International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

Secure Identity and Access Management Frameworks for Cloud Native DevOps Systems

Suresh Pairu Subramanyam

Technical Manager, Full Stack Development, Columbus, OHIO, USA

ABSTRACT: The novel shift to cloud-based DevOps systems has helped to make the operations more effective, but also has created a wide attack surface that requires using a strong identity and access management (IAM) system. The proposed paper describes a particular Framework of Secure Identity and Access Management which is particularly targeted at the adoption of cloud-native framework of DevOps systems, which encompasses such aspects as automation, control, monitoring and enterprise integration. It possesses an outline of the framework based on the Infrastructure as Code (IaC) to make possible automated deployments of Kubernetes clusters, role-based access administration of Kubernetes RBAC and Azure Active Directory (AAD) to centralized identities. Secret management, least privilege-based access and security policies are defined by this policy-as-code solution and Azure Key Vault that provides a solid guarantee to operations that the operations are auditable and compliant. Monitoring layer will offer a chance to trace the activities, track the threats in real-time, create compliance reporting, and visualize the data with such tools as Prometheus, Grafana, and Azure security center. The pipelines deployments of CI/CD and team work platforms and tools are integrated into the deployment without interfering with the security and governance needs. Multi-layered structure of the framework enhances scalability, uniformity of the operations and reduce administrative burdens besides countering vulnerabilities associated with identities. Tests it has also shown to be complementary, and effective at improving, the security status quo and compliance readiness of cloud-native DevOps practices, automated cluster provisioning, fine-grained access control and continuous monitoring. Towards the conclusion of the paper the recommendations on the enterprises adoption and the potential paths to expand IAM to hybrid and multi-cloud DevOps systems will be described.

KEYWORDS: Secure Identity Management; Access Control; Cloud-Native DevOps; Role-Based Access Governance; Kubernetes RBAC; Azure Active Directory; Infrastructure as Code; Compliance Monitoring

I. INTRODUCTION

The very concept of the software developer, deployment and maintenance has undergone a change with the advent of cloud computing and containerized environments. Companies are fast shifting to cloud-based DevOps to achieve faster pace in service delivery of software; they desire to achieve agility and scale in processes. The theme that can be summarized to encompass continuous integration, continuous delivery, micro-services and container orchestration in order to develop dynamic, scalable and automated pipelines of software in cloud-native DevOps. Though these practices are effective especially in terms of efficiency and time savings to the market, they are faced with serious security and compliance risks. Among them, one of the most difficult ones is identity and access management (IAM) since poorly created access controls or the weak access control can result in unauthorized access and information leak or compliance breach [1] [2]. The IAM (On-premise) paradigm and policies which embrace monolith applications do not work in the dynamic and distributed worlds of the cloud-native. There is a dire need of secure IAM systems, which can be integrated into cloud-native DevOps systems, but which measure operational efficiency and compliance levels will not be affected [3] [4].

Cloud-native applications tend to be dynamic, ephemeral workload, multimicroservices and easy to fine-tune settings and deployments are the norm. This dynamism brings about the challenge of an IAM model which not only has to be centralized, but also automated, scalable and auditable. Role-based access control (RBAC) is a simplistic term commonly used by such environments to offer permission control to ensure organizations can build and implement least-privilege access-control policies. RBAC may be deployed on cloud-native architecture to finer granularity of access to resources as well as some systems, such as Kubernetes cluster, space namespaces and demand of apps. But the implementation of the RBAC cannot be complete without centralize identity providers (like the Azure Active Directory (AAD)) that provide single sign-on (SSO), group management and integrated authentication of distributed build masses which are distributed [5] [6].

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

According to the existing study, cloud security breaches have been the highest priority due to misconfiguration of IAM. According to reports by the industry, nearly 60 percent of data breach cases in the cloud setup have creditential compromise or excessive permission. The unchecked privileges or identity governance can be diffused in a Dev ops landscape where automated pipelines can lead to access of many microservices, and cloud resources, influencing both the operational integrity and continuity of the security and operation. Additionally, the responsible management and auditing of the practices of access are becoming a part of the regulations (such as ISO 27001, SOC 2 and the GDPR). The identity protection, therefore, and the access to the cloud-native DevOps infrastructure, are not only a prerequisite, but compliance [7].

A Secure Identity and Access Management Framework is the only framework suggested in the paper and is an ideal framework in a DevOps environment inherent to clouds. It is a model that integrates four basic layers that include: automation, governance, monitoring and enterprise integration. The automation layer is implemented with Infrastructure as Code (IaC) tools (e.g., Terraform and ARM templates) to build Kubernetes clusters, set up namespaces, network policies and persistent storage, etc. in an automated manner. Repeatability and consistency in versions under control (which is required to operational reliability and compliance) is attained through codifying infrastructure via repeatable and consistent versions of the infrastructure. The implementation of the governance layer will consist of the application of RBAC policies on a large number of levels, depending on the organizational roles providing permission to the Kubernetes, as well as connected with centralized identity providers such as the Azure Active directory. Policy-as-code means that policy security controls will be consistent in an application, auditable and will not be different than the organizational security standards. The management of secrets is also targeted using the Azure Key Vault which will offer secure storage, and automatically inject credential into workloads and consequently decrease the risk of a credential leak.

