UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

Identity Access Management Systems: A comparative review

Shibham Karmakar
Ks781india@gmail.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Pallabi Sarkar
pallabisrkr@gmail.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Prashant GK
prashantgk@outlook.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Shreenita Saha
shreenita2003@gmail.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Ritindranath Tagore
ritintagore@gmail.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Wrishita Paul
paulwrishita@gmail.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Susmit Basak
susmitbasak469@gmail.com
VIT Bhopal University, Sehore, 466114, Madhya Pradesh, India

Abstract: Identity Access Management (IAM) systems are critical components in modern digital infrastructures, providing essential capabilities for managing user identities and controlling access to resources within organizations. [1] This review paper explores the evolution, architecture, and key functionalities of IAM systems, highlighting their role in enhancing security and compliance in increasingly complex IT environments. The paper provides a comprehensive overview of various IAM components, including authentication, authorization, and auditing, and examines the challenges and best practices associated with implementing these systems. Additionally, emerging trends such as Zero Trust Architecture, AI driven identity management, and the impact of cloud computing on IAM are discussed to offer insights into the future trajectory of these technologies. This review examines existing literature to highlight essential factors organizations must address when implementing IAM systems, stressing the importance of developing solutions that are robust, scalable, and adaptable to meet changing cyber threats and regulatory demands.

Keywords: Digital infrastructures, User identities, Access control, Security, Compliance, IT environments, Authentication, Authorization, Auditing, Zero Trust Architecture, AI-driven identity management, Cloud computing, Emerging trends, Challenges, Best practices, Scalable solutions, Cyber threats, Regulatory requirements

1. REQUIREMENTS OF SUCH STUDIES

In the modern digital landscape, in cybersecurity, strong Identity and Access Management (IAM) solutions are becoming essential.. As organizations depend more on digital platforms for their operations, the rising threat of cyberattacks and data breaches has underscored the critical role of effective IAM solutions in protecting sensitive data. Conducting a thorough review of different IAM systems is crucial for understanding their unique features, advantages, and shortcomings, allowing organizations to make well-informed decisions that align with their specific security requirements. With the evolution of technology, IAM systems have become more sophisticated, incorporating multifactor authentication, biometrics, and artificial intelligence to enhance security [1] [2]. However, the diversity and complexity of these systems can be overwhelming, necessitating a detailed analysis to elucidate their functionalities and practical applications. [3] This review study aims to fill the gap in current literature by providing a systematic com parison of IAM solutions, highlighting best practices, and identifying

emerging trends. This paper explores the IAM systems landscape to provide valuable insights into their effective implementation, focusing on mitigating risks, ensuring compliance with regulatory standards, and safeguarding organizational assets against unauthorized access. Ultimately, this research will serve as a crucial resource for IT professionals, security experts, and decisionmakers seeking to enhance their cyber security posture in an era where the integrity and confidentiality of digital identities are paramount. The growing complexity of cyberthreats highlights the need for a thorough evaluation of Identity and Access Management (IAM) systems in cyber security. Cyberspace. [3] With cyber adversaries leveraging advanced techniques to exploit vulnerabilities, traditional security measures frequently prove inadequate, highlighting the need for more robust and adaptable IAM solutions. These systems are not merely about preventing unauthorized access but also about ensuring seamless and secure user experiences across a multitude of devices and platforms. [1] The increasing adoption of cloud ser vices, remote work environments, and The Internet of Things (IoT) has significantly broadened the attack surface, making it essential for organizations to implement flexible and resilient IAM frameworks. In addition, regulations and data protection laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) enforce strict requirements on how organizations handle and safeguard user identities.[1] A thorough review of IAM systems will assist businesses in coordinating their security plans with these regulatory requirements., thereby avoiding hefty penalties and reputational damage. Additionally, IAM systems are pivotal in fostering trust and confidence among customers, partners, and stake holders by demonstrating a commitment to protecting personal and sensitive information. [4] [3] Another critical aspect driving the need for this review is the rapid pace of technological advancements. Advancements in artificial intelligence, machine learning, and blockchain are consistently transforming the IAM landscape. For instance, AI-driven IAM solutions can provide predictive analytics to preempt potential security breaches, while blockchain-based identity management offers decentralized and tamperproof authentication mechanisms. [2] [4] Evaluating these emerging technologies within the context of IAM systems is essential to understand their potential benefits and challenges, ensuring that organizations can leverage them effectively. [1] Moreover, IAM systems play a crucial role in enabling digital transformation initiatives. As businesses strive to innovate and remain competitive, they must adopt IAM solutions that are scalable, flexible, and capable of supporting diverse and evolving user needs. [2] This review will delve into the various architectural models of IAM, such as centralized, decentralized, and hybrid approaches, examining their suitability for different organizational contexts. In order to provide a thorough understanding of an organization's security posture, it will also investigate how IAM might be integrated with other security measures, such as threat detection and response systems.. A comprehensive review of Identity and Access Management systems is indispensable for navigating the complexities of modern cyber security. By systematically analyzing the wide array of available IAM solutions, this study will give businesses the information they need to implement effective and futureproof security strategies. It will bridge the knowledge gap, offer practical recommendations, and highlight innovative trends, ultimately contributing to the enhancement of global cyber security resilience. This research will be a valuable asset for academic scholars, industry practitioners, and policymakers, fostering a deeper understanding of IAM systems' critical role in protecting digital identities and maintaining trust in the digital age.

