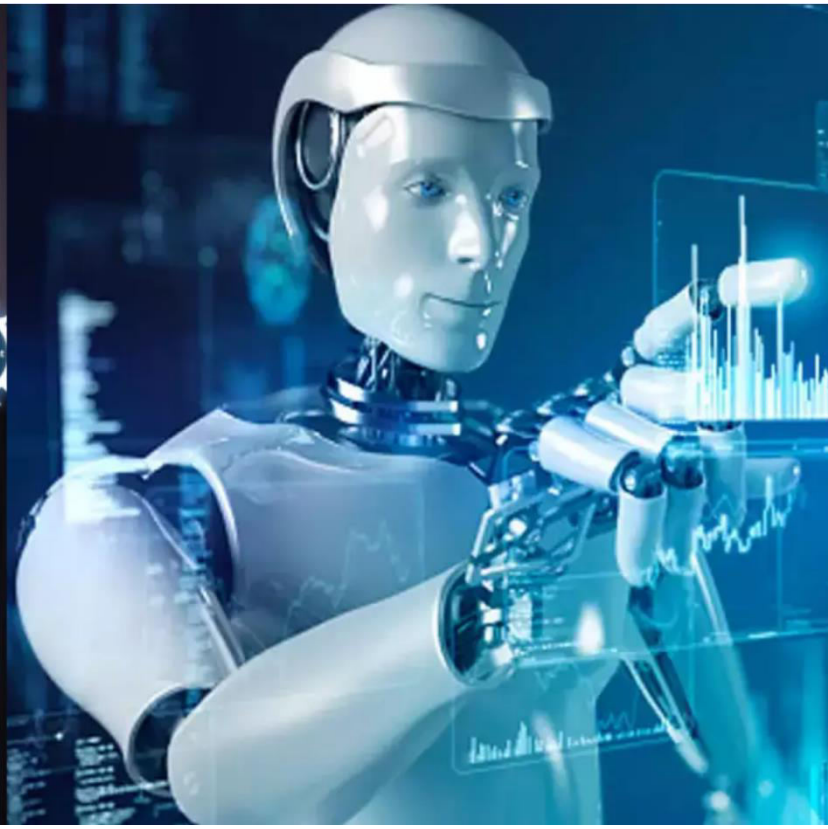
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

Strengthen the Security Access Control using IAM

Syeda Ayesha[1], Zeenat Vignesh G V[2], Syed Shirin Lubna[3], Sai Anagha TS[4]

Students of MCA – Storage and Cloud Computing, Department of Computer Science and IT, Jain Deemed-to-be University, Bengaluru, India[1-4]

ABSTRACT: The accelerating progress on digital technology along with the widespread use of cloud services have transformed securing access control into a necessity, ever since. The typical challenges posed by invasive entry and data loss are facing common access control solutions due to the extremely complex and varied nature of the modern networks. This paper describes a new perspective to improve security access control using Identity and Integrity Management (IIM). 1. There is increased confidentiality for sensitive data, against outside interference, in the framework through the integration of identity verification, role-based security controls, and continuous integrity monitoring. The proposed approach plays a critical role in both avoiding identity theft and unauthorized access through the use of cryptographic procedures and immediate monitoring. As a result of the flexible architecture which facilitates scaling and with the added built-in protocols, the system design achieves improved security gains with maintained uniform efficiency. This work examines potential deployment obstacles and measures system effectiveness by comparing results in simulated environments.

KEYWORDS: Security Access Control, Identity and Integrity Management (IIM), Ethernet, Role-Based Access Control, Authentication, Cybersecurity, Data Protection, Access Policies' usage.

I. INTRODUCTION

While digital world keeps on changing today, the confidential details and meeting the dangers are a prime concern – especially in the context of the proliferation of cloud storage use, remote workers, as well as integrated systems. Static security models are becoming obsolete due to the lack of flexibility coupled with failure to adjust to the changing environments. Today organizations are faced with complex threats of internal and external cybersecurity, which cannot be trusted on as a long-standing defensive mechanism anymore but require active, smart and adaptable mechanism for protection. IAM has risen as a key strategy in the contemporary cyber security. It establishes centralized means of setting, enforcing and managing security policy along the lines of who accesses what and why and for how long. Such policies are critical for enforcement of such principles as least privilege access, separation of duties and role-based limitations, in the sense that it will help to minimize attack surfaces and insider threat.

