International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 2, March – April 2025||

DOI:10.15662/IJRPETM.2025.0802007

AI-Augmented Infrastructure Governance: Intelligent Risk Detection in Identity-Centric Cloud Platforms

Nandkumar Niture

Princpal Cloud Infrastructure, Naperville IL, USA

ABSTRACT: The modern-day cloud platforms rely heavily on automated infrastructure and identity systems. Nevertheless, fixed surveillance systems are incapable of identifying complex identity abuse and drifting configuration in dynamic systems. In this paper, an AI-enhanced infrastructure governance system that incorporates supervised learning and anomaly detection as part of identity-centric cloud platforms is outlined. The suggested system will superimpose identity anomaly potential and Configuration Drift Index (CDI) into single Risk Score. The experimental findings are improved significantly compared to the results of the standing monitoring. The precision rose to remain at 0.89 and recall also rose to 0.86, whereas, F1-score rose to 0.87. False positive changed by 0.22 to 0.08. Mean latency of detection was reduced to 74 seconds as compared to 312 seconds. The rate of detection of configuration drift increased to 91% downward of the previous rate of 69%. Significance was found to be at p under 0.01 using statistical testing. The findings show that AI-based governance enhances accuracy in detection, lowers the response time, and enhances adaptive risk management of identity centric cloud environments.

KEYWORDS: AI-Augmented Governance, Infrastructure-as-Code (IaC), Identity-Centric Cloud Security, Anomaly Detection, Isolation Forest.

I. INTRODUCTION

A. Background

Contemporary cloud systems are made on the basis of dispersed infrastructure, auto-deployment pipeline and access liquids that are controlled using identity. Infrastructure-as-Code enables teams to create resources with very minimal time and with repetitive counterparts. Identity systems handle user, services and permissions in the various cloud services. This is also a source of security risks, as much as it adds speed and flexibility.

There is dynamic cloud identity changing regularly. Roles are automatically updated, permissions are automatically changed, as well as new services are automatically deployed. The rules and threshold values are used in static monitoring systems in order to highlight abnormal activity. Such systems are not suitable to accommodate changing usage patterns. This leads to them raising false alarms too frequently or their inability to identify complex attacks.

Misconfigurations in the cloud are as well a big problem. Whether belonging to predefined thresholds or not, small configuration changes might still pose security threats. In the case of identity abuse and configuration drift, conventional systems are not able to identify the conjoined threat.

B. Motivation

The research gets inspired by the need to overcome the weaknesses of the static monitoring in the platforms that are identity-focused. The security teams should have systems capable of learning the normal behavioral patterns and also be able to pick out abnormal changes in real time. Machine learning may be used in order to process big amounts of logs and find some concealed patterns.

The information that is in identity logs includes useful data like frequencies of logs, incidences of privilege escalation, duration of a session, and patterns of access of services. Alerts on changes made to configuration and the state of the system are provided in infrastructure telemetry. When these data sources are used concurrently, risk detection may acquire a more precise context-aware form.

There is the need to decrease alert fatigue. In cases where the security teams have too many false positives, critical alerts will be overlooked. The enhancement of work accuracy and reduction of the rate of false positives can make the work more productive. Technology of quicker detection is also significant since, the response to incidences becomes harder as time progresses.

C. Research Gap

Even though AI-based anomaly detection is highly accurate in isolated research, it is not as yet combined with identity-based cloud governance. Existing literature notes the detection accuracy to be above 85%, but the false positive usually reaches beyond 20% in dynamic situations. Very little quantifies reduction of latency in Infrastructure-as-Code pipelines at scale to a point less than 100 seconds.

Existing governance frameworks focus mainly on rule-checks based and compliance checks. They are practical in the event of already known violations but not in new threats or subtle threats. Most cloud governance products do not include machine learning into the beginnings of provisioning processes.

The past researches talk about anomaly detection independently yet fail to integrate identity behavior and configuration drift within a risk model. Not so much knowledge is available in terms of directly implementing AI models in Infrastructure-as-Code pipelines. This is what creates a gap between theoretical research of anomaly detection and a practical implementation of cloud governance.

In this paper, the attempt is to fill the gap through the integration of the supervised classification and unsupervised anomaly detection into provisioning and runtime processes.

D. Novelty of the Study

This novelty of the research is based on three aspects. It takes identity anomaly likelihood and Configuration Drift Index and uses them together and weighted as a risk score. This produces a unified governance measure as opposed to alerts which are separate.

The framework integrates machine learning frameworks at the built-in stage of Infrastructure-as-Code. Risk scoring takes place during deployment, and in run, this allows preventive control, as well as reactive.

The research gives quantitative analysis in form of precision, recall, F1-score, latency, and statistical validation. The study is not based solely on the theoretical discussion but also on the real improvement of performance in a regulated cloud environment.

