International Journal of Artificial Intelligence Research and Development (IJAIRD)
Volume 2, Issue 1, January-June 2024, pp. 113-122. Article ID: IJAIRD_02_01_011
Available online at https://iaeme.com/Home/issue/IJAIRD?Volume=2&Issue=1
Impact Factor (2024): 6.98 (Based on Google Scholar Citation)
Journal ID: 234A-56Z1, DOI: https://doi.org/10.17605/OSF.IO/76DG5

© **IAEME** Publication

OPEN ACCESS

ANALYSIS ON THE ROLE OF ARTIFICIAL INTELLIGENCE AND IDENTITY AND ACCESS MANAGEMENT (IAM) IN CYBER SECURITY

Kaushik Reddy Muppa
Advisory Manager, Deloitte, Ashburn, VA, United States

ABSTRACT

The major purpose of this article is to investigate how identity and access management systems are utilized in a variety of different sectors. When it comes to the protection of sensitive information, the IAM system often possesses a collection of functions that have been predetermined. In the context of identity and access management (IAM), authentication is an essential component since it can validate the identity of authorized service providers. With an eye toward IAM systems, this article aims to provide a summary of research on intelligent authentication. These research projects are evaluated using the essential criteria for intelligent authentication that have been suggested. The results of this investigation indicate that a fully functional authentication system cannot be created and implemented at this time. Users must have separate identities and permissions to access all applications, system software, database platforms, etc., to effectively manage today's complex IT environments. The investigation makes use of a mixed-methods approach, which combines qualitative and quantitative research approaches together. To understand the present and future of AI in IAM, we surveyed 582 cybersecurity experts and used multiple regression analysis to look at how different aspects affect system efficacy. 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. According to the results, there are strong relationships between these variables and AI's performance in IAM.

Keywords: Identity and Access Management (IAM), Artificial Intelligence, Information Technology (IT), Cyber-Security.

Cite this Article: Kaushik Reddy Muppa, Analysis on the Role of Artificial Intelligence and Identity and Access Management (IAM) In Cyber Security, International Journal of Artificial Intelligence Research and Development (IJAIRD), 2(1), 2024, pp. 113-122. https://iaeme.com/Home/issue/IJAIRD?Volume=2&Issue=1

1. INTRODUCTION

The technology and business processes that make it possible for the appropriate identities to gain access to the appropriate assets at the appropriate time for the appropriate reasons are what make up digital identity and access management [1,2]. This management system also eliminates the possibility of unauthorized access and fraud.

The sole aspect of identity management that is covered in this guide is the digital identity of an individual, software application, or device; it does not address their physical identity [3]. Usernames, passwords, and email addresses are examples of unique verified traits and credentials that are used to authenticate users, determine permissions, provide access, and monitor activities (Figure 1). Digital identity is represented by distinct attributes and credentials.