2. LITERATURE REVIEW

2.1 Previous Development

The development of Identity and Access Management (IAM) systems has been influenced by the increasing complexity of digital environments and the rising demand for strong security measures. IAM's origins date back to the early days of computing, when mainframe systems relied on basic username and password authentication to manage access control. [2] However, as networks expanded and organizations began to rely on more interconnected systems, the limitations of these early methods

became apparent. In the 1990s, the concept of Role-Based Access Control (RBAC) emerged as a significant milestone in IAM development. RBAC introduced the idea of assigning permissions based on user roles rather than individual identities, allowing for more streamlined and scalable management of access rights.[5] At the turn of the millennium, federated identity systems emerged, allowing users to access various services across different domains with a single set of credentials. This era also saw the introduction of Single Sign-On (SSO) technologies, which enhanced the user encounter by getting rid of having to keep track of numerous logins. In the 2010s, the dawn of cloud computing drove the development of cloud-based IAM solutions, which offered organizations greater flexibility and scalability. The incorporation of machine learning (ML) and artificial intelligence (AI) into IAM systems in recent years has made it possible to implement more advanced and flexible security features, like automatic threat detection and behavior-based authentication..[3] Decentralized identity systems, leveraging blockchain technology, have also emerged as a promising approach to enhance user privacy and control over personal data.[4]

2.2 Key Models and Frameworks

Numerous frameworks and approaches have been created to guide the implementation of IAM systems. One of the most widely adopted models is RBAC, or role-based access control, arranges rights based upon user roles inside a company. This paradigm simplifies the management of access rights by enabling administrators to assign roles to users based on their job functions, instead of setting permissions for each user individually. [5] RBAC is particularly effective in environments with well-defined roles and responsibilities, offering a balance between security and ease of management. Another important model is Attribute-Based Access Control (ABAC), which adopts a strategy that is more thorough by basing access decisions on a mix of environmental factors, resource features, and user qualities. ABAC offers greater flexibility than RBAC, enabling dynamic, context-aware access control policies.[5] However, its complexity can be a challenge to implement and manage, especially in largescale environments. Discretionary Access Control (DAC) and Mandatory Access Control (MAC) are other conditional models employed in IAM. Users can control who has permission to use their personal resources thanks to DAC, making it perfect for settings that value adaptability. approach that enforces access rules set by a central authority, making it suitable for high-security settings like government and military systems.

2.3 Comparison of Approaches

When comparing different IAM systems and methodologies, each possesses a unique set of benefits and drawbacks. RBAC is praised for its simplicity and ease of use, making it suitable for organizations with clear hierarchical structures.[5] However, it may not be as effective in dynamic environments where roles and responsibilities frequently change. ABAC, while offering more granular control and flexibility, can be more difficult to implement and maintain due to its complexity. This complexity can lead to potential performance issues, especially in realtime decision-making scenarios. Cloud-based IAM solutions offer scalability and ease of integration with modern cloud services, making them an attractive option for organizations adopting cloud-first strategies.[6] However, they also introduce challenges related to data privacy and the dependency on thirdparty providers for security. Decentralized identity systems, on the other hand, empower users with greater control over their identities and reduce reliance on central authorities. Despite this, they face challenges in widespread adoption, interoperability, and the need for a robust underlying infrastructure.[4]

2.4 Technological Advancements

Recent technological advancements have had a profound impact on IAM. The incorporation of AI and ML into IAM systems has led to more intelligent and adaptive security measures. For example, behavior-

based authentication leverages machine learning to examine user behavior and identify any irregularities that might signal unauthorized access, providing a proactive approach to identifying potential threats in real time. Cloud-based IAM solutions have also progressed, enabling organizations to efficiently manage identities across various cloud environments. These solutions offer scalability, cost-effectiveness, and ease of deployment, making them increasingly popular for modern enterprises. Moreover, decentralized identity systems, which use blockchain technology, are gaining attention for their ability to enhance user privacy and mitigate identity theft risks. These systems empower users to maintain authority over their private information, removing the need for a central authority to manage identities.

2.5 Challenges Identified

Despite the advancements in IAM technologies, several challenges remain, as highlighted in existing literature. One of the primary challenges is scalability, particularly in large organizations with a vast number of users and resources. [5] Managing access control and maintaining consistent security policies across various systems can be both complex and resource-intensive. Privacy is another major challenge, especially with increasing concerns about how personal data is gathered, stored, and utilized. IAM systems must find a balance between ensuring security and respecting users' privacy rights. Additionally, managing identities across diverse systems and platforms presents a significant challenge. As organizations adopt a combination of on-premises, cloud, and hybrid environments, maintaining uniform identity management practices across these platforms can be difficult. [6] Additionally, the evolving nature of cyber threats requires IAM systems to be continuously updated and adapted, which can be resource-intensive and challenging to manage. In summary, the literature on IAM reflects the ongoing evolution of identity management practices and technologies. Although substantial advancements have been made in creating more advanced and adaptable IAM systems, challenges like scalability, privacy issues, and the complexity of managing identities across various systems remain significant obstacles. Addressing these challenges is crucial for organizations aiming to enhance their security measures and safeguard their digital assets in an interconnected environment.

3. FUNDAMENTALS OF IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity Access Management (IAM) is a key component of cybersecurity designed to ensure that only authorized users have access to the appropriate resources at the necessary times. At its core, IAM includes several essential concepts critical to securing digital environments. The first aspect is authentication, which involves confirming a user's or system's identity using credentials like biometric data, security tokens, or passwords. Once authentication is complete, authorization defines the resources the verified user can access and the actions they are permitted to take. [1] Another critical concept is Identity Federation, which links a user's identity across multiple systems or organizations, allowing a single identity to be used across different platforms. This not only improves security but also simplifies access across different domains. Single Sign-On (SSO) is a feature within IAM that enhances the user experience by enabling users to authenticate once and gain access to multiple systems without having to log in to each one individually. [4] This reduces the need for managing multiple passwords and improves both security and productivity. To strengthen security, Multi-Factor Authentication (MFA) requires users to provide two or more verification factors before gaining access, such as something they know (like a password), something they have (like a smartphone), or something they are (like a fingerprint) [5]. This layered approach greatly minimizes the risk of unauthorized access resulting from compromised credentials. [2] IAM systems consist of several key components that collaborate to manage identities and control access to resources. Identity Providers (IdP) are systems or services responsible for managing user identities and providing authentication services. These providers verify users' identities and issue authentication tokens that Service Providers (SP), which are systems or applications

relying on IdPs for user authentication, use to grant access.[6] Directories, such as LDAP and Active Directory, serve as central databases that store user identities, credentials, and attributes, providing a reference point for authentication and authorization decisions. Additionally, user repositories store detailed information about users, including their roles and permissions, and are often integrated with directories to manage identities and control access effectively. Collectively, these concepts and components form the backbone of a strong IAM system, vital for preventing unauthorized access, ensuring regulatory compliance, and enhancing user experience in a secure digital environment. Grasping and implementing these elements is crucial for organizations to protect their digital assets and uphold the integrity of their systems.

