Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 8s (2025)

Enhanced Privileged Access Management with Identity Access Management to Improve the User's Safety Measures in Online Circumstances

K. R. Sumathi[1], Dr. A. Aruljothi[2]

[1]Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Coimbatore, Tamil Nadu, India
sumathi228@gmail.com

[2]Associate Professor, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Coimbatore, Tamil Nadu, India
tamil.aruljothi@gmail.com

Article History:

Received: *28-10-2024*

Revised: *26-11-2024*

Accepted: *20-12-2024*

Abstract:

Network safety measures are any actions done to protect the information integrity and usability of the user/customer network. Hardware and software technology issues are mutually exclusive. It chases many threats. It prevents intrusions from entering the user network or from spreading. Businesses that network computers and systems may experience issues with one user that impacts the network as a whole. Although networking has many advantages, it also raises the threat of safety measures troubles like information loss, safety measures flaws, unauthorized intrusions similar to hackers, viruses. The risk of unauthorized access or network damage can be reduced by the user taking preventative measures. Since it might not be feasible or economical to completely eliminate all risks, the importance of conducting an IT risk assessment cannot be emphasized when choosing what steps to take. Privileged Access Management techniques and tools are utilized to implement control over prominent admittance and acquiescence for customers, user-accounts, progressions, and methods in Information Technology surroundings. Through reducing their attack surface, privileged access management helps companies lessen the damage that external attacks and internal carelessness or misconduct can cause to their operations. The possibility of implementing Privileged Access Management and the effects ofPAM in the current situation are similar to an overview of user-related risks. In addition to comparing it with the current approaches, this paper suggested an improved PAM with IAM adoption.

Keywords: Privileged Access Management, Network Security, Identity Access Management, Risk Assessment, and Cyber Threats.

1. Introduction

The cyber security tactics and tools for managing prominent admittance and acquiescence for identities, users, defined-accounts, progression, and systems throughout Information Technology surroundings make up privileged admittance administration. PAM assists organizations in reducing their assault shell and avert or lessening the destruction caused by insider issues and outside assault by suitably sizing restricted admittance organizes. Although concession organization involves a multiplicity of tactics, restraining admission rights and authorization for users, defined-accounts, appliances, systems, devices-including IoT, and computing progression to the bare least amount

requisite to carry out regular, approved tasks is known as enforcement of least privilege. Privileged access management is regarded by forecasters and technologists as one of the nearly all critical safety measures regulations for lowering virtual threat, addressing conformity initiatives, and being qualified for cyber assurance. It is also known as PAM, PIM or simply opportunity administration. The larger field of identity and admission management includes dispensation administration.

Fine-grained organize, visibility, and auditability over every qualifications, privileges, and admission are provided by PAM and IAM operational collectively. PAM adds further grainy visibility, organize, and auditing above advantaged identities and session-related activities, while IAM controls provide identity authentication to assurance the right client has the right admittance at the accurate time. In a gradually more perimeter-less, work-from-wherever world, PAM is at the hub of individuality safety measures, which is essential to safeguarding endeavor assets and clients as well as addressing Paths to Privilege-TM. Strong PAM controls are necessary to safeguard the identity infrastructure, which includes the IAM and IGA toolkits, from the growing threats.

In the situation of IT, dispensation is the power that a scrupulous account or progression possesses contained by a network or computer-system. The ability to override or get around some security restrictions is known as privilege. It can include the ability to do things like shutting along systems, loading mechanism drivers, configuring networks or systems, provisioning and configuring user-accounts and cloud occurrences, and more. By giving users, apps, and other method processes the prominent rights to admission specific possessions and carry out work-related tasks, privileges serve an essential operational function. At the identical occasion, organizations countenance a momentous safety measures threat due to the opportunity of dispensation being harmed or distorted by insiders or peripheral attackers. OS, file systems, applications, DB, hypervisors, cloud administration platforms, and supplementary systems are all pre-configured with privileges for dissimilar client accounts and procedures. Convinced kinds of advantaged clients, like a system or complex administrator, can also endowment rights.