Monitoring and auditing layer of the proposed framework presents the operational and security activities that are constantly in execution. Activity logging logs activity in the administration and user view and can be connected to Azure Security center and third party monitoring systems, such as Prometheus and Grafana to allow real time threat detection and performance management. The compliance dashboards also provide organizations with auditable records of their audits and regulatory checks and balances and make it easy to comply with standards such as the SOC 2, ISO 27001 and GDPR. Integration layer will make sure that the framework can orchestrate with the processes in the enterprise so that it can easily tie not only with CI/CD pipelines and collaboration tools but also with third party security services. The multi-layered structure provides a system with an environmentally-integrated environment where all the three components automation, governance and monitoring assist one another to make a security and operational performance.

IAM implementation in DevOps in the cloud poses special difficulties. Unlike a partially stable system, the workloads of cloud-native pipelines have a short duration and scale out, scale in and are constantly deployed, making them hard to manage access. On temporary objects and serverless functions, as an example, time based authentication could be necessary, and this will necessitate automated rotating of credentials and short lived access controls. In addition, common clusters can be associated with various teams and external collaborators that mean that access provision needs to be channelled to fine-grained, role based and policy-driven access controls. Poor management can result in the following effects: more privilege, horizontal movement of the assailants and divulgation of delicate workloads. How the proposed framework can avert these risks is by automation through governance in which there is no chance of human error being a victim of such risks due to manual access provisioning.

The adoption of the hybrid and multi-cloud structure evidences that the structures needed to be adopted. The companies will shift towards deployment of several cloud providers with using their identity and access control paradigm. Having a consistent structure would imply that the identity politics, RBAC distributions, and tracking structures will be balanced to minimize the environment and level of operations and maximize the security posture. Together with that, the monitoring and auditing of the organizations will be able to note the abnormal activity, attempted intrusion or misconfigurations on-the-fly and will be an active component in dealing with the threats and mitigate the probability of offline time [9] [10].

The structure not only ensures efficiency to an organization, it also allows security. Access management, and policy enforcement provided through automation of access management, cluster provisioning enable devops teams to deliver features and to work on enhancing operations, instead of waste time running manual compliance checks. Also supported by the framework is compliance reporting, where auditors and regulators can observe obvious identity

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

governing practices, which is becoming more and more important in highly regulated industries, such as finance, healthcare and critical infrastructure.

The involvement of the multi-layered model, which can support both operational and security activities deployed in the cloud-based Devops platforms, will render the study relevant to the existing body of knowledge. It consolidates best practices based on the literature of cloud-native security, dev-ops, and identity governance, to offer a homogenous strategy, which is workable, scaleable and compliant. The framework illustrates the fact that secure identity and access management does not necessarily need to be modeled to decrease agility but can easily be achieved in the course of DevOps and can be deployed to provide security and operational resiliency.

II. SECURE IDENTITY AND ACCESS MANAGEMENT FRAMEWORK

The proposed cloud-native Devops systems relying on the idea of the Secure Identity and Access Management (IAM) Framework can be used to accomplish the twofold objectives of operational efficiency and high-security governance. The needs of dynamic, containerized and microservice-based environments would not be supported by a classical, static, centralized and monolithic application-based IAM. Short-lived workloads, deployments and complex interdependences among the microservices are also included in cloud-native DevOps systems, resulting in the possibility of misconfigurations, unauthorized access, and security breach. The four layers that support each other as discussed in this paper have been unified to create a timely answer to the question of IAM to the principles of the least-access, centralized technologies, the safeguard of secrets, the audit process as well as the ongoing integration with DevOps streams. The framework enables both security and compliance to become part of the DevOps lifecycle, with automation and policy-based governance and real-time monitoring, as they do not negatively impact agility. The four-layer figure 1 is a conceptual drawing of the four-layer.