4. IMPLEMENTATION OF IAM SYSTEMS

4.1 Current Implementation Strategies

A systematic approach that satisfies the organization's operational and security goals is necessary when implementing Identity and Access Management (IAM) systems [11]. Performing a comprehensive risk assessment to find potential weaknesses and rank IAM goals is a commonly used tactic. This is often followed by a phased deployment, which starts with critical systems and gradually extends to less critical areas. This gradual approach enables organizations to evaluate the IAM system in a controlled setting, make necessary refinements, and ensure seamless integration with existing processes before implementing it on a larger scale. Best practices emphasize the importance of defining clear governance structures and establishing a robust policy framework. This entails adopting the principle of least privilege, ensuring that users receive only the minimum access necessary to perform their tasks. [12] Role-Based Access Control (RBAC) is frequently used in this context, as it simplifies access management by associating permissions with defined roles rather than individual users. [5] More complex environments might implement Attribute-Based Access Control (ABAC), which uses dynamic attributes to provide more granular access control, although this can increase the complexity of the IAM system. By evaluating whether the requester's request contains the appropriate properties, it decides whether to give access. ABAC is able to effectively segregate access control and policy management since subject and object attributes are established independently.[8] Single Sign-On (SSO) and Multifactor Authentication (MFA) [2] are seen to be crucial for improving security without sacrificing usability. While SSO lessens the hassle of multiple logins while preserving a high level of security across several platforms, MFA provides an extra layer of protection by demanding multiple forms of authentication. Other essential elements include frequent audits and ongoing monitoring, which help firms identify and address unwanted access attempts, enforce adherence to security guidelines, and adjust to changing threats.

4.2 Technology Stack

The technology stack for IAM implementations typically includes a combination of software platforms, authentication protocols, and infrastructure components. Leading IAM platforms like Okta, Microsoft Azure Active Directory, and IBM Security Identity Governance and Intelligence provide comprehensive solutions for managing identities, roles, and access policies. These platforms are often complemented by specific protocols designed to facilitate secure authentication and authorization processes. OAuth (Open Authorization) is a commonly used delegated access protocol that gives third-party apps access to user data without disclosing login credentials. This is especially helpful in cloud environments where safe interaction between several applications is required. Another important protocol that makes Single Sign-On (SSO) possible is Security Assertion Markup Language (SAML), which permits identity providers to share authentication details with service providers. This is crucial for ensuring seamless user experiences across multiple platforms while maintaining high security levels.

[13] Lightweight Directory Access Protocol (LDAP) and its extensions are commonly used to manage user information in directory services like Microsoft Active Directory. These directories serve as the backbone of many IAM systems, storing user identities, credentials, and group memberships that drive authentication and authorization decisions. In terms of infrastructure, organizations might deploy IAM systems in on-premises environments, cloud platforms, or hybrid setups, depending on their specific requirements and regulatory constraints.

4.3 Integration with Existing Systems

Successful IAM implementations must integrate seamlessly with existing IT systems, including HR databases, cloud services, and legacy applications. Integration with HR systems is crucial, as these systems typically serve as the authoritative source of identity information. Automated user account provisioning and de-provisioning based on HR data lowers the risk of illegal access by ensuring that access permissions are issued and revoked in line with changes in employment status. Cloud-based services present both opportunities and challenges for IAM integration. Modern IAM solutions are built to seamlessly integrate with various cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, using protocols like OAuth and SAML to manage authentication and authorization. These integrations allow organizations to extend their IAM policies to cloud-based applications, ensuring consistent security practices across onpremises and cloud environments. Legacy systems, however, often require customized solutions to integrate with modern IAM platforms. These systems may not natively support contemporary authentication protocols, necessitating the development of custom connectors or the use of middleware to bridge the gap. Ensuring that IAM policies are consistently applied across both modern and legacy systems is critical to maintaining a cohesive security posture. Organizations must carefully plan these integrations, often requiring detailed assessments of legacy systems to understand their limitations and develop appropriate solutions. The implementation of IAM systems is a complex but essential undertaking for modern organizations.[14]

4.4 Case Study [23]

BACKGROUND: In 2003, Drew University initiated a comprehensive project to overhaul its account management procedures, which were previously handled manually. The university recognized the need to adopt a more efficient and secure approach to managing user identities and access across its IT infrastructure, which was becoming increasingly complex. The manual procedures that were a major part of the old system were not only time-consuming but also prone to mistakes and security flaws. This situation necessitated the implementation of an automated provisioning system based on Novell Identity Management technologies. The university's IT environment was diverse, encompassing a range of third-party and custom-built applications. These included everything from the campus ID card system to a specialized portal for admitted students. The primary goal was to create a unified system that could manage identities across all these platforms, streamline access control, and improve the overall efficiency of the university's IT operations.

CHALLENGES: Drew University encountered several significant challenges during the implementation of the IAM system. One of the most pressing issues was the integration of the new system with the university's existing legacy systems, some of which had been in operation for over two decades. These legacy systems were deeply embedded in the university's operations, making it difficult to transition to a new system without disrupting essential services. The diversity of identity formats and authentication methods across various platforms further complicated the integration process. Each system had its own protocols for managing user identities, which made it challenging to establish a consistent and unified identity management framework. Moreover, the university had to deal with numerous ad-hoc connections between different systems, which had been established over the years to facilitate various

operations. These connections were often inefficient and difficult to manage, leading to increased operational costs and potential security risks. Another challenge was ensuring that the new system could scale effectively to meet the increasing demands of the university. As more and more staff, instructors, and students need access to a variety of IT tools, the IAM system needed to be robust enough to handle large volumes of user data and access requests.