Any account that grants access and permissions beyond those of non-privileged accounts is regarded as privileged. Any user, who currently uses privileged access, like through a privileged account, is considered a privileged user. Compared to non-privileged accounts and users, privileged users and accounts present significantly greater risks due to their increased access and capabilities. Super user accounts, a type of privileged account, are mainly used for administration by specialized IT staff members and offer nearly limitless authority to carry out commands and modify the system. Super user accounts are commonly referred to as "Administrator" in Windows systems and "Root" in Unix/Linux systems. With the ability to create or install files or software, modify files and settings, and remove users and data, super user account privileges can grant unrestricted access to files, directories, and resources along with full read, write, and execute capabilities. Permissions for other users can even be granted and revoked by super users. Super user accounts can easily cause catastrophic damage to a system, or even the entire enterprise, if they are misused, either maliciously or inadvertently (for example, by accidentally deleting a crucial file or typing a powerful command incorrectly).

Controlling privilege risk is difficult for organizations with nascent and mostly manual PAM procedures. To increase security and compliance, automated, enterprise-class PAM security

solutions can scale across millions of privileged accounts, users, and assets. The most effective solutions can streamline processes to significantly lower administrative complexity while automating the identification, management, and monitoring of identity-related paths to privilege. An organization will be more successful in minimizing the attack surface, minimizing the impact of attacks (by hackers, malware, and insiders), improving operational performance, and lowering the possibility of user error if its privilege management implementation is more automated and sophisticated.

Examples of privileged accounts typically in an organization:

- **Local administrative accounts:** Non-personal accounts provided that organizational admittance to the confined congregation or occurrence only.
- **Domain administrative accounts:** Advantaged organizational admittance across all workstations and servers contained by the sphere.
- **Break glass (also called emergency or firecall) accounts:** Unprivileged clients with managerial admittance to protected systems in the container of a disaster.
- **Service account:** advantaged confined or field accounts that are utilized by an appliance or examine to interrelate with the OS.
- **Active Directory or domain service accounts:** Facilitate password transform to accounts, etc.
- **Application accounts:** Utilized by applications to admittance DB, run consignment jobs or scripts, or grant admittance to supplementary appliances.

This research study's first section provides a brief overview of Identity Access Management and Privileged Access Management. Numerous ongoing research projects that have been tested in the areas of identity access management and privileged access management are described in the second section. In section three, the improved model utilizing Identity Access Management and Privileged Access Management was covered. In section four, the improved model was illustrated and contrasted with current approaches. The potential and expectations of privileged access management, identity access management, and the associated future research scope are covered in section five, also known as the conclusion section.

2. Review of Related Literature

Siddhesh et al: Monitoring and managing access to vital internal systems, networks, and data is the main goal of Privileged Access Management (PAM), a crucial security tactic. This study offers a thorough introduction to Privileged Access Management, analyzes its applicability to contemporary cyber security, and enumerates the essential ideas and elements required to create a successful PAM program. The study also offers deployment best practices and talks about the advantages and disadvantages of PAM. The study provides insights into the current state of PAM and anticipated changes by carefully examining the corpus of previous research, industry reports, and case studies.

Target Corporation is the subject of the first case study. In 2013, Target Corporation experienced a significant security breach that resulted in the theft of millions of customer credit card

numbers. The incident happened when hackers used credentials they obtained from a third- party supplier to access Target's network. The significance of privileged access control in preventing unwanted access to vital systems and data was highlighted by this incident. After the incident, Target Corporation strengthened their security posture by implementing a powerful Privileged Access Management system. Implemented were stringent access controls, reliable authentication procedures, session auditing, and privileged account monitoring. Target was able to control and keep an eye on privileged access with the aid of the PAM system, which decreased the likelihood of additional mishaps. The significance of PAM in thwarting external attacks and safeguarding confidential client data is illustrated by the Target Corporation example.

The second Sony Pictures Entertainment case study A well-known cyberattack on Sony Pictures Entertainment in 2014 resulted in the theft and leakage of private information, including staff emails and sensitive company documents. Because they used stolen privileged credentials to gain access to the company's network, a group of hackers were held accountable for the incident. Sony Pictures Entertainment strengthened their security procedures following the attack by implementing Privileged Access Management. PAM systems were used to enable multi-factor authentication, manage and keep an eye on privileged accounts, and apply the least privilege principle. Sony Pictures Entertainment was able to limit access to critical systems and lessen the possibility of insider threats thanks to these safety precautions. The Sony Pictures Entertainment case highlights how crucial PAM is for defending against both internal and external threats. Organizations can improve their security posture and lower their risk of data breaches and unauthorized access by putting PAM into place [09].