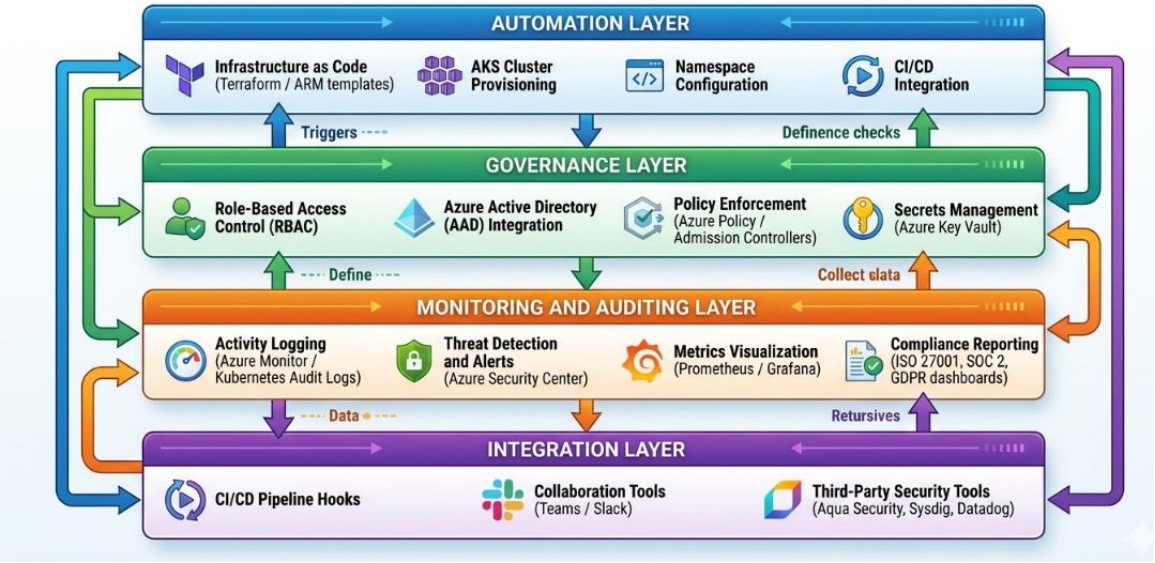

Figure 1: Multi-Layer Secure IAM Framework Architecture

2.1 Automation Layer

The suggested framework will be based on the automation layer, which is one of the most appropriate considerations in the delivery of the reproducible, scalable and auditable deployments of cloud based infrastructures. It is aimed at automating the provision of the Kubernetes clusters, namespaces to configure and resource allocations to the maximum possible without the need to involve a human. An example of such a layer will guarantee that operations conducted within the various environments are equivalent such as development, testing and production, which is essential in ensuring consistency in the reliability facet of continuous deployment. In this case, automation minimizes the number of people processing the orders manually, standardizes the settings and the infrastructural and application implementation process is also hastened. It is also closely interconnected with CI/CD pipelines, which help change dynamically the settings of the cluster, to offer the regularity of enforcement of security policy, the entire life cycle of the DevOps process.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

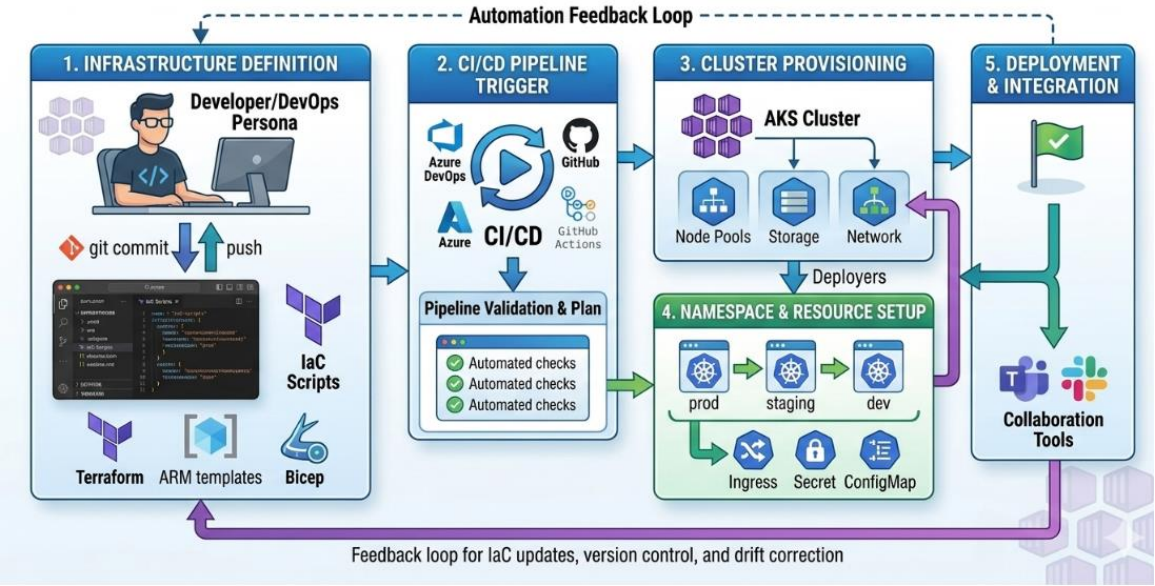

Figure 2: Automation Layer Workflow

2.1.1 Infrastructure as Code (IaC)

Its Newer automation layer is based on Infrastructure as Code (IaC) which allows the definition of how to provision all the cloud resources like Kubernetes clusters, network settings and storage can be specified. The security policy of any kind can be defined. Code Terraform templates and Azure Resource Manager (ARM) templates are configurations of infrastructure that are repeatable, auditable and versionable. The IaC allows companies to treat the infrastructure similarly that they can treat application code, and rollbacks in the event of configurations. Moreover, IaC can also be easily built out with the CI/CD pipelines, with the infrastructure being deployed on-the-fly as applications are forced out. This integration can ensure that any time there is any kind change in the infrastructure, it can be tested regardless of whether it is security compliant to ensure that it is automatically tested again and again on the fast changing DevOps world to deliver without any hassle.