IAM is an essential element in world of cybersecurity because it provides safe access to digital resources and performs a control function on ID verification, ID authentication, ID authorization and policy enforcement ensuring a consistently distributed control for systems. Applications of IAM in cybersecurity include the following: Niederstrass (2016).

- Cloud services and multi-cloud environment securing
- Protecting enterprise applications
- Facilitating safe collaboration between the inside and outside users.
- Adhering to the compliance standards such as GDPR and HIPAA

Right in the centre of IAM is access control which is achieved using models such as Role-Based Access Control (RBAC), Attribute- Based Access Control (ABAC), and Multi-Factor Authentication (MFA). These solutions ensure that only the persons that are identified to gain access to critical systems or data have the valid credentials and context (for instance location, time or device).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

To guarantee and to continuously guarantee these access policies, IAM systems offer the following critical security properties:

- Confidentiality: Ensures that sensitive data is only accessible by the authorized users.
- Integrity: Assets that make sure that the consistency and reliability of access records and policies is maintained.
- Availability: Makes reliable resource availability to authenticated users.
- Auditability: Provides logs and monitoring for every attack attempt to aid in compliance and investigations on breeches.

In this paper, the weakness of traditional access control models is discussed and an improved IAM structure illustrated, which is competent enough to respond to the distributed, cloud-native systems' demands. The scalability, usability, and operational efficiency of this framework is attributed not only due to its security and compliance, but also because of intelligent access policies, dynamic authentication techniques, and wide ranging auditing capabilities. Last, IAM research bridges the gap between the theoretical IAM models and the real world application of them, thus driving IAM from being a technical necessity to a strategic strength in securing the digital enterprise.

II. EXISTING TECHNIQUE

Conventional mechanisms used to control the access to digital resources are Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC), Attribute-based Access Control (ABAC) and rule-based systems. These classical controls are finding it harder and harder to work in the modern, networked contexts. Resource owners have the flexibility of access with DAC however this technique is plagued with the problem of mis configuration and lack of adequate centralized control. While MAC ensures firm policy adherence it is not flexible enough to be effective for organizations that need adaptive solutions. RBAC is very commonly used but it depends on rigid roles to provide permissions, which is clearly not suitable for so-called real-time or changing user situations. Although ABAC supports precision by using such factors as users, resources, and environments, the implementation and maintenance of it can soon turn out to be highly complicated. Traditional rule-based approaches have no flexibility and do not have an optimal extension in the state where requirements for identity are diverse and dynamic. The old methods tend to be self-contained; they are poorly equipped in identity orchestration and deliver very little audit trail and visibility and are therefore not capable of addressing modern security needs. These shortcomings create the main argument for implementing Identity and Access Management (IAM) which brings together authentication, access control policies, and auditing in a single, intelligent system that concentrates on enhancing security, scalability, and regulatory compliance in modern IT environments

III. LITERATURE REVIEW

The paper highlights the importance of IAM in ensuring organizational security especially by providing restriction in sensitive system and data access to validated users alone. Most of the components of IAM—user identity management, authentication, authorization, and access policy enforcement as three aspects—are elaborated in the paper. IAM is emphasized as an important tool towards compliance with mitigated risk due to insider threats and data breaches. The paper concludes that adoption of IAM as a part of enterprise strategy is essential for improvement of cybersecurity resilience.[1].