Xiao et al: Conventional clustering examination considers only the remoteness feature. Traditional clustering algorithms typically cannot produce practical results when the groupings circumstances include factors supplementary than detachment. This study suggests a time-constrained clustering algorithm for diminutive extent datasets called TCPAM and be relevant it to a mobile policy relevance. It is foundation on the PAM grouping procedure and has a specific relevance environment. In order to group the information objects according to the "principle of proximity" and "time constraints" of the double limitations, the algorithm adds restrictions to the clustering process that combine the distance and time factors. The authors' proposed algorithm can accomplish a high-quality grouping presentation, according to the experimental results. Every group has a delegate entity preferred by the authors, and the outstanding things are sorted by detachment and positioned in the contiguous group. To enhance the performance of the results, the authors then frequently swap out the central point for non-center points. A cost function that takes into account how different the representative object is from other objects is used to estimate the quality of the clustering result. This discrepancy is the result of the time and distance factors added together. Every iteration analyzes every pair of objects, with one object serving as the central point and the other as the non-center point. We estimate the quality of clustering results for every possible pair. To reduce the overall cost, one central object can be swapped out for a non-center one. The new focal points for the following iteration are the best representations of the objects created in the previous one [10].

Samuel et al: The incorporation and efficacy of AI in cloud environments' Individuality and Admittance Administration are examined in this extensive study. It mainly addresses the

opportunities and challenges in cloud computing by concentrating on how AI can improve client validation, endorsement, and admittance manage. Both quantitative and qualitative analyses are used in this mixed-methods study. While multiple regression analysis looks at how different factors affect system effectiveness, a survey of 582 cyber security experts offers imminent into the probable and contemporary situation of Artificial Intelligence in Identity Access Management. Four hypotheses are investigated: how software and hardware arrangements affect system accurateness, how computational surroundings influence dependability, how demographic aspects affect client recognition, and how technical advancements affect scheme concert and recognition.

The results show a strong relationship between these variables and AI's performance in IAM. Particularly, organism accurateness is prejudiced by hardware arrangements and safety measures concerns; scheme dependability is prejudiced by variations in the computational surroundings; client recognition is prejudiced by demographic factors; and concert and recognition are enhanced by enhancement like client feedback, AI expertise advancements, unremitting erudition algorithms, and scheme intelligibility. For efficient IAM in cloud environments, these insights highlight the necessity of cutting-edge hardware, standardized software, client-centric intend, and ongoing advancements in Artificial Intelligence technologies. The study offers practical suggestions for cloud service contributors and developers, stressing the value of implementing adaptive algorithms, guaranteeing transparency, and incorporating users in development processes. Future research avenues include examining demographic-specific reactions to AI-integrated IAM resolutions and conducting longitudinal studies on the effects of technological advancements [11].

Ievgeniia et al: One area that presents many difficulties is Identity Access Management (IAM), especially when it comes to distributed or cloud-based systems and remote connectivity. Even though proceeding investigate has projected an extensive variety of technological solutions, their recognition is relentlessly hindered by the steps concerned in their incorporation and accomplishment in the viable segment. From the standpoint of the beneficiaries, the study attempts to describe the present perception and security concerns related to IAM solutions. Forty-five cyber security experts from various organizations around the world were interviewed for the analysis. The difficulties and weaknesses of on-premises and cloud-based IAM deployment models serve as the study's specific focal point.

The interviewees pointed out that there are differences in the problems that affect on-premises and cloud IAM resolutions. Evasion configurations, deprived administration of non- human identities like user-service accounts, pitiable credential administration, poor admittance evaluation, deprived API arrangement, and imperfect log scrutiny were the primary issues facing cloud-based IAM solutions. The difficulties with on-premise solutions, on the other hand, included Multi-Factor Authentication, unsafe default configurations, inadequate skill sets needed to supervise IAM solutions steadily, inadequate password procedure, un-patched vulnerabilities, and Single-Sign negotiation that compromised multiple entities. The study also found that 41% of respondents think on-premise resolutions are added protected than cloud-related ones, despite the cloud-related IAM resolutions ' growing functionality. According to respondents, because of intricacy of the fundamental resolutions, difficulties in organization permissions, adherence to active IAM policy related things; cloud IAM might potentially interpretation organizations to a greater assortment of

vulnerabilities [12].