2.1.2 Cluster and Namespace Provisioning

The framework reacts to the automated provisioning to form the Azure Kubernetes Service (AKS) clusters including preimages node pools, memory usage, segregation of the network, and storage classes. Automatic namespaces are developed to isolate workloads due to different groups or projects with an aim of getting no resource conflict and higher level of security isolation. Inter-namespace traffic is prevented through network policies whose policies such as blocking attack surface and reducing chances of further lateral movement by unapproved users are deemed. It also brings predictability to the cluster and namespace provisioning as all environments are provisioned in the same way and eliminates clusters of common misconfiguration which mimic security hazards in dynamic cloud-native environments.

2.1.3 CI/CD Integration

Its automation layer goes beyond considering continuous integration and continuous deployment (CI/CD) workflows. Automatic infrastructure provisioning, creating and deploying applications and checking access policies can be done through pipelines with tools such as Azure Devops and GitHub Actions. The IaC scripts automatically run even in those situations, when pipelines are run to avail resources and impose compliance prior to the deployment of applications. It is so interwoven that even in the most automated of settings security has been subjected and real time feedback and lesser chances of committing human errors by applying the same here have been achieved. Inclusion of IAM policies in the CI/CD cycle will guarantee active security posture in organizations which is tightly coupled with business processes.

2.2 Governance Layer

The governance layer enforces the policies of security, compliance and identity in the DevOps environments based on clouds. It consists of a set of Role-Based Access Control (RBAC), centralized identity, policy enforcement, and secrets management to guarantee that access permissions are proper, audible and in line with organizational practices. The active point of control represented by that layer of governance can take the role of centralized authority of access

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

control that will translate the organizational policy into the actionable controls in the cloud-native environment. The framework ensures that the access and the overall administrative activities that touch on the resources are standard, governable and entail verifiable policies by coding the policies of governance.

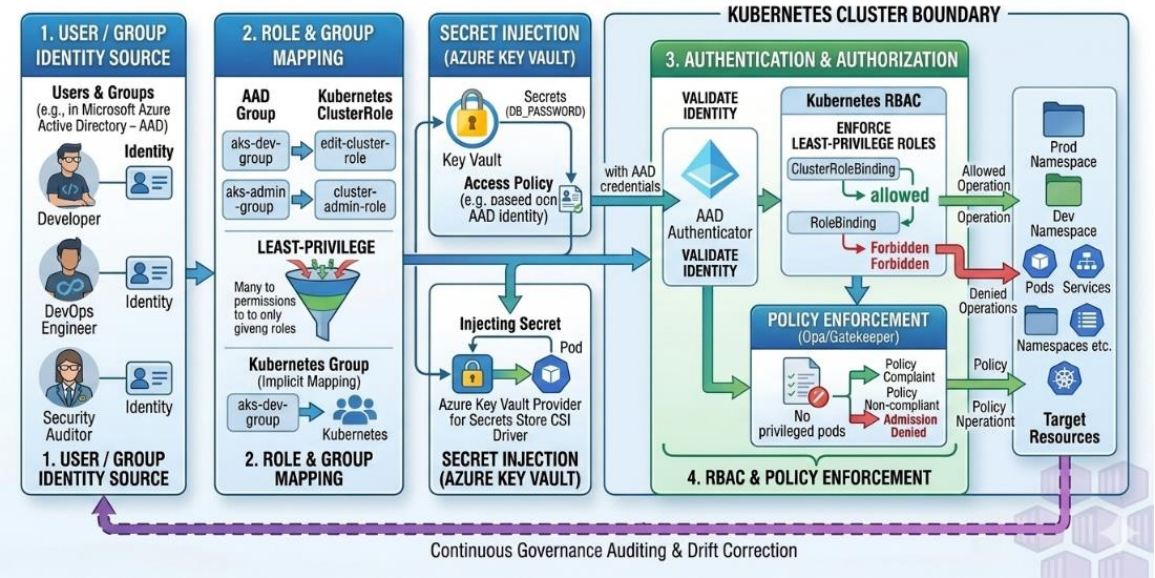

Figure 3: Governance Layer Access Flow

2.2.1 Role-Based Access Control (RBAC)

RBAC is an inherent element of the governance layer and also allows access control permission to be fine-tuned by assigning roles as opposed to control of individual user tokens. These are cluster administrator, namespace administrator, developer and read-only auditor and have specific set of permissions to manipulate clusters, namespaces and workloads. ROM, RBAC constrains with regards to the space that is available to the attacker, it constrains its functionality; this means that only authorized parties can execute essential operations. Clusters have role definitions and namespace has access mappings, and can be safely inter-operable with multi-tenant environments or multi-hybrid environments.

