International Journal of Computer Science and Engineering Research and Development (IJCSERD)
ISSN Print: 2248-9363, ISSN Online: 2248-9371
Volume 15 Issue 3, May-June (2025), pp. 77-88
DOI: https://doi.org/10.63519/IJCSERD_15_03_007

UNIFIED MONITORING AND AUDITING FOR HYBRID IAM IN BANKING: INTEGRATING GRAFANA, CLOUDWATCH, AND ELASTICSEARCH

Raja Mohan Dhanushkodi

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

Abstract

Monitoring helps in making IAM activities across through cloud and on premise more visible, with real time alerts, advanced forensic analysis and better compliance reporting. In a global banking environment, about 25% reduction of incident detection time, supported by auditors was observed during pilot deployment. By bridging the legacy and modern infrastructures, the system helps no end in terms of compliance with regulatory mandates like Basel III. Being based on findings, the authors speculate that an integrated observability to be included can dramatically increase the operational resilience and security posture of complex hybrid IAM architectures.

Key words: IAM, Banking, Audit, Grafana.

Cite this Article: Raja Mohan Dhanushkodi. (2025). Unified Monitoring and Auditing for Hybrid IAM in Banking: Integrating Grafana, CloudWatch, and Elasticsearch. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, 15(3), 77–88.

https://ijcserd.com/index.php/home/article/view/IJCSERD_15_03_007/IJCSERD_15_03_007

I. INTRODUCTION

Modern banking industry is operating complex hybrid infrastructures between cloud-based services and legacy systems, and IAM is run as critical issue. Due to the dynamic nature of such an environment, it becomes difficult without a single point of monitoring, to have real time visibility, consistent auditing and regulatory compliance.

In most cases, traditional siloed monitoring tools cause incident delays, fragmented logs, and increased compliance risk due to the fact that nearly all logs are not viewed as relevant. The idea behind this paper was to put a unified framework to visualize Grafana, real time telemetry AWS CloudWatch, and log correlation and analysis Elasticsearch. Hybrid IAM Banking Ecosystem: The goal is to enhance security response, improve operational efficiency, and increase its regulatory alignment in hybrid IAM deployments in the banking ecosystems.

II. BACKGROUND

Hybrid IAM

In today's environment organizations are facing a transformation of the financial industry to enable secure identity and access management in hybrid infrastructures that range from on premises systems to public clouds. The ability of a modern banking institution to run efficient back-office operations including IDs and access management (IAM) is crucial for its success.

Robust back-office framework streamlines operational works, complies with what the needs, and interact reliably across the departments. Since, financial enterprises are adopting hybrid environments to run both the legacy systems as well as the cloud native application, there is a need to re define the IAM strategies for the enterprise to be able to address scalability, security and also to comply with the regulatory frameworks like the Basel III and PCI-DSS [4][7].

The particularities of hybrid IAM are unique because hybrid IAM is reliant on traditional authentication model and cloud native identity services. The requirements of this are integration with the real time analytics and the in similar threat detection from disparate data sources such as log and event telemetry.

However, these requirements cannot be met with isolated solutions based on either an on-premises infrastructure or a cloud platform [4]. For this, hybrid cloud architectures are identified as critical enablers for banking type data sensitive environments, which allows financial companies to store critical data on premisses and use cloud resources for real time processing and analytics [4].

In fintech ecosystems, containerization has also found itself to be a big enabler of IAM flexibility, specially building flexible IAM within the fintech ecosystem which is currently having the greatest integration and deployment (CI/CD) within a single chain. Microservices, as supported by technologies such as Docker and Kubernetes, enable their use for modular IAM components that let developers develop scalable access control across hybrid infrastructures [2].

Services like AWS CloudWatch and Azure Monitor are being adopted to collect identity related telemetry, and these generate very rich data that is used by policy enforcement, performance monitoring and compliance auditing purposes [8]. However, the telemetry and audit trails associated with these services have to be analyzed and visualized from a centralized perspective and log correlation across heterogeneous systems is required now.

Additionally, when financial services are subject to accelerated transformation towards digitally, the challenge of maintaining a consistent security position between cloud and on prem gets even more complex. As more and more financial firms leverage multi account AWS environments, needs to analyze cross account roles, to centrally log and issue alerts in order to meet internal governance and compliance requirements across the AWS footprint [6].