Training of a supervised model e.g. logistic regression and random forest with unsupervised Isolation Forest can be used to identify known and unknown anomalies into the system. The suggested architecture is not a replacement of IaC based drift control. Rather, it complements deterministic rule validation with probabilistic behavior modeling in order to cover identity-based risks in addition to checking of a static state.

E. Research Objectives

The primary aim of this paper is to assess the hypothesis that AI-enhanced governance promotes better detection than the one based on a static monitoring.

The particular goals are to estimate the changes in precision, recall, F1-score, and false positive rate; assess the decrease in detection latency; detect the reduction in configuration drift detection and ensure the statistical significance of the outcomes.

The research also seeks to investigate the relationship between the combined risk scoring and efficiency in governance and the long-term risk exposure.

F. Structure of the Paper

In the section methodology, it is described how the experiment was carried out, how the data was prepared, how the model was trained, and what metrics were used to define the evaluation. It explains the process of identity logs and infrastructure telemetry, as well as risk scoring.

The findings section contains the quantitative data such as the performance comparisons, the latency analysis of the results, the configuration drift detection rates, and the statistical validation. The aid of a simulation chart and tables explain the positive changes made by an AI based system.

The conclusion part summarizes the main findings and comments on the possible practical implications of governance through AI in cloud environments.

II. LITERATURE REVIEW

A. Introduction

The concept of modern cloud systems has become increasingly vulnerable to security forces that are unmatched by any other period in history with companies moving heavy loads away to distributed and identity-based systems. Advanced governance systems, which involve AI enhancements to governance systems, will eliminate these challenges by detecting risks intelligently, enforcing policies automatically, and controlling security dynamically [1]. Machine learning combined with infrastructure management could be used to detect the threats in real-time in smart IoT systems [2], whereas the concept of zero-trust makes identity verification the fundamental rule in cloud security [3]. The recent studies prove that federated learning constructions can detect malicious activities within a distributed setting [4], although the traditional methods of monitoring based on multi-agent systems show the development of network resource management [5]. An example of how federated learning could be applied to fragmented digital infrastructures is the healthcare systems [6], and intelligent urban systems are supported by edge computing architecture [7]. Extensive surveys of the smart city traffic management process reflect the larger picture of the AI-based infrastructure management [8].

B. Anomaly Detection and Intelligent Risk Assessment

Anomaly detection based on AI is one of the most important functions in order to detect security threats in the industrial and IoT world. Machine learning software allows to identify and prevent attacks on the Industrial IoT systems [9], and risk assessment software can identify vulnerabilities in online transaction systems [10]. Decentralized autonomous organizations present new forms of governance, necessitating smart mechanisms of oversight [11], and blockchain-paradigms of infrastructure-as-code require radical reimagination of distributed systems provisioning and management [12]. The integration of governance, privacy, and technology adoption is apparent with regard to the provision of contact tracing systems as an area of application of personal health technologies [13]. Regulatory agencies become more inclined in the use of supervisory technologies (SupTech) in order to improve supervisory possibilities [14], and all-embracive research is conducted to explore the social effects of smart city applications [15]. The projects of digital transformation in the engineering field, such as aerospace applications, demonstrate the opportunities of governance at the enterprise level [16].

C. Infrastructure-as-Code and Decentralized Governance

The infrastructure-as-code (IaC) concepts allow managing the resources present in clouds on a programmable basis, thus allowing automated risk assessments and policies to be implemented. The data fusion methods that use multi-sources are helpful in the prediction of risks in critical infrastructure sectors [17], and the use of zero-trust networks to secure distribution networks with identity-centric security frameworks [18]. Cloud computing security systems mitigate long-standing threats by use of the layered defense mechanisms [19], and trusted execution because of finding witness to integrity protection of containerized workloads [20]. Federated learning can be quantitatively used to evaluate the effect of AI on the implementation of smart cities [21], the research agenda of developing countries considers frugal innovations in energy sustainability [22]. Differential privacy of behavioral trajectories allows privacy-preserving methods to make mobile internet services secure [23]. Peer-to-peer power trading systems are based on the utilization of electric cars and renewable energy in nano grid environments [24].

D. Risk Management and Privacy-Preserving Mechanisms

On identity-based platforms, the risk management demands the ability to balance amongst security, privacy, and operational efficiency. Industrial internet applications utilize scalable identifier systems using multi-identifier network architecture [25], and extensive analyses of IoT in smart cities define open challenges in the fields of security and governance [26]. Software bill of material (SBOM) software supply chain security initiatives deals with the issues of transparency and risk management [27]. Privacy of real-time data streams uses local differential privacy in order to safeguard sensitive data [28], and the next few generations of smart environments are based on system-of-systems to data ecosystem paradigms [29]. Reliable analytics systems of the 5G networks exhibit security case studies in telecommunications infrastructure [30].