3. Methodology

PAM is a set of procedures, guidelines, and tools that help businesses control their online personas. The management and security of administrators and users with higher rights is the specific focus of PAM systems. IAM enables enterprises to authenticate and authorize all of their users across their whole attack surface and technologies such as Active Directory, including internal staff, external clients, partners, and vendors. In order to conceal certain unique requirements in the specific environmental usages, the suggested model integrated the PAM and IAM. Figure 01 shows how PAM and IAM are combined.

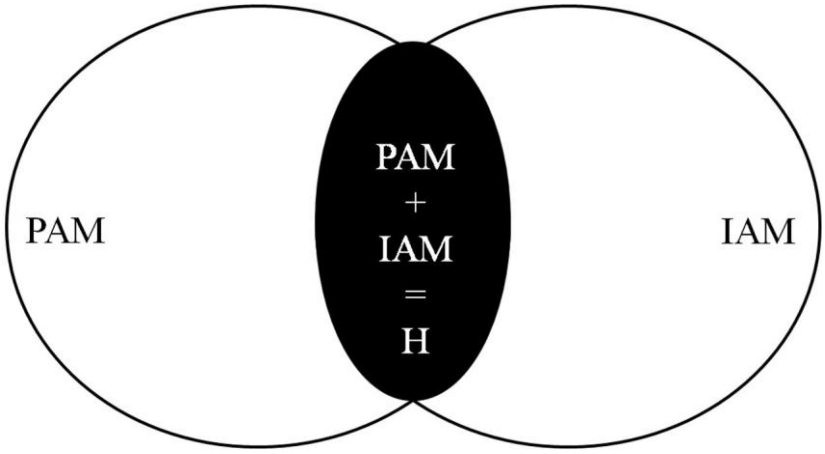

Figure.01 Combined PAM and IAM Model.

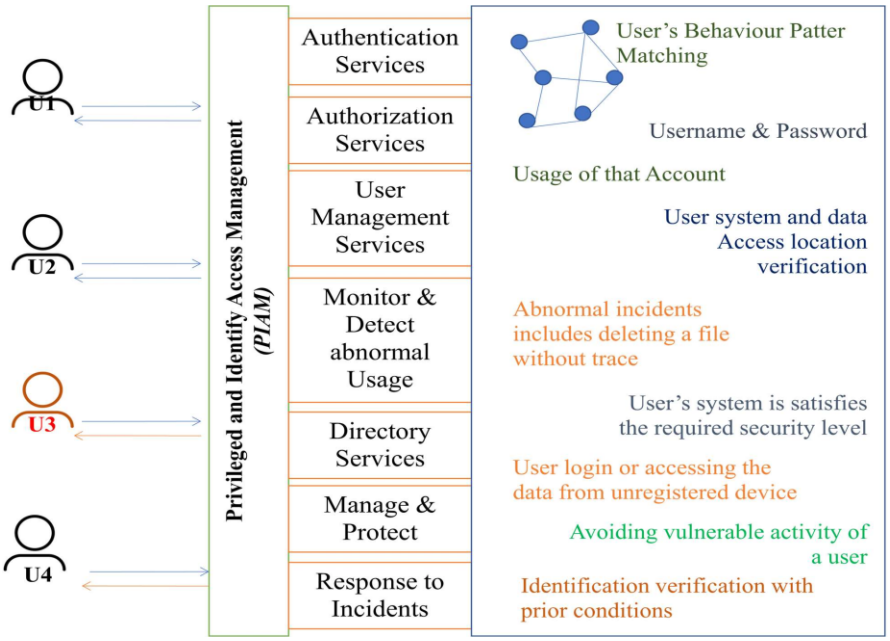

Figure.02 Proposed Methodology

To ascertain whether a user is being fabricated, the pattern of their behavior is compared. One popular technique for account login and workplace authentication is the verification of the username and password. The way the account is used can reveal information about the user. In the event that a