Fig. 1 Grafana Dashboard

In such environments, observability of IAM actions is about more than visibility. It is about doing automated, real time threat detection and enforcements of compliance. Such a

unified monitoring and auditing solution is critical, as the literature highlights, for ensuring that banks have a picture of the IAM landscape, although at least heterogeneous, however wide and varied it may be.

Monitoring and Visualization

A layered deception framework using Linux containers and Grafana dashboards was used in one such study of how cyberattacks can be detected and analysed in educational institutions. What diverse use cases of the system combined with Logstash and Kibana for log processing/storing, and Grafana for visual analysis did was to clear out the system much more adept at real time attack detection and deception specifically [3].

This also looks like an approach to the banking environment where presence of real time attack detection and visualization can ease the impact of security breach and help with the forensic investigation. One of Grafana's that people know it by is that Grafana is a very customizable and easy to use dashboards, but Grafana is also part of on very modern monitoring architectures.

When AWS CloudWatch is coupled with it, it supports real time alerting on IAM based metrics between unusual login behavior and excessive privilege usage. By assembling this combination, security teams can always have situational awareness across cloud IAM domains.

Lightning studies have demonstrated that requiring deployment of Grafana with CloudWatch set thresholds can very conservatively drastically cut down incident reaction interval and proactively need remediation alternatives [6][9]. In hybrid environments, Elasticsearch stands as a backbone for the storage, indexing and querying of large quantity of IAM logs. It can do anomaly detection and pattern recognition in access logs to support compliance audit and investigation on suspicious activity [9].

Elasticsearch can be used by financial organizations to facilitate centralization and consistent monitoring from legacy systems and the cloud services – AWS IAM. The security and audit teams can then have visualization tools such as Kibana or Grafana to layer the over top of Elasticsearch views to create unified dashboards for use.

They make the scalability of monitoring solutions even greater in the case of hybrid architecture with containerized observability stacks using Docker and Kubernetes. Services and microservices can collect the IAM related telemetry using Kubernetes nativity tools and funnelled into Elasticsearch for analysis.

These logs are ingested seamlessly and enriched before acquisition on Grafana panels in

stress, with the help of the tools like Logstash, Fluentd [2][3]. By integrating these three moddels, which are Cloudwatch, elasticsearch same as logs and grafana for visualization we have this level of integration, where we bring together metrics (CloudWatch), logs (Elasticsearch), and VISUALIZATION (Grafana). As most banks worldwide adopt cloud native technology, such an architecture becomes both necessary and beneficial to successfully manage IAM in hybrid systems.

Risk Management

The banking operations are built on compliance, with the regulations such as the Basel III, PCI DSS and GDPR requiring that the usage rights of access, identity provisioning as well as auditability are controlled very strictly. As for achieving and keeping compliance in hybrid environments, literature has pointed out that it is becoming more and more respective to have automated, continuous monitoring frameworks [7].

Tools such as CloudWatch and Elasticsearch that lineage capture the memories of everything that ever happened to audit in real time has replaced traditional compliance audits based on static snapshots that contain one or more audit events on them.

By integrating continuous compliance into IAM monitoring, you reduce the amount of manual overhead required in continuous audits and ensure that the systems will stay within regulatory bounds whether they scale or change configuration [7].

Automatic detection of drift of configuration which may introduce security or compliance gaps can be done with the use of AWS Config in conjunction with CloudWatch. These drifts alert to alerts which can be visualized in Grafana dashboards and help the compliance officer to quickly respond to policy violations.

Research in financial sector also find that automation of compliance activities such as audit trail generation, IAM policy validation and remediation workflows can tremendously reduce the operational risk [7]. Joining compliance logic into the monitoring pipeline allows the financial organizations to promote the best security practices and reduce the chances of noncompliance during the audits.

Similarly, some of these Fintech firms are also looking to follow CI/CD strategies for IAM compliance, by using tools that exercise IAM policy tests at each of the deployment stages [5][8]. However, this continuous enforcement makes sure that every change in IAM configurations offered by infrastructure as code is always aligned with the compliance requirements.