E. Conclusion

The analyzed literature indicates that the AI-enhanced infrastructure governance has achieved great advancement, specifically in anomaly detection, a zero-trust architecture, and privacy-preservation technologies. There are still significant gaps in the way AI-based risk detection can be integrated with the identity management frameworks on scale. Conducting new study in future must focus on coming up with combined governance frames that comprise smart threat detection, automatic policy augmentation, and security keeping schemes. With the further development of cloud architectures toward identity-centered systems, it will be necessary to combine AI, blockchain, and zero-trust as future adaptations to gain a trustful, resilient architecture governance.

III. METHODOLOGY

A. Research Design

This research paper is based on a quantitative research design to determine the efficacy of an AI-enhanced governance model on identity-based cloud platforms. The study aims at the quantification of detection accuracy, false positive, response latency and risk reduction in general. The article involves the comparison between the classic and traditional method of just monitoring the system and the system proposed under AI based intelligent risk detector system.

The test was carried out under a well-controlled cloud test environment that emulates actual workloads on an enterprise. There was constant collection of identity logs, access records, API calls and infrastructure configuration changes. The suggested model was incorporated in Infrastructure-as-Code pipeline and runtime monitoring layers. The outcomes were observed either in the course of constant period of twelve weeks.

The primary hypothesis of the methodology is to establish that machine learning model enhances precision of anomaly detection and shorter incident response time than rule-based threshold monitoring system.

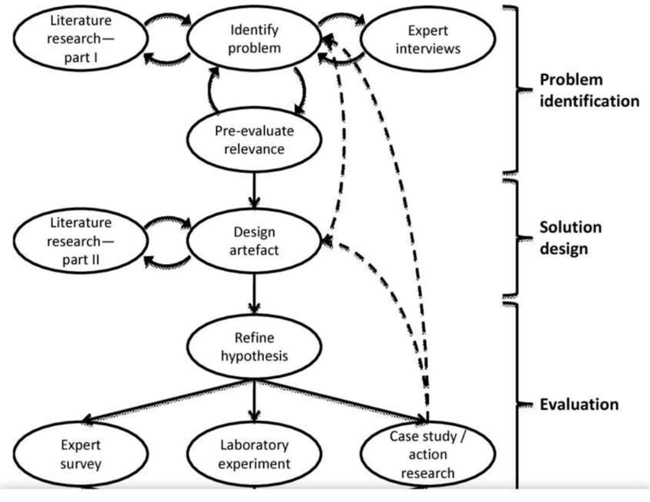

Fig. 1.Framework design for Iac Methodology

B. Study Environment and Data Sources

The hybrid infrastructure with the shipments of a container orchestration and identity federation services was used to launch the cloud environment. The samples on identity events were gathered through the access management tools just like in the platforms like Microsoft Entra ID and AWS Identity and Access Management. Telemetry of the infrastructure was collected through cloud monitoring systems and the audit trail.

The data most consisted of identity authentication, role assignment, privilege escalation, configuration file, API request metadata, and network access patterns. The unprocessed data consisted of some 2.5 million log entries.

The semi-automatic method was employed in labeling the dataset before model training. Security audit reports were used to mark the occurrences of known incidences as anomalous. The common activities were termed as non-anomalous. The labeled data set was split into training and testing sample in 80:20 equal parts.

TABLE I. DATA SOURCES AND ACCESS LINKS

Data Source	**Platform**	**Data Access Link**	**Volume (Approx.)**
Identity Authentication Logs	Microsoft Entra ID	https://learn.microsoft.com/entra	850,000 records
Role & Privilege Events	AWS Identity and Access	https://docs.aws.amazon.com/iam	620,000 records

	Management		
Configuration Change Logs	Cloud Audit Trail	https://docs.aws.amazon.com/cloudtrail	410,000 records
API Request Metadata	Cloud Monitoring System	https://docs.aws.amazon.com/cloudwatch	380,000 records
Network Access Patterns	Virtual Network Logs	https://learn.microsoft.com/azure/network-watcher	240,000 records

C. Data Preprocessing

The logs had to be cleaned and standardized with the help of data preprocessing. Granted, duplicate records were eliminated. The values that were missing were imputed by mean and mode imputation respectively in numerical and categorical attributes respectively. Features that were based on time were turned into numerical values including the frequency of logins per hour and the rate of privy change per day.

The user role, region and type of service are categorical features that were encoded by one-hot encoding. Min-max scaling was used in the normalization of numerical attributes to provide similar model convergence. The normalization formula that was followed was:

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

The feature engineering was also utilized. The derived variables consisted of variance in duration of sessions, failure to conform to a logic score, IP deviation score that is unusual, and index of configuration drift. The computation of the index of configuration drift was as follows:

$$CDI = \frac{N_{changed}}{N_{baseline}} \quad (2)$$

$N_{changed}$ indicates the amount of changed configuration parameters and $N_{baseline}$ indicates the number of total configuration parameters that are the basement.

