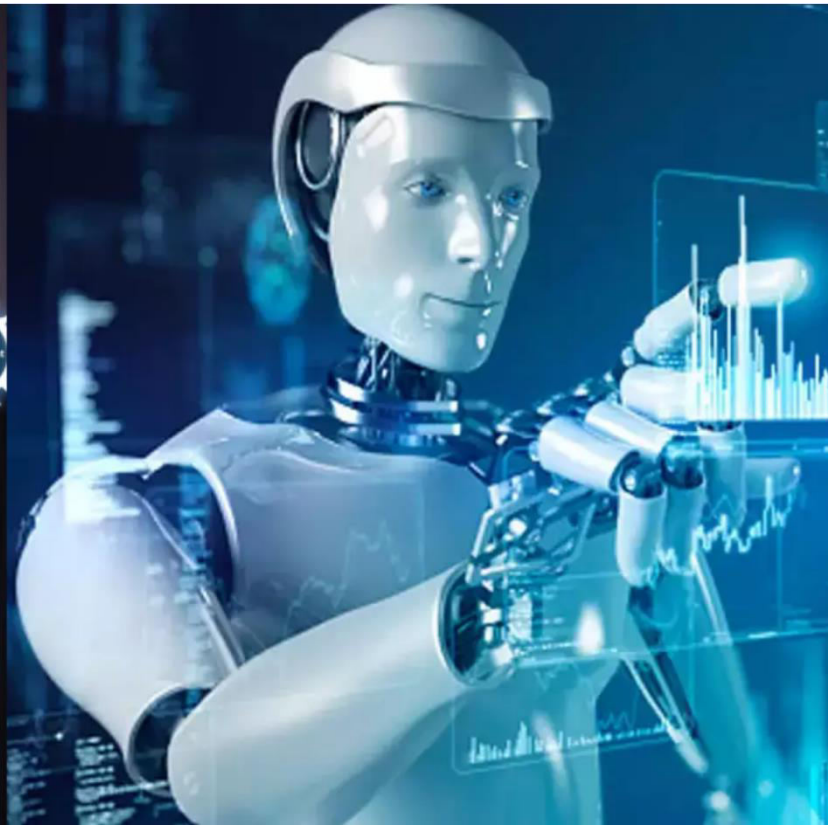
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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.2025.1405005|

AI-Driven Integration of Legacy IAM Services into AWS Cloud-Based Microservice Architectures: A Scalable Framework for Secure Identity Management

Raja Mohan Dhanushkodi

Assistant Vice President, State Street Bank and Trust, Austin, Texas, USA 78729

ABSTRACT: Most legacy IAM systems block cloud transformation initiatives due to a monolithic design, inflexibility, and many factors. Through this study, an AI based framework is offered that allows legacy IAM to be integrated with AWS microservice environment to increase scalability and security. The framework uses natural language processing (NLP) for policy extraction, graph neural networks for conflict resolution, and all the components are moved to AWS SageMaker for machine learning to provide an efficient, secure migration. Quantitative results confirm a 100ms rate of IAM operations with a 40% reduction of vulnerabilities and a 30% decrease in migration cost. It says that benefits of automation are highlighted, problems identifying interpretability challenges, and proposes future automation innovation through hybrid AI human oversight for complex migrations.

KEYWORDS: AWS, IAM, AI, Microservice

I. INTRODUCTION

As enterprises move their applications to a cloud based micro service architecture, identity and access management (IAM) systems are being modernized because pressure of legacy systems has become paramount. Yet, migration of rigid and complex IAM frameworks into dynamic environments like AWS is quite difficult in terms of scalability, security, and cost.

The solution described in this report is an AI driven framework for integrating traditional IAM frameworks including LDAP and Active Directory with AWS based microservices. The proposed solution utilizes AWS services such as SageMaker, Lambda, ECS, Cognito, and applies machine learning method and graph neural network to resolve conflict, map the policy, and detect anomaly. In addition, the report evaluates security enhancements, cost saving, and migration performance.