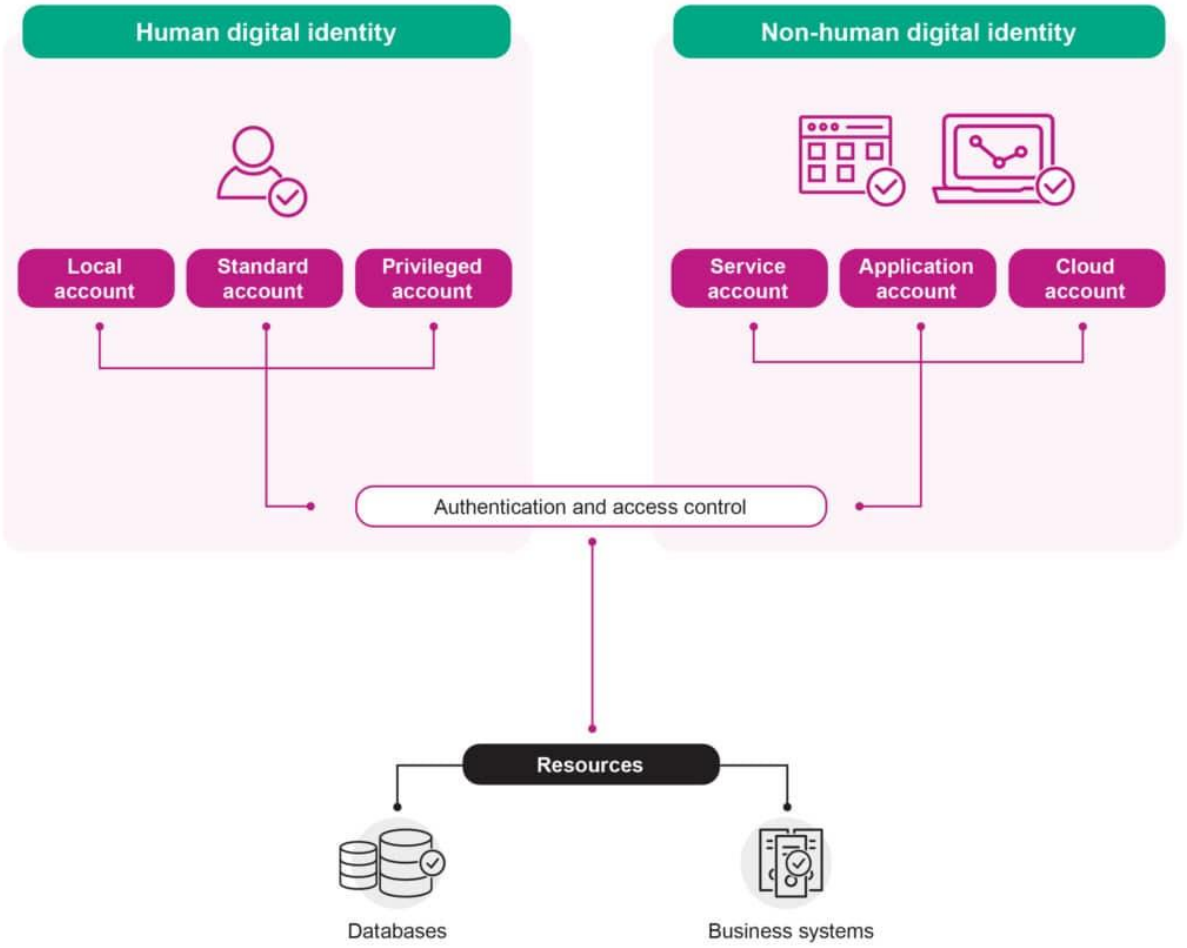

Figure 1: Simplified overview of identity, accounts, and access

The abbreviation for "Identity Access and Management" is "IAM." In layman's words, it restricts access to vital data while allowing employees to read, copy, and alter content that is related to their jobs. This information may contain sensitive information as well as information that is specific to the company.

This article serves as an introduction to the IAM IT security discipline as well as the architecture for managing digital identities. Additionally, it prevents the provision of identity, which is necessary for gaining access to resources and carrying out particular duties [4,5]. If you surpass your objective, IAM will ensure that the appropriate resources, including the database, application, and network, are accessible to you. Everything is proceeding according to the schedule.

1.1. Problem statement

To manage cybersecurity risks and other information security problems, the key problem that this paper addresses and answers is developing a knowledge of how artificial intelligence interacts with Identity Access Management. This understanding is necessary to manage these concerns. Cybercriminals gain an understanding of how businesses normally manage security and create more covert methods for infiltrating the networks of their victims. It is no longer possible for human monitoring to detect unauthorized efforts to gain access since it requires meticulous study rather than human observation. Companies are responding by putting more faith in AI to enhance their identity and access management (IAM) policies, which in turn strengthens access security and protects users' identities. IAM, which stands for identity and access management, needs to undergo some sort of transformation. The concept of identity has been expanded to include not just human users but also devices and applications, which has resulted in a challenging situation for those who are responsible for managing identities. With hundreds or even thousands of identities, a normal corporate network must cope with a wide variety of challenges regularly. Each of these identities suffers from its own unique set of problems. When cloud services make it possible for users to access networks from any location and device, and when the photos are entered by employees who are flexible or who work remotely, the scenario becomes more problematic. When consumers, clients, or third parties obtain access, it becomes difficult, if not impossible, for IT teams to administer the rules of identity and access management (IAM) on their own.