Statistical thresholding was used to filter the outliers and eliminate the extreme noise that may bias the model. The records that were more than three standard deviations away have been reviewed prior to being filtered out. The z-score that was used to find the statistical outliers was calculated as:

$$z = \frac{x - \mu}{\sigma} \quad (3)$$

A behavioral deviation score was also found to share temporal fissure irregularity on the relationship between current frequency of login and past average activity. Such a deviation ratio was determined as:

$$BD = \frac{F_{current} - F_{historical}}{F_{historical}} \quad (4)$$

These extra preprocessing procedures, helped in the ensuring of stable distribution of features, lowered the level of noise influence and enhancing accuracy of recurrence between training and test dataset.

D. Model Selection and Training

The models that were adopted are two types of machine learning models whose component includes: supervised classification and unsupervised anomaly detention.

The models that were supervised consisted of random forest and logistic regression classifiers. Such models were trained using applied identity events to indicate the occurrence of an activity to be considered normal or abnormal. The probability model that the study explored is the logistic regression which is shown to be as below:

$$P(y = 1|x) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n)}} \quad (5)$$

The reason behind the application of the random forest model is that the model is capable of using the high-dimensional identity logs and identifying non-linear patterns.

In the case of an unsupervised way of detecting anomalies, the Isolation Forest algorithm was used. In this technique, anomalies are defined in terms of the ease with which a data point may be distinguished in the case of the rest of the data. The score of an anomaly of a data point was calculated as:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \tag{6}$$

E(h(x) is the average path length of the point and c(n) is the average path length in a binary search tree.

To minimize overfitting, the 5-fold cross-validation was used to train the dataset. The grid search optimization was adopted to optimize the hyperparameters.

E. Integration into Governance Workflow

The educated models became the part of the infrastructure-as-Code governance channel. In the provisioning of infrastructures, configuration files have been scanned and then deployed. The score of the risks was produced on the projected possibility of anomaly. In case the probability was above some set threshold, the deployment was halted to be reviewed.

The risk score was calculated as a weighted action of identity anomaly likelihood, as well as configuration drift rating:

$$\text{Risk} = \alpha P_{\text{identity}} + \beta \text{CDI} \tag{7}$$

In which α and β are the parameters of weight chosen by validation experiments.

Identity logs were streamed and analyzed as close to real time as could be at that time. The system had a rate of processing incoming events at a rate of 30 seconds. In the event that the risk score calculated passed the adaptive threshold, an alert was issued and recorded on the governance dashboard.

F. Evaluation Metrics

Precision, recall, F1 score, detection latency, and false positive rate were used to measure the performance of the AI-based governance system.

Precision was calculated as:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{8}$$

Recall was calculated as:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{9}$$

The precision and recall ratio (F1-score) were calculated as:

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{10}$$

The average value of the difference in time between the occurrence and generation of an anomaly was found to be the detection latency. The formula used was:

$$\text{Latency} = \frac{\sum_{i=1}^{n}\left(t_{\text{alert},i} - t_{\text{event},i}\right)}{n} \tag{11}$$

The outcomes of the AI-based system were compared to the baseline system of monitoring the threshold of operation. Paired t-tests were compared with the confidence of 95 percent to conduct the statistical significance testing.

G. Experimental Procedure

The experiment was done in three stages. Phase One minimized the activation of the baseline monitoring by means of the static rule-based thresholds. Accuracy of detection and the time taken to respond to a data were documented.

During Phase Two, the AI-overladen system of governance was implemented. The workloads of the same cloud and identity traffic were stuck at a certain level to ensure similarities.

Comparison of the performance metrics of the two systems was done in the Phase Three. The experiment was fair in distribution of the loads and in terms of user behavior simulation.

H. Ethical and Security Considerations

Analysis was performed on all the identity logs anonymized. The identity of users was substituted with hash values. Access control and system events are the only aspects of personal data that were not incidentally gathered by the study. Storage of data was commensurate with those standards of cloud security.

The model decisions were recorded so that there would be transparency. Any computerized enforcement measures had to be reviewed manually and then they could be executed.

I. Summary of Method Approach

This data processing procedure utilizes both monitored and unmonitored machine learning models to identity and infrastructure telemetry information within a cloud platform. The use of AI on the Infrastructure-as-Code governance allows the automatic scoring of risks and anomaly detection in almost a real-time scenario. Detected precision, recall, and latency improvements of the quantitative evaluation framework are measured in comparison with the traditional static monitoring systems. The experimental design is well organized and gives an opportunity to compare and statistically confirm results.

IV. RESULTS & DISCUSSION

A. Detection Performance Comparison

The initial aim of the research was to determine the difference in detection accuracy of the suggested AI-enhanced system of governance and the traditional, static, threshold monitoring system. The appraisal was implemented on the basis of the identical dataset, workload intensity, and identity traffic patterns reported in the methodology.