user's login location deviates from the norm, it will be considered. To determine a user's authenticity, their system and data access location are verified. An example of an abnormal occurrence is the removal of a file without leaving any trace, which is prohibited by certain criteria. Once their system meets the necessary security requirements, the user is permitted to perform their essential tasks. Additionally taken into account are user logins and data access from unregistered devices. preventing undesired activity by avoiding a user's vulnerable behavior and using preconditions for identification verification. Figure 02 displays the combined PAM and IAM model.

The user's behavior pattern is compared to determine whether or not the user is being fabricated. Verification of username and password is a common method of account login and workplace authentication. Information about the user can be gleaned from how the account is used. A user's login location will be taken into account if it differs from typical login locations. Verification of the user's system and data access location is used to assess the authenticity of a user. The removal of a file without leaving any outline, which is outlawed by several criterion is an instance of an uncharacteristic occurrence. The user is allowed to carry out their essential tasks once their system satisfies the relevant security requirements. User logins and data access from unregistered devices are also considered. employing identification verification with preconditions to stop unwanted action and stopping a user's vulnerable behavior. The suggested approach is described in Figure 3.

- **Authentication Services:** An identity verification method for software systems, apps, or websites that works similarly to passwords is called an authentication service. It is intended to verify clients' (or users') identities to servers (a computer program) and vice versa.
- **Authorization Services:** Verification of the user's authorization to access a specific resource is done by the authorization service. After authentication, authorization services control user permissions, deciding what resources or actions are permitted. Such as Policy-Based Access Control, Role-Based Access Control, and Attribute-Based Access Control.
- **User Management Services:** An organization for administration client admittance to devices, system-software, and services is called client administration. It spotlights on tracking convention and calculating admittance and exploit authorizations. Roles, groups, and admission policies are all managed by user management services, which also handle user creation, updates, and deletion.
- **Directory Services:** A DB utilized to store and administer client and reserve information is called a directory service. Directory services store data like passwords, usernames, client predilections, apparatus data, and supplementary contents. They are also notorious as register, client stores, uniqueness stores, or indeed LDAP directories.
- **Response to Incidents:** An organization's response to a cyber attack or information contravene is known as occasion reaction, or IR. In regulate to lesser the probability of reoccurring incidents, an attempt is made to promptly distinguish an assault, lessen its consequences, contain harm, and tackle the root reason. Response to Incidents is the methodical process of handling and controlling system failures or cyber security breaches in order to reduce damage and quickly resume operations.
- **Monitor & Detect abnormal Usage:** unusual Examining particular data position and identifying

infrequent events that appear suspicious due to their deviation from the established pattern of behaviors is known as usage detection. It entails monitoring system activity to spot odd or unauthorized activity that might point to abuse or security risks.

- **Manage & Protect:** Control and safeguard user-related data and network data transmission from online attacks. Implementing tactics, instruments, and procedures to stop, identify, and address malevolent activity is part of the fight against cyber threats. These include risk management, safeguards, monitoring and recognition, incident response, and frequent updates.

4. Results and Discussions

Table.01 Comparison of Proposed method with Existing Methods

S. No.	Information security component	Mansour et. al	ISO/ IEC	Eloff et. al	Veiga et. al.	Tudor et. al	Proposed Model
1.	Governance	Y	X	X	X	X	Y
2.	Security strategy	Y	Y	X	Y	X	Y
3.	Leadership	Y	Y	Y	Y	Y	Y
4.	Security organization	Y	Y	Y	Y	Y	Y
5.	Policies, standards, and guidelines	Y	Y	Y	Y	Y	Y
6.	Measurement metrics & ROI	Y	X	Y	Y	X	Y
7.	Compliance and monitoring	Y	Y	Y	Y	Y	Y
8.	User management	Y	Y	X	Y	X	Y
9.	Training & awareness	Y	Y	X	Y	Y	Y
10.	Ethics	Y	Y	Y	X	X	Y
11.	Privacy	Y	Y	X	Y	X	Y
12.	Trust	Y	Y	X	X	Y	Y
13.	Certification	X	X	Y	X	X	X
14.	Best practice	Y	Y	Y	Y	Y	Y
15.	Asset management	Y	Y	Y	X	Y	Y
16.	Physical and environmental security	X	Y	Y	Y	Y	X
17.	Technical operations	Y	Y	Y	Y	Y	Y
18.	System acquisition, development and maintenance policy	Y	Y	Y	Y	X	Y
19.	Incident management plan	Y	Y	X	Y	X	Y
20.	Business Continuity plan	Y	Y	X	Y	Y	Y
21.	Disaster recovery plan	Y	X	X	Y	Y	Y
22.	Risk assessment process and Plan	Y	Y	Y	Y	Y	Y
Number of components with Y (Yes) %		86%	81%	64%	72%	59%	90%
Number of components with N (No) %		14%	19%	36%	28%	41%	10%

