The Critical Role of Identity and Access Management in Cybersecurity

SHARAD SHARMA

(CISSP, Sr. Member IEEE, Alumni IIT Kanpur)

Abstract:

The research investigates Identity and Access Management (IAM) which has served and will continue to serve as the essential foundational base for both legacy and contemporary cybersecurity systems. The research shows that previous security models have lost their effectiveness because modern networks operate without fixed secure boundaries, high adoption of cloud applications utilizing including Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) models and organizations now use hybrid work models utilizing both on-prem applications and utilizing Cloud platforms and cloud applications) while dealing with sophisticated cyber threats and zero day vulnerabilities. The research investigates how IAM developed from its basic Information Technology (IT) management duties into an advanced security system which defends different types of Identities including but not limited to Digital, Silicon (Machine and non-human) and Privileged protection. The main subjects of this paper focus on Zero Trust fundamentals and Privileged Access Management (PAM) operations and cloud identity management difficulties and security versus user experience tradeoffs. The research shows that IAM functions will continue to play a critical business requirement which protects organizations from risks while following regulations and adhering to compliance and supporting their digital transformation journey. The research explores future development paths which unite artificial intelligence systems with decentralized identity management systems.

Keywords: Identity and Access Management (IAM), Cybersecurity, Zero Trust Security, Privileged Access Management (PAM), Multi-Factor Authentication (MFA), Access Control, Digital Identity, Cyber Threats, Authentication, Authorization, Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS), Security Framework, Segregation of duties (SOD), Bring your own Device (BYOD), Identification, Authentication, Authorization, and Accountability (IAAA).

1. Introduction: The Evolving Cybersecurity Landscape

Decades ago, cybersecurity relied heavily on shielding a well-delineated network boundary - think of it as a digital stronghold guarded by firewalls, intrusion detectors, and Virtual Private Networks (VPNs) (Kang et al., 2023). Inside that zone, people and systems were assumed safe; danger came only from outside. The options to access infrastructure and applications were limited yet secure with limited exposure outside the secure organization firewall. Yet today's digital landscape has shattered those assumptions. Cloud tools now dominate IT environments, smartphones and tablets spread data thin, and workers log in from countless locations far from

central hubs. With Bring your own device (BYOD), the boundaries of accessing the applications and data continue to change who can access what and how they can access it. With Artificial Intelligence fast gaining acceptance, this boundary will continue to fade as the barrier between digital and silicone identities continue to erode. These changes have worn down the old defenses until they no longer hold. Zero-day vulnerabilities will continue to grow. Out here, the old barriers around companies simply don't hold like they used to - people, programs, files spread wide across different places now (Ghadge, 2024; Umoga et al., 2024).

Nowhere is change more evident than in how threats unfold today. With system defenses once central, attackers now aim at who gains entry - people and machines alike. Instead of breaching wires, they test weak spots in logins, often through fake emails or reused passwords. Insider risks play a growing role, allowing intruders through trusted gates. As a result, verifying identity has shifted from an afterthought to the main challenge (Alsirhani et al., 2022). Evidence shows up clearly in big data leaks, where hacked login - especially those with high access rights - open doors to steal more info and take over systems. At that point, proving an outside party truly is who they say they are becomes the main shield, not just one part of many. Nowhere is this change clearer than in how Identity and Access Management operates. Once confined to technical backend tasks, it now plays a central role in cyber defense (Daah et al., 2024; Kang et al., 2023). Think of it as giving controlled access - to who, what, when, and where - in real-time situations. Its scope covers rules, tools, and workflows tied to managing user identities from creation through deletion. Authentication, permission decisions, and tracking events fall under its influence too. When the outer shield of the network fades, what remains shifts around each person and their machine. With Artificial intelligence advancement, creating, discovering and managing agentic identities will further strengthen the importance of IAM. Decisions about safety now depend on who you are, where you are, how your gadget runs, plus what actions you've shown lately - not just whether a port is open (Ghadge, 2024).

The research establishes that an advanced IAM framework stands as the essential element which will establish an organization's cybersecurity defense system. The system presents IAM as the main operational framework which controls present-day digital systems and cloud ecosystems instead of functioning as an additional support system. IAM protects organizational assets through its ability to control and protect all types of identities while enforcing the principle of least privilege in a world without digital boundaries. The research investigates IAM architectural foundations and deployment methods and security vulnerabilities which prove its essential position in modern cybersecurity systems.