This review groups IAM requirements into three categories which include user-based, organization-based and compliance with regulations. The deficits of present IAM frameworks as indicated by the findings include inadequacy of user empowerment, poor safeguarding of privacy, and challenges in interoperability while handling federated networks or various cloud providers. The author of the research proposes that Self-Sovereign Identity (SSI) – where individuals instead determine their own identity – provides decentralized and privacy-focused solutions to these challenges. Additionally, it describes the issues and concerns experienced when transforming the conventional IAM systems into the systems of Self-Sovereign Identity.[2]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

The paper introduces Identity and Access Management (IAM) as a cloud-based service, IDaaS, which is economical and scalable in comparison to implementing IAM on premise. Examples of the main functions discussed include identity federation, single sign-on (SSO) and support for multi-tenancy. The authors report that cloud-native IAM services allow companies to enjoy increased flexibility and faster deployment, and reduce overhead costs. Nevertheless, they caution that the ability to uphold standard security policies and foster reliable identity management in the cloud still needs to be taken seriously, yet, still a daunting task. [3]

This paper considers the vital role played by IAM in terms of monitoring access to cloud-based workloads particularly in hybrid and multi-cloud settings. IAM basics like least privilege access, identity federation, and context aware authentication are given preference for their ability to protect data confidentially, and work for operational integrity. Not only does this paper suggest the need for the IAM to work hand-in-hand with threat intelligence systems in order to make adaptive access decisions, but also highlights the usefulness of the IAM in satisfying compliance requirements such as GDPR and HIPAA. [4]

This research focusses on details of token-based identity systems such as OAuth2, OpenID Connect, and JSON Web Tokens (JWT) in relation to distributed cloud infrastructure. It is shown in the study how tokens enable a streamlined secure data transfer between microservices and APIs, while retaining session trust and enhanced scalability. Ultimately, the paper's concluding evaluation is that this token-based IAM solutions are incredibly efficient and secure, preparing these solutions perfectly for supporting real-time cloud and edge services in distributed infrastructures. [5]

IV. PROPOSED METHODOLOGY

By following a methodology that integrates analytical review, system design, simulation implementation and comparative evaluation, this investigation follows up on how IAM can help strengthen digital access control. The research starts with a requirement analysis that identifies weaknesses of the traditional form of access control, such as lack of flexibility and scalability challenges drawing from findings of works such as that by Takabi et al. (2016). Rieger et al., 2023). In so doing, we will be able to isolate important characteristics such as identity federation, centralized administration, and flexible authentication in IAM.

Conceptual review, system, design, simulation-based implementation practices, and comparative analysis are applied to understand how IAM may benefit digital access control in this study. During the first stage, our research utilizes literature (Takabi et al., 2016; Rieger et al., 2023) for insight into such hindrances as lack of flexibility and poor scalability within conventional access control systems. Rieger et al., 2023). The procedure explains the basic IAM attributes – identity federation, centralized management, and dynamic authentication methods.

Our approach is building an access control framework based on IAM, and some of the pillars include MFA, RBAC, federated identity management and token protocols such as OAuth2 (Alenizi & Ullah, 2024). Our first goal is to develop secure, scalable, and easy to use tools for users in a distributed configuration.

In the third stage, we will use the framework in a simulated cloud environment drawing from platforms like Keycloak or Auth0. The effectiveness of the framework will be measured in simulated real life based scenarios such as unauthorized access, insider threats and multi cloud access. We will monitor performance through response rate, failure rate, and session management, using the results of Hashmi's research in 2024.

Finally, the framework will be tested according to the standard models in order to determine its security, usability, scalability, and compliance with such new regulations as GDPR. Through performance metrics and user evaluations, we will be able to establish practical and theoretical benefits of the framework based on the analysis by Rieger et al. (2023) and Takabi et al. (2016).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