**Y = Yes, X = No*

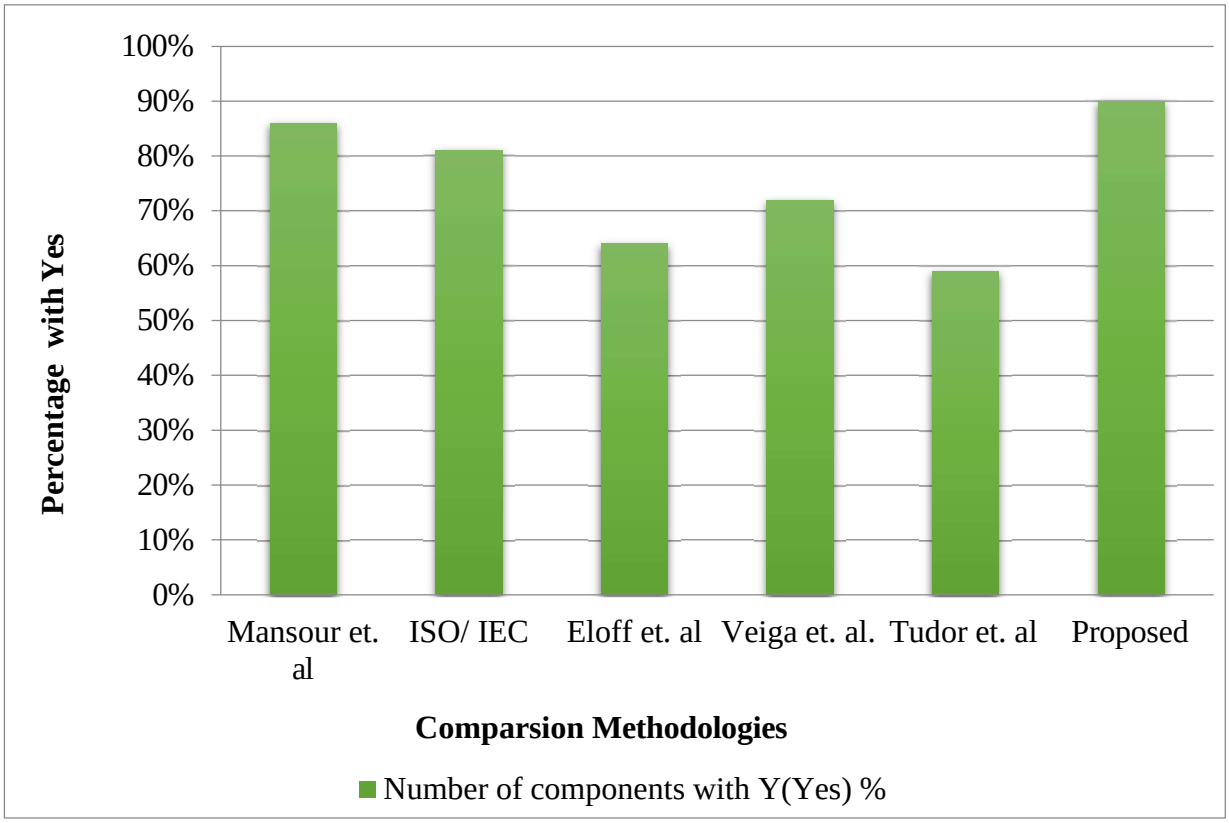

Figure.03.Comparison of different information security components with Positive percentage