2. The Pillars of IAM: Core Concepts and Components

Identity and Access Management exists as a defined security discipline which combines multiple security principles with connected system elements. The core concept is to enforce the principle of least privileges and identify who has access to what, how and when. The Identification, Authentication, Authorization, and Accountability also referred to as IAAA model serves as its

core structure to explain how digital identities get established and managed through its identification and authentication and authorization and accountability process (Glöckler et al., 2023; Singh et al., 2023).The process of Identification requires users to state their identity through username or email entry, but Authentication requires users to prove their identity by providing their credentials which include passwords and tokens and biometric data. The system provides users with access to particular resources and privileges after they complete identity verification through the least privilege principle which gives users only needed permissions for their work (Sandhu & Samarati, 1994). The system maintains Accountability through its detailed audit logs which monitor all user activities by tracking individual user identities to stop unauthorized access and enable forensic investigations.

Modern IAM frameworks operationalize the IAAA model through several key technological and procedural components. User Lifecycle Management (ULM) enables automated user account administration through its user provisioning system and access right modification tools and de-provisioning process which runs when users move between joiner-mover-leaver events thus reducing the number of inactive user accounts that grant unauthorized access. The access of the user is aligned with his lifecycle events which are typically managed using organizations human resource (HR). Single Sign-On (SSO) provides improved security and user-friendly experience through its capability to let users authenticate once for accessing various software systems which share a connection. The system protects users from password exhaustion and system vulnerabilities through its authentication process. It is also a great tool to provide end user a seamless experience and manage access via a single password. This greatly reduces the organizations operations reducing the large number of password management requests. The authentication pillar requires Multi-Factor Authentication (MFA) as its security measure which demands two or more verification factors from different categories (knowledge, possession, inherence also known as what you know, what you have and what you are) to stop credential-based attacks which need to safeguard all privileged access (Fugkeaw, 2023; Naik and Jenkins, 2016).The concept of Federated Identity enables organizations to share authentication services through standard protocols which include Security Assertion Markup Language (SAML) and OpenID Connect to let trusted identity providers (IdPs) handle authentication for service providers (SPs) who need secure cloud service integration and collaborative work. These processes have continued to strengthen the IAM processes limiting the attack surface area and also allowing organizations to focus more on business with lowered concerns for security breaches. With Information Technology (IT) landscape becoming more and more complex and introduction of Artificial Intelligence, these protocols will have to be strengthened to address the modern cybersecurity threats.

IAM is typically enforced using multiple access controls models. The common ones are Role based access controls (RBAC), Attribute based access controls (ABAC) or Policy based access controls (PBAC). These frameworks allow for enhanced compliance and support the operational model by introducing automation and reducing access by exceptions. IAM also manages access

governance which is enforced using user access reviews, allowing for both preventive and detective Segregation if Duties (SOD) and approval-based access requests with proper controls. IAM works as the entry point for accessing any resources and thus forms the foundational block for Cybersecurity

3. From Perimeter to People: The Zero Trust Security Model

The Zero Trust security model serves as the architectural solution to the dissolved network perimeter because it represents a complete reversal of the conventional "trust but verify" security method. The National Institute of Standards and Technology (NIST) defines Zero Trust through its core principle which demands organizations to authenticate all users because they should never grant trust to anyone. Access to information is based on the assumption that no one should be granted access unless authenticated and trusted. Even an end user might be attempting to secure access to system via a trusted VPN, he should still provide credentials to ensure he is what he claims to be. The context of who is accessing what and how is based on the principle of zero trust.