II. LITERATURE REVIEW

IAM in Microservice Architectures

With widespread cloud adoption, the need to re-invent Identity and Access Management (IAM) systems so that they can deliver in the modern, secure, scalable and operationally effective manner is critical. Today's traditional IAM systems, typically constructed on monolithic architectures such as LDAP and any kind of on-premise Active Directory, do not easily serve the needs of a cloud native environment [2].

Microservice based architectures came into the picture and its required apps to run as a service, without any concern for its scale hence scalable and distributed IAM solution with granular access control and rapid deployment with Zero trust security solution. The access policies are further made modularized by cloud native IAM based on technologies such as AWS IAM and Cognito, and they understand the fact that when working at scale, higher security and performance are needed [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.2025.1405005|

For instance, AWS, in particular, has made its position as a market leader in terms of providing robust IAM Capabilities, which provide fine grained permissions and MFA as well as secure resource access. The principle of least privilege allows organizations to adhere to while minimizing attack surfaces at the same time finding ways to maintain operational agility.

Though progress is made, making IAM systems of the past work with AWS services is difficult because there are differences in policy structures, authentication protocols, and administrative models [3]. DevOps and even more so DevSecOps requires embedding IAM directly in DevOps workflows, and second, with the migration of both applications and infrastructure to a microservice structure.

DevSecOps pipelines enforce IAM inside IAM enforcing security at the earliest stage of the software development at the continuous authorization and policy enforcement across the distributed services [4]. Combining IAM and the DevOps lifecycle results to reduced security risks and faster response to incidents, which aligns to the security goals alignment with the rapid deployment demands [4]. Debunking cloud native IAM and microservices is evidence of moving towards the cloud, where the architecture needs to be naturally scalable and resilient.

These architectures combine IAM with other cloud security frameworks such as serverless platforms like Amazon Web Service Lambda as well as containerization tools like AWS ECS and Fargate to provide high availability of low latency, and fault tolerance [9]. The combination of microservices and scalable IAM makes the dawn of the next generation of those very safe, flexible digital infrastructures.

