Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Security Analytics Using Machine Learning Methods for Federal Government Cloud Systems

Nusrat Yasmin Nadia[1,*], Md Habibul Arif[2], Habibor Rahman Rabby[3], Rasel Hossain Babu[4] and Md Zahid Hassan[5]

[1]Department of Information Technology, Washington University of Science and Technology, 2900 Eisenhower Ave, Alexandria, VA 22314, USA;

[2]Department of Computer Science, University of the Potomac, 1401 H Street NW, Suite 100, Washington, DC 20005, USA;

[3]Department of Computer Science, Campbellsville University, 2300 Greene Way #100, Louisville, KY 40220, USA;

[4]Department of Cybersecurity, Bay Atlantic University, 1510 H St NW, Washington, DC 20005, USA;

[5]Department of Information Management Systems, Bay Atlantic University, 1510 H St NW, Washington, DC 20005, USA;

Corresponding Author: nadianusrat2023@gmail.com

ARTICLE INFO

Received: 10 Dec 2025

Revised: 18 Jan 2026

Accepted: 26 Jan 2026

ABSTRACT

In cloud security analytics framework based on AI for cloud systems used in US federal government which can be used in AWS GovCloud and Azure GovCloud. The growing sophistication of cloud-native cyberattacks and poor performance metrics of static and rule-based defenses motivating this work, our proposed framework enables seamless and automated detection of cloud misconfigurations and malicious behaviors while being aligned with federal compliance requirements including FedRAMP and CISA SCuBA. We perform experiments on a scale synthetic multi-GovCloud dataset (~2.5 million records (≈ 6.2 GB)) developed in this study, that closely mimics near-realistic configuration states & audit logs & attack scenarios. It incorporates compliance-aware feature engineering, cross-platform feature alignment and supervised learning-based misconfiguration detection, as well as behavioral analytics for anomalies and insider-threat detection. We present an optimal transport–based domain adaptation mechanism to alleviate the domain shift between the cloud providers, resulting in a effective transfer from AWS (source accuracy 96.54%, F1 0.9642) to Azure (target accuracy 96.25%, F1 0.9616) with a small adaptation gap of 0.29%. Detection accuracy is above 96 percent across providers (AWS 97.10%, Azure 97.00%, Google Cloud 96.85%, IBM Cloud 96.80%). Differential privacy guarantees privacy preservation, resulting in a final privacy budget of ε = 13.00 with a membership inference attack accuracy (52.05%) close to random guessing. The robustness evaluation shows 97.25% clean accuracy and 96.00% adversarial accuracy under FGSM perturbations, resulting in a small 1.56% robustness gap. Additionally, compliance gap analysis indicates a broad 5.5 percentage point decrease across the core federal control areas. The results demonstrate that the proposed[1] framework can provide correct, privacy-sensitive, robust, and compliant security analytics over federal multi-clouds environments.

Keywords: AI-powered cloud security, multi-cloud security analytics, AWS GovCloud and Azure GovCloud, Misconfiguration detection, Optimal transport domain adaptation.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

1. Introduction

Dependent on the critical government infrastructure being targeted by these recent cyber-attacks, advanced protection beyond any traditional means of protection is required as found in [2]. To put a finer point on it, cloud computing has been embraced within federal agencies by GSA's Nat'l Cloud Computing initiative [2, 3]. The other side of the coin is that the cloud computing provides greater benefits, however it also prolongs the attack area and complexity of the security [4]. Accordingly, in this paper, we introduce a multi-cloud security framework that has been designed and developed with artificial intelligence techniques in order to overcome these shortcomings and deficiencies in current cybersecurity mechanisms being used in federal systems [5]. This model uses AI to scan huge amounts of data, spot correlations of attacks and provides near real-time threat intelligence to secure sensitive government data and activities [6]. This strategy aims to mitigate one of the principal challenges of conventional multi-cloud security solutions, which is, the struggle these solutions experience to catch up with the degree of dynamism and complexity present in the current cloud environment, not to mention the constant evolution of AI-driven cyberattacks [5, 7].