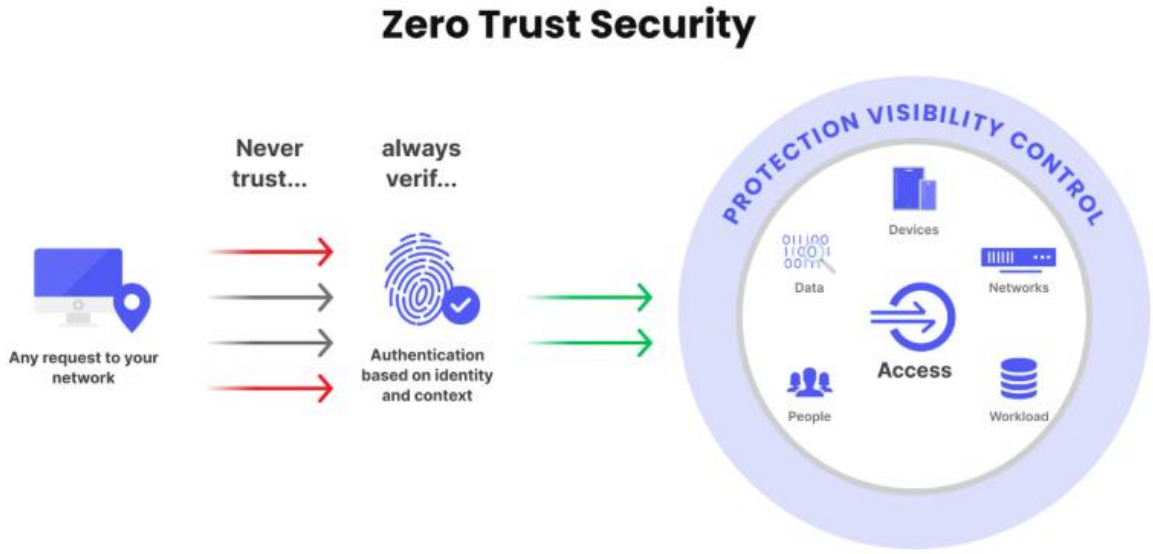

Figure 1. Core Principles and Domains of the Zero Trust Security Model (Bairyev, 2023).

The operational deployment of Zero Trust requires Identity and Access Management as its core enabling component to execute the principles which Figure 1 demonstrates. Every access request must undergo strong dynamic authentication and authorization according to Zero Trust architecture (ZTA) which IAM frameworks already perform as their core function. The three essential identity-based elements for implementation include user identity and device identity and adaptive access policies (Rivera et al., 2024). The first step of user identity verification requires password authentication elimination because users must use strong phishing-resistant multi-factor authentication (MFA) which delivers exact identity verification. The system needs to

verify both device identity and health status because an unauthorized user accessing a vulnerable or non-standard device creates an extreme security threat. The system depends on IAM systems which connect to endpoint detection and response (EDR) tools to check device status whether it is compliant and centrally managed or not before allowing system access. Based on the Identity profile , risk score and what is the intended transactions, the user is allowed or is challenged for additional authentication (Meng et al., 2022).

Multiple architecture has been identified to enforce Zero trust architecture. The concept to continuously challenge the identities to present their credentials is one of the most discussed architectures. The concept relies on continuously identifying the context of who is attempting to access what and policies are put in place to monitor the activities. Transactions that require elevated access are monitored with higher priorities and will ask the user to present their credentials if required. Defining the policies and what should and should not require additional authentications are incorporated in the architecture. All the policies are defined with the IAM framework that serves as the entry point for accessing any system or application.

4. Guarding the Crown Jewels: Privileged Access Management (PAM)

Digital identity security requires Identity and Access Management systems, but privileged account protection needs specialized security protocols which go beyond typical security measures. Privileged Access Management (PAM) functions as a vital high-security IAM component which handles the protection and tracking of authorized access to critical organizational systems and sensitive information (Singh et al., 2023).

Access within systems is segregated as privileges and non-privileged access. A user attempting to see his profile vs ad administrator attempting to update a user's banking information are example of non-privileged vs privileged access. Privileged access provides permissions and ability to perform activities within a system that is not available to all the users and is typically assigned to administrators and controllers. Users who do not have access to privilege access can be grated privileged access for a temporary period after proper approvals are granted. The table below shows the different types of privileges access associated with different types of accounts