2. LITERATURE REVIEW

User identity management is a standard component that enables easily auditable access to certain limited assets while also providing security for limited assets. To ensure that the job identities and nature of the appropriate individuals can be easily accessed via the use of appropriate tools, the phrase "Identity Access Management" is used. To manage digital identities and monitor user access, the framework incorporates a variety of processes, regulations, and technologies. One of the main reasons identity management is important is to increase data security, regulate user data access, and prevent unauthorized access. Assistance in identifying unauthorized access, reducing data breaches, and proposing important business sector information is provided to any firm. We may classify the components of Identity and Access Management (IAM) into four broad groups: "authorization," "authentication," "central user repository," and "user management" [6]. Users will never be able to remember all of their passwords if they have several accounts since passwords are among the most important and widely used authentication techniques in the modern world.

Regularly, it compels users to select less secure passwords, which is detrimental to the users' ability to protect their passwords. It has come to our attention that it is becoming increasingly simple for malicious actors to gain access to such accounts and to hijack the credentials of users. The cloud platform known as "SailPoint" is designed to help users preserve identity security by assisting them in recognizing the identities of all the secure information and the accesses to it [7].

By utilizing this identity management solution, organizations may streamline the process of managing digital identities, employee permissions, data access, information security, and compliance. In a similar vein, it has also been observed that the platform of identity security that is proposed by 'CyberArk' is the most expandable and comprehensive one, and it assists in the protection of essential assets and identities in the region of zero trust. It is an all-encompassing "security-focused identity and access management" system. "Okta," on the other hand, is an identity and access management platform that is compatible with all relevant existing solutions and can be used neutrally and straightforwardly.

It also chooses the most effective technologies. Cross-chain transactions are proposed as a means of practicing diverse accesses [8]. These transactions are used for identity authentication as well as access control of various participating nodes.

As part of this study endeavor, Identity and Access Management (IAM) proposes chances to conveniently access all different kinds of cloud-resourced project-level access. It makes it possible to keep IAM standards to gain access to the data that is required to do the operation. Many different kinds of adjustments are used to achieve identity verification and access control to sustain transaction circulation [9]. These adjustments are made to keep the chain intrusion at a modest level. On top of that, the IAM scheme makes it easy to convert using cross-chain identities even when dealing with illegal transactions recorded on different chains. Identity and access management (IAM) is never risk-free in the cloud, but with the help of cloud providers, you can easily handle a wide variety of potential issues. Consequently, it is equally important to handle all the risks related to identity and access management (IAM), such as the fallout from cyber criminals, improper vendor management, industrial espionage, or abuse by privileged users [10].

3. KEY COMPONENTS OF IDENTITY AND ACCESS MANAGEMENT

The majority of identity and access management solutions share the same functions, even though certain solutions are more complicated than others. certain functions are responsible for attaining the benefits that were covered earlier. Identification and access management (IAM) and interest in multi-layered systems are both on the rise as a result of the fact that ninety-five percent of businesses have deployed them for a justifiable cause. The operation of each essential component of identity and access management (IAM) should be investigated, as should how the network as a whole protects confidential corporate information.

3.1. Identity Management

As mentioned before, the identity management part of identity and access management (IAM) relies on a database that stores user records. Aside from storing login passwords and identifying information, it also keeps track of names, phone numbers, email addresses, and other data that has been collected over time.