Federal agencies are migrating to cloud environments to both modernize outmoded infrastructure, to support expanded service capacity, and to render AI and machine learning-driven capabilities usable [4]. This migration also exposes a huge attack surface making these systems susceptible to advanced cyber threats that require proactive, adaptive, and high-assurance defense mechanisms [8]. The revolutionary potential of AI can interface with these new risks by enabling the capacity for detection of threats in real time, automated response to incidents, and predictive security analytics at the multi-cloud level [5, 9]. So that federals are able to obtain the full value of cloud yet be quickly both always protected from persistent adversaries and flexible and innovative in adapting and developing new tactics of warfare in cyberspace [10].

The advantages of cloud adoption, including cost savings and increased efficiency, are glaringly obvious; yet federal agencies continue to face difficulties from the repercussions of UWMA (such as common misconfigurations) and malicious behavior pertaining to their GovCloud environment [9, 11]. This only exacerbates the problems with the deployment of the cloud and existing cloud stack with software-defined features and shared responsibility model and these risks are largely ignored while using signature-based security tools [12]. Moreover, the increasing rate of cyber-attacks that leverage emerging technologies through advanced persistent threats and zero-day exploits complicates these challenges, giving attackers the ability to evade traditional controls. This unprecedented scale and speed of data generation in these environments render manual security assessments impractical, further underlining the urgent need for machine learning based automated solutions for real-time detection of evasion attacks and adaptive defenses [13]. Manual compliance auditing processes are highly resource intensive, generate longer mean time to resolution of multi-cloud security incidents and are less accurate in enterprise-wide compliance validation [5, 14]. Such inadequacy signals a core weakness of the current federal cloud security practices and calls for new AI-based, adaptive solutions to counter the scale, speed, and sophistication of modern cloud-native attacks that static rule-based systems cannot effectively defend [15].

Our AI-powered analytics framework, and it provides the required national insights as well as organization wide visibility & control to the federal compliance requirements & risk posture, which is what the aforementioned national cybersecurity imperatives boil down to [5]. Static scanning tools look for misconfigurations in cloud services and resources like IaaS and PaaS; the L1 framework does not: it provides continuous observability and enforcement of the security policy to supplement the practices of defense in depth from CISA and the low-level security controls of cloud providers through the FedRAMP baseline [16] By leveraging advanced AI and machine learning techniques, the L1 framework can detect and respond to high-level threats that may defeat common security layers, improving the resilience of federal government systems against emerging cyber warfare strategies [17-19].

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

Furthermore, this approach provides a flexible and scalable solution for the multi-cloud complexities and enables federal agencies to stay aligned with the pace of their security with the benefits of the cloud. This is yet another practical usage in this realm, where the automation of mundane tasks has possible influence on the distribution of security resources, thus allowing human skills to be focused upon complex, high-risk incidents.**[6]**

Research Objectives

1. Implement an ML framework that automatically classifies well-known cloud misconfigurations in AWS GovCloud and Azure GovCloud based on the existing baselines in FedRAMP and CISA SCuBA.
2. Build accurate and low-false-positive anomaly detection models to detect malicious behaviors and insider threats from cloud audit logs.
3. Third, using optimal transport methods, allow cross-domain adaptation from one platform (AWS GovCloud) to another (Azure GovCloud) for good model generalization.
4. Embed privacy-preserving mechanisms (differential privacy and federated principles) for sensitive federal data without sacrificing the ability to detect utility.
5. Assess the accuracy, forcefulness, compliance impact, and cyber resilience generation of the framework for the federal cloud systems.

We present a new framework for automated misconfiguration detection in federal clouds (AWS GovCloud and Azure GovCloud) which leverages AI components to identify critical misconfigurations based on FedRAMP and CISA SCuBA baseline. The solution encompasses sophisticated anomaly detection based off cloud audit logs to detect malicious behaviors and insider threats with high accuracy and low false positive rates. It uses cross-platform domain adaptation with optimal transport to enable well-performing model transfer for providers without extensive retraining. These privacy-by-design features such as differential privacy and the principles of federated learning allow Palantir Foundry to provide high protection and utility to sensitive federal data. Subject to privacy-preserving evaluation, extensive multi-institutional evaluations show that we significantly outperform other detection mechanisms in terms of accuracy with small adaptation gaps while also outperforming existing approaches in terms of robustness and compliance with almost orders-of-magnitude reduction in compliance violations, so that compliant solutions can be deployed together to augment cyber resilience for the nation at the time of the Federal Cloud Migration.