Account Type	Example	Typical Privileges	Primary Risk
Human privileged accounts	Application administrators, operations team, Devops, Infrastructure administrators Admins,	Deploy and configure applications, manage the applications as part of operations team , apply	Utilizing approved access to perform malicious activities, identity theft leading to gain

		patch	unlawful access.
Service accounts	Accounts which are used to integrate two or more applications and also perform Create, read, update and delete (CRUD) operations within an application or infrastructure or APIs	Integrate two or more applications , , perform CRUD operations, develop reporting or custom scripts	Access to service accounts with provides access to hackers to take complete controls over the application.
Domain/System	Built-in OS/Platform Accounts (e.g., root, Administrator, SYSTEM)	Highest level of control over a domain, server, or workstation.	Primary target for attackers; compromise leads to total system control.
Emergency/Break-Glass	Designated Personnel for Crisis	High-level access, typically inactive until an emergency.	Weak controls on activation, poor auditing, potential for misuse.
Privileged Business User	Executives, Finance, HR Personnel	Access to sensitive business data (financial, PII, PHI, intellectual property).	Data exfiltration, privacy violations, targeted social engineering.

Table 1. Taxonomy of Privileged Accounts

The scientific evidence together with logical reasoning demonstrates that PAM functions as security control within IAM which protects organizations from major security incidents. The Verizon Data Breach Investigations Report shows that credential theft remains the main method which attackers use to access systems while they seek to obtain privileged user credentials. The obtained credentials enable attackers to circumvent all standard security measures which protect the system, so they gain full access to the system. A well-designed PAM system protects against this threat because it implements the least privilege principle which grants users and systems only required permissions at the lowest possible level for their assigned tasks during the shortest needed time period. The attack surface becomes smaller when PAM performs vaulting operations and rotation and tight credential management which disrupts the attack chain to prevent adversaries from performing lateral movement and privilege escalation (Alsirhani et al., 2022).

Effective PAM is implemented through a combination of technological controls and governance practices. The main practice of Just-In-Time (JIT) Access requires users to request elevated privileges which get approved through an approval process that enables access for specific tasks during scheduled time frames. The standing privilege now has a much smaller area which can be used for exploitation. The Session Monitoring and Management system enables users to monitor their active privileged sessions which they can both monitor and control. The system contains three security elements which track user activities for auditing purposes and forensic investigations and allow security staff to watch users actively and to halt any questionable behavior right away. The Secrets Management system operates as an automated solution which handles sensitive application credentials through password storage and rotation and API key and certificate provisioning to stop secret exposure when using hardcoded values. These practices combine to convert privileged access from its current state as a dangerous security flaw into an active security system which receives auditing and maintains complete control over the most critical IAM framework assets (Singh et al., 2023).

5. IAM in the Cloud and Hybrid Environment

With introduction of cloud platforms whether they are public or private cloud, the IAM framework has undergone and will continue to go through major changes, Zero trust architecture will be the foundational block for access management to any system or application. Security stops being optional when systems move to cloud or hybrid cloud. With shared responsibilities coming into focus with what cloud platforms provide vs what is shared and what is managed by organizations, IAM will be the core of security. Think of it like a split job description: users pick up certain duties, Cloud vendor handles others, under what experts call the cloud shared responsibility model. It falls to the Cloud service providers (CSP) to protect core infrastructure - things like data centers, hyperscalers, or virtualization platforms. The control of what is hosted in Cloud and applications is now a shared responsibility. IAM now carries heavy weight - shaping who accesses platforms like AWS IAM or Microsoft Azure Active Directory or Google Cloud IAM becomes key to locking down security and blocking leaks. When settings go wrong - when too many rights are granted or files sit exposed online - problems follow fast. These lapses show up again and again as major risks in cloud setups (Alsirhani et al., 2022; Naik and Jenkins, 2016).

The new system creates major difficulties when organizations need to handle user identities which exist between different system environments. Organizations need to handle their extensive identity environment which includes their existing on-premises directories (Microsoft Active Directory) and their public cloud services (AWS, Azure, GCP) and their numerous independent Software-as-a-Service (SaaS) applications. Users end up with multiple credentials and permissions spread across different systems because of this situation. Security policies receive uneven enforcement which results in poor user access management and restricted access rights monitoring and an increased risk of attacks. Solution is to centralize the Identity and access management and enable the Identity Federation. This is achieved with protocols like Service Providers or Relying Parties) is established through standardized protocols which include

Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) and OAuth 2.0.Idenitity Federation will allow all the authentication and authorization to be routed via central Identity provider. This will allow for central place to monitor the authentication of user, utilize single password for accessing multiple applications a systems spread across Cloud, on-prem and hybrid environment. From operations perspective, this will reduce the operations ticket for managing multiple passwords spread across different applications. Also, central Identity providers will become a single source for enforcing organizations security policies like minimum password age, password requirements and maximum password age. Central Identity provider will also allow the audit and compliance ask for the organization.