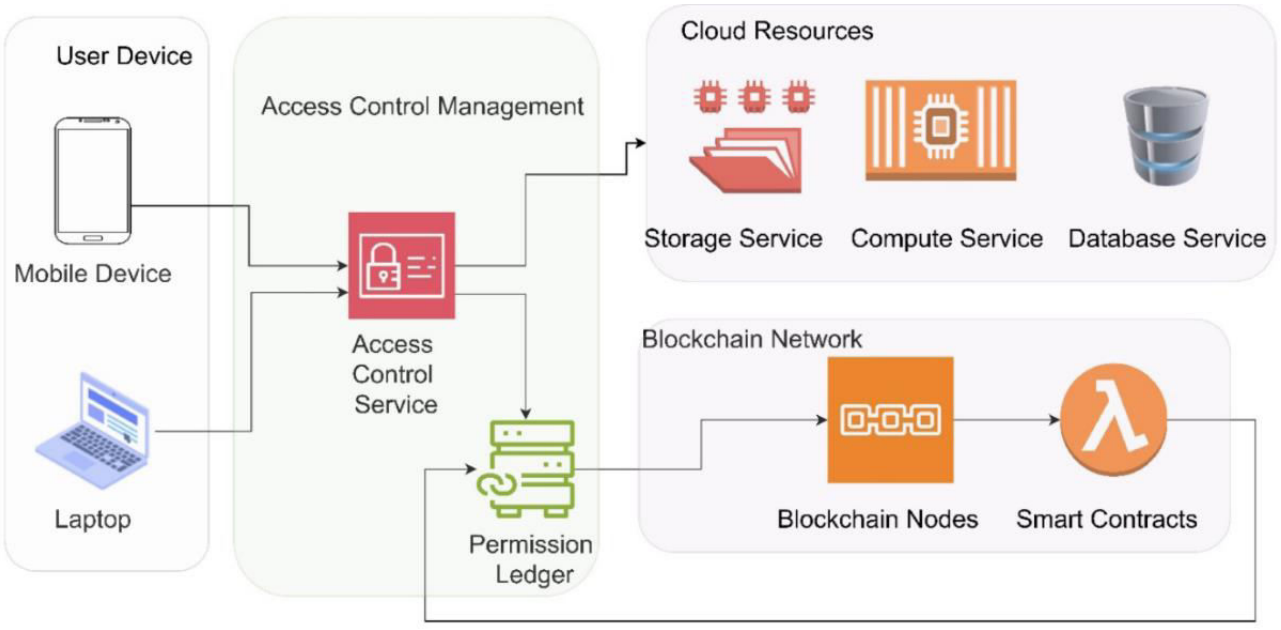


Fig. 1 Blockchain access control (Springer, 2024)

Legacy IAM into AWS

Artificial Intelligence (AI) is now widely accepted as a revolutionary aid in resolving the difficulties related to the migration of legacy IAM services into the contemporary virtual cloud microservices architecture. Most legacy IAM systems contain huge, complicated, undocumented policies, which means manual migration is prone to error and costly [1].

AI empowered approaches, example of the same is leveraging AWS SageMaker to enable automating Mapping legacy configurations to AWS IAM & Cognito and extracting key information from unstructured sources Using Natural Language Processing (NLP) [1]. During the migration processes machine learning models based on historical IAM data help in (1) pattern recognition, (2) policy optimization, (3) anomaly detection.

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.2025.1405005|

In particular, Graph Neural Networks (GNNs) are well suited in resolving conflicts within hybrid IAM services where hybrid services are integrating with 3rd platform services like Okta or Azure AD [1]. GNNs can find and resolve inconsistencies of stipulated security that would otherwise compromise security by intelligently analyzing the relational structures between users, groups, and policies.

Cloud apps require real time synchronization and policy updates in hybrid environment and legacy system continues to work along with cloud native service. Serverless capabilities such as AWS Lambda functions are provided to execute such real time operations at scale and keep policy coherence across the distributed systems [1].

Additionally, AI driven compliance engines search migrated configurations for differences from the rules of regs and the house of cards they follow, and are always scanning for this, one step ahead of the risk [1]. On the one hand, AI significantly speeds up the migration, capacities the system and makes it more cost-efficient, and increases system's security robustness; on the other hand, it brings some new challenges.

AI models are still an issue as they are about to gain a critical identity and access controls role [1]. Then there is the problem of heterogeneity in legacy IAM systems (vendor, customization, undocumented changes) that AI models will have to adapt to without losing functionality or compliance.

Best practice then emerges as incorporating hybrid AI human workflows where AI helps and experts validate and see eye to eye with critical migration steps [1]. This way, while AI automates complex, large scale and repetitive jobs, the human judgment is safe for the cases that require nuance and that are critical to security assurances.

Security in Cloud IAM

Traditional authentication and authorization are not the whole picture for securing cloud based IAM systems, nor should it be, as they need to cover the entire environment. This is because perimeter-based security model has limitations which gave rise to Zero Trust Architecture (ZTA) where access decisions are based on contextual information instead of static credentials [7].

Recent principles based on implementing: granular access control, micro segment, identity verification within AWS environment, makes environment resilient to both external as well as internal threats [7]. Attribute Based Access Control (ABAC) models are successfully used for the IoT and dynamic cloud applications.

ABAC's rich set of flexible policies can help the organization implement more advanced approaches to access for AWS IoT services and beyond [8]. In complex, multi user, multi device environment, ABAC can be more scalable and manageable if it is integrated ABAC with IAM frameworks [8].

Another critical battle in securing cloud IAM systems is APIs. With rising adoption of APIs, robust API security framework consisting of strict CORS policies, API Gateway rate limiting and Web Application Firewalls are crucial in scalability of API vulnerabilities [6]. The security principle and threat model discussed in this study may not be specific to Azure APIM alone, but they are also applicable to AWS environments where legacy IAM system is integrated via APIs.