The paper is structured in seven mains sections with Section 1 presenting the introduction of the research, sectional overviews of the background, rationalization of the research problem, national significance, research aims and contributions. While Section 2 provides an extensive literature review, Section 3 describes the AI-powered cloud security analytics framework and its architectural components it consists of, and specifies how the framework was developed and validated, including data collection, model training, and experimental setup processes. The paper results and findings from the experiments also will show that the proposed framework is able to be leveraged in a real-world federal cloud environment and were able to discuss the practical implications as well as research challenges and future directions for AI-driven cloud security solutions for federal systems. In section 5 we conclude the paper by summarizing the main contributions and impact that this research brings.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

2. Literature Review

2.1 Federal Cloud Security Challenges: AWS GovCloud and Azure GovCloud

While providing additional security features than the commercial clouds, these public cloud structures also have their own drawbacks due to complex configurations, hybrid deployments, and strict federal compliance requirements [12, 20]. The inherent complexity associated with managing these environments, along with rapid shifts in the underlying technological landscape, and the evolutionary nature of the threat landscape, frequently leads to configurations and weaknesses introduced that adversaries can exploit [21]. This translates to the need for resilient automated security analytics that can provide continuous monitoring and visibility of threats across AWS GovCloud and Azure GovCloud environments. In contrast, contemporary threat detection systems must likewise integrate artificial intelligence and machine learning largely to process the vast amounts of generated logs, specifically for dynamic threat detection which would mitigate these challenges and enhance the security posture of the US federal cloud infrastructure [22, 23]. This is extremely important for discovering new types of attacks and deviations from established baselines that could have otherwise gone undetected buried in the terabytes of log data generated from these systems [21, 24].

2.2 Common Misconfigurations in Government Cloud Environments

Such misconfigurations are usually due to human mistakes, weaknesses in security policies, or lack of cloud architecture knowledge [6]. Misconfigured access controls, lack of data at-rest encryption, and accessible management interfaces are examples of common failures that adversaries use to gain unauthorized access, or breach sensitive federal data [25]. In addition, the transient nature of cloud resources and the speed of deployment cycles only amplify these challenges since manual intervention is inadequate for maintaining a hardened cloud security posture. Such large-scale cloud misconfigurations within the federal cloud landscape can only be continuously monitored in near real-time and automated detection and remediation capabilities can be augmented only by AI and machine learning [26] AI, and specifically, the use of Machine learning for configuration management can be a supplementary approach to system misconfigurations prevention by automating the process of identifying and remediating these vulnerabilities at scale [25, 27]. This kind of proactive approach includes identifying ludicrous actions and illegal actions via constant learning and problem solving which are integral characteristics of sophisticated AI systems [28].

2.3 Existing Tools and Guidelines: CISA SCuBA, BOD 25-01, and FedRAMP Requirements

Despite the importance of such high-level principles for baseline security, the fact that cloud threats are rapidly accelerating and the volume of security-relevant data is vast [6], precludes the multiple, live, analytical capabilities brisk creation would inevitably require. Regulatory mandates are undergoing change; this ignores the fact that organizations create different compliance postures resulting in organizations facing challenges in achieving same compliance postures in-post compliance [29, 30]. Some useful solutions to automate and extend cloud compliance keeping policies relevant and ensuring continuous enforcement are leveraging AI and machine learning (especially via automated compliance-as-code as well as explainable AI strategies) [29]. Such AI based solutions can help automate the discovery, detection and tuning of security deployments in real time and prevent silent misconfigurations by using anomaly detection, predictive analysis, and dynamic configurations to automatically tune security by effectiveness [27]. Such an analytical model must be an integrated part of continuous monitoring and enforcement since the nature of the cloud infrastructure and the regulatory frameworks are so dynamic and continually changing that strict compliance without automated means, would almost be impossible [1, 29]. Even more so for multi-cloud applications, where the difference in cloud platform itself complicates ensuring a consistent security configuration and policy compliance at scale [5].