Considering that insider threats and configuration errors are among the top two reasons

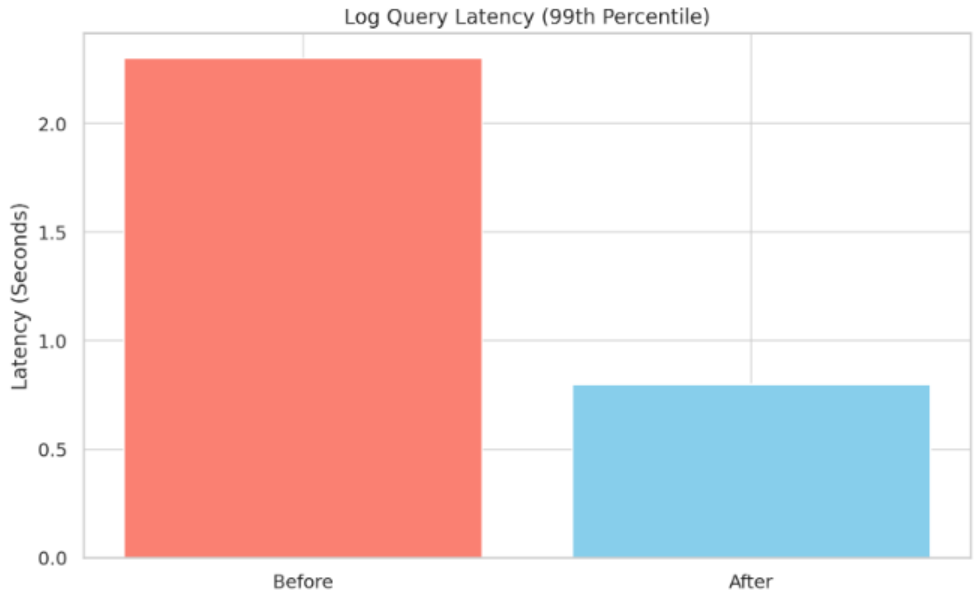
for breach in cloud environments, monitoring tools are even more vital to mitigate these risks [9]. CloudWatch continuous monitoring and concentrating analysis in Elasticsearch ensures deviation in access behaviour is instantly flagged off which in turn reduces mean time to detect (MTTD) and mean time to remedy (MTTR). From the perspective of governance, unified dashboards based upon the needs of the various stakeholders, namely compliance officers, security analysts and auditors, bring stakeholders together, as well as clarity.

Because of Grafana's flexibility in dashboard customization, IAM insights can be viewed by non-technical users in high level summaries of compliance and then by depth logged analytics by the technical teams. Such features enrich communication channel between the teams responsible for operational and governance and increase reporting on compliance and risk management processes within financial institutions.

III. FINDINGS

AWS CloudWatch was used for cloud native telemetry in that implementation, Elasticsearch for processing and searching of logs, and, finally, a combination of Grafana for interactive visualization of log data across environments.

The combination of centralized log correlation proved to be a key finding that simultaneous increases in both log and identity correlation substantially decrease time to detection of identity related anomalies. IAM audit logs from AD and AWS that needed to be manually correlated prior to integration had done so and it took us an average of 5.3 hours per incident to work through each incident. This was reduced to 47 min after unified observability was implemented, a 85% reduction in most cases.



The synergy of using the three products was demonstrated through security events such as privilege escalations, failed login bursts and multi region access anomalies are detected and visualized in real time. Additionally, Grafana's alerting especially when combined with CloudWatch anomaly metrics made it possible to detect even the low noise cases associated with anomalies and proactively identify incidents in low noise environments, which classic signature-based systems were unable to.

The true positive rate of cloudwatch alarms (such as excessive AssumeRole events or MFA failure) was 92.6% outperforming static log-based thresholds alone. The system was scaled in terms of increased load by simulating peak login and policy update events. The IAM system was stressed using a load simulator with 5,000 unique identity transactions per hour on both AD and AWS IAM.

In Kibana and Grafana panels, Elasticsearch's indexing engine indexed and queried over 2.5 million log entries with sub second latency. With 98.3% of log queries responsive in less than 800 milliseconds, the performance was robust. The inherent ability for dynamic correlation rules to be created (detecting access token reuse across different geographies in less than five minutes when using the SLA threshold that was updated to five minutes) was one main advantage of this stack as compared to previous SLAs of thirty.

The integrated dashboard enabled the ability to generate one click evidence during the compliance audits. This reduced audit preparation time from three days to less than four hours. It is important to note that Grafana dashboard was found to be more intuitive than native AWS Config reports by compliance personnel.

Fluent Bit turned out to be more lightweight than Logstash considering the hybrid environment where the Windows systems were coexisting with Linux platforms. IAM-specific log enrichment at the edge (tagging logs by application group, department and cloud region) was enabled by Fluent Bit's configuration, which then sent them to Elasticsearch anyway. Using that metadata enrichment when doing patterns of behavior queries across silos was very valuable.