A cloud-based environment requires organizations to establish a strong IAM system which functions as an essential framework to protect their digital assets while following regulations and maintaining operational management of their dispersed systems (Chadwick et al., 2013; Naik and Jenkins, 2016).

6. The Human Element: Usability, Training, and Insider Threats

A complex Identity and Access Management framework becomes vulnerable to attacks when it does not consider the human elements which include users who need to use the system every day and authorized personnel who could exploit their authorized access. The design process of IAM systems requires developers to solve the core problem which exists between security requirements and user convenience needs. IAM controls which are both complicated and overbearing in their design create security risks because users will avoid them which leads to security weaknesses. Users experience MFA fatigue when they receive too many push notifications which causes them to approve fake authentication requests to stop the alerts or they disable MFA completely. The design principle shows that security systems which fail to provide user-friendly access will not receive regular use which would defeat their intended function. Organizations need to create strong security controls which operate continuously without disrupting user activities to achieve successful IAM implementation through transparent security. The concept of continuous monitoring and context-based authentication and authorization will ensure that user will only be prompted for presenting their credentials if they perform a transaction that requires additional scrutiny or performing privileged transactions.

The system design process receives its essential non-technical support from proactive security awareness training which enables IAM systems to function effectively. Social engineering attacks through phishing and spear-phishing represent the main attack method which attackers use to steal credentials because these methods exploit human behavior instead of system weaknesses. Organizations need to establish training programs which extend past basic annual compliance modules to provide ongoing interactive simulation exercises for human firewall development. Users who receive education about phishing attacks and credential value and suspicious activity reporting will actively join the security system. The cultural transformation enables users to become the initial security barrier which decreases the chances of credential

harvesting attacks that would target IAM systems (Ayoola et al., 2024; Carella et al., 2017; Moallem, 2019).

IAM functions as the main technical security system which protects organizations from insider threats that stem from either intentional or unintentional actions. IAM protects systems through its strongest security measure which is the privilege of least privilege that enforces strict access control. The system protects itself from account compromises through access restrictions which grant users and systems only the essential permissions needed to execute their tasks. The operational system enables this practice through segregation of duties (SOD) which functions as a control mechanism within Identity Governance frameworks. SOD policies prevent conflicts of interest because they create distinct permission sets for each user which blocks individuals from carrying out and concealing fraudulent or destructive activities. IAM systems implement SOD through two security mechanisms which combine role engineering with continuous access certification campaigns. Enabling both preventive and detective SOD within the IAM framework is vital for overall security from user's perspective. Organizations can establish behavioral standards through the integration of user behavior analytics (UBA) with IAM log data which detects unusual activities when users attempt to access protected data at unusual times or request more information than their authorized access permits.

7. IAM as a Compliance and Risk Management Enabler

The essential features of Identity and Access Management (IAM) enable organizations to achieve compliance and risk management requirements under GDPR and HIPAA and SOX regulations through its built-in audit trail functionality and access review system. The IAM framework is one the key pillars that allows for reporting and managing the regulatory requirements and acts as a key component to audit artifacts to enable and manage the compliance requirements since it acts as the gatekeeper for any identity to access any artifact.

IAM enables GDPR compliance through its authentication and authorization systems which protect data by monitoring access activities continuously thus supporting data minimization and purpose limitation requirements. The IAM system audit trails serve as evidence for compliance because they monitor user data access activities through recorded user identities and accessed data and time stamps and access conditions which allows organizations to prove compliance during breach investigations and regulatory reporting (Chhetri et al.,2022). HIPAA requires organizations to create secure systems which protect personal health information (PHI), medical information from unauthorized users. IAM systems enables access to the data based on the context and trust score of identity accessing this information. IAM systems allow for enforcing both preventive and detective segregation of duties both at coarse grained level and fine-grained level and acts as a key control for SOX compliance.