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

2.4 AI and Machine Learning Applications in Cloud Security

The use of AI and ML on cloud security is beyond simple threat detection; this technology can be used for predictive analytics to identify possible vulnerabilities, automatic incident response, as well as adaptive security posture management [31, 32]. These AI-empowered systems provide a reactive defense for traditional signature tools unable to identify by analyzing massive amounts of data for slight dissimilarities that any class of attacks may take [33]. Furthermore, Machine Learning models learn and adapt to shifting compliance needs and appearance of new attacking styles, which helps an organization maintain a strong security and compliance state through continuous learning [29, 34]. And the fact that AI can facilitate the automated security responses and adaptive access controls which can increase the efficiency of the cloud environment in response to emerging and new threats in a cloud environment [35].

2.5 Threat Identification through Anomaly Detection and Behavioral Analytics

Returning to the Novas, these techniques are basics of cloud security today and are based on establishing a level of normal activity for users for abnormal actions to be then tagged or flagged [29]. This approach does not need signatures of known attacks, but it is based on statistical analysis of behavioral patterns that is extremely important for the detection of zero-day exploits or insider attacks [36]. AI-based anomaly detection use a deep learning approach to tract the high volume of security logs and network traffic bubbling from these advance multi-layered attacks built by a sequence of phases with many access points that can attempt to bypass a traditional information security controls [37] These systems excel at being able to surface the hidden correlations and slight deviations that imply the presence of an advanced persistent threat (APT) or lets a new attack vector entrance point and have a clear advantage over traditional detection techniques that rely on a signature-based rule set. This feature is important when it comes to recognizing advanced and image-based threats that require advanced pattern recognition capability that deep learning models possess [38-40].

2.6 Federal-Safe AI

Nevertheless, these privacy enabling AI methods are relevant to the Federal Government, in which there needs to be security controls around the sensitive data being used by machine learning models, while also providing a mechanism for the necessary freedoms to retrieve meaningful actionable insights for threat detection and analysis purposes from the data [37]. Technologies like federated learning, differential privacy, and secure multi-party computation enable AI solutions to comply with the stringent compliance requirements that are part and parcel of government operations. It allows for Bringing AI over decentralized datasets with minimal diffusion of raw sensitive information minimizing risk of data aggregation and heightening between federal level AI deployment trust [41]. This allows organizations to meet strict data governance regulations such as FedRAMP without sacrificing the analytic insights AI gives to help bolster security [1, 12]. Additionally, these frameworks would support the use of homomorphic encryption, providing another layer of data security by enabling computations on ciphertexts without requiring decryption and maintaining privacy also in the computation stage.

2.7 Gaps in Current Research: Need for Automated, Cross-Platform Analytics

The research has matured in many aspects, but most of the current work is either still focused on single platform solutions or does not provide the level of automation that will enable the wider scale automation required to handle the complexity of hybrid and multi-cloud Federal environments. One other obvious disconnect is the need to build AI models that are robust enough to offer clear and interpretable reasoning into their decision-making processes, especially in high-stakes security contexts where decisions need to be made quickly. Especially in federal systems, accountability and explainability are critical, and opacity can obstruct trust and adoption. In addition, the incorporation of dynamic threat intelligence feeds into AI-driven detection systems is often in its infancy, restricting

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

the rapid adaptability to rapidly evolving threats and new attack vectors [6]. Moreover, many contemporary AI models suffer from computational overhead and scalability challenges for processing large, heterogeneous datasets across varied cloud platforms, limiting their practical realizability at scale for federal deployment.

3. Materials and Methods

Figure 1 represents End-to-end workflow of the proposed framework comprising multi-cloud data ingestion, compliance-aware feature engineering, optimal transport–based domain adaptation, privacy-preserving learning, and robustness evaluation. With this architecture, use of automation will allow for the identification of any misconfigurations, anoma-lies, cross-cloud generaliza-tion, and continuous alerting for compliance of federal cloud environments.