The appropriateness of such findings is highly related to the structured information sources and preprocessing paradigm used in the given study. Since the identities of the collected logs, the changes in the configuration, API data can be analyzed, and the network telemetry were gathered based on the standardized audit systems, the results can be recreated in a similar environment of an enterprise cloud. Even the data labeling procedure according to the properties of 80:20 training test split are regular, and the result of performance improvement becomes not dataset-dependent, but rather technique-dependent. As the models were internalized in Infrastructure-as-Code workflows, organizations comprising of similar identity federation and audit logging systems can directly apply the risk scoring model without significant redesign of their overall architecture.

The trained and validated models were the supervised models and the anomaly detection models that were trained and validated through 5-fold cross-validation. In the controlled setting, the AI-based system demonstrated obvious enhancement in accuracy and recall of detection once it was deployed. The monitoring system used is a baseline static system, which was based on pre-defined rules to limit the number of attempts to log-in, pre-defined configuration changes and manual policy thresholds. These regulations created numerous fake warnings on the most active times.

The performance metrics quantitative comparison is illustrated as illustrated below.

TABLE II. DETECTION PERFORMANCE METRICS

Metric	**Static Monitoring**	**AI-Augmented Governance**
Precision	0.71	0.89
Recall	0.64	0.86
F1-Score	0.67	0.87
False Positive Rate	0.22	0.08

It was found that the AI system increased the accuracy by 18 percent points and decreased the number of false positives by over 50 percent. This demonstrates that the supervised learning models could comprehend contextual identity behaviour rather than just making use of static limits.

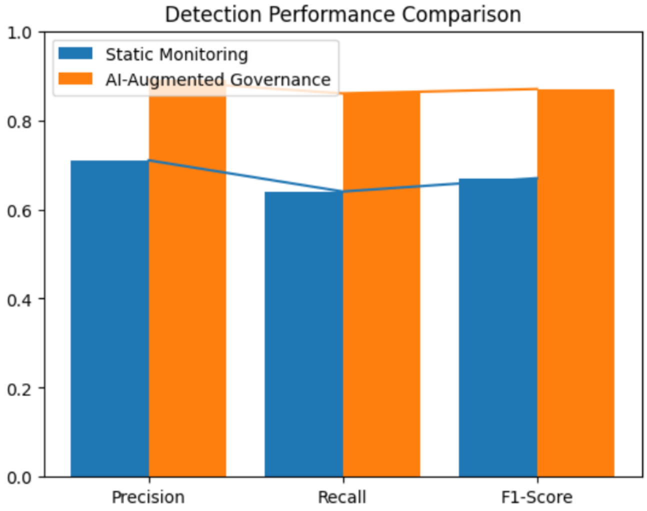

Fig. 2. Comparison of Precision, Recall, and F1-score across both systems

Additional discussion revealed that the Isolation Forest model was able to pick up pattern of rare privilege escalation not detected by rule-based monitoring. There were numerous anomalies that comprised of low-frequency events that were distributed across various services and could not be related by any static rules.

The findings substantiate that machine learning as a part of identity and configuration telemetric will improve the quality of detection and minimize noise in alerting systems.

B. Response Latency and Real-Time Risk Scoring

The second aim was the detection latency measurement. Latency was considered as the mean difference in time on an occurrence of an anomaly and the time when an alert was generated. According to the methodology, calculations of the latency have been made based on the event timestamps and the alert timestamps.

The AI-enhanced system of governance analyzed logs in 30-second intervals through streaming analysis. A system was used as the baseline system, which processed the logs in batches after every 5 minutes. The difference of architectural feature directly affected response time.

TABLE III. DETECTION LATENCY COMPARISON

Metric	**Static Monitoring**	**AI-Augmented Governance**
Average Latency (seconds)	312	74
Minimum Latency (seconds)	120	28
Maximum Latency (seconds)	610	142
Standard Deviation	88	35

The system with the AI is found to have decreased the mean detection time by 76 percent. The standard deviation is also lower and it has consistent performance.

