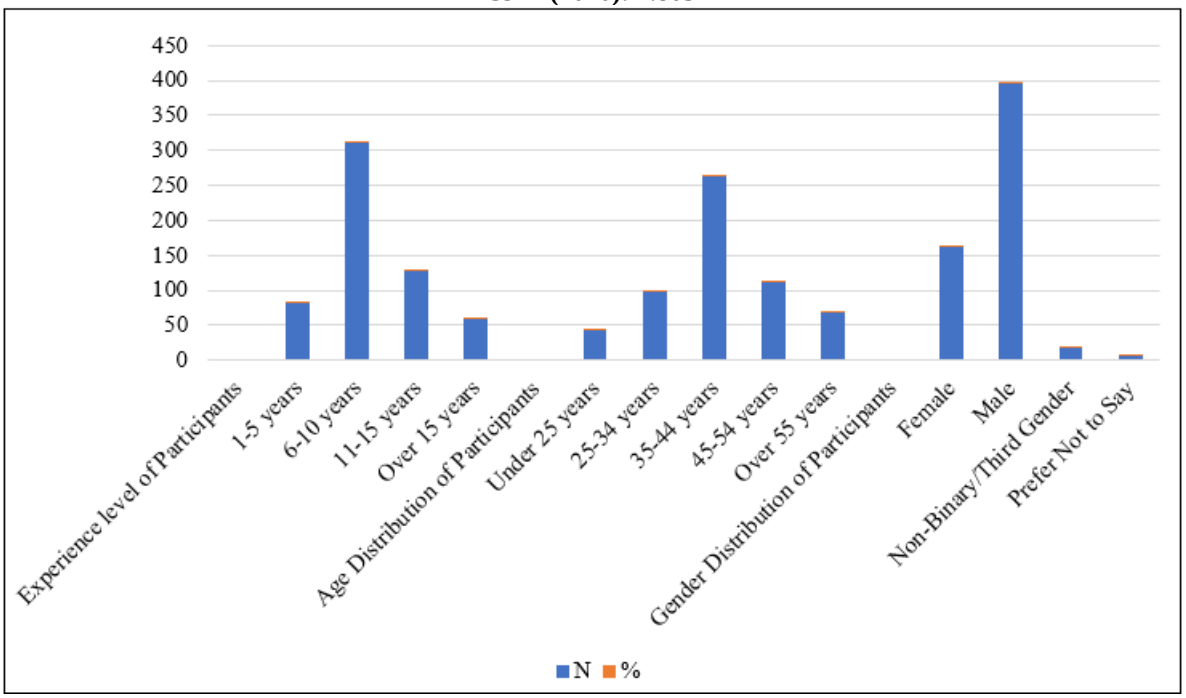

Table 2: Participants' responses to questions on Hypothesis variables

	SA	A	N	D	SD
H1Parameters					
Observed Variations inaccuracy	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
H3Parameters					
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
H4Parameters					
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