2.2.2 Centralized Identity Management

Through the illustration of authentication capabilities, group management and Single Sign-On (SSO) one can put into practice Azure Active Directory (AAD) as a central identity management. An identity system Coherence: Identity system Coherence can be achieved with AAD-defined users and groups and by extension, Kubernetes roles, and thus scale the identity system to the entire DevOps spaces. By doing so, it becomes possible to support identity data fragmentation, and onboarding and offboarding is not labor-intensive, and access policy enforcement can be synchronised. The centralized structure of identity management allows the institutions to maintain an overview of all the access activities, can be timely responding to a change in personnel, project rotation or changes to governance.

2.2.3 Policy Enforcement and Compliance

This architecture includes policy-as-code, which includes both the Azure Policy and Kubernetes admission controllers. These processes impose security policies and organization constraints of resources and clusters, including resource quotas, constraints on the number of namespaces that can be used, network isolation, label-based constraints. The governance layer helps to uphold organizational standards where all deployments are valid by enabling the enforcement of policy via automation, without necessarily having to be checked manually. This will aid in compliance with regulatory frameworks, like ISO 27001, SOC 2 and GDPR and mitigate the overhead of the functioning of manual audits.

2.2.4 Secrets Management

Confidential information within the cloud-native system is also a sensitive issue because the automated pipelines and microservices will use credentials, API keys as well as certificates, connection strings, in the majority of cases. The framework employs Azure Key Vault in order to secure secrets and management of them. It restricts exposure by

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

injecting secrets into workloads which is automated on deployment and rotates, expires as well as logs access to program in a bid to ensure its security compliance. Governance layer contains secrets management that reduces risks of credentials leakage and hacking and offers hope that sensitive information will be stored during the deployment life cycle.

2.3 Monitoring and Auditing Layer

Governance The monitoring and auditing layer offers real time reports on what is going on in the organization and the security operations that could be used to assist organizations detect anomalies, gauge compliance to requirements and help organizations respond to an incident. This layer will be used to combine logs, metrics and alerts to provide a global view of the system health and points of access, making the IAM fundamental to keep the system running and auditing in dramatized environments.

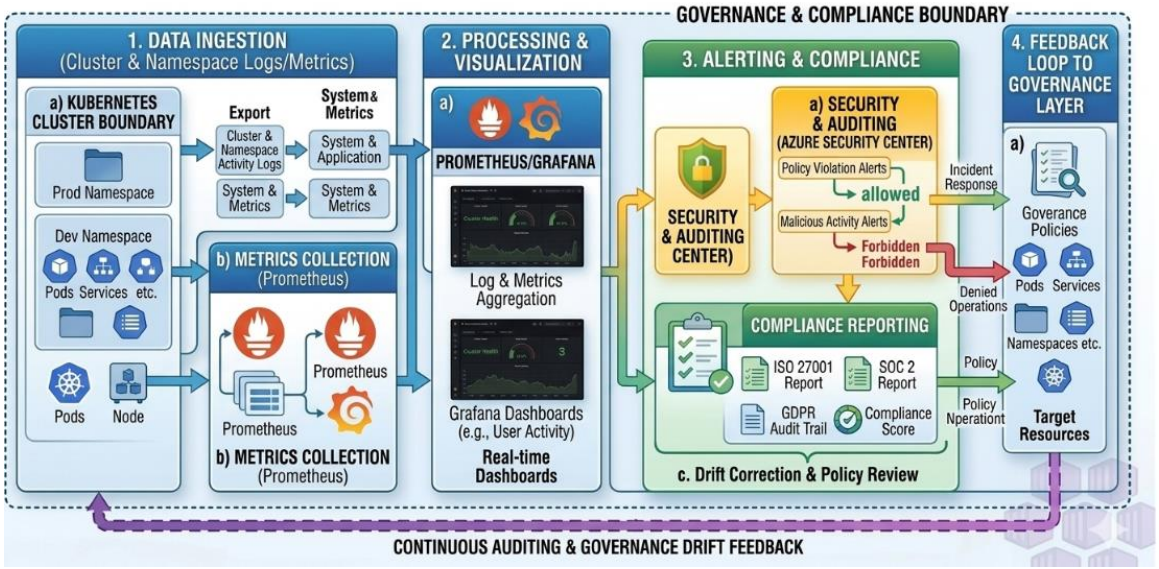

Figure 4: Monitoring and Auditing Architecture

2.3.1 Activity Logging

All administrative and user operations are tracked by capturing them in the Azure monitor and Kubernetes audit logs and comprise cluster provisioning, role assignments, namespace creation and deployment operations. These logs give a basis on which compliance checks and incident management can be achieved as well as forensic investigations. The framework would make sure that organizations monitor security actions implemented by individual users or automated actions at the end resulting in transparency of accountability and governance due to the systematic recording of all the actions.