As soon as a new employee or customer is brought on board, the database is updated with their fundamental information. The information about them is updated by any changes that occur in their account or duties within the firm. If they decide to depart, the records ought to reflect that as well. To determine whether or not an individual who is attempting to log in is a legitimate user, identity management checks make use of the information contained inside the database. In addition, this implies that the database must be kept up to date at all times to guarantee that your IAM system can make appropriate decisions regarding the users that are provided.

3.2. Access Management

IAM works for your company in several different ways, and this is among them. Following the verification of a user's identification, the user's permissions are examined first. Who is authorized to utilize what regions, resources, and data, and how may they use it? In the organization, the things that they should be able to access are determined by factors such as their role, agreement, duties, and security clearance. The corporation is responsible for determining the permits of its employees as well as the customers it serves. It is common practice to use privileged access management (PAM) and role-based access control (RBAC) as methods for defining boundaries and safeguarding the data of all individuals from being compromised.

3.3. Authentication and Authorization Tools

To grant users access to resources and validate their identities, an identity and access management system (IAM) makes use of a variety of software applications. The usage of usernames and passwords, multifactor authentication, risk-based authentication, and single sign-on are examples of common but effective techniques that are frequently included in identity and access management strategies. On the other hand, more complicated solutions are frequently required as well, particularly in the case of medium to big organizations.

For example, when someone creates an account or tries to make a purchase, fraud monitoring systems use information gathered from online sources such as social media profiles, digital footprints, fingerprinting of devices and browsers, and IP analysis to confirm the person's identity.

If the supplied details trigger a blacklist alert or do not match, the IT department can take appropriate action. This action may include preventing this individual from entering the system or deleting their compromised account. It is already estimated that fraud costs the global economy $5.1 trillion annually; therefore, preventative measures of this kind are necessary.

3.4. Encryption

IAM is not an exception to the rule that cybersecurity programs are pointless if they do not include encryption. Data that is being transferred from one location to another is protected from being hacked or stolen by this component. Everything in a business setting, from passwords to transactions, needs to be encrypted at a high level. This includes the encryption of sensitive information.

If, for example, you implement solutions that are hosted in the cloud in addition to those that are hosted on-premises, then this additional layer of protection is doubly vital to defend your operations.

3.5. Auditing

The database that you use for identity management is not the only thing that requires ongoing security monitoring. The best way to ensure that all of your IAM procedures are functioning properly is to check on their progress frequently. Some of the most critical parts of effective auditing are setting up analytics, paying close attention to reports, and acting on promising or suspicious patterns. By going through these steps again and again, you will learn all there is to know about identity and access management (IAM) and how it might impact your company.

4. METHODS

The selected methodology aims to accomplish the goal of offering a thorough comprehension of how AI can improve user authentication, authorization, and access control. A mixed-methods approach is utilized in the research, which integrates quantitative data analysis with qualitative observations. Both the quantitative and qualitative parts of the study are important; the former mainly analyses survey data obtained from cybersecurity specialists, and the latter synthesizes findings to provide actionable advice. Through the utilization 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 collection that was utilized in this investigation. An exhaustive collection of seven hundred questionnaires was sent out to a carefully selected group of cybersecurity professionals. The selection committee prioritized candidates with backgrounds in cloud computing, identity and access management, and artificial intelligence.

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. 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. The significant number of replies and excellent quality of those replies show that this is a topic that is rapidly gaining attention from professionals in the field. The goal of this research is to examine several cloud-based Identity and Access Management (IAM) systems that are powered by artificial intelligence (AI) and how their users perceive them.

The study makes use of Multiple Regression to accomplish this, and it provides essential insights into how various factors, such as technological setups and user demographics, influence the effectiveness of IAM. The study uses a four-point agreement scale (from "Strongly Agree" to "Strongly Disagree") to collect first-hand accounts from cybersecurity experts. This paves the way for the mapping of expert views, which exposes complex patterns of comfort and concern. Beyond this, the use of multiple regression analysis in inferential statistics expands the scope, allowing for the perception and accuracy of predictions in AI-powered access and identity management.