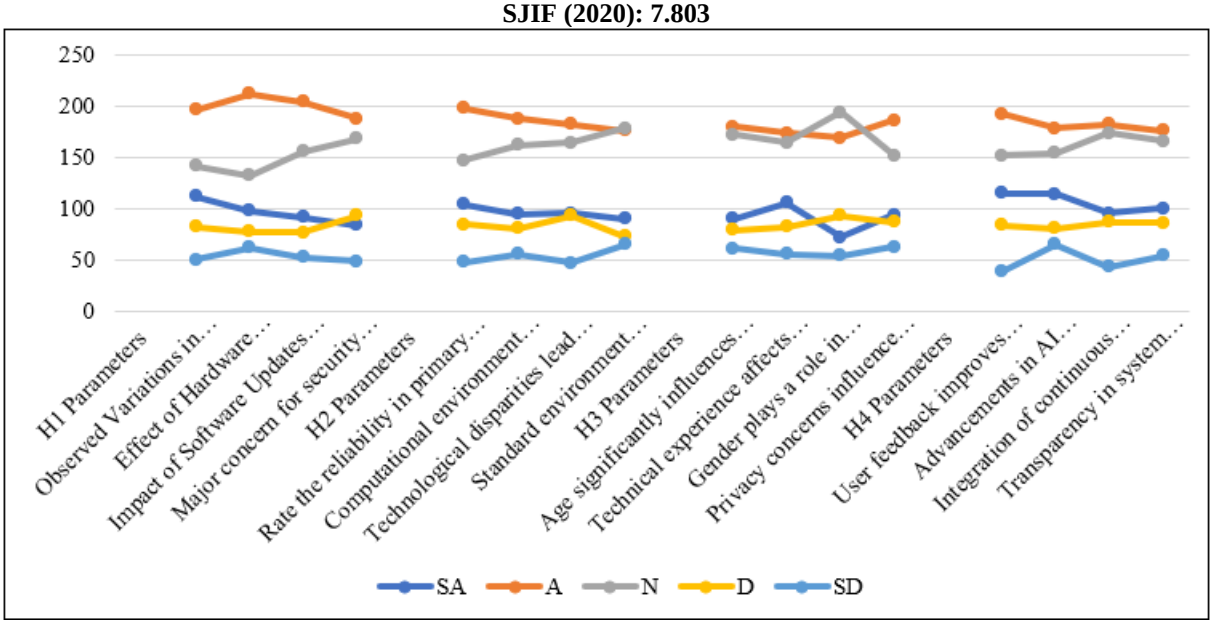

Table 3: Participants' responses to questions on Hypothesis variables

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 Authentication Systems				

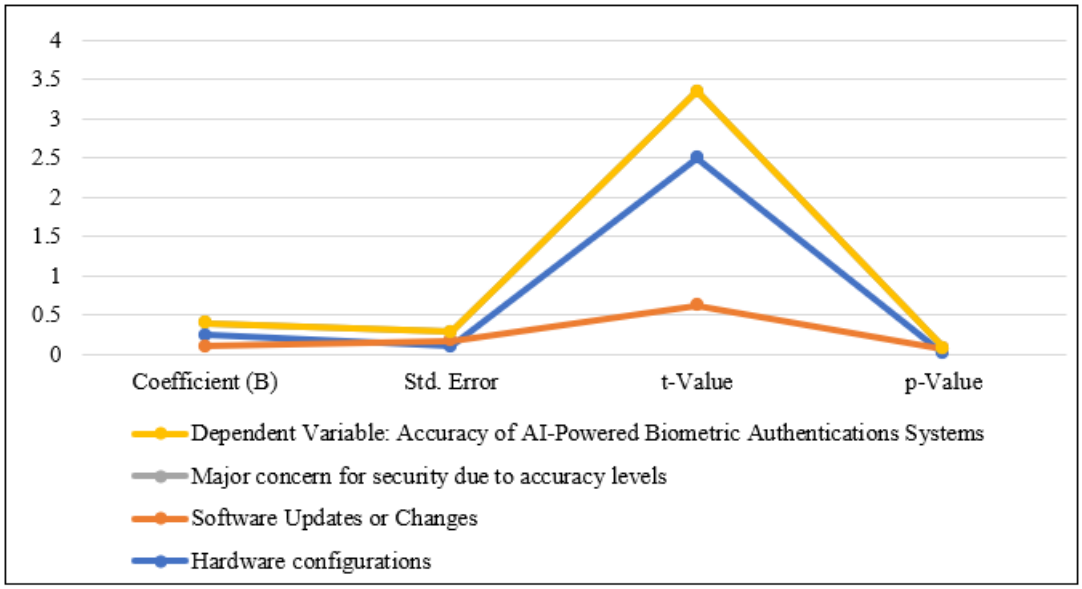

Table 3: Inferential Statistics for Hypothesis 1: The accuracy of biometric authentication systems that are powered by artificial intelligence varies greatly across different cloud platforms due to differences in the configurations of the computer's hardware and software. The multiple regression analysis for Hypothesis 1 indicates the impact of a variety of parameters on the accuracy of biometric authentication systems driven by artificial intelligence that are deployed in cloud platforms. When it comes to hardware configurations, a coefficient of 0.25 and a standard error of 0.10 indicate that there is a positive association between the level of sophistication of hardware configurations and the accuracy of AI - based biometric systems that are hosted on cloud platforms. More evidence that this association is statistically significant is provided by the t - value of 2.50 and the p - value of 0.013. These values indicate that enhancements to the hardware configurations of these systems are likely to result in an increase in the accuracy of these systems.