The Automated or Manual User Access Reviews (UAR) system together with certification processes help organizations maintain compliance through their scheduled verification of user access permissions. The automation system reduces human errors while minimizing

administrative tasks because it enables users to connect access logs to their positions and it will automatically revoke system permissions when users lose their access rights. UAR along with enablement of SODs in the organization helps to cater to the compliance requirements of the organization. Performing periodic UAR every quarter and providing the mitigating controls to address existing SOD are vital to adhere to the compliance requirements. IAM system can be enabled to perform different types of UAR like manager certification, privileged access owner certification. IAM system can also enable both preventive and detective SOD at both coarse- and fine-grained level.

The access governance system of IAM fulfills compliance requirements through its access governance system which performs detailed auditing and automated access certification functions. The system functions as an essential cybersecurity instrument which helps organizations to identify and minimize their security weaknesses. Organizations need IAM to function because it handles both access control and compliance requirements in their complex security environment.

8. Challenges and Future Trends in IAM

The current challenges of Identity and Access Management (IAM) stem from three main issues which include identity sprawl and system complexity and the need to merge legacy systems. The growth of digital identities across various cloud and on-premises and hybrid systems creates management difficulties which simultaneously increases the number of potential attack entry points. The system faces complexity because it needs to handle multiple identity types which include human users and services and workloads while dealing with complex permission systems designed for cloud-native environments. The new identity management system implements blockchain-based decentralized technology which enables users to manage their digital identities while maintaining their information safety from unauthorized access. Self-Sovereign Identity (SSI) models let users maintain control of their cryptographically verified credentials which they store in digital wallets, so they need fewer centralized authorities to protect against single points of failure and data breaches. The systems encounter obstacles for complete market adoption because their advanced design structure and new concepts lead to difficulties when users try to operate them (Glöckler et al.,2023; Khayretdinova et al.,2022; Ghaffari et al.,2021).

Password less Authentication through FIDO2 standards has become more popular because it provides a secure authentication method which protects users from phishing attacks and credential theft. The authentication system of FIDO2 enables users to authenticate through phishing-resistant cryptographic credentials which include security keys and biometric authentication for better security and user experience. Organizations keep implementing this technology because they need to improve their authentication security systems which defend Zero Trust environments (Alsirhani et al.,2022).

The second main challenge is the multiple deices which at times are non-compliant and becomes the source of exploitation. Device management software should be enabled to ensure that only trusted devices can be used to access the rightful information.

The third main challenge is to manage the expected proliferation of privileged identities in the ecosystem, Discovery and management of these identities will be a major challenge. Unless there is a centralized IAM system to manage these identities, it will lead to existence of rogue identities in the ecosystem.

The solution to IAM challenges involves using AI/ML for adaptive security systems and decentralized identity systems and password less authentication methods which provide users with better control and stronger access security. The present market patterns confirm IAM stands as a fundamental requirement which will help establish future security frameworks that must defend sophisticated cloud-based systems.

9. Conclusion

Out in the real world of digital setups, something called Identity and Access Management now acts like an invisible shield. With more companies shifting workloads into cloud-based systems, this monitoring tool becomes central to Zero Trust setups - always checking who someone is, not just letting them in by default. Instead of making assumptions, it decides whether to allow entry based on shifting danger levels at any moment. Control tightens when access gets split into tiny pieces, rights stay minimal by design, while newer ways to confirm identity - like multiple steps or skipping passwords entirely - get woven right in. What stands out is how it handles high-level risks - by regularly checking who has access, capping those rights over time. It also shrinks exposure points using smart access rules that adjust as needed. Another key point comes from meeting legal standards, thanks to precise logs kept on record activities. These records help meet recurring checks needed under rules like GDPR, HIPAA, and SOX . Further privilege access needs to be centralized and access to them should be via approved channels and all privileged actions should be logged for audit purposes.

A fresh approach to identity and access management goes beyond typical tech spending - it quietly shapes how safely an organization moves forward online. When smart permission systems, machine-learning powered threat spotting, and automated rule-following are woven into daily operations, risk drops while speed stays intact.