5. RESULTS AND DISCUSSION

Table 1. Participants' demographics

	N	%
Experience level of Participants		
1-5 years	81	14.09%
6-10 years	311	53%
11-15 years	127	21%
Over 15 years	59	9%
Age Distribution of Participants		
Under 25 years	41	6%
25-34 years	97	18%
35-44 years	261	44%
45-54 years	111	18%
Over 55 years	67	10%
Gender Distribution of Participants		
Female	161	27%
Male	395	67%
Non-Binary/Third Gender	17	2%
Prefer Not to Say	5	0.99%

An overview 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 (53%) have between six and ten years of experience. This suggests that there is a sizable workforce that is probably up-to-date on the latest developments and challenges in AI and IAM and may even be combining traditional and cutting-edge approaches.

Those who have 11-15 years of experience (21%) bring dimension to the conversation because they have most likely witnessed the development of IAM systems and the early integration of AI. 14.09 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 time.

The age distribution shows that the 35–44-year-old group makes up a disproportionately large percentage (44%), suggesting that this is an experienced and mature cohort that is likely to hold key positions or have access to important decision-making opportunities. Along with the pool of seasoned professionals, the second biggest group consists of individuals aged 45 to 54 (18%). Both the views of those over the age of 55 (10%) and those between the ages of 25 and 34 (18%) originate from earlier and later stages of their respective professional lives. People younger than 25 years old make up 6% of the total population. The gender breakdown shows that men make up the bulk of the participants (67%), which is in line with general tendencies in the cybersecurity and technology industries.

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 nonbinary or third gender (three percent) or prefer not to say (one percent).

Table 2: Responses to Hypothesis 1: Due to variations in computer hardware and software configurations, the accuracy of AI-powered biometric authentication systems varies substantially across various cloud platforms.

Regarding Hypothesis 1, Despite the variable levels of precision that may be attained by biometric systems powered by artificial intelligence, most participants stated that their accuracy improved over time. As a result, it is clear that changes to the system's hardware and software parameters significantly impact its performance.

There is also a significant issue regarding security as a result of varied levels of accuracy, which highlights the essential requirement for high accuracy to guarantee robust security in identity and access management systems. When it comes to Hypothesis 2, which is all about how reliable these systems are in different kinds of computing, the results show that most people agree that AI systems are quite reliable when used in mainframes. Reliability is believed to be affected by variations in computational environments, while security concerns are believed to be caused by technology variances.

It is a widely held view that the quality of AI systems in identity and access management could be improved by standardizing surroundings. Age is considered a crucial component that influences user acceptance, and technical experience is also seen as having an impact on trust in these systems. This is about 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 is 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 centered 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.

Table 2. Participants' responses to questions on Hypothesis variables

	SA	A	N	D	SD
H1 Parameters					
Observed Variations in accuracy	111	195	141	81	49
Effect of Hardware Configuration	97	211	131	77	61
Impact of Software Updates or Changes	91	203	155	77	52
Major concern for security due to accuracy levels	83	187	167	92	48
H2 Parameters					
Rate the reliability in primary computational environment	103	197	146	84	47
Computational environment variations affect reliability	94	187	161	80	55
Technological disparities lead to security concerns	95	181	163	92	46
Standard environment improves reliability	89	175	177	72	64
H3 Parameters					
Age significantly influences acceptance	89	179	171	78	60
Technical experience affects trust	105	173	163	81	55
Gender plays a role in acceptance	71	168	193	92	53
Privacy concerns influence acceptance	93	185	151	86	62
H4 Parameters					
User feedback improves system design	114	197	151	83	38
Advancements in AI technology lead to better performance	113	177	153	80	64
Integration of continuous learning algorithms is crucial	95	181	173	86	42
Transparency in system increases trust and acceptance	99	175	165	85	53

Table 3. Participants' responses to questions on Hypothesis variables

Independent Variable	Coefficient (B)	Std. Error	t-Value	p-Value
Hardware configurations	0.24	0.9	2.49	0.012
Software Updates or Changes	-0.14	0.07	-1.87	0.060
Major concern for security due to accuracy levels	0.29	0.10	2.72	0.006

Table 3: Inferential Statistics for Hypothesis 1: Due to variations in computer hardware and software configurations, the accuracy of AI-powered biometric authentication systems varies substantially across various cloud platforms.