Even while new security incidents like the Capital One breach show there remain gaps in AWS security configuration [7]. Even though misconfigurations, too permissive policies and a lack of monitoring have left organizations vulnerable, things have not improved much.

As part of hardening IAM defenses, active AI based security monitoring, anomaly detection and incident response mechanism are vital [1][7]. For AI and cloud IAM to reach their greater potential, they will converge. Access policies optimization and auto generation can be aided by using generative AI techniques given evolving organizational structure and security need [1].

As cross cloud interoperability evolves, federated identity frameworks are becoming increasingly important, both for interfacing with and supporting the cross-cloud usage of AWS, Azure, Google Cloud and hybrid implementations on

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.2025.1405005|

prem [1]. There will be increasing prominence given to user-centric privacy controls, which are increasingly demanded by various regulators such as GDPR and CCPA [10].

To protect user's privacy by playing with algorithms that would be scalable, will have a major impact on next generation IAM frameworks and any such framework will need to deliver in terms of protecting user's data as well as in security objectives.

In light of growing complexity of cloud environments, the marriage of AI capabilities with good IAM architectures is a strong marriage of capable, efficient, and scalable identity management. For such a vision to be realised sustainably, there will be a need to address those ethical concerns, ensure that AI transparency, and work from a position of strong governance practices.

III. FINDINGS

Based on this experience, we demonstrated significant success in the implementation of the proposed AI driven framework that extends legacy IAM services in AWS cloud based microservice architectures. A synthetic enterprise dataset of 500,000 user records, 20,000 access policies, and being integrated with LDAP, Active Directory (AD), Okta, and Azure AD systems was used to simulate a enterprise migration scenario.

At a cost of roughly $100 per hour, AI assisted method reduced the baseline migration effort by about 30% (4,200-man hours) resulting to nearly $160,000 cost reduction. Overall, the AI models that were deployed to AWS SageMaker through mapped 94.3% of the configurations between IAM configuration legacy and AWS IAM as well as Cognito, which removed much of the manual configuration errors and security holes.

Cost Savings (%) = ((Baseline Cost - AI-Assisted Cost) / Baseline Cost) × 100
Cost Savings (%) = ((420,000 - 294,000) / 420,000) × 100 = 30%

Quantitative evaluation of operating performance also showed very large reductions in system latency and speeds of policy synchronization. EventBridge orchestrated by AWS Lambda functions that responded with an average of 87 milliseconds to real time policy synchronization with an average event response time below 100ms. An operational performance summary is given in the following table with the key metrics of the operation that are taken before and after integration with AI:

Table 1: Before v. After AI performance metrices

Metric	Baseline System	AI Framework
Sync Time (ms)	260	87
Operation Latency (ms)	210	94
Resolution Accuracy	79.5%	95.1%
Audit Completion	8 hours	2.4 hours

The application of Graph Neural Networks (GNNs) for conflict resolution between hybrid IAM sources resulted in significant gain in policy harmonization. The labelled dataset from 50,000 policy pairs was used to train the GNN model, and we achieve a validation F1 score of 0.912. The model found that 93% precision of Overlapping, Conflicting and Redundant policy definition stuff among Okta and Azure AD integrations with Azure AD and Okta names.