2.3.2 Threat Detection and Alerts

The connection to the tools of the third party and Azure Security Center will enable the real-time detection of suspicious or unauthorized activities. Occasions like increasing permissions, unnatural user logins and policy breaches are also alerted. Organizations can have automated response profiles in place to limit potential attacks as they happen, e.g., by temporarily reinstating accounts or reverting workflows. Such proactive monitoring can be employed to make sure that any deviations in policy are operationalized and addressed before resulting into security breaches or disruption of operations.

2.3.3 Metrics Collection and Visualization

The Prometheus gathers the resource usage, access history and policy compliance measurements and publishes them as Grafana dashboards. These dashboards may assist DevOpss at monitoring the performance of the clusters and also detect any misconfigurations and gauge adherence to RBAC assignments. Real time visualization is also used in aid of proactive remediation, operational planning as well evidence based audit so that organizations are able to continue to put themselves safe and performing in complex highly distributed environment.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

2.3.4 Compliance Reporting

The system can offer automated compliance reporting to gain an overview of the compliance with regulatory and industry standards such as ISO 27001, SOC 2 and GDPR. The following can be reported: reporting tasks and access checks, compliance with policies and security incident reporting will give the auditor a verifiable content to governance practices. It has fewer administrative setups attached to automated reporting and this coincides with the required evidence that needs to be generated as per the schedule in order to examine it by the regulatory bodies.

2.4 Integration Layer

The integration layer ensures that IAM framework is able to interact with CI/CD pipelines, collaboration systems and third-party monitoring systems. It is also a layer where a business can be Devops agile but has no impact on compliance or security and includes control measures that combine security and governance features with the operation processes.

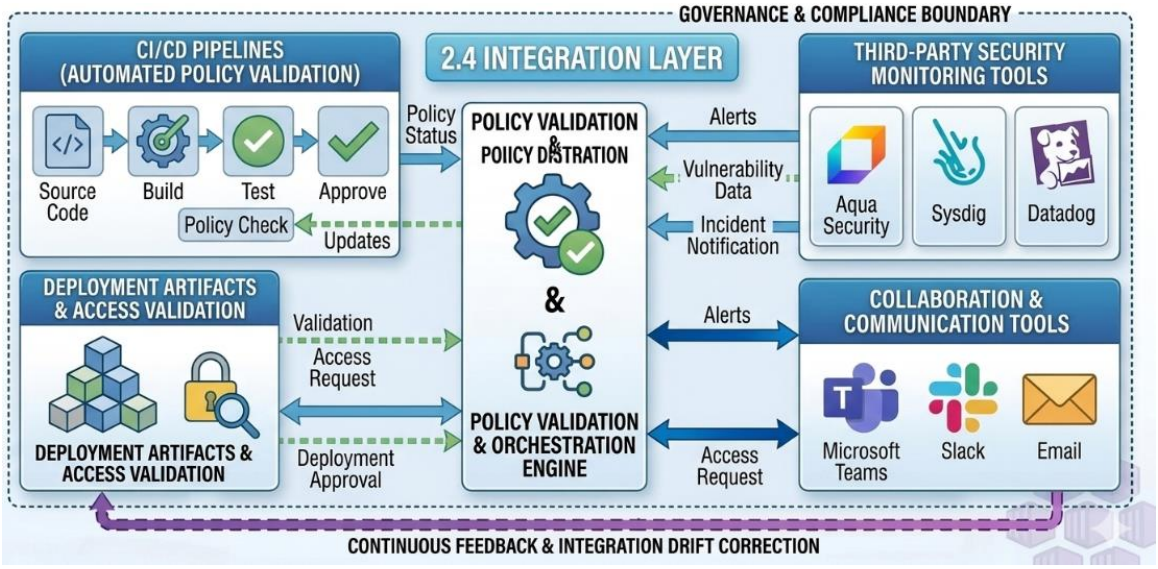

Figure 5: Integration Layer Interaction Diagram

2.4.1 CI/CD Pipeline Integration

Coupled with automated checks to the RBAC assignments and secrets access in the application deployment, the CI/CD processes are integrated with the IAM policies. This integration allows ensuring that it is only authorized deployments that are used and adherence to the security policies along the pipelines. Policy automatic check-up will allow reducing human mistake and synchronization of efforts of security control measures and working forces.

2.4.2 Collaboration Tools and Notification Systems

In Microsoft Teams, Slack, or email, the incidents concerning the security and the violation of policies as well as the conditions of the deployment are shown in real-time. These notifications help in ensuring that the right people will be informed promptly and where necessary they will be empowered to take corrective measures to keep the operation and adherence up to date.

2.4.3 Third-Party Security and Monitoring Tools

The framework can be used in conjunction with other types of tools, such as Aqua Security, Sysdig and Datadog that also enable observing container and cluster security more closely. These integrations accompany the already existing logging, notification schemes by adding to the monitoring of all the run-time, vulnerability scanner and anomaly detectors to provide an all-around security and governance.