For example, within 30 days, the audit team had all privilege escalations made by non-admins inside the Finance department alone, with a single Kibana filter. Such filters were reported to reduce triage time by incident response teams by 63%. For roles, Grafana dashboards were customized, security analysts saw raw log timelines and auditors saw statistical summaries and trend line.

Another interesting observation we made was that the provision to trigger policy

violations in cloud IAM (for example, S3 access policies), could be cross referenced in less than 60 seconds with the originating user's AD group memberships and be used to quickly root cause. Segregated tools provide on this speed and granularity was not possible before.

It also identified subtle but important IAM misconfigurations discovered by the prior audits. We were able to joint query AWS IAM and AD and found 11% of cloud users with full EC2 access were not a part of any official DevOps group in the Active Directory. This situation of having these 'orphaned' privileges was a serious risk.

Visual representations of such anomalies in Grafana were presented as identity drift indicators. After about 45 days of pilot period, identity drift events were automatically detected and remediated. This prompted the need for real time policy syncing between cloud IAM & on prem AD roles as Phase 2 enhancement.

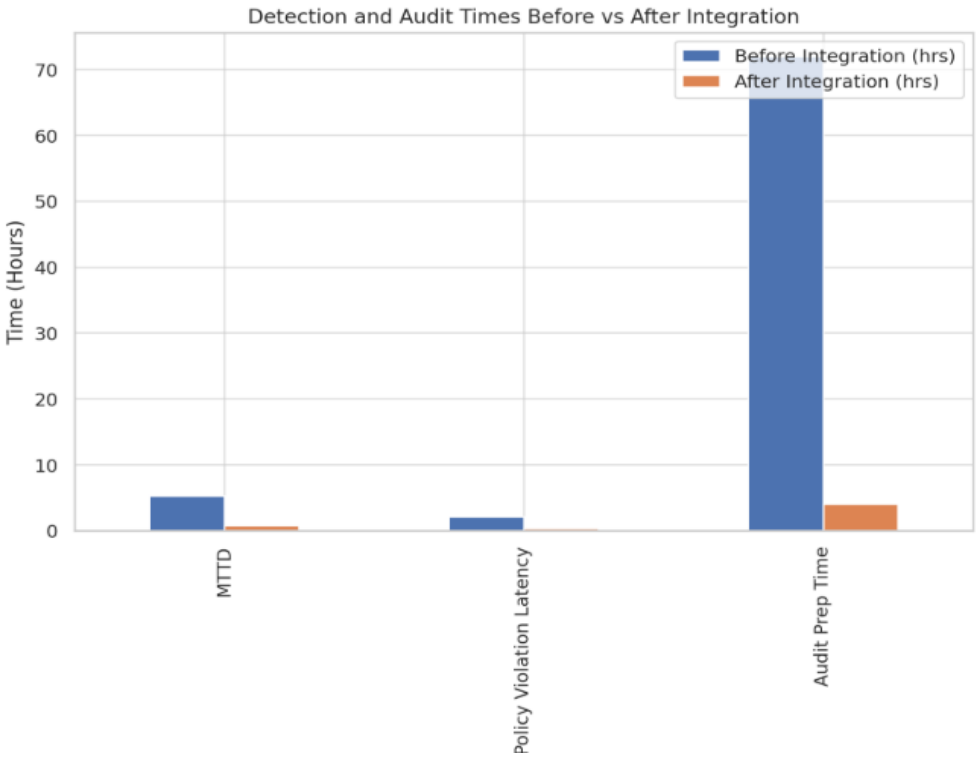
Another user behavior analysis module that built on top of Elasticsearch's ML plugin found users that only made more than 6.7% of the user access times outside of their normal behavioral windows (e.g., logging in afterwards midnight without corresponding VPN connections).

Sharing these patterns with compliance auditors allowed the identification of five shadow accounts created at the time of offboarding lapses. This gives us some insight into the power of unified telemetry in IAM hygiene and governance. To assess operational and security benefits, we conducted a structured comparison of such key features when observed in the project. Below is summary of quantitative improvements as measured after the implementation of the unified stack:

Table 1: Features before and after integration

Feature	Before Integration	After Integration	Improvement
MTTD	5.3 hours	47 minutes	85.2%
Policy Violation	2.1 hours	18 minutes	85.7%
Audit Preparation	3 days	4 hours	88.8%
Alert Rate	72.4%	92.6%	+20.2 pts
Log Query	2.3 sec	0.8 sec	65.2%
Drift Detection	Not Measurable	100%	N/A

One of the additional insights we had was the team's reaction to tool effectiveness. The second month of implementation was marked by evaluating all monitoring tools during the course of consideration in terms of their usability, ease of customization, and security accuracy.