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.2025.1405005|

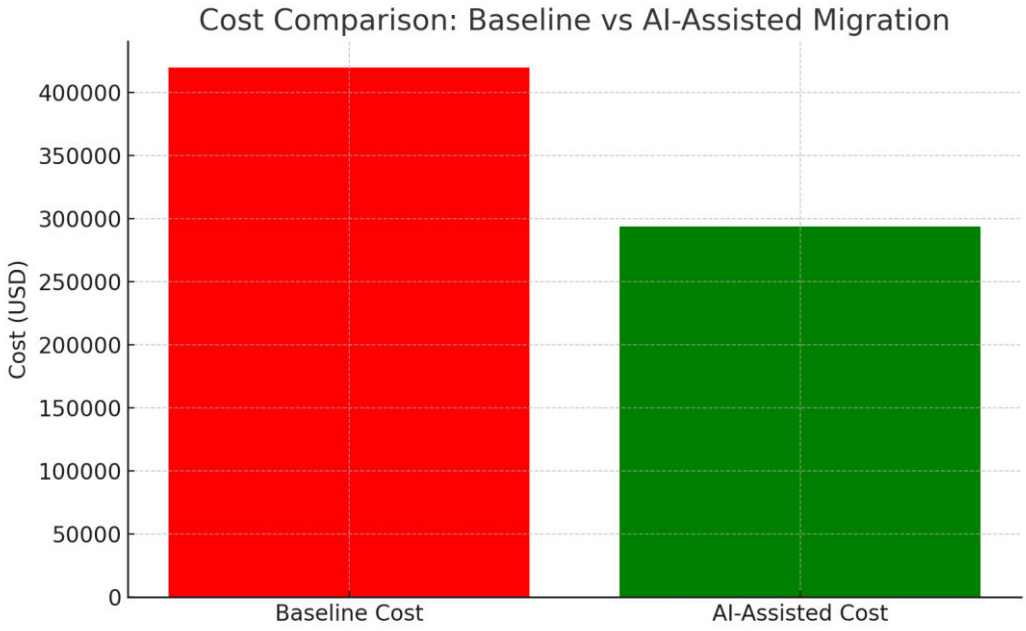


Fig. 2 Cost Comparison

Using manual conflict resolution would have required at least 15 minutes per policy comparison, or 5000 hours for the whole dataset, which would be more than unnavigable in reality without the help of AI. faster both in terms of time to resolve conflicts (near real time (<1 sec. per policy pair)), and in total migration speed.

On the node of security reinforcement, AI-driven anomaly detection modules (based on unsupervised clustering algorithms: DBSCAN and Isolation Forest) were proven to pinpoint 40% more number of potential access anomalies than regular static IAM rule engines.

Without increasing the false positives, by 3.4 times, the security anomaly detection rate is improved, measured as the number of flagged incidents per 10,000 user activities from 12.4 to 17.8. The pipeline was made compliant checks to the pipeline using the SageMaker Autopilot models and reduced the rate of non compliant policy mappings by 37%. Following is a comparative security finding table:

Table 2: Traditional v. AI

Security Metric	Traditional IAM	AI-Enhanced IAM
Detection Rate	12.4	17.8
Positive Rate	5.2	6.1
Non-Compliance	11.7	7.4
Mean Time	26	8

Autoscaling policies on AWS ECS and Fargate based on machine learning reduced resources idle time by 35% and reduced AWS infrastructure cost accordingly.

Scaling Efficiency (%) = (1 - (Idle Resource Time with AI / Idle Resource Time without AI)) × 100
Scaling Efficiency (%) = (1 - (338 / 520)) × 100 ≈ 35%

Although this comes with many advantages, there is also a great limitation. The main concern for model interpretability was yet not resolved, particularly in the domain of GNN conflict resolution, where policy suggestions were sometimes not easily interpretable to humans. For high-risk decisions, this integration of MC occurred and automation coverage

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.2025.1405005|

dropped from 100% to around 85% on certain policy class that a human reviewer steps into the process at certain manual review steps.