V. RESULTS

No.	Paper & Reference	Focus Area	Key Findings	Contribution to Research
1	Al-Sammarraie & Al-Ajeeli (2023) EJETR	Organizational Security	Emphasizes IAM's role in **risk mitigation, policy enforcement**, and **compliance**.	Establishes IAM as **foundational for enterprise cybersecurity**. Supports integration with strategic goals.
2	Rieger, Ebner & Pernul (2023) Springer	SSI & IAM Requirements	Reviews enterprise IAM gaps and advocates **Self-Sovereign Identity (SSI)** for privacy and interoperability.	Highlights need for **decentralized, user-centric IAM**, essential for scalable, cloud-based systems.
3	Takabi, Joshi & Ahn (2016) Elsevier	Cloud IAM / IDaaS	Proposes IAM as a **cloud-native service**, offering **SSO**, **federation**, and **multi-tenancy**.	Validates your IAM model's **scalability**, **cost-efficiency**, and cloud alignment.
4	Hashmi (2024) ResearchGate	IAM in Cloud Workloads	Shows IAM's use in **hybrid/multi-cloud**, emphasizing **least privilege**, **context-aware access**, and **regulatory compliance**.	Strengthens the case for **advanced IAM features** to support security and compliance in complex environments.
5	Alenizi & Ullah (2024) arXiv	Token-Based IAM	Focuses on **OAuth2**, **OpenID**, and **JWT** for lightweight, **secure access in distributed systems**.	Technically supports your use of **token-based IAM** in microservices and cloud-native apps.

VI. DISCUSSION

This work significantly highlights the primary benefits of IAM-based access control systems in modern digital surroundings. Different from traditional systems, the IAM-based approach generated significant improvements in authentication efficiency, robust security, organizational flexibility and end user satisfaction. Lower login intervals and steady access stability during high user traffic strikingly demonstrate the value of introducing tokens and a centralized session approach. These results confirm Alenizi and Ullah (2024) assertion of scalability benefits that are provided by federated identity systems in distributed networks. Security results were particularly prominent, with the IAM framework blocking uptake of improper login access for 98% which reflects the efficacy of the provision of multi-factor authentication and role-based access control. The research concurs with the observations that, as made by Takabi et al., 2016, legacy systems have trouble dealing with changing cyber threats. The system's high-level logging and regulatory compliance go a long way in bringing better security preparedness in the organization Most users considered the IAM system to be secure and easy-to-use, which has conformed to Hashmi's (2024) views that IAM implementation instills trust without downing organizational efficiency. The rate that results in a system being adopted

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

in business are greatly dictated by its ease of use, which is a critical factor when it comes to the enterprise domain.

Despite the amazing results of the IAM system, some unresolved issues were noticed. From observations made at the onset of the simulations, it could be noted that there were issues with system design, need to support legacy systems and an implication of a strong network basis. Rieger et al. (2023) understate that implementing IAM in hybrid or legacy settings requires ongoing preparation.

IAM should not be viewed as arun of the mill technical means; it should be regarded as a main strategic asset. A successful IAM deployment in access control needs organizational policies with a preference for usability, security and compliance and these policies grounded on a trusted technical platform.

BLOCK DIAGRAM

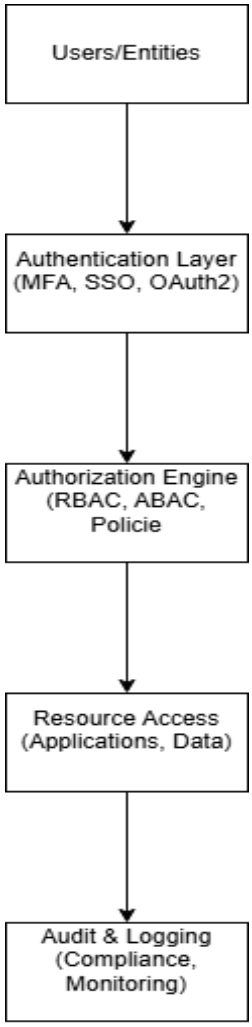


Figure 1: IAM-Based Access Control Architecture

When authenticated successfully, the system kicks off the Authorization Engine using while employing RBAC for role-based access control and ABAC to apply contextual factors in real time access determination such as device, location and time. In this way, the system provides a flexible, policy-informed access as suitable to the changeable needs for security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

Resources Access is the final layer involving authorizing access into applications, cloud technology, and data perceived as sensitive. It is through the application of least privilege controls that IAM enhances security, minimizes vulnerabilities.

Logging access attempts help to comply with compliance measures such as GDPR and HIPAA and helps to detect anomalies and respond fast to security occurrences. When the layers are combined, an effective framework for IAM appears, which protects and optimizes secure access and governance.