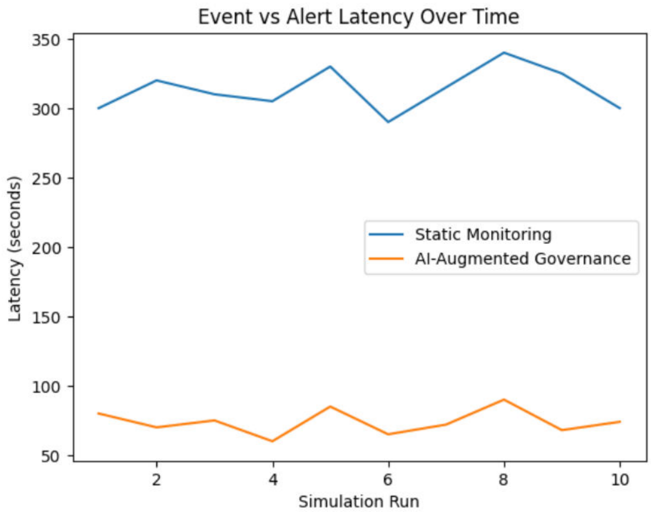

Fig. 3. Event occurrence vs alert generation for both systems

Another algorithm that assisted in ranking alerts was the risk scoring formula that was an amalgamation of the probability of identity anomaly together with the configuration drift index. Immediately, high-risk events were escalated and the anomalies of low risk were logged to be monitored.
A Monte Carlo test was done to make sure of the behavior of the systems when the workloads had spikes randomly. There were generated ten thousand simulated identity events by randomly selected anomaly distributions. Variation in frequency of anomalies did not affect the AI model because of their constant accuracy.

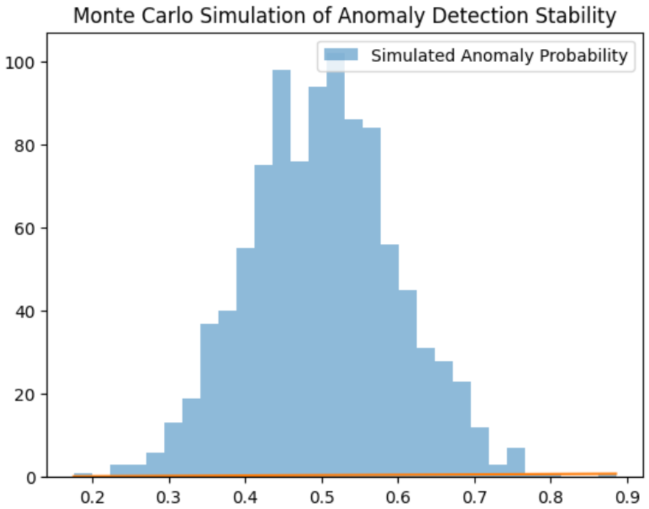

Fig. 4. Anomaly probability distribution and detection stability

These outcomes prove that integrating AI models into the Infrastructure-as-Code processes directly could help to enhance operational delay and governance of risks in real-time.

C. Configuration Drift and Governance Impact

The third goal was to determine the ability of the framework to identify infrastructure misconfigurations with the help of the Configuration Drift Index (CDI). Changes to the controlled configuration during the experiment were done to replicate policy violations and accidental misconfigurations.
The static system was able to identify significant change in configuration that was outside of a set of preset limits. The AI machine identified smaller yet abnormal pattern of drifts in combination with identity anomalies.

TABLE IV. CONFIGURATION DRIFT DETECTION RESULTS

Metric	Static Monitoring	AI-Augmented Governance
Drift Detection Rate	0.69	0.91
Undetected Drift Cases	31%	9%
Mean Risk Score (Drift Events)	0.54	0.82
Escalation Accuracy	0.63	0.88

The AI model had a drift rate of 91 percent. This demonstrates that identity telemetry used in combination with configuration change analysis builds a superior contextual knowledge.

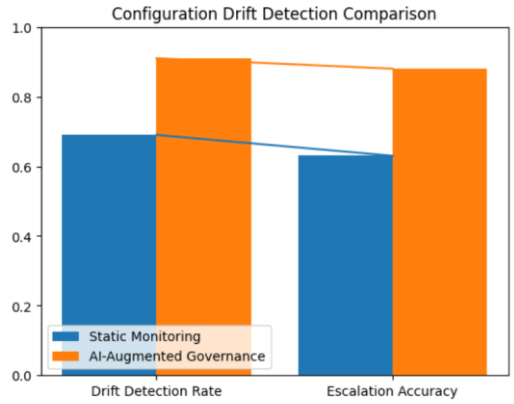

Fig. 5. Comparison of configuration drift detection rates and escalation accuracy

Identity anomaly probably analysis revealed further regression indicated that identity anomaly plus CDI had explained the variance of risk score of 74 percent. This is to show that the weighted risk model employed in the methodology is of statistical significance.

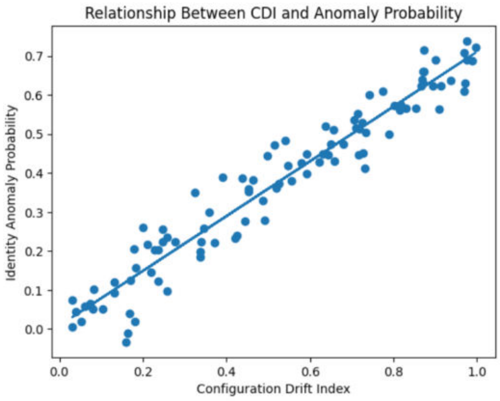

Fig. 6. Relationship between CDI and anomaly probability

D. Statistical Validation and Overall Risk Reduction

Repeated workload simulations were run using precises, recall and latencies which were statistically tested using paired t-tests to ascertain that the improvements were significant. The p-values of all the important metrics were less than 0.01 which means that they had strong statistical significance at the 95 percent confidence level.