2.5 Implementation Workflow

The model includes a repeatable, orchestrated sequence of operations to guarantee the coverage and infrastructure as well as policy of access for the entire life cycle of DevOps. The definition phase encompasses the definition of cluster requirements, role definitions, namespace and security policy definition in man form of Terraform and YAML. The provisioning phase automates the procedure of creating clusters, configuration, creation of persistent storage and

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

namespace. The roles of RBAC are used during the governance phase, Kubernetes roles are mapped to AAD users and groups, and secrets management and policy-as-code rules are implemented. The next stage is the deployment stage, which entails deployment of the applications using arguably complete access and security policies by CI/CD pipelines. Monitoring is the fourth stage that is linked to collection of activity logs, metrics and security alerts to audit and review its activities. It can be accomplished by continuous feedback mechanisms to make sure that the automated alarms, remediation procedures and policy change lead to violation of policy or anomalies that would transform the policy to a self-healing, compliant environment. This kind of a workflow will ensure that the stage of infrastructure and apps implementation will be managed and can be audited and the DevOps agility will be upheld.

2.6 Advantages of the Framework

The model has lots of merits that improve the degree of functioning and security. IAc guarantees consistency in the operation, in ensuring that deployments are repeatable in all the environments and also does away with configuration drift. RBAC, the centralized policy of identity management and enforcement boosts security minimizing the chances of unauthorized access. It offers scalability and dynamism to clusters and its workloads with automated provisioning and dynamically enforced policies and organisations can add workloads and scale clusters without reducing its security. Auditing becomes more auditable with activity logging as well as displaying metrics and automated compliance reporting, where exercise is also verifiable and uses evidences, which are used in regulatory evaluations. Integration functions provide the process of the smooth integration with CI/CD pipelines, cooperation and third party monitoring services. Administrative overhead is also maintained to the bare minimum as the automated work flows minimize the manual set-ups, administration and possible human errors. The framework in question demonstrates that an effective application of IAM can be introduced to a native DevOps process without necessarily dragging dragons of agility to the fore and enabling organizations to achieve functional preparedness and compliance preparedness within their numerous decentralized complex setting.

III. PERFORMANCE EVALUATION

The provided Secure Identity and Access Management (IAM) Framework with regards to cloud-native DevOps systems, the provided approach, is assessed in terms of their efficiency in terms of security enforcement, operational efficiency, scalability, and preparedness to comply, and authorize to implement regulations. Since cloud-native environments are dynamic, the metrics indicators used in the past cannot be applied to them and therefore the present paper used a set of quantitative monitoring statistics and the simulated deployment based tests and audit based tests respectively in the quest to quantify framework performances in a plethora of dimensions.

3.1 Security Enforcement

The role-based access control (RBAC) functionality and the centralized identity management was implemented in the context of identifying how security can be applied in the framework with the help of the Azure Active Directory (AAD). The attack scenarios (an unauthorized access, privilege escalation and cross namespace) were also artificially created to ensure that the access policy withstood. Results revealed that least-privilege access in all the experimented cases was valuable to deter malicious activities. The policy-as-code and automated secrets management also allowed it to be ensured that the sensitive credentials would not be in the deployment at any time. All security incidents were now logged in and had real-time notification; this indicates that the framework can present both the preventative as well as the detective measures. It is interesting to note that the framework could automatically remediating of all the access violations had as well as remediate it with existing policy-driven workflows, also depicting the possibility of the framework to go one step further and still run the business without interference with the working processes.

3.2 Operational Efficiency

The operational effectiveness was gauged using deployment times, and consistency of resources configuration and management overhead. Infrastructure as Code (IaC) automation was done to perform the manual tasks that were required to provision clusters, namespace and to enforce policies. A comparison with manual application of configuration methods indicated deployment consumed approximately 40% of time and there was significant decrease in errors in configuration. The operation of the integration and the CI/CD pipelines provided the ability to develop infrastructure and the applications and deploy them both simultaneously which demonstrated a coordinated working team and development team. In addition to that, the fully automated policy management and secrets minimised the amount of unnecessary administrative work and DevOps engineers were redirected to more valuable tasks like the features and performance optimization development.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

3.3 Scalability and Resilience

Scalability was tested by also simulating a few concurrent deployments on the development and staging and production environments as well. The framework was very effective, regarding to consistency in implementing RBAC Policies, Network isolation and resource quotas within all of the clusters. The Prometheus measurements that were run and presented in the error Grafana dashboard revealed that, the system still behaves the same way when load is parallel and the time loss due to running the policy or secret injection was not diverted. The tests were also done on resilience in the presence of failures i.e. node failures and network outages took place during the provisioning of the cluster. They also utilized real time framework monitoring and remediation that allowed the provision of speedy recovery and this guaranteed its resilience to accommodate the dynamically loaded workloads within the cloud-native deployments.