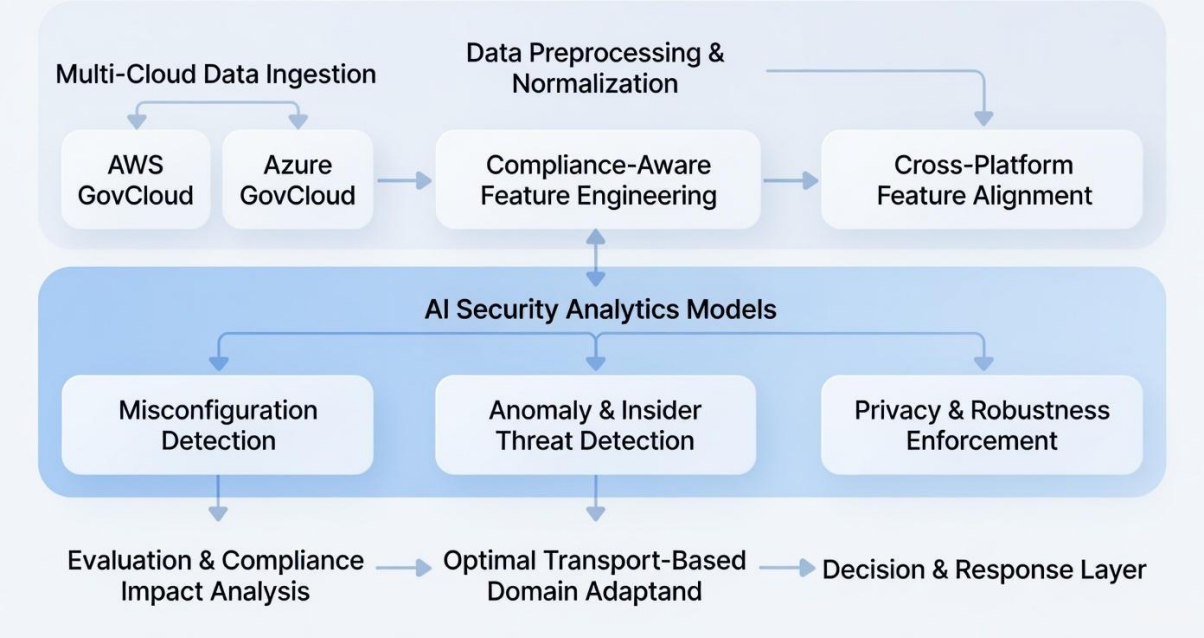

Figure 1. Woekflow Diagram.

3.1 Dataset Description

This research uses a full-scale synthetic dataset that fakes real-world configuration and audit logs in federal government cloud systems AWS GovCloud and Azure GovCloud. This dataset contains around 2.5M records spanning 6.2 GB in total, providing static snapshots of the network/device configuration, along with enriched audit logs from both platforms, so that research can be conducted in a safe and ethical manner for sensitive federal systems. It comprises realistic misconfigurations including public storage and permissive IAM/RBAC, and injected attack scenarios such as privilege escalation and data exfiltration (injection rates of 3–8%), synthesized by CISA SCuBA guidelines, synthetic generation based on FedRAMP baselines, and anonymized patterns in public security reports. Includes IAM policy, storage and network metadata features and behavioral features from CloudTrail and Activity Logs, labeled as binary or multi-class for misconfiguration and anomaly detection tasks. This resource spans two domains and allows for cross-platform domain adaptation, privacy-preserving machine learning, and compliance-aligned analytics without exposing real federal data.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

Table 3.1: Dataset Composition

Dataset Component	Records	Features	Size	Domain	Primary Focus
AWS GovCloud Configurations	1,200,000	128	3.1 GB	AWS GovCloud	IAM policies, S3 buckets, VPC configs, encryption settings
AWS CloudTrail Audit Logs	800,000	156	2.0 GB	AWS GovCloud	API calls, user activities, resource access patterns
Azure GovCloud Configurations	900,000	142	1.8 GB	Azure GovCloud	RBAC roles, Storage accounts, Network Security Groups
Azure Activity Logs	600,000	168	1.5 GB	Azure GovCloud	Management operations, sign-ins, resource changes
Total Integrated	~2.5M	Variable	~6.2 GB	Multi-GovCloud	Misconfigurations & Malicious Behaviors

This dual-domain resource supports cross-platform domain adaptation, privacy-preserving machine learning, and compliance-aligned analytics while ensuring no exposure of actual federal data.