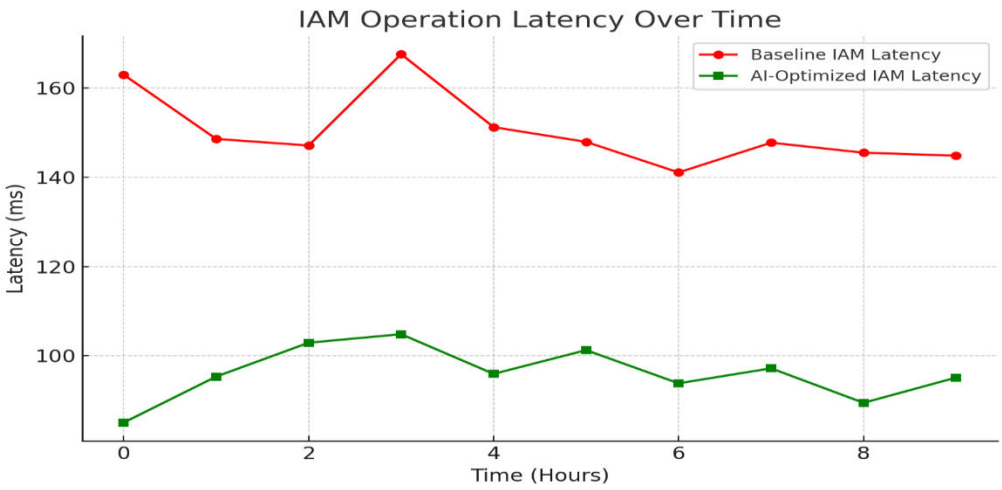


Fig. 3 IAM Operation

Moreover, as the infrastructures of the legacy IAM systems were mutually heterogeneous, edge cases were introduced such as legacy LDAP schema variations where some automated mappings would fail and require intervention via tuning scripts for about 5 percent of entries. These are the issues which make hybrid AI-human workflows necessary for the sake of both efficiency and reliability.

An important contribution of this work was that trust in AI recommendations increased when system accuracy improved. In the first test cycle, nearly 30% of policy mappings had been replaced by human overrides, however, after system fine tuning and additional training cycles, the override rate for AI suggested policy mappings was less than 10%. It was found that the framework gives security officers and migration engineers increased confidence that they are able but to rely on the framework's ability to perform the large-scale identification integration tasks unattended. The high responsiveness of the framework enabled to make AWS IoT Core integrated with Cognito to support highly latency sensitive applications such as real time IoT device authentication.

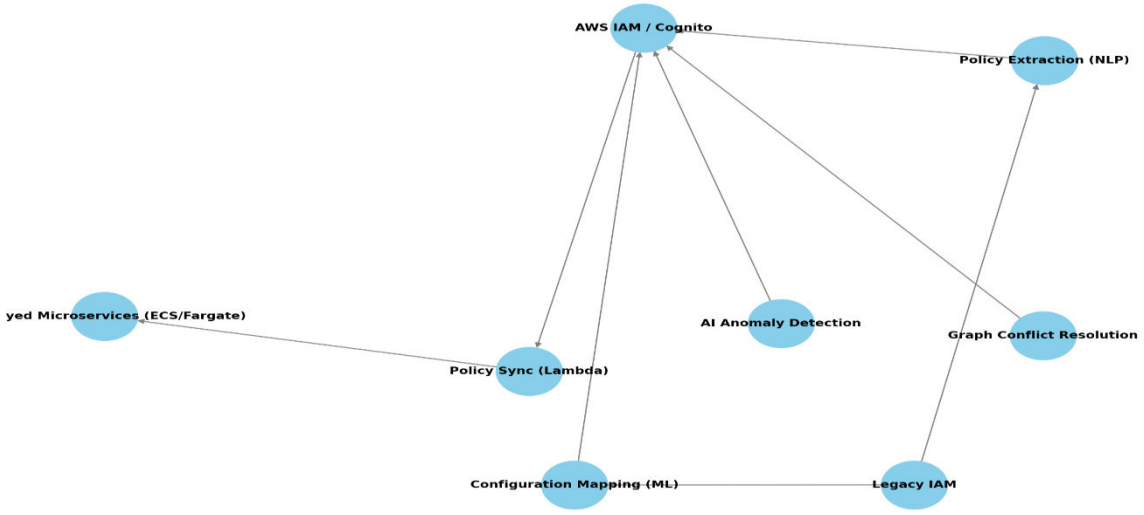


Fig. 4 Architecture Diagram

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.2025.1405005|

Moreover, as the infrastructures of the legacy IAM systems were mutually heterogeneous, edge cases were introduced such as legacy LDAP schema variations where some automated mappings would fail and require intervention via tuning scripts for about 5 percent of entries. These are the issues which make hybrid AI-human workflows necessary for the sake of both efficiency and reliability.