So, companies should focus on security built around individual identities. Think of IAM not just as a tool but as the core barrier against modern threats. Today's networks are scattered, often running in clouds - this reality demands new thinking. When done right, risk drops quietly, legal obligations get easier to meet. A space where trust grows tends to last longer than one built on guesswork.

10. References:

1) Ghadge, N. (2024). Enhancing threat detection in Identity and Access Management (IAM) systems. International Journal of Science and Research Archive, 11(2), 2050–2057. https://doi.org/10.30574/ijsra.2024.11.2.0761
2) Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595
3) Alsirhani, A., Ezz, M., & Mohamed Mostafa, A. (2022). Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. Computer Systems Science and Engineering, 43(3), 967–984. https://doi.org/10.32604/csse.2022.024854
4) Umoga, U., Sodiya, E., Amoo, O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. International Journal of Science and Research Archive, 11(1), 1810–1817. https://doi.org/10.30574/ijsra.2024.11.1.0284
5) Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. Electronics, 13(5), 865. https://doi.org/10.3390/electronics13050865
6) Fugkeaw, S. (2023). Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud. IEEE Access, 11, 25480–25491. https://doi.org/10.1109/access.2023.3255885
7) Naik, N., & Jenkins, P. (2016, March 1). A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards. https://doi.org/10.1109/mobilecloud.2016.22
8) Singh, C., Thakkar, R., & Warraich, J. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research, 8(4), 30–38. https://doi.org/10.24018/ejeng.2023.8.4.307
9) Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. Business & Information Systems Engineering, 66(4), 421–440. https://doi.org/10.1007/s12599-023-00830-x
10) Meng, L., Huang, D., An, J., Zhou, X., & Lin, F. (2022). A continuous authentication protocol without trust authority for zero trust architecture. China Communications, 19(8), 198–213. https://doi.org/10.23919/jcc.2022.08.015
11) Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic Access Control and Authorization System based on Zero-trust architecture. 123–127. https://doi.org/10.1145/3437802.3437824
12) Jose Diaz Rivera, J., Muhammad, A., & Song, W.-C. (2024). Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. IEEE Open Journal of the Communications Society, 5, 2792–2814. https://doi.org/10.1109/ojcoms.2024.3391728

13) Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., & Germonville, D. (2013). Adding Federated Identity Management to OpenStack. Journal of Grid Computing, 12(1), 3–27. https://doi.org/10.1007/s10723-013-9283-2

14) Moallem, A. (2019). Cybersecurity Awareness Among Students and Faculty. Crc. https://doi.org/10.1201/9780429031908

15) Ayoola, V., James, U., Idoko, I., Ijiga, O., & Olola, T. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global Journal of Engineering and Technology Advances, 20(3), 094–117. https://doi.org/10.30574/gjeta.2024.20.3.0164

16) Li, W., Cheng, H., Wang, P., & Liang, K. (2021). Practical Threshold Multi-Factor Authentication. IEEE Transactions on Information Forensics and Security, 16, 3573–3588. https://doi.org/10.1109/tifs.2021.3081263

17) Sanders, M. W., & Yue, C. (2019). Mining least privilege attribute-based access control policies. 404–416. https://doi.org/10.1145/3359789.3359805

18) Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. 4458–4466. https://doi.org/10.1109/bigdata.2017.8258485

19) Chhetri, T. R., Kurteva, A., Delong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. Sensors (Basel, Switzerland), 22(7), 2763. https://doi.org/10.3390/s22072763

20) Sutradhar, S., Karforma, S., Bose, R., Roy, S., Djebali, S., & Bhattacharyya, D. (2023). Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A block-chain-based approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems, 4, 49–67. https://doi.org/10.1016/j.iotcps.2023.07.004

21) Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2021). Identity and access management using distributed ledger technology: A survey. International Journal of Network Management, 32(2). https://doi.org/10.1002/nem.2180

22) Khayretdinova, A., Kubach, M., Sellung, R., & Roßnagel, H. (2022). Conducting a Usability Evaluation of Decentralized Identity Management Solutions (pp. 389–406). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-33306-5_19

23) Bairyev, M. (2023, February 28). What is Zero Trust Architecture and How Does It Work? *Custom Software Development Company*. https://maddevs.io/blog/what-is-zero-trust-network-architecture/