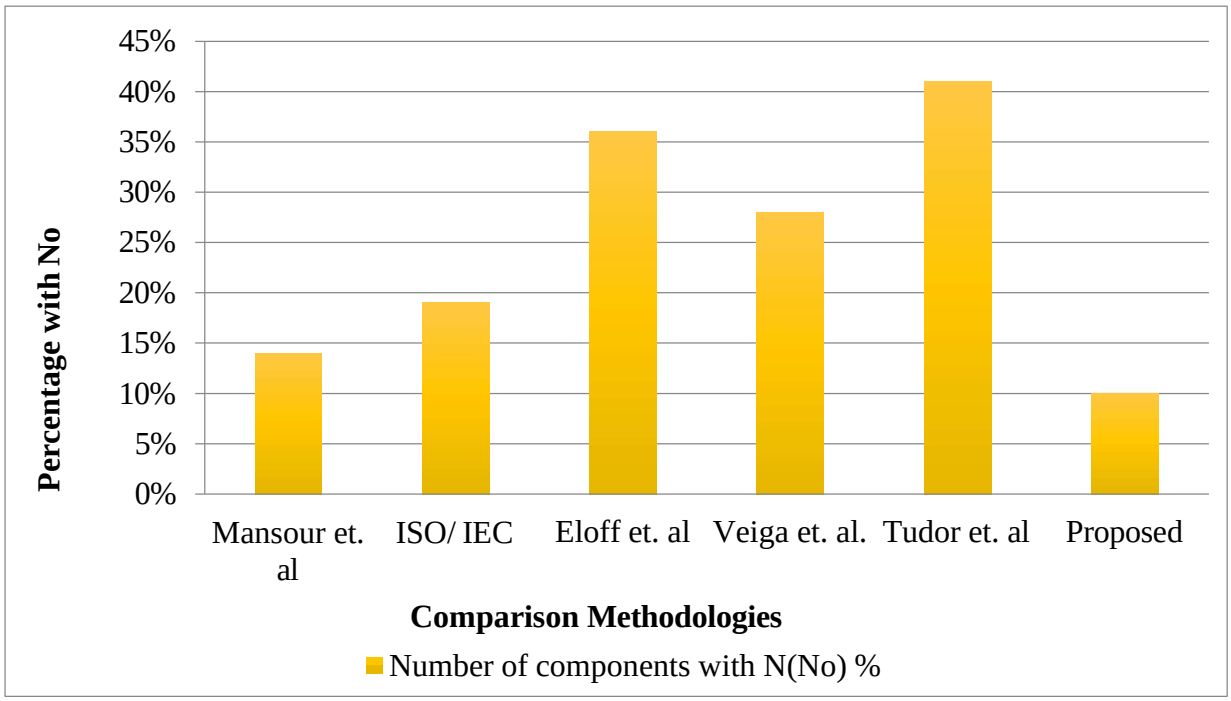

Figure.04.Comparison of different information security components with Negative percentage

The effectiveness of the projected concept in relation to the obtainable data safety measures mechanism is displayed in Table 01. Figures 03 and 04 showed the percentages that were positive and negative between the exiting methods.

5. Conclusion and Future Scope

This study compared and found all of the access management components that other researchers have previously recommended. The proposed system integrates privileged access management with Active Directory collaboration. It is simple to see that the framework techniques discussed in this research paper are more dependable and protected to afford effective admittance control for advantaged clients when compared to previous frameworks. Standards for security and validity are examined for the approach described here. Global technological advancement has led to an emphasis on well-organized, business- and government-oriented intelligent control measures within the organization. Although protecting sensitive government or commercial information from hostile or unauthorized attacks is typically challenging for top organizations, the suggested approach by one of the current approaches may be an essential tool. This study only intends to develop a more digitalized cyber security system that preserve be utilized by mutually communal and classified enterprises in order to establish a confidence environment for whichever firm. Privileged Access Management will lead the industrial sector in the future in a more secure manner. It also shields its users and customers from unethical virtual threats.

References

[1] A. Sharma, S. Sharma and M. Dave, "Identity and access management- a comprehensive study," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 1481-1485.