SOLUTION: To overcome these challenges, Drew University adopted a comprehensive set of Novell Identity Management solutions, including: Meta-Directories: The university utilized meta-directories to centralize and manage user identity data from various sources. This strategy helped standardize the different identity formats across systems, leading to a more consistent and efficient identity management process. Automated Provisioning: The implementation of an automated provisioning system replaced the manual processes for managing user accounts. This significantly reduced the time and effort required for creating, updating, and deleting accounts, while also enhancing the accuracy and security of the university's identity management. Single Sign-On (SSO): By introducing SSO technology, users could access Several services and apps using one set of login credentials. This not only simplified the user experience but also reduced the number of passwords needing management, thereby improving security. Integration with Legacy Systems: A significant achievement of the project was the successful integration of the IAM system with Drew's legacy systems. The university established a unified identity management bridge, replacing the numerous ad-hoc connections previously in place. This approach not only cut costs but also extended the life and utility of the legacy systems.

RESULTS: The deployment of the Novell Identity Management system yielded several positive outcomes for Drew University: Enhanced Security: The new IAM system strengthened the security of the university's IT infrastructure by providing better control over user identities and access rights. The combination of SSO and automated provisioning reduced the threat of unauthorized entry and data breaches. Operational Efficiency: Automating identity management processes led to significant improvements in operational efficiency. Tasks like creating and updating user accounts, which previously required manual intervention, were now automated, allowing IT staff to focus on more strategic initiatives. Cost Reduction: By replacing numerous ad-hoc connections with a single, unified identity management framework, the university achieved operational cost savings. The streamlined system also required less maintenance, further contributing to cost efficiency. Scalability: The new IAM system proved to be scalable, accommodating the university's growing number of users and applications. This ensured that the system could continue to meet the university's needs as it expanded.

CONCLUSION: The successful implementation of Novell Identity Management at Drew University underscores the importance of a well-planned and customized IAM strategy in a complex IT environment. By addressing the challenges of legacy systems, diverse identity formats, and the need for scalability, the university established a robust and efficient identity management framework. This case study demonstrates the potential benefits of IAM systems, including enhanced security, operational efficiency, and cost savings, serving as a valuable reference for other institutions considering similar initiatives. By following best practices, learning from real-world examples, choosing the right technology stack, and ensuring smooth integration with existing systems, organizations can significantly improve their security posture while enabling efficient access management. This strategic approach to IAM implementation helps safeguard critical assets, comply with regulatory requirements, and adapt to the evolving threat landscape.

5. CHALLENGES AND ISSUES IN IAM

5.1 Security Risks

Security risks are among the most critical challenges in the implementation and management of Identity and Access Management (IAM) systems. The potential threats associated with IAM are varied and can have significant consequences if not properly mitigated. Identity theft is a primary concern, where attackers gain unauthorized access to legitimate user credentials. This can occur through various means, such as weak passwords, social engineering, or data breaches. Once an attacker gains control of an identity, they can access sensitive systems, steal data, and perpetrate further attacks within an organization, often going undetected for extended periods. [15] Phishing remains a prevalent method for attackers to compromise IAM systems. By tricking users into disclosing their credentials via phony websites or emails, attackers can bypass authentication mechanisms, especially if Multi-Factor Authentication (MFA) is not enforced. Insider threats also pose a significant risk; employees or other insiders with legitimate access to systems may misuse their privileges either maliciously or inadvertently. IAM systems must, therefore, include robust mechanisms for auditing and monitoring in order to identify and address such hazards. Security risk analysis is essential in IAM to identify and prioritize potential vulnerabilities. Organizations must continuously assess their IAM systems against emerging threats, making certain that security measures are current and in line with the most recent threat intelligence. To reduce the risk of identity theft, phishing, and insider threats, this involves implementing robust authentication measures, adhering to the principle of least privilege, and regularly reviewing access permissions.

.*Scalability*

Scalability is another significant challenge in IAM, particularly for large or distributed organizations. As companies expand, the quantity of consumers, gadgets, and apps that need to be managed can increase exponentially. This presents several issues, including the complexity of managing a large number of identities, the performance of IAM systems under heavy load, and the ability to maintain consistent access policies across a dispersed infrastructure.[16] In distributed environments, such as those spanning multiple geographic locations or utilizing cloud services, ensuring that IAM systems can scale to accommodate the volume of access requests and the diversity of platforms is crucial. Traditional on-premises IAM solutions may struggle with scalability, leading organizations to adopt cloud-based IAM services that offer more flexibility and dynamic scaling capabilities. However, these solutions also introduce new challenges, such as ensuring data privacy and compliance across different jurisdictions. Moreover, scaling IAM systems effectively requires careful planning around the architecture, including the deployment of redundant systems to ensure high availability and load balancing to manage traffic. Organizations must also consider the potential impact on performance, as increased load can lead to slower authentication times and affect user experience. Ensuring that IAM systems can scale efficiently while maintaining security and performance standards is a critical challenge for any organization. [17]

5.2 Compliance and Regulations

IAM systems are subject to a wide array of regulatory requirements [19], which vary depending on the location and industry. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., the General Data Protection Regulation (GDPR) [18] [20] in the EU, and various other data protection regulations worldwide impose strict guidelines on how businesses manage and secure personal data. These rules have an effect on IAM since they specify how identities are maintained, how sensitive data access is restricted, and how breaches must be reported. Compliance with these regulations requires organizations to implement robust IAM systems that can enforce access controls, protect personal data, and provide detailed audit trails. For example, under GDPR requires businesses to make sure that only authorized personnel can access personal data. and must be able to demonstrate compliance through regular audits. Similarly, HIPAA requires healthcare organizations to implement safeguards to protect electronic health information, including strict access controls and monitoring.

[18][20] Serious consequences, such as fines and harm to one's reputation, may arise from breaking these rules. Consequently, organizations must integrate compliance considerations into their IAM strategy, ensuring that their systems are designed to meet regulatory requirements from the outset and are updated frequently to account for modifications in the legal landscape.