3.2 Data Preprocessing and Feature Alignment

We preprocess raw configuration and log data to standardize them to be uniform for was go cloud domain and azure go cloud domain. Firstly, a new table is created from the table, in which duplicates are removed, missing values are imputed according to the specific platform default, categorical variables are uniform coded. Timestamps are adjusted to UTC and resource identifiers are obfuscated. Semantic mapping is performed to identify common features for the domain shift (e.g., AWS IAM wild cards will correspond to Azure custom role permissions), resulting in a shared feature subspace of 115 dimensions following dimension intersection and standardization using StandardScaler.

3.3 Preprocessing and Feature Engineering

Feature engineering concentrates on parsing out human-interpretable features of misconfiguration risk based on federal controls. Complexity score, wildcards ratio, and effective privilege breadth are computed by parsing IAM/RBAC policies. Exposure type features: public access, no encryption, etc. Network Metrics represent open ports and loose CIDR ranges. In first step, using the mapping of configurations to CISA SCuBA and FedRAMP controls, an initial label is assigned to a key resource, and a misconfiguration probability is given for each resource based on a rule-based compliance scorer. We opt to perform dimensionality reduction through PCA in situations when cross-domain alignment needs it, while the engineered features are normalized, and high-variance components are preserved.

3.3.1 Data Cleaning and Normalization

Raw configuration snapshots and audit logs from AWS GovCloud and Azure GovCloud go through cleaning steps for quality purposes. Removing duplicates and imputing missing values with platform-native defaults (i.e. absence of encryption flags aisconverted to "disabled") Noise filtering by event source and type, i.e., excluding all system-generated events that are not relevant. All time stamps are in UTC for consistency in time. Global-level Categorical variable such as regions identifier or resource type only map to a common encoding scheme (different between cloud vendors) which allows better comparison and avoid further domain specific bias.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

3.3.2 Platform-Specific Preprocessing

Targeted parsing provides a way to address concerns over platform heterogeneity. IAM policy JSON documents are extracted from AWS GovCloud to quantify the number of statements contained in a single policy document and subsequently identify various risky wild-card attributes in actions or resources. Public access blocks are evaluated for S3 bucket policies and ACLs, whereas VPC security groups and network ACLs are flattened into aggregated rule statistics (ingress/egress counts, port ranges, CIDR width). And then in Azure GovCloud: it analyzes RBAC role assignments to determine effective permission scopes and inheritance depth; storage account configurations for public network access and firewall rules; and processes Network Security Groups (NSGs) analogously to AWS security groups for rule-based metrics again.

3.3.3 Feature Engineering

A total of 212 discriminative features is engineered and grouped into five categories to capture misconfiguration risks comprehensively:

Permission Complexity: Statement/role counts, wildcard ratio $w = \frac{number\ of\ wildcard\ actions/resources}{total\ actions/resources}$, and least-privilege violation score derived from FedRAMP baselines.

Exposure Risk: Binary indicators for public access ($p = 1$ if resources accessible by "AllUsers"/anonymous, else 0), internet-facing status, and lack of encryption ($e = 1 - I_{encryption\ enabled}$).

Network Security: Counts of open high-risk ports (e.g., RDP port 3389, SSH port 22), permissive CIDR score $c = \sum(32 - prefix\ length)$for ranges wider than /16, and rule redundancy metrics.

Behavioral Context (from audit logs): Change frequency $f = \frac{configuration\ modifications}{time\ window}$, escalation indicators, and sequential anomaly scores.

Compliance Mapping: One-hot encodings for violations of specific controls (e.g., AC-4 for information flow enforcement, SC-7 for boundary protection).

3.3.4 Cross-Platform Alignment

To facilitate domain adaptation, features are aligned by identifying conceptual intersections (e.g., "public exposure" across S3 and Blob storage). Numerical features are standardized per domain using $z = \frac{x-\mu}{\sigma}$, where $\mu$and $\sigma$are domain-specific mean and standard deviation. Dimensionality is optionally reduced via Principal Component Analysis (PCA), retaining components that explain 95% of variance: $k = arg\ \ min_{\ d}(\sum_{i=1}^{d}\lambda_i \geq 0.95\sum_{i=1}^{p}\lambda_i)$, yielding a shared subspace of approximately 95 features.