Table 4: Hypothesis 2

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				

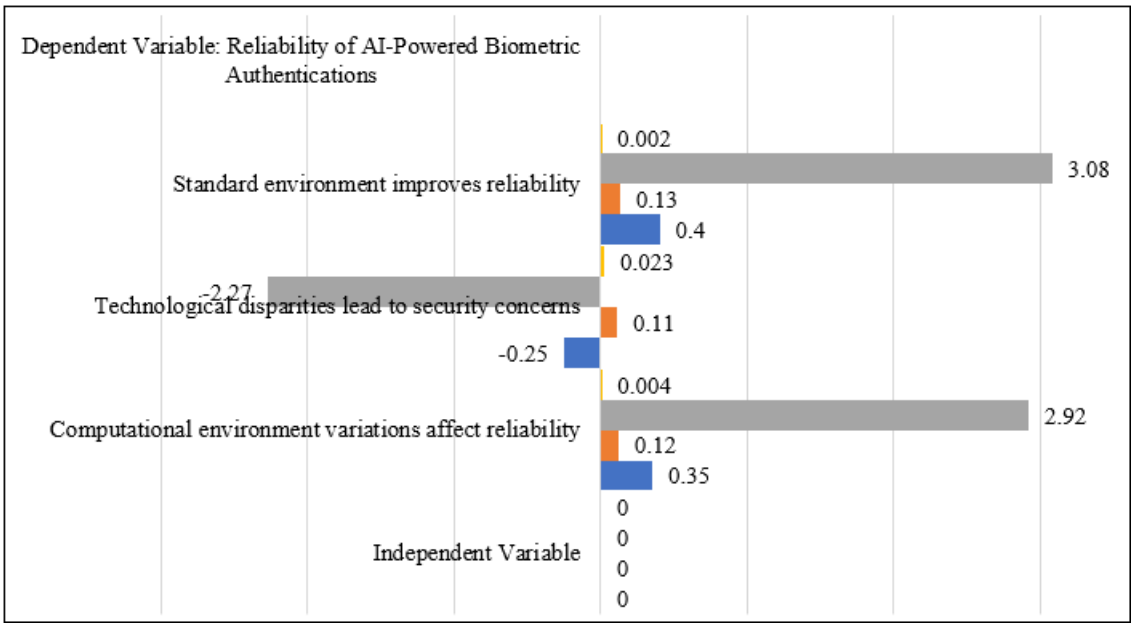

Table 5: Participants' responses to questions on Hypothesis variables

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				

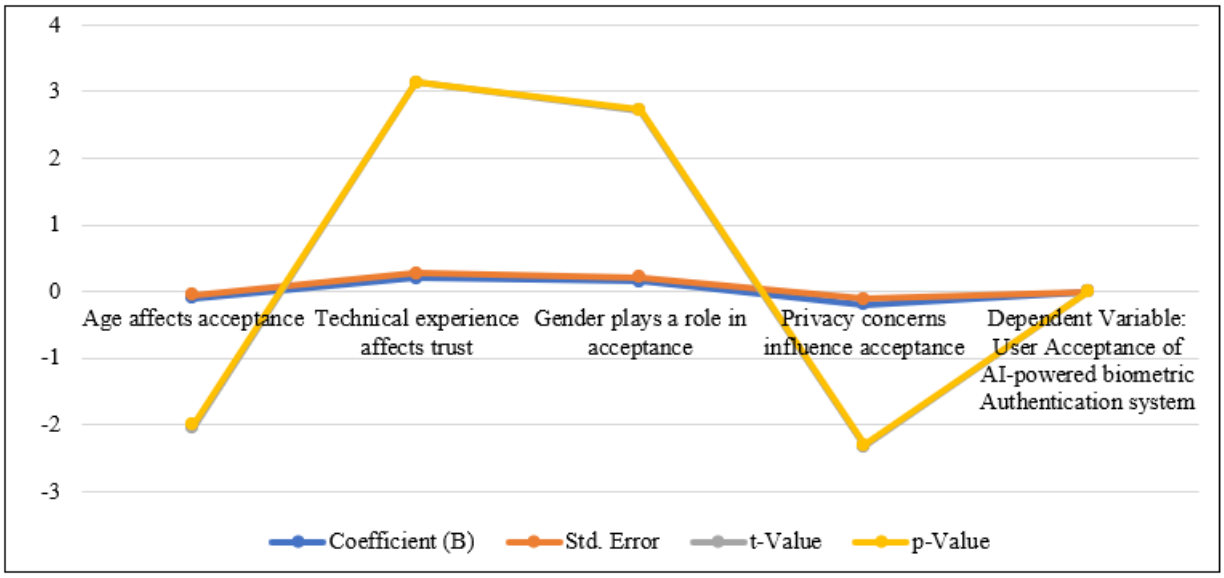

Table 5: Inferential Statistics to Hypothesis 3: There are variances in trust and perceived ease of use across different user groups, which is driven by demographic factors. User acceptability of AI - powered biometric authentication systems is influenced by these characteristics. Age has a negative impact on acceptance, with a coefficient of - 0.10, according to the multiple regression analysis for Hypothesis 3, which shed insight on how demographic factors influence the acceptability of AI - powered biometric identification systems. This indicates that acceptance reduces with rising

age, a relationship that is statistically significant as evidenced by a tvalue of - 2.00 and a p - value of 0.046. This data demonstrates that acceptance declines with growing age. When compared to older groups, this data suggests that younger populations may be more open to these technologies than older population groupings. There is a positive correlation between trust in these systems and technical experience, as demonstrated by the findings. Individuals who have more technical experience tend to have better faith in AI - powered biometric identification systems, as indicated by a coefficient of 0.20, a t - value of 2.86, and a p - value of 0.004. These findings are statistically significant. The importance of being familiar with and having a grasp of technology in developing acceptance is highlighted by this evidence. A coefficient of 0.15 indicates that the influence of gender on acceptance is also considerable. This is another major factor. There are differences in acceptability levels between the sexes, as indicated by this conclusion, which is supported by a t - value of 2.50 and a p - value of 0.013. This finding suggests that gender - specific characteristics may play a role in how these technologies are seen and embraced.

5. Discussion

In cloud environments, the findings of the study highlight the significance of hardware configurations in affecting the accuracy of biometric authentication systems that are powered by artificial intelligence applications. This is in line with the findings of the research, which proved that modern hardware can achieve a high level of authentication accuracy when imaging iris and veins on the finger. According to the findings of this study, the favourable impact of hardware configurations is a monument to the changing technological landscape, which is characterised by changes in hardware that directly influence system performance. On the other hand, the impact of software updates or modifications on system accuracy is less clear. This situation is a reflection of the dynamic nature of software development and the various consequences that it has on system performance. Moreover, the worry for security that arises from the levels of accuracy is a reflection of the growing awareness and importance of accuracy in biometric systems. This is in line with studies that emphasise the significant role that accuracy plays in guaranteeing the security of identity and access management systems. The focus placed on accuracy is in line with the growing security requirements in cloud computing, particularly with regard to the protection of sensitive data from hitherto unknown dangers. Researchers have demonstrated that differences in the cloud computing environment have a major impact on the reliability of AI - based biometric authentication solutions. It is clear that this discovery is in agreement with the difficulties that have been brought to light in the research literature concerning cloud - based biometric systems and their reliance on certain technology frameworks.