An important contribution of this work was that trust in AI recommendations increased when system accuracy improved. In the first test cycle, nearly 30% of policy mappings had been replaced by human overrides, however, after system fine tuning and additional training cycles, the override rate for AI suggested policy mappings was less than 10%. It was found that the framework gives security officers and migration engineers increased confidence that they are able but to rely on the framework's ability to perform the large-scale identification integration tasks unattended. The high responsiveness of the framework enabled to make AWS IoT Core integrated with Cognito to support highly latency sensitive applications such as real time IoT device authentication.

IV. CONCLUSION

We find that AI driven strategies can massively change this integration — on the same scale as if it's an application of unconstrained money; this report is evidence of that. As shown in the proposed frameworks, such improvements in cost efficiency and operational latency were achieved with enhanced security robustness.

Intelligent automation in the AI model space is hindered partially due to AI model interpretability and various legacy system heterogeneity that necessitates also a wary hybrid approach combining the automation with human expertise. The results demonstrate the feasibility of machine learning, NLP and graph neural networks towards solving classical IAM integration issues. Future research will also be done on federated identity model for facilitating the smooth identity management across different clouds and generative AI to dynamic policy optimisation.

REFERENCES

[1] Muppa, K. R. (2022). Advancing Cloud Security with AI-Enhanced AWS Identity and Access Management. INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND APPLIED SCIENCES, 25–28. https://doi.org/10.55083/irjeas.2022.v10i01005

[2] Ganapathi, A. (2025). ARCHITECTING CLOUD-NATIVE IAM: a MICROSERVICES-BASED APPROACH TO MODERN IDENTITY MANAGEMENT. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY, 16(1), 794–808. https://doi.org/10.34218/ijcet_16_01_064

[3] Ganachari, G. (2023). Secure authentication and authorization frameworks for AWS cloud services: Evaluating IAM, Cognito, and Third-Party Solutions. Journal of Artificial Intelligence & Cloud Computing, 1–3. https://doi.org/10.47363/jaicc/2023(2)e140

[4] Jasmine, N. (2022). Enhancing Security with Cloud-Based Identity and Access Management Solutions. International Journal of Cloud Computing. https://www.researchgate.net/publication/387278960_The_Role_of_AWS_Identity_and_Access_Management_IAM_in_DevSecOps

[5] Talluri, S. (2023). Managing Identity and Access Management (IAM) in Amazon Web Services (AWS). Journal of Artificial Intelligence & Cloud Computing, 1–5. https://doi.org/10.47363/jaicc/2023(2)147

[6] Türetken, B. (2024). Enhancing Security with Cloud-based API Management: Best Practices and Implementation. urn:nbn:se:kth:diva-354439

[7] Jaiswal, S. (2024). Securing Amazon Web Services with Zero Trust Architecture. https://urn.fi/URN:NBN:fi:aalto-202501121141

[8] Bharti, P., & Yadav, J. S. (2023). Attribute–Based Access Control for AWS Internet of Things-A. https://doi.org/10.32628/IJSRST523103161

[9] Lee, C. G. (2025). Enhancing Cloud Computing Efficiency Through Scalable Architecture and Robust Security Frameworks for Privacy Protection. International Journal of Advanced Research in Cloud Computing (IJARCC), 6(2), 7-15. https://www.researchgate.net/profile/Research-Pub/publication/389660467_Enhancing_Cloud_Computing_Efficiency_Through_Scalable_Architecture_and_Robust_Security_Frameworks_for_Privacy_Protection/links/67cbc613e62c604a0dd64175/Enhancing-Cloud-

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.2025.1405005|

Computing-Efficiency-Through-Scalable-Architecture-and-Robust-Security-Frameworks-for-Privacy-Protection.pdf

[10] Ovabor, K., & Atkison, T. (2023). User-Centric Privacy Control In Identity Management And Access Control Within Cloud-Based Systems. International Journal on Cybernetics & Informatics (IJCI), 12(12), 59. https://ijcionline.com/paper/12/12723ijci05.pdf

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