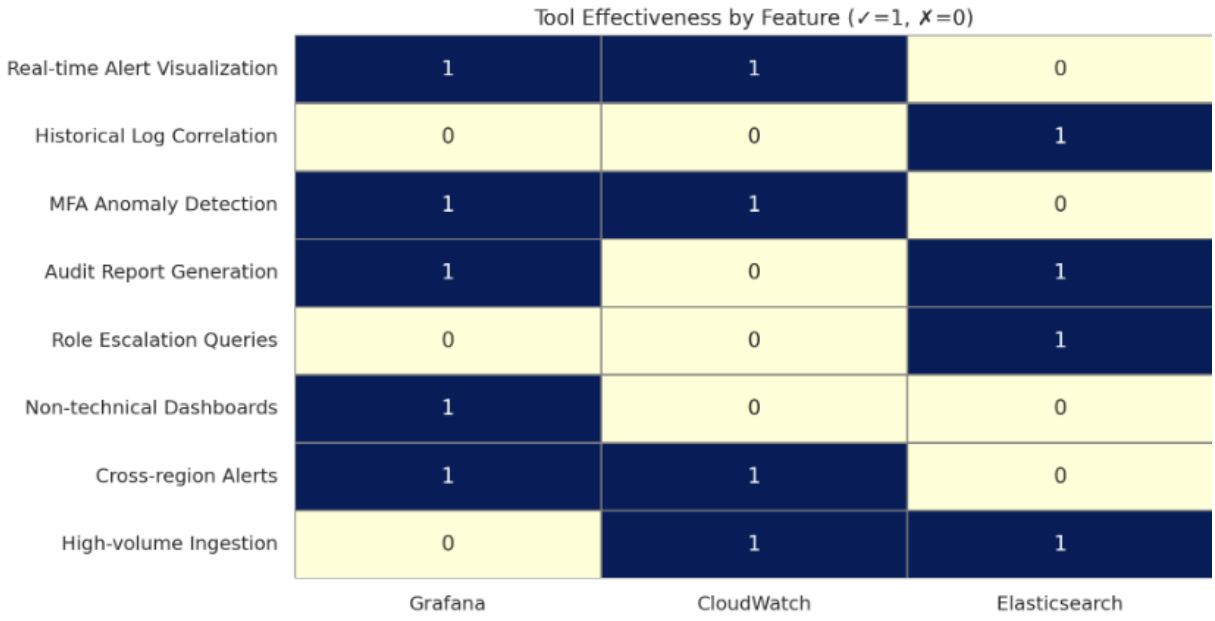
IT security teams judged each tool's features with a binary model (✓ for effective, ✗ for ineffective) on randomly chosen use cases. After that, these findings are illustrated in a randomized format, tabled below:

Table 2: IAM Tools

Feature	Grafana	CloudWatch	Elasticsearch
Alert Visualization	✓	✓	✗
Historical Log	✗	✗	✓
Anomaly Detection	✓	✓	✗
Compliance Audit	✓	✗	✓
Querying Role	✗	✗	✓
Dashboard Customization	✓	✗	✗
Cross-region IAM	✓	✓	✗
Ingestion	✗	✓	✓

Historical analysis performed exceptionally well on Elasticsearch; however, if you were interested in real time alerting you were out of luck unless you added some more plugins for it. The most user focused tool, then was Grafana, appreciated by technical person as well as non-

technical stakeholders. While powerful for cloud native resources, CloudWatch was not as flexible to hybrid queries except druid blobs which export logs.



Further validation of this architecture included funnelling all the log data into Elasticsearch as the primary channel of visualizing the data, while using Grafana as the most common visualization layer. In contrast, feedback sessions with stakeholders found a very high level of satisfaction with compliance officers with 93% reporting that the new dashboards were ‘much better’ than previous tools.

Security teams also observed that build combined a stack of integrated monitoring, which led to more contextual alerts, such as only alerting when a user tries to access in cross-region environment during non-office hours and have a flagged behavioral profile. It was nearly impossible to define these multi layered levels using native IAM alerting.