6. Conclusion and Recommendation

This study's results on AI in IAM have several theoretical and practical consequences. Investing in modern hardware and striving for technological consistency are necessary for cloud service providers. This is because system correctness and dependability are affected by hardware configurations and technological standardisation. There may be less performance variation among cloud platforms if this method is implemented. System developers should take a more user - centric approach, taking into account the different needs of users and their privacy sensitivity, as user acceptability places a strong emphasis on user demographics and privacy concerns. The study's findings allow for the following recommendations:

a) To improve the accuracy and reliability of AI - powered biometric systems, cloud service providers should invest in top - of - the - line hardware. At the same time, they should work to standardise software and computing environments to help decrease inequalities and increase system reliability.
b) Developers working on cloud systems should solicit user input early on and use it to make the system more trustworthy and easy to use; developers working on AI systems should prioritise the use of continuous learning algorithms to make the system dynamic and responsive to new security threats.
c) In order to gain customers' trust and encouragement, cloud providers need be more clear about how their AI - powered services operate and handle data.

References

[1] Behera NKS, et al. Futuristic person reidentification 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. c om/wp - content/uploads/2021/05/The - Roleof - Individuals - in - the - Data - Ecosystem. pdf

[8] Yan W, Tang J, Stucki S. Design and implementation of a lightweight deep CNNbased 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/11610/2396 8

[10] Enterprise Management Associates, Inc (2020) Contextual awareness: advancing identity and access management to the next level of security effectiveness. https: //www.enzoic. com/wp - content/uploads/EMA - Contextual - Awareness - Report - 03.2020 - ENZOIC - SUMMARY. pdf. Accessed 9 Aug 2023

[11] Schlackl F, Link N, Hoehle H (2022) Antecedents and consequences of data breaches: a systematic review. Inf Manag 59 (103): 638. https: //doi. org/10.1016/j. im.2022.103638

[12] Sadler T, Hancock J (2020) A Stanford deception expert and cybersecurity CEO explain why people fall for online scams. https: //www.fastcompany. com/90542273/a - stanford - deception - expert - explains - why - people - fall - for - online - scams. Accessed 9 Aug 2023

[13] Naidoo R (2020) A multi - level influence model of COVID - 19 themed cybercrime. Europ J Inf Syst 29: 306–321. https: //doi. org/10.1080/0960085X.2020.1771222

[14] elocity Smart Technology (2021) Velocity smart market research report 2021. https: //www.velocity - smart. com/en - gb/velocity - smart - technology - market - research - report - 2021. Accessed 9 Aug 2023

[15] Irwin L (2021) The cyber security risks of working from home. https: //www.itgovernance. co. uk/blog/the - cyber - security - risks - of - working - from - home. Accessed 9 Aug 2023

[16] Haber MJ (2020) Privileged access management. In: Privileged attack vectors, Springer, Heidelberg, pp 151–171, https: //doi. org/10.1007/978 - 1 - 4842 - 5914 - 6_11

[17] Globenewswire (2020) New ESG &JumpCloud study uncovers IT's biggest identity and security challenges due to COVID - 19. https: //www.globenewswire. com/news - release/2020/10/02/2102941/0/en/New - ESG - JumpCloud - Study - Uncovers - IT - s - Biggest - Identity - and - Security - Challenges - Due - to - COVID - 19. html. Accessed 9 Aug 2023

[18] Deloitte (2020) Impact of COVID - 19 on cybersecurity. https: //www2. deloitte. com/ch/en/pages/risk/articles/impact - covid - cybersecurity. html. Accessed 9 Aug 2023

[19] Buck C, Olenberger C, Schweizer A, Völter F, Eymann T (2021) Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero - trust. ComputSecur 110 (102): 436. https: //doi. org/10.1016/j. cose.2021.102436

[20] Sartor S, Sedlmeir J, Rieger A, Roth T (2022) Love at first sight? A user experience study of self - sovereign identity wallets. In: Proceedings of the 30th European conference on information systems, AIS. https: //aisel. aisnet. org/ecis2022_rp/46/. Accessed 9 Aug 2023