The results of the multiple regression analysis for Hypothesis 1 show how different parameters affect the accuracy of cloud-based biometric authentication systems powered by AI. Regarding hardware configurations, a coefficient of 0.24 and a standard error of 0.9 suggest that the accuracy of cloud-hosted AI biometric systems is positively correlated with the degree of complexity of hardware configurations. The t-value of 2.49 and the p-value of 0.012 support the idea that this correlation is statistically significant. These values indicate that enhancements to the hardware configurations of these systems are likely to increase the accuracy of these systems.

CONCLUSION

This research on artificial intelligence in identity and access management has several consequences, not just for theory but also for practice. The effects of hardware configurations and technology standardization on system accuracy and reliability highlight, first, the need for cloud service providers to invest in state-of-the-art hardware and strive for technological consistency. It is possible that this method could reduce the amount of variation in performance that exists between the various cloud platforms. Furthermore, the idea that system engineers should adopt a more user-centric approach, taking into consideration a wide range of user requirements and privacy concerns, is suggested by the fact that user acceptance is influenced by user demographics and privacy concerns.

REFERENCES

[1] C. Gunter, D. Liebovitz and B. Malin, "Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems", IEEE Security & Privacy Magazine, vol. 9, no. 5, pp. 48-55, 2011.

[2] M. Bezzi, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen and K. Zhang, Privacy and Identity Management for Life. Berlin: Springer, 2010.

[3] K. Bryson, M. Luck, M. Joy and D. Jones, "Agent interaction for bioinformatics data management", Applied Artificial Intelligence, vol. 15, no. 10, pp. 917-947, 2001. Available: 10.1080/088395101753242688.

[4] D. Cole, "Artificial intelligence and personal identity", Synthese, vol. 88, no. 3, pp. 399-417, 1991. Available: 10.1007/bf00413555.

[5] N. Sgouros, "Interaction between physical and design knowledge in design from physical principles", Engineering Applications of Artificial Intelligence, vol. 11, no. 4, pp. 449-459, 1998. Available: 10.1016/s0952-1976(98)00037-2.

[6] Divyabharathi DN, Cholli NG. A review on identity and access management server (keycloak). Int J Secur Priv Pervasive Comput (IJSPPC). 2020;12(3):46–53.

[7] Mohammed IA. The interaction between artificial intelligence and identity and access management: an empirical study. Int J creat Res Thoughts (IJCRT), ISSN. 2021;2320(2882):668–71.

[8] Cameron A, Williamson G. Introduction to IAM Architecture (v2). IDPro Body of Knowledge. 2020;1(6). doi: 10.55621/idpro.38.

[9] Carnley PR, Kettani H. Identity and access management for the internet of things. Int J Future Comput Commun. 2019;8(4):129–33.

[10] Saranya N, Sakthivadivel M, Karthikeyan G, Rajkumar R. Securing the cloud: an empirical study on best practices for ensuring data privacy and protection. Int J Eng Manag Res. 2023;13(2):46–9.

Citation: Kaushik Reddy Muppa, Analysis on the Role of Artificial Intelligence and Identity and Access Management (IAM) In Cyber Security, International Journal of Artificial Intelligence Research and Development (IJAIRD), 2(1), 2024, pp. 113-122

Abstract Link: https://iaeme.com/Home/article_id/IJAIRD_02_01_011

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJAIRD/VOLUME_2_ISSUE_1/IJAIRD_02_01_011.pdf

Copyright: © 2024 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

This work is licensed under a **Creative Commons Attribution 4.0 International License (CC BY 4.0)**.

✉ **editor@iaeme.com**