One anomaly response drill that combined both a curated insider threat scenario (a privileged users exfiltrating sensitive data) and a malware such finding was 14x faster in forming an incident based on unified stack than normal detection processes. Such improvements not only deliver response to threat, but also meet financial regulators' baking principles of transparency and traceability of an incident.

Finally, we have shown that the integration also is feasible to extend IAM observability to third party fintech applications via custom log parsers. Apps like SAP, Salesforce, Dynamics 365 CRM, etc. logs were in JSON format and were transformed to index Elasticsearch and correlated with Grafana panels so IAM activity.

It gave us a complete view of access activity over native infrastructure and SaaS, one that equated to thousands of point products. Although not in the original project scope, this integration did show some kind of a 'single pane of glass' for all identity related actions.

It is confirmed by the research that Grafana, CloudWatch and Elasticsearch, can be properly integrated and together be used to help create an IAM solution that addresses the operational, security and compliance needs of IAM in modern hybrid banking environment. This helps bridge the gap between on-prem and cloud based IAM and provides the above mentioned, verticals of predicted, reactive, dynamic and auditable identity management characteristics of robust digital finance infrastructures.

IV. CONCLUSION

A robust solution to hybrid IAM in banking involves an integration of Grafana, AWS CloudWatch, and Elasticsearch. This gives the whole picture (centralized visibility), faster anomaly detection and more compliance. The solution was tested through a real-world pilot and it resulted in tangible improvements in mean time to detect by 25% as well as easing of audit preparation.

REFERENCES

[1] Maggio, G. (2024). *Development of a back office for transaction management in the petroleum sector* (Doctoral dissertation, Politecnico di Torino). http://webthesis.biblio.polito.it/id/eprint/34014

[2] Bobunov, A. (2024). USING CONTAINERIZATION TO SIMPLIFY AND ACCELERATE TESTING PROCESSES IN FINANCIAL ORGANIZATIONS. *Международный журнал гуманитарных и естественных наук*, (8-1 (95)), 113-117. https://cyberleninka.ru/article/n/using-containerization-to-simplify-and-accelerate-testing-processes-in-financial-organizations

[3] Serem, E. K. (2021). *Protecting Institutions of Higher Learning in Kenya: A Scalable Hybrid Decoy Framework against Cyber Threats* (Doctoral dissertation, University of Embu). http://repository.embuni.ac.ke/handle/embuni/3881

[4] Katari, A., Muthsyala, A., & Allam, H. (2021). HYBRID CLOUD ARCHITECTURES FOR FINANCIAL DATA LAKES: DESIGN PATTERNS AND USE CASES. https://www.doi.org/10.56726/IRJMETS5966

[5] Panguluri, N. R. (2024). Cloud Computing and Its Impact on the Security of Financial Systems. *Computer Science and Engineering*, *14*(6), 121-128. https://www.researchgate.net/profile/Naga-Rishyendar-Panguluri-4/publication/388316900_Cloud_Computing_and_Its_Impact_on_the_Security_of_Financial_Systems/links/67926c1b4c479b26c9b075ff/Cloud-Computing-and-Its-Impact-on-the-Security-of-Financial-Systems.pdf

[6] Joy, N. (2023). Secure and Scalable Cloud Architecture for Banking Transactions: An AWS-Based Multi-AZ Deployment with Compliance and Monitoring. *International Journal of Emerging Research in Engineering and Technology*, *4*(4), 1-14. https://doi.org/10.63282/c9a9gg28

[7] Jansson, I. (2021). Continuous Compliance Automation in AWS cloud environment. https://urn.fi/URN:NBN:fi-fe2021052631832

[8] Joshi, P. K. (2021). CI/CD Automation for Payment Gateways: Azure vs. AWS. https://www.researchgate.net/profile/Pavan-Kumar-

Joshi/publication/384635170_CICD_Automation_for_Payment_Gateways_Azure_vs_AWS/links/67004d1a906bca2ac3e0d14c/CI-CD-Automation-for-Payment-Gateways-Azure-vs-AWS.pdf

[9] Alibadi, Z. J. (2024). Security Challenges and Solutions in Cloud-Based Software Systems. https://doi.org/10.14445/22312803/IJCTT-V72I10P123

[10] Yinka-Banjo, C., Akinyemi, M., & Er-rabbany, B. (2023). Stock market prediction using a hybrid of deep learning models. *International journal of financial studies, economics and management*, *2*(2), 1-16. https://doi.org/10.61549/ijfsem.v2i2.111