[2] Vivek Ramakrishnan, Pete Dnyandeo Jageshwar, “Identity and Access Management: Concept, Challenges, Solutions A Small Snapshot Review”, International Journal for Research in Applied Science & Engineering Technology, Vol.12, No.02, Feb 2024, pp.579 – 584.

[3] Shabana Mulla, “A literature review on the tools for Identity Access Management using AI”, Journal of Emerging Technologies and Innovative Research, Vol.09, No.10, Oct 2022, pp.33-37.

[4] Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer and Josef Küng, “A systematic literature review for authorization and access control: definitions, strategies and models”, International Journal of Web Information Systems, Vol. 18 No. 2/3, 2022, pp. 156- 180.

[5] Deepak H. Sharma, C.A. Dhote, Manish M. Potey, “Identity and Access Management as Security-as-a-Service from Clouds”, Procedia Computer Science, Vol.79, 2016, pp. 170-174.

[6] Mayuri Dhamdhere, Sridevi Karande, “Identity and Access Management: Concept, Challenges, Solutions”, International Journal of Latest Trends in Engineering and Technology Vol.08, No.01, pp.300-308.

[7] Kaushik Reddy Muppa, “Study 0n Cloud-Based Identity and Access Management in Cyber Security”, International Journal of Data Analytics Research and Development, Vol. 02, No.01, Jan-Jun 2024, pp. 40–49.

[8] Ishaq Azhar Mohammed, “Systematic Review of Identity Access Management in Information Security”, International Journal of Innovations in Engineering Research and Technology, Vol. 04, No. 07, Jul-2017, pp. 01-07.

[9] Siddhesh Bhargude, “Privileged Access Management: Ensuring Security and Accountability”, International Journal of Advanced Research in Science, Communication and Technology, Vol.03, No.01, July 2023, pp. 647-651.

[10] Xiao Dong, Zhongnan Zhang, “Research and Implementation of PAM Algorithm with Time Constraints”, 2014 International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS), 2014, pp. 108 – 111.

[11] Samuel Oladiipo Olabanji, Oluwaseun Oladeji Olaniyi, Chinasa Susan Adigwe , Olalekan Jamiu Okunleye and

Tunbosun Oyewale Oladoyinbo**, "**AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems**",** Asian Journal of Research in Computer Science Vol.17, No.03, 2024, Page 38-56.

[12] Ievgeniia Kuzminykh, Bogdan Ghita, Abhishek Singh, "Ind ustry Perception of Security Challenges with Identity Access Management Solutions", IEEE International Black Sea Conference on Communications and Networking, Tbilisi, Georgia, 24th – 27th June 2024.

[13] Varuna, W. Rose, M. Harshini, and K. T. Baby. "An intelligent forecasting system for unauthorized URL identification using deep learning." *International Journal of Health Sciences* I: 7832-7842.

[14] Prakash, G., P. Logapriya, and A. Sowmiya. "Smart Parking System Using Arduino and Sensors." *NATURALISTA CAMPANO* 28.1 (2024): 2903-2911.

[15] K T, S., P, S. S., Kumar E, B., L R, S., J, V., & R., N. (2024). Experimental Assessment between Dissimilar Techniques and Methodologies to Sports Knee Injury using Magnetic Resonance Imaging. *South Eastern European Journal of Public Health*, 1635–1644. https://doi.org/10.70135/seejph.vi.2167

[16] Ashfauk Ahamed, A. K., et al. "Prediction Of The Growing Stock In Stock Market On Analysis Of The Opinions Using Sentiment Lexicon Extraction And Deep Learning Architectures." *Frontiers in Health Informatics* 13.3 (2024): 1382-1392.

[17] Saranya, S. Sakthi, and W. Rose Varuna. "SOIL CLASSIFICATION USING MACHINE LEARNING FOR CROP SUGGESTION." *Machine Intelligence Research* 18.1 (2024): 299- 318.

[18] Abinaya, S., and W. Rose Varuna. "Autism Spectrum Disorder Prediction by Bio-inspired Algorithm with Blockchain based Database." *International Research Journal on Advanced Science Hub* 5.05 (2023): 413-417.