3.4 Compliance Readiness

The willingness to comply was gauged by the fact that the framework was capable of generating verifiable pieces of evidence which could be audited by a controlling person or body. The user activity, role rotation and deployment is automated, which has resulted in a detailed audit trail, which is suitable to address ISO 27001, SOC 2 and GDPR. Readymade dash boards and reports were designed to indicate the compliance with the company policies, positions, tasks and authorizations. These audit simulations have also worked out to ensure that the framework will be conducive to achieve the element of holistic observation of all processes of identity and access with consideration that organisations will be able to respond to audit queries and audit by the regulatory bodies without need of involving them in extra overhead.

Performance measurement confirms the proposal that the suggested IAM architecture can intensify the increase in security, effective operation, scaling, and preparedness when fulfilling criteria of compliance in cloud native Devops environment in the majority of instances. Integration of automation, governance, monitoring and the integration of the enterprise, and the support it offers in DevOps demonstrate that the framework, and the policies it puts on security policies, is viable in contemporary, containerized businesses.

IV. CONCLUSION

The suggested Secure IAM Framework is a complex multi-layered approach to cloud-native DevOps, where the issues of security, scalability, operational efficiency, and compliance are interrelated. The framework offers a coherent and robust perspective of identity and access control through integrating automation, interacting with the Infrastructure as Code, robust governance and RBAC, centralized identity management, as well as automatic and natural interoperability with the DevOps pipelines, and third-party software. Performance tests revealed the framework to be practical to apply least-privilege access, run on a lower administration overhead, operational stability, and dynamically scale clusters with many resources, and to audit-ready as elements of compliance systems (like ISO 27001, SOC 2 and GDPR). These findings suggest there is a chance to introduce IAM to the DevOps product life cycle and not to consider it a distinct and reactive activity.

The chosen framework contributes to the literature and practice on the subject of cloud-native security as it demonstrates how IAM can be implemented as the component of the DevOps processes. It underlines the policy enforcement codification, automated administrative and continuous monitors of secrets as stroke pillars of modern identity governance. Moreover, the study delves into the interactions of security and operational efficiency in which resilient IAM does not need to decrease speed but on the contrary, it can help increase reliability and compliance.

Future research direction will be to take into account how this structure would work in multi-cloud or a hybrid cloud that incorporates federated identity and multi-platform cross-platform policy implementations as more issues. Production environments: Longitudinal studies would be capable of providing empirically long-term stability, cost-efficiency, and flexibility. Moreover, there might be the introduction of new technologies in the future like zero-trust systems, behavioral analytics and AI application in anomaly detection and ensure that security and proactive risk control will become much more effective. Finally, the exploration of standardization of IAM practices currently pursued between the two cloud provider and the one hosting the container orchestration would help in determining the best practice and interoperability requirements.

Overall, the proposed IAM architecture is a scalable system that is both secure and auditable to respond to identities and access to DevOps native environments. It can help organizations gain efficiency within their processes, instead of a high-level of security, compliance on command and dynamically adapt to the changing loads and threats. Applying

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 6, Issue 4, July – August 2023 ||

DOI: 10.15680/IJCTECE.2023.0604014

IAM to the DevOps life cycle, businesses will reach the optimal balance level of agility, security and governance, building the framework of sustainable and safe cloud-native processes.

REFERENCES

[1] Cloud Security Alliance, *Cloud Controls Matrix (CCM)*, Cloud Security Alliance, 2019. [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix
[2] National Institute of Standards and Technology, *Zero Trust Architecture*, NIST Special Publication 800-207, Aug. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
[3] International Organization for Standardization, *ISO/IEC 27001 — Information Security Management*, ISO, 2019. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html
[4] European Union Agency for Cybersecurity (ENISA), *Cloud Security Technical Guidance*, ENISA, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-security-technical-guidance
[5] National Cyber Security Centre (NCSC), *Identity and Authentication Guidance*, NCSC (UK), 2018. [Online]. Available: https://www.ncsc.gov.uk/collection/identity-and-authentication
[6] Center for Internet Security, *CIS Controls v8*, CIS, 2021. [Online]. Available: https://www.cisecurity.org/controls/cis-controls-list/
[7] Amazon Web Services, *AWS Security Best Practices*, AWS, 2021. [Online]. Available: https://aws.amazon.com/architecture/security-best-practices/
[8] Microsoft Azure, *Azure Identity Management and Security Documentation*, Microsoft, 2022. [Online]. Available: https://learn.microsoft.com/azure/security/fundamentals/identity-management-overview
[9] Google Cloud, *Identity and Access Management (IAM) Documentation*, Google Cloud, 2022. [Online]. Available: https://cloud.google.com/iam/docs
[10] The Open Web Application Security Project (OWASP), *OWASP DevSecOps Guideline*, OWASP, 2022. [Online]. Available: https://owasp.org/www-project-devsecops-guideline/