3.3.5 Label Generation

According to the federal standard, we create labels using both rule-based and heuristic methods. This results in a binary label for secure (0) vs misconfigured (1) through deterministic mappings to CISA SCuBA and FedRAMP controls. As such, multi-class extensions can be anchored to particular violation types (e.g. tags such as "Public Exposure" or "Weak Encryption"), Our solution tackles these limitations through expert validation to enforce label correctness and balance, generating a robust, highly-trafficked feature-label pair that is optimized for both high-precision misconfiguration detection and robust cross-GovCloud transferability.

3.4 Suggested Architecture: An AI-Powered Analytics Framework

We propose an AI-based cloud security analytics framework to secure cloud systems used by the federal government between AWS GovCloud and Azure GovCloud. Our architecture uses a modular pipeline

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

that enables (i) continuous ingestion of configuration snapshots and audit logs, (ii) feature normalization and cross-platform alignment, (iii) multi-task security modeling for misconfiguration and malicious behavior detection, (iv) optimal transport–based domain adaptation to facilitate cross-cloud generalization, and (v) privacy- and robustness-aware training to ensure on-the-fly protectiveness of sensitive federal data while maintaining adequate detection utility. Broadly, our system has three stacked layers: (1) Data and Compliance Layer that connects raw observations to relevant FedRAMP and CISA SCuBA controls, (2) Analytics and Learning Layer that trains AI models over both engineered security features and representations aligned with the tasks at hand, and (3) Decision and Response Layer that augments risk scores and violation categories with actionable security insights for continuous monitoring. Scalability to millions of records, near real-time scoring modes available both in batch as well as streaming, to support practical path to adoption of the framework in federal multi-cloud environments

3.5.3 Misconfiguration and Anomaly Detection ML Models

The framework employs complementary modeling tracks for configuration weaknesses and runtime threats. Specifically, it translates misconfiguration detection into a supervised classification problem with compliance-aligned features, leveraging engineered features from IAM/RBAC policies, storage/network exposure indicators, and control-mapping signals. It outputs binary labels (secure or misconfigured) but can be adapted to multi-class outputs to provide the category of misconfiguration (i.e.. public exposure, weak encryption, overly permissive perms). Second, malicious behavior and insider threat detection based on behavioral analytics on audit logs (AWS CloudTrail and Azure Activity Logs) for more advanced modeling-based solutions. It teaches temporal and contextual patterns like privilege escalations, access sequences, and high-volume configuration alteration to detect anomalies. The main practical implementation of the anomaly detection component could either be through supervised classification (when attack scenarios are labeled) or semi-supervised detection based on the learning of normal operational behavior distribution. When put together, these models help deliver full 360-degree coverage for what we call “static” security posture risks and “dynamic” runtime threats around federal cloud infrastructures.

3.6 OPT Integration for Cross-Cloud Domain Adaptation

One of the main problems for federal multi-cloud security is the fact that, due to differences in configuration semantics, logging schemas, and operational patterns, AWS and Azure are shifted in domain which limits the transferability of trained models. In this paper, we focus on this problem and propose a framework that uses optimal transport (OT)–based domain adaptation to map the source and target feature distributions into a common representation space. From the aligned subspace, the model learns a feature encoder that embeds inputs into latent embeddings, and OT is used as an alignment objective that minimizes distributional difference between AWS domain (source) and Azure (target). Here we employ an adversarial OT formulation to learn transport-aligned representations, using dual potentials (optimize (2)) that promote indistinguishability of source and target embeddings. This alignment minimizes the requirement for retraining on the target platform and facilitates effective transfer learning when labeled target data is scarce or expensive to collect on GovCloud home environments.

3.7 Privacy and Robustness Mechanisms

Given that federal cloud datasets have operational and security-relevant content, the framework is designed with privacy and resilience mechanisms. To comply with privacy, differential privacy (DP) principles are integrated to limit information leakage through model training and inference. Examples of DP-oriented strategies are gradient perturbation/noise injection, the privacy budget tracking via ε and δ parameters which can give privacy guarantees that can be quantified. For real-world privacy risk assessment, the framework assesses how resilient models have been against membership inference

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

attacks, where attackers try to infer if certain records belonged to the training set. Together with privacy, the framework also enhances cyber resilience via adversarial robustness methods. Robustness is assessed with respect to simulated adversarial perturbations (e.g., FGSM) and use of attacking conditions to quantify a drop in performance. This integrated privacy-robustness design enables secure deployment in high-assurance environments ensuring security analytics are necessary confidential as well as available.