5.3 User Experience

Balancing security with usability is a perennial challenge in IAM. While strong security measures are necessary to safeguard sensitive information and systems, if they are not implemented carefully, they frequently result in a difficult user experience. For instance, requiring complex passwords and frequent password changes can lead to user frustration and may even encourage risky behavior, such as writing down passwords or utilizing the same one for several accounts. [22] Similarly, the implementation of Multi-Factor Authentication (MFA), while significantly enhancing security, can be seen as an inconvenience by users, particularly if the authentication process is slow or requires multiple steps. This can result in resistance to security measures, with users seeking to bypass or disable them, thereby undermining the effectiveness of the IAM system. To address these challenges, organizations must consider the trade-offs between security and usability in their IAM design. Using user-friendly authentication techniques like biometrics or adaptive authentication is part of this., which adjusts security requirements based on the context of the access request. Additionally, the use of Single Sign-On (SSO) can preserve a high degree of security while improving the user experience by lowering the frequency of logins. [21]

In conclusion, the challenges and issues in IAM are multifaceted, with security risks, scalability, compliance, and user experience all requiring careful consideration. Security risk analysis is paramount to identify and mitigate threats such as identity theft, phishing, and insider attacks. Scalability challenges must be addressed to ensure IAM systems can grow with the organization, while compliance with regulation laws like GDPR and HIPAA are crucial. Lastly, to guarantee that IAM systems are both efficient and easy to use, striking the correct balance between security and usability is essential. For IAM systems to be implemented and maintained successfully in any business, several issues must be resolved.

6. EMERGING TRENDS IN IAM

As new technologies emerge, digital ecosystems become more complex, and cyber threats become more sophisticated, the role of IAM (Identity and Access Management) is always changing. Several emerging trends have ben shaping the future of IAM, influencing how organizations secure identities and manage access in an increasingly interconnected world. Vendor techniques, technological advances, practices and processes, business drivers, and security features for authorization, authentication, administration, and audit are all part of the evolution of identity and access management. [7]

6.1 Decentralized Identity

Decentralized identity management represents a significant shift from traditional, centralized IAM systems, offering a new paradigm in how identities are managed and verified. Traditional IAM systems rely on centralized identity providers (IdPs) to authenticate users and control access to resources. However, this centralization introduces vulnerabilities, such as single points of failure and potential privacy concerns, as users' identity data is stored and managed by third-party entities by granting people more control over their own identification data, decentralized identity—which is frequently built on blockchain technology—tries to overcome these problems. In a decentralized identity model, individuals establish and control their digital identities through the use of cryptographic keys, which are stored on a distributed ledger. This approach allows users to share verified identity attributes (e.g., age,

citizenship, qualifications) with service providers without relying on a central authority. These transactions are safe, transparent, and impenetrable thanks to the usage of blockchain technology. [4] The potential impact of decentralized identity is profound. By enabling users to selectively provide only the information that is required, it claims to improve privacy by lowering the danger of identity theft and data breaches. By enabling users to selectively provide only the information that is required, it claims to improve privacy by lowering the danger of identity theft and data breaches. However, the widespread adoption of decentralized identity faces challenges, including the need for standardization, interoperability among different blockchain platforms, and the management of cryptographic keys by users, which can be complex.[4]

6.2 AI and Machine Learning

As IAM systems develop, artificial intelligence (AI) and machine learning (ML) become more and more important because they improve security and efficiency. Behavioral biometrics is one of the most important areas of IAM where AI and ML are being used. [3] By analyzing trends in user conduct, such as typing speed, mouse movements, and consumption habits, behavioral biometrics generate a dynamic profile of the user, in contrast to traditional biometrics, which depend on static attributes like fingerprints or facial recognition. A stronger defense against identity theft and account takeover attempts is provided by this profile, which is updated often and may be used to authenticate users in real-time. Risk-based authentication, which evaluates each authentication attempt's risk level based on a number of variables like user behavior, device specs, and geolocation, also benefits from machine learning. Machine learning algorithms examine historical data to detect anomalies in user behaviour that may signal a compromised account. For instance, if a user usually logs in from a specific location but suddenly tries to access their account from another country, the system can identify this as a high-risk event and request additional verification, such as Multi-Factor Authentication (MFA). AI-driven IAM systems can also automate the detection and response to security incidents. These technologies can detect possible security problems faster than human analysts by continuously observing access patterns and abnormalities, allowing for more rapid and effective responses. As these technologies continue to advance, we can expect AI and ML to further enhance the intelligence and adaptability of IAM systems, making them more resilient against evolving cyber threats.[3]

6.3 IAM in Edge Computing and IoT

New issues for IAM are brought about by the quick spread of Internet of Things, or IoT, gadgets and the emergence of edge computing. Traditional IAM techniques are less successful on IoT devices because they frequently have limited computing power and may operate in areas with sporadic connectivity. Additionally, the sheer number of IoT devices, each potentially requiring its own identity and access control, adds significant complexity to IAM systems. A better standard for distributed access control is necessary due to the Internet of Things' rapid expansion. The four benefits of blockchain technology for assessment control are non-tampering, scalability, data encryption, and decentralization. [8] One of the primary challenges in managing identities in IoT and edge computing environments is the need for lightweight and scalable IAM solutions that can operate efficiently on resource-constrained devices. Traditional IAM protocols may be too resource-intensive for IoT devices, leading to the development of specialized protocols designed for low-power environments. These protocols must also be secure enough to prevent unauthorized access and tampering, which are significant concerns in IoT networks. IAM is made more difficult by edge computing, which processes data closer to its source rather than depending on centralized data centers. IAM systems must be able to function autonomously and safely at the network edge in edge contexts, frequently with no supervision from central authorities. This decentralization requires robust identity management that can handle the dynamic nature of edge computing, where devices frequently join and leave the network. To address these challenges, solutions

such as decentralized identity management, discussed earlier, and distributed IAM architectures are being explored. These approaches aim to provide secure and scalable identity management for IoT and edge computing by leveraging technologies like blockchain and distributed ledgers, which can operate in a decentralized manner without requiring constant connectivity to a central server.[4]

6.4 Zero Trust Architecture

IAM plays a crucial role in the Zero Trust security model, which is transforming traditional network security approaches. Zero Trust architecture is built on the principle that no device or user, whether inside or outside the network, should be automatically trusted. Rather, each access request needs to be approved, verified, and validated on a regular basis. Because they enforce stringent access rules and guarantee that only authorized and authorized individuals are allowed to use resources, IAM systems are essential to Zero Trust. This approach requires a robust and dynamic IAM infrastructure that can handle continuous authentication and real-time access decisions When the emphasis is on safeguarding individual resources and data, regardless of where they are located, traditional perimeter-based security solutions are inadequate in a Zero Trust setting. Granting access to resources requires identity management and authentication, and the zero-trust paradigm necessitates the use of more robust identity authentication methods including multifactor authentication, improved biometric authentication, and continuous authentication mechanisms. [9]