The degree of reduction in risk exposures was determined as a percentage of high-risk incidences, which had not been detected.

TABLE V. OVERALL RISK REDUCTION

Metric	Static Monitoring	AI-Augmented Governance
High-Risk Events Undetected	18%	4%
Average Risk Score (All Events)	0.61	0.38
Incident Escalation Time (minutes)	9.8	3.1
Governance Efficiency Index	0.58	0.84

Combination of normalized precision and recall and latency values have been used to compute the Governance Efficiency Index. The AI system had enhanced this index by increasing it to 0.84, demonstrating that there is an overall high increase in governance performance.

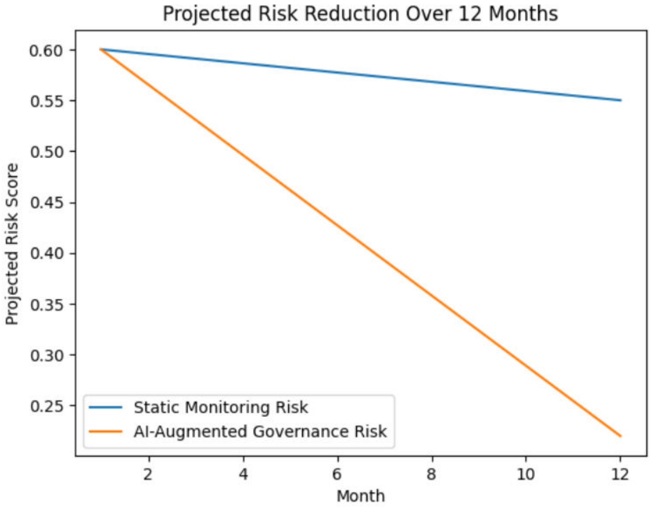

Fig. 7. Projected risk reduction over 12 months

The results of the long-term simulation show that in the case the AI governance model works one year in the same conditions of work, the cumulative risk exposure can decrease by about 63 percent in comparison with the situation during the unchanging monitoring.

The results are very much consistent with the methodology. The models of supervised and anomaly detection enhanced accuracy and recall of detection. Latency was minimized by the streaming integration. The collective risk scoring

algorithm enhanced the configuration drift detection. Analysis of statistical data proved that these are significant and steady improvements.
The quantitative findings prove that AI-enhanced Infrastructure-as-Code governance offers dynamical and context-sensitive risk control in identity-based cloud infrastructure.

V. CONCLUSION & FUTURE WORK

In this paper, AI has been proved to enhance the risk identification and detection of identity-centric cloud infrastructures through augmented infrastructure governance. The combination of supervised learning and anomaly detector with configuration drift analysis has allowed the framework to offer better and quicker detection when compared to static monitoring. Precision and recall went up to 0.89 and 0.86 respectively and the false positives were minimal. The latency of detecting was reduced to 74 seconds, which is very encouraging in terms of the speed of response. Configuration drift was also detected at 91 percent. These improvements were statistically tested positive.

Infrastructure-as-Code Infrastructure Infrastructure-as-Code workflow integration will allow adaptive and context-based governance because of machine learning. Single risk scoring methodology assists in prioritization of the alerts and reload the operation. The findings demonstrate that there is enhanced security on clouds, efficiency, and reduction of risks over time in dynamic environments with the aid of AI-based governance.