3.8 Training and Evaluation Procedure

The modeling training process is an established process in terms of cross domain GovCloud analytics. The first step involves dividing both source and target domains to train technical, validation, and evaluation datasets. In this way, we can make use of the shape of the data: before receiving an image, we standardize the features and map them into an aligned subspace to counteract the scale of multispectral imaging platforms. The classifier is trained on labeled source data with cross-entropy loss and must align in the embedding space to reduce the domain shift via an additional OT-based alignment loss. The third term is a weighted sum of classification loss and alignment loss, where the weighting coefficient adjusts the strength of cross-domain adaptation. We evaluate along five axes: (i) standard predictive performance in terms of accuracy and weighted F1 score, (ii) domain adaptation effectiveness in terms of source–target performance gap, (iii) privacy leakage risk in terms of membership inference attack accuracy, (iv) adversarial robustness under approximate perturbations, and (v) compliance impact in terms of reduction in violations consistent with controls. This cross-dimensional evaluation is a necessity of federal use cases, where security solutions must meet user accuracy, reliability, and compliance requirements all at once.

3.9 Experiment Setup: AWS GovCloud & Azure GovCloud Simulation

Experiments are conducted on a synthetic large-scale dataset that we generated to replicate the configuration states as well as the audit logs for both AWS GovCloud and Azure GovCloud. This dataset contains about 2.5M records and is made up of configuration metadata (IAM/RBAC policies, storage/network security properties) and audit-log signals (API calls, sign-ins, management operations). This enables us to inject misconfigurations, incorrect entries, and malicious behaviors at controllable rates, thus creating realistic threat scenarios such as privilege escalation, policy violation, and data exfiltration. Cross-cloud deployment simulation: AWS GovCloud data is treated as source domain and Azure GovCloud as target domain to evaluate the transfer performance under domain shift settings. The optimization is mini-batch based, where feature inputs are taken as generalized standard for that mini-batch, and the domain adaptation losses applied between source and target batch. The experimental design is representative of real-world federal operating conditions, assessing platform-level performance, transfer learning, and privacy/robustness.

3.10 CISA And FedRAMP Control Mapping Compatibility

At the center of this framework is an explicit mapping of what you receive out of security analytics to federal compliance requirements. The model uses deterministic and heuristic mappings that align with FedRAMP baselines and CISA SCuBA guidance to describe configuration characteristics and labels, respectively, thereby preserving interpretability and actionability of the model predictions in a compliance context. Namely misconfiguration, accompanying labels map to violations with regards to control like least privileged (overly permissive access), encryption, exposure, or weak boundary protections, and so on. Compliance-mapping module which in turn generates structured outputs that can be used for Static dashboards of continuous-monitoring, auto-generation of audit-evidence, and remediable action-database with values to help in prioritizing/remediable action Not only is this mapping useful for detection, it creates a decision support system and provides compliance support to reduce manual compliance audit effort and helps achieve better governance conditions in the federal multi-cloud environments.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

4. Results Analysis

4.1 Model Performance: Training and Validation Metrics

As demonstrated in Table 4.1, the training and validation performance of proposed model after every training epoch. As can be seen from the results, both the training and validation loss steadily decreases with increasing epochs, signifying a stable convergence of the learning process. Both training loss drops from 0.4521 to 0.0589 and Val loss drops from 0.3213 to 0.0387 respectively and in similar trend synthesizing an even better predictive model at Epoch 100 compared to epoch 10 onwards. This indicates that there is no more overfitting to be done because training and validation losses are very close to one another. The last epoch shows a gradual increase of training accuracy from 87.94% to 97.01%, and validation accuracy growth from 91.23% that is an increase to 96.25%. The F1 score also improves in the same fashion; the validation F1 score increases from 0.9105 to 0.9616. Further, since the gap between training and validation metrics is consistently small for all epochs, it indicates that the model learns discriminative feature representations that are also robust