Context-aware access controls are one of Zero Trust IAM's primary characteristics. These controls evaluate the context of an access request by considering factors such as the user's identity, location, device type, and behaviour patterns. AI and ML, which can evaluate enormous volumes of data to ascertain the proper degree of trust for every access request, make this context-aware approach possible. Additionally, Zero Trust places a strong emphasis on the least privilege concept, guaranteeing that users have the bare minimum of access privileges. This restricts the possible harm from compromised accounts and shrinks the attack surface. Implementing Zero Trust IAM requires integrating various security technologies, such as MFA, SSO, and risk-based authentication, into a cohesive strategy that can adapt to changing threats and user behaviors. In summary, emerging trends in IAM are reshaping the landscape of identity management. Decentralized identity management offers a promising alternative to traditional IAM, potentially revolutionizing how identities are managed and verified across borders. AI and machine learning are enhancing the intelligence and adaptability of IAM systems, particularly in areas like behavioral biometrics and risk-based authentication. The challenges of managing identities in IoT and edge computing environments are driving the development of lightweight and scalable IAM solutions. Finally, Zero Trust architecture is redefining security models, with IAM playing a central role in enforcing strict access controls and continuously validating trust. As these trends continue to evolve, they will significantly impact the future of IAM, offering new opportunities and challenges for organizations worldwide.

7. TYPES OF IAM

7.1 On premise IAM [10]

Control and security are two major benefits of traditional identity and access management (IAM) systems, in which the identity management infrastructure is fully housed in an organization's own data center. Organizations benefit from complete authority over their IAM environment, including user identities, authentication, authorization, and auditing. This is especially crucial for businesses dealing with sensitive data or operating under stringent regulations, as they can ensure data storage and security align with their specific requirements. On-premise IAM systems can be customized to fit an organization’s unique business processes, offering user-specific customization and seamless integration

with existing legacy systems. Additionally, these systems typically deliver better performance, as they are not reliant on external factors like internet connectivity, and can be modified to satisfy particular legal needs, guaranteeing data sovereignty and compliance.

However, on-premise IAM systems come with notable drawbacks, primarily related to cost and complexity. The initial setup involves significant expenses, including hardware, software licenses, and implementation services, and ongoing costs for maintenance, upgrades, and skilled IT personnel can be substantial. Managing these systems is complex, requiring specialized staff to handle configurations, patches, and updates, and integrating with modern cloud services and mobile applications can be challenging. Furthermore, scalability is a concern, as expanding an on-premise IAM system necessitates additional investments in hardware and infrastructure, making it less flexible compared to cloud-based solutions. This can pose problems for organizations experiencing rapid growth or changes in size or structure, potentially leading to performance issues or the need for costly upgrades.

7.2 Cloud IAM

Cloud-based IAM is a modern approach to managing digital identities, authentication, authorization, and access control through services hosted on remote servers managed by thirdparty providers. This Identity as a Service (IDaaS) model allows organizations to efficiently manage user identities across various applications, platforms, and devices via the cloud. Cloud IAM offers several benefits, including greater control with advanced security, allowing fine-grained permissions for specific actions on cloud resources. It also offers scalability, allowing organizations to support an increasing number of users and devices without significant infrastructure investments. Increased collaboration is another advantage, as it simplifies granting and revoking access for teams, fostering better teamwork. Additionally, cloud IAM can be costefficient, reducing the risk of unauthorized resource usage and potentially lowering overall cloud costs. [24]

However, cloud-based IAM has its drawbacks, particularly regarding dependency on third-party providers. Organizations rely on these providers for uptime, security, and data management, making them vulnerable to service disruptions or outages. The limited customization options in cloud IAM solutions can also be a challenge, as they are often designed to meet the needs of a broad customer base, which may not allow for custom integrations or configurations. Data privacy and compliance concerns are significant, especially for organizations in regulated industries, as storing sensitive identity data in the cloud may complicate compliance with data residency laws. Over time, subscription-based pricing can lead to higher total costs compared to on-premise solutions, and vendor lock-in may make switching providers difficult and expensive. Additionally, the centralized nature of cloud services poses security risks, and latency or performance issues can arise, particularly in regions with less reliable internet infrastructure. [25]

7.3 On-Premise vs. Cloud IAM Systems

On-premise IAM systems offer organizations complete control over their infrastructure, software, and data, enabling deep customization tailored to specific business needs. This control allows organizations to address strict compliance and confidentiality requirements more effectively, keeping sensitive data within their own environment. On-premise IAM systems are ideal for organizations that view identity management as a core competency, allowing for finely tuned solutions that can provide a competitive edge. However, this level of control comes with complexity and higher upfront costs, as organizations must manage and maintain the systems themselves. Onpremise IAM is well-suited for secure and fast access within a network, but it may struggle to keep up with the demands of modern distributed workforces and cloud-based applications.

On the other hand, cloud-based IAM provides standardized solutions that, while limited in customization, offer scalability, consistency, and ease of use. Cloud IAM is particularly attractive for organizations looking for convenience and access to cutting-edge technologies without the need for significant upfront investments. The subscription-based model of cloud IAM spreads costs over time, though long-term expenses may accumulate, and vendor lock-in can pose challenges. Cloud IAM excels in connecting remote workers and integrating with other cloud services, making it ideal for modern, distributed teams. However, organizations must weigh the trade-offs, including potential latency, security concerns, and dependency on the provider for uptime, disaster recovery, and support, with less visibility and control during incidents.

7.4 Federated IAM [26][27]

Secure cross-organizational access management is made possible by federated IAM (Identity and Access Management), which enables users to access numerous apps, systems, or services from other organizations using a single set of logininformations. This system is especially beneficial for organizations collaborating with external partners, vendors, or customers, as it allows them to authenticate and authorize users from different identity providers without creating new accounts. By leveraging protocols like WS-Federation or Security Assertion Markup Language (SAML), federated IAM enables Single Sign-On (SSO) without passwords, enhancing user experience, centralizing authentication, and improving security. The system reduces the risk of password-related vulnerabilities, scales well in environments with multiple external partners, and minimizes administrative overhead by managing user identities through trusted identity providers. Additionally, federated IAM supports compliance and auditability by providing detailed logging and auditing capabilities.

However, implementing federated IAM comes with challenges, particularly in terms of complexity and dependency on trust relationships. The initial setup requires a deep understanding of identity protocols and security practices, and the security of the system relies on the strength of the trust relationships between identity providers and service providers. Organizations using third-party identity providers have limited control over the authentication process and security policies, which can introduce vulnerabilities. Data privacy and compliance can also be challenging, especially when sharing identity information across organizational boundaries. Additionally, organizations may face vendor lock-in and performance issues, as reliance on external identity providers can lead to latency, particularly if they are located in different geographical regions. These factors must be carefully considered when adopting federated IAM solutions. [26][27]

7.5 Privileged Access Management [28][29]

Privileged Access Management (PAM) is an identity security solution designed to protect businesses from cyber threats by monitoring, detecting, and preventing unauthorized access to critical resources. PAM integrates people, processes, and technology to provide visibility into privileged account usage and user activities. By restricting administrative access to a limited number of users and implementing additional security layers, PAM strengthens system security and minimizes the risk of data breaches by malicious actors. A few of PAM's advantages are its substantial risk reduction. through the enforcement of least privilege, enhanced security by securing and monitoring privileged accounts, compliance support with regulatory requirements through detailed audit trails, and improved operational efficiency by streamlining privileged account management. [29]

However, implementing and managing a PAM solution can present challenges. The complexity of deploying PAM requires careful planning and coordination across various teams and systems, which can be daunting in complex IT environments, especially those with legacy systems. Additionally, there may

be resistance from privileged users who view PAM controls as obstacles to performing their duties. The integration of PAM into existing processes can also be difficult, and the cost of deploying and maintaining a PAM solution can be substantial, requiring ongoing investment in both technology and management efforts. Despite these challenges, the security and compliance benefits of PAM often outweigh the associated complexities and costs. [28]

7.6 Identity as a service

Identity-as-a-Service (IDaaS) is the term for cloud-hosted identity and access management (IAM) services that offer a centralized platform for safely managing user IDs. With features such as Multi-Factor Authentication (MFA), Single Sign-On (SSO), and access governance, IDaaS streamlines identity management by automating processes, increasing productivity, and strengthening security. The capability to scale of IDaaS makes it ideal for organizations with growing user bases, while its cost effectiveness eliminates the need for expensive on-premises infrastructure. IDaaS also supports compliance efforts by offering tools for access control, auditing, and reporting, ensuring sensitive data is well-protected. Additionally, the streamlined access processes and SSO enhance user experience by allowing quick and easy access to necessary resources, boosting productivity and satisfaction. [30]

However, adopting IDaaS presents challenges, including dependency on cloud providers for availability, security, and compliance, which can impact access to critical resources if issues arise. Integrating IDaaS with existing on-premises systems, legacy applications, and other cloud services can be complex, requiring careful planning. Data residency and privacy concerns are also significant, particularly in regions with strict data regulations. IDaaS platforms may not offer the same level of customization as on-premises IAM solutions, posing difficulties for organizations with unique requirements. Furthermore, vendor lock-in is a potential risk, as switching providers after adopting an IDaaS platform can be costly and challenging. [31]

7.7 Role Based Access Control

An access management technique called role-based access control (RBAC) gives people permissions according to their jobs inside a company. This method simplifies the process of managing user permissions by grouping users into roles according to their responsibilities and then assigning permissions to these roles rather than to individual users. By doing so, RBAC streamlines user assignments, ensuring that users have privileges consistent with their role's responsibilities. This approach not only reduces the complexity of access management but also minimizes errors associated with managing permissions individually.

The benefits of RBAC are numerous, including simplified access management, enhanced security, and improved compliance. By managing permissions at the role level, RBAC significantly reduces administrative overhead and complexity. It lowers the danger of unwanted access by enforcing the concept of least privilege, which guarantees that users have only the rights required to carry out their job tasks. RBAC also helps organizations meet regulatory requirements by providing a structured and auditable method for assigning and managing permissions. The scalability of RBAC makes it particularly useful for growing organizations, as roles can be easily assigned without the need to manage individual permissions. Moreover, RBAC ensures consistency and standardization across the organization by centrally defining roles and their associated permissions. [32]

Despite its advantages, RBAC comes with challenges that can complicate its implementation and maintenance. One significant challenge is "role explosion," where the number of roles proliferates in complex organizations, making the system difficult to manage and potentially negating its benefits. The

initial setup of an RBAC system can also be complex and time consuming, requiring a deep understanding of organizational roles, responsibilities, and workflows. Furthermore, RBAC can be rigid compared to more flexible access control models like Attribute-Based Access Control (ABAC), which makes it possible to make context-based, more detailed access decisions. If roles are not carefully defined, they may end up with excessive permissions, leading to over-privileged users and compromised security. Regular audits and updates are essential for maintaining and governing RBAC systems to ensure they align with organizational changes and security policies.

REFERENCES

1 I. A. Mohammed," Systematic review of identity access management in information security," International Journal of Innovations in Engineering Research and Technology, vol. 4, no. 7, pp. 1-7, 2017.

2 B. O. ALSaleem and A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," IEEE Xplore, Mar. 01, 2021. https://ieeexplore.ieee.org/document/9428806

3 S. Laato, A. Farooq, H. Tenhunen, T. Pitkamaki, A. Hakkala, and A. Airola, "AI in Cybersecurity EducationA Systematic Literature Review of Studies on Cybersecurity MOOCs," IEEE Xplore, Jul. 01, 2020.

4 Oliver Hasan Padmanegara, Ratna Komala Putri, R. Yuliani, and E. K. Masli, "Blockchain and The Public Sector: BlockchainBased Identity Management Systems for Public Services and The Impact on Privacy and Security Risks," Aug. 2023, doi: https://doi.org/10.1109/icondbtm59210.2023.10326737.

5 "Leveraging access control mechanisms of Android smartphones, using context-related role-based access control models," Ieee.org, 2024. https://ieeexplore.ieee.org/document/5967517 (accessed Aug. 15, 2024).

6 G. Ducatel, "Identity as a service: A cloud based common capability," 2015 IEEE Conference on Communications and Network Security (CNS), Sep. 2015, doi: https://doi.org/10.1109/cns.2015.7346886.

7 M. Snehi, J. Snehi, and R. Dhir," Issues and Emerging Trends in Identity Management," International Journal of Computers Technology. [8] H. Liu, D. Han, and D. Li," Fabric-IoT: A Blockchain Based Access Control System in IoT," Journal of Computer Networks and Communications, 2020 doi.org/10.1109/ACCESS.2020.2968492

8 H. Liu, D. Han, and D. Li," Fabric-IoT: A Blockchain Based Access Control System in IoT," Journal of Computer Networks and Communications, 2020 doi.org/10.1109/ACCESS.2020.2968492

9 C. Liu, R. Tan, Y. Wu, Y. Feng, Z. Jin, F. Zhang, Y. Liu, and Q. Liu," Dissecting Zero Trust: Research Landscape and Its Implementation in IoT,"

10 T. Kodam," A Roadmap for Ensuring SAML Authentication Using Identity Server for On-Premises and Cloud," M.Sc. thesis, Dept. of Computer Science, Erasmus University Rotterdam, 2019. https://www.divaportal.org/smash/get/diva2:1316547/FULLTEXT01.pdf.

11 M. K. Hamza, H. Abubakar, and Y. M. Danlami, "Identity and Access Management System: A Web-Based Approach for an Enterprise," Path of Science, Nov. 2018, doi: https://doi.org/10.22178/pos.40-1.

12 Georgios Katsikogiannis, S. Mitropoulos, and Christos Douligeris, "An Identity and Access Management approach for SOA," Dec. 2016, doi: https://doi.org/10.1109/isspit.2016.7886021.

13 B. H. PETERSON, "Managing Multiple Identities," Journal of Accountancy, Sep. 2008. https://www.journalofaccountancy.com/issues/2008/sep/managing- multiple-identities.htm

14 Olivier Toelen, "Identity and Access Management,", Apr. 2018, doi: https://doi.org/10.1002/9781119549413.ch4.

15 P. Arias-Cabarcos, F. Almena´rez-Mendoza, A. Mar´ın-Lo´pez, D. D´ıaz-Sa´nchez, and R. Sa´nchez-Guerrero, "A Metric-Based Approach to Assess Risk for 'On Cloud' Federated Identity Management," Journal of Network and Systems Management, Jul. 2012, doi: https://doi.org/10.1007/s10922-012-9244-2.

16 M. Hummer, S. Groll, M. Kunz, L. Fuchs, and G. Pernul, "Measuring Identity and Access Management Performance an Expert Survey on Possible Performance Indicators," Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018, doi: https://doi.org/10.5220/0006557702330240.

17 M. C. Mont, Y. Beresnevichiene, D. Pym, and S. Shiu, "Economics of Identity and Access Management: Providing decision support for investments," 2010 IEEE/IFIP Network Operations and Management Symposium Workshops, 2010, doi: https://doi.org/10.1109/nomsw.2010.5486588.

18 A. Hindle, "Impact of GDPR on Identity and Access Management," IDPro Body of Knowledge, vol. 1, no. 1, Mar. 2020, doi: https://doi.org/10.55621/idpro.24.

19 T. D. Breaux and A. I. Anton, "Analyzing Regulatory Rules for Privacy and Security Requirements," IEEE Transactions on Software Engineering, Jan. 2008, doi: https://doi.org/10.1109/tse.2007.70746.

20 A. Cormack, "An Introduction to the GDPR (v2)," IDPro Body of Knowledge, Jun. 2021, doi: https://doi.org/10.55621/idpro.11.

21 Pooya Jaferian, "User-centered design of identity and access management systems," Jan. 2014, doi: https://doi.org/10.14288/1.0167054.

22 M. Kunz, A. Puchta, S. Groll, L. Fuchs, and G. Pernul, "Attribute quality management for dynamic identity and access management,", Feb. 2019, doi: https://doi.org/10.1016/j.jisa.2018.11.004.

23 E. Axel Larsson, "A case study," Nov. 2005, doi: https://doi.org/10.1145/1099435.1099472.

24 I. A. Mohammed," Cloud identity and access management – a model proposal," Journal of Innovations in Engineering Research, 2019.

25 M. Waters," Evaluating identity and access management (IAM) as a cloud service," Research Gate, Sept. 2016.

26 J. Basney, H. Flanagan, T. Fleury, and J. Gaynor," CILogon: Enabling federated identity and access management for scientific collaborations," 2019. https://pos.sissa.it/351/031/pdf.

27 A. Karantjias, T. Stamati, and N. Polemi," A Synchronous, Open, User-Centric, Federated Identity and Access Management System (OpenIdAM)," Electronic Journal of., 2009.

28 S. Mandru," Privileged Access Management and Regulatory Compliance," Journal of Artificial Intelligence, Machine Learning Data Science, 2024.

29 S. K. Mandru," PAM (Privileged Access Management) and DevOps: Secure Management of Privileged Accounts," Journal of Artificial Intelligence, Machine Learning Data Science, 2022.D. H. Sharma, C. A. Dhote, and M. M. Potey," Identity and Access Management as Security-as-a-Service from Clouds," Procedia Computer Science, vol. 85, pp. 132-139, 2016. https://www.sciencedirect.com/science/article/pii/S1877050916002489/pdf.

30 T. H. Vo, W. Fuhrmann, K. P. Fischer-Hellmann, and S. Furnell," Identity-as-a-Service: An Adaptive Security Infrastructure and PrivacyPreserving User Identity for the Cloud Environment," Future Internet, vol. 11, no. 5, 2019. https://www.mdpi.com/1999-5903/11/5/116/pdf.

31 D. Ferraiolo, J. Cugini, and D. Kuhn, "Role-Based Access Control (RBAC): Features and Motivations."