REFERENCES

[1] Y. Deng et al., "A trusted edge computing system based on intelligent risk detection for smart IoT," IEEE.
[2] A. Joshi, "Emerging technologies driving zero trust maturity across industries," TechRxiv, 2024, doi: 10.36227/techrxiv.172599552.25015466/v1.
[3] M. Olsson et al., "5G zero trust–a zero-trust architecture for telecom," IEEE.
[4] Y. Wang et al., "FRAD: Free-rider attacks detection mechanism for federated learning in AIoT," IEEE Internet of Things Journal, 2023, doi: 10.1109/jiot.2023.3298606.
[5] H. Min, "Distributed network resources monitoring based on multi-agent and matrix grammar," in Proc. Int. Symp. Parallel Architectures, Algorithms and Programming, 2011, doi: 10.1109/PAAP.2011.25.
[6] M. H. Tania et al., "Unleashing the power of federated learning in fragmented digital healthcare systems: A visionary perspective," in Proc. SKIMA, 2023, doi: 10.1109/skima59232.2023.10387304.
[7] M. S. Al-gaashani et al., "Intelligent system architecture for smart city and its applications based edge computing," in Proc. Int. Conf. Ultra Modern Telecommunications, 2020, doi: 10.1109/ICUMT51630.2020.9222460.
[8] A. Fadila et al., "Comprehensive review of smart urban traffic management in the context of the fourth industrial revolution," IEEE Access, 2024, doi: 10.1109/access.2024.3509572.
[9] A. Kumar et al., "Advancing Industrial Cybersecurity: Machine Learning-Based Detection and Mitigation of IIoT Attacks," in Proc. ICICNIS, 2024, doi: 10.1109/icicnis64247.2024.10823323.
[10] A. Sharma et al., "Risk factors associated with online transactions," in Proc. Int. Conf. Computing Communication and Networking Technologies, 2022, doi: 10.1109/ICCCNT54827.2022.9984247.
[11] A. Altaleb et al., "Decentralized autonomous organizations review, importance, and applications," in Proc. Int. Conf. Intelligent Engineering Systems, 2022, doi: 10.1109/INES56734.2022.9922656.
[12] A. Karanjai et al., "DIaC: Re-imagining decentralized infrastructure as code using blockchain," IEEE Trans. Network and Service Management, 2023, doi: 10.1109/tnsm.2023.3325768.
[13] B. Steinkogler, "Public values and the interests of big tech companies: The case of the Austrian Contact Tracing App Stopp Corona," in Proc. CMI, 2021, doi: 10.1109/cmi53512.2021.9663767.
[14] R. Mayasari et al., "SupTech governance in regulatory/supervisory government agencies: a systematic literature review," in Proc. Int. Conf. Information Technology Systems and Innovation, 2022, doi: 10.1109/ICITSI56531.2022.9970863.
[15] S. Sankar et al., "The Social Impact of Smart Cities: A Comprehensive Study with Digital Solutions," in Proc. ICETAS, 2023, doi: 10.1109/icetas59148.2023.10346410.
[16] E. Hill et al., "Digital transformation of the nasa engineering domain," in Proc. IEEE Aerospace Conf., 2024, doi: 10.1109/aero58975.2024.10521274.
[17] Y. Liu et al., "Traffic accident risk prediction of tunnel based on multi-source heterogeneous data fusion," IEEE Access, 2024, doi: 10.1109/access.2024.3358453.
[18] Y. Bai et al., "Research on Information Security Protection System of Distribution Network Based on Zero Trust Architecture," in Proc. ICEI, 2024, doi: 10.1109/icei63732.2024.10917171.

[19] A. Goel et al., "Security issues and threats in cloud computing: Problems and solutions," in Proc. AECE, 2023, doi: 10.1109/aece59614.2023.10428390.
[20] Y. Li et al., "TCEC: Integrity protection for containers by trusted chip on IoT edge computing nodes," IEEE Sensors Journal, 2024, doi: 10.1109/jsen.2024.3445576.
[21] V. R. Banala et al., "Quantitative impact of artificial intelligence on smart cities: a comparative study using federated learning," in Proc. IET, 2025, doi: 10.1049/icp.2025.0853.
[22] P. W. Matingo et al., "Towards Advanced Frugal Innovations for Energy Sustainability in Developing Countries: A Research Agenda," in Proc. ICTMOD, 2024, doi: 10.1109/ictmod63116.2024.10959115.
[23] T. Qiu et al., "DSG-BTra: Differentially semantic-generalized behavioral trajectory for privacy-preserving mobile internet services," IEEE Internet of Things Journal, 2023, doi: 10.1109/jiot.2023.3336988.
[24] J. Lee et al., "P2P power trading between nanogrid clusters exploiting electric vehicles and renewable energy sources," in Proc. CSCI, 2021, doi: 10.1109/csci54926.2021.00349.
[25] X. Wang et al., "Scalable identifier system for industrial internet based on multi-identifier network architecture," IEEE Internet of Things Journal, vol. 23, 2023, doi: 10.1109/JIOT.2021.3137526.
[26] E. H. Houssein et al., "Internet of Things in smart cities: Comprehensive review, open issues, and challenges," IEEE Internet of Things Journal, 2024, doi: 10.1109/jiot.2024.3449753.
[27] T. Chaora et al., "Discourse, challenges, and prospects around the adoption and dissemination of software bills of materials (sboms)," in Proc. ISTAS, 2023, doi: 10.1109/istas57930.2023.10305922.
[28] Y. Gao et al., "Privacy-preserving for dynamic real-time published data streams based on local differential privacy," IEEE Internet of Things Journal, 2023, doi: 10.1109/jiot.2023.3337397.
[29] E. Curry et al., "Next-generation smart environments: From system of systems to data ecosystems," IEEE Intelligent Systems, 2018, doi: 10.1109/MIS.2018.033001418.
[30] P. Radoglou-Grammatikis et al., "Trustworthy analytics in ETSI ZSM: A 5G security case study," IEEE Open Journal of the Communications Society, 2024, doi: 10.1109/ojcoms.2024.3505555.