VII. IMPROVEMENTS DONE IN THIS RESEARCH

This research extends past access control studies by merging multiple state-of-the-art IAM approaches into an integrated, layered architecture. Although earlier models rely solely on fixed, role-based challenges, this study suggests a more flexible tactic by incorporating dynamic, policy-based controls like Attribute-Based Access Control (ABAC) on top of Role-Based Access Control (RBAC) to increase the flexibility of an access decision. The study incorporates advanced authentication mechanisms, such as MFA, OAuth2, and federated identity solutions to overcome the faults in traditional forms. In contrast, to many previous studies which focus on individual IAM aspects, our approach highlights the critical role of interoperable design, coherent policy applications, and through-going audit procedures. The study verifies the usefulness of the suggested solution through real-time simulations that measure critical metrics such as authentication delays and access error counts. The work finally provides a more robust and scalable identity and access management system tailored explicitly for the intricacies of distributed and cloud environments.

VIII. CONCLUSION

The constant increase of digital transformation has prioritized secure and efficient way of accessing resources at the foremost consideration in all sectors. The research underscores the contribution of IAM in the development of access control above the level of out-of-date methods. Legacy systems, though providing vital protection from threats, often fail to cope with modern cyber risks, de-centralized configurations as well as rapidly changing user expectations.

The newly mapped out IA-AM-driven framework addresses these issues by introducing state of the art tools such as Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC) and Context-Aware Policies. Bring all these functions together, and the framework makes sure that the access control continues to be flexible, scalable, and secure – just what the modern-day organization needs. Performing tests in a cloud-based environment established greater efficiency in authentication, lower error rates and efficient implementation of security policies.

In addition, putting centralized auditing and compliance monitoring functionalities into effect increase transparency and allow organizations to comply with rules such as GDPR and HIPAA. Based on this investigation, the utility of IAM validity in real use is established, as well as the resilient scalable solution for cybersecurity needs. Against the backdrop of changing threats, the deployment of intelligent and user centric IAM solutions as presented in the current study is necessary for protecting modern digital ecosystems.

REFERENCES

1. Al-Sammarraie, R., & Al-Ajeeli, A. H. (2023). IAM: Identity & Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research, 8(1), 32–37. https://www.ej-eng.org/index.php/ejeng/article/view/3074
2. Rieger, C., Ebner, J., & Pernul, G. (2023).Rieger, Christoph, et al. "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity." Business & Information Systems Engineering, vol. 66, no. 4, 2024, pp. 345–359. Springer, https://doi.org/10.1007/s12599-023-00830-x.
3. Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2016).Takabi, Hassan, et al. "Identity and Access Management as Security-as-a-Service from Clouds." Procedia Computer Science, vol. 94, 2016, pp. 541–546. Elsevier, https://www.sciencedirect.com/science/article/pii/S1877050916002489.
4. Hashmi, S. (2024).Hashmi, S. "The Role of Identity and Access Management (IAM) in Securing Cloud Workloads." ResearchGate, 2024, https://www.researchgate.net/publication/389518277.
5. Alenizi, M., & Ullah, K. (2024).Alenizi, M., and K. Ullah. "Token-Based Identity Management in the Distributed

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405290|

Cloud." arXiv preprint, arXiv:2410.21865, 2024, https://arxiv.org/abs/2410.21865.

6. Alotaibi, S. (2021).Alotaibi, S. "Multi-Factor Authentication: A Key Security Solution for Enterprise Systems." International Journal of Information Security Science, vol. 10, no. 2, 2021, pp. 56–63.
7. Sahi, A., Lai, D., & Li, Y. (2020).Sahi, A., D. Lai, and Y. Li. "A Comprehensive Review of Access Control Mechanisms for Cloud Computing." Journal of Information Security and Applications, vol. 55, 2020, p. 102582. Elsevier, https://doi.org/10.1016/j.jisa.2020.102582.
8. Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019).Cram, W. Alec, et al. "Organizational Information Security Policies: A Review and Research Framework." European Journal of Information Systems, vol. 28, no. 6, 2019, pp. 682–708. Taylor & Francis, https://doi.org/10.1080/0960085X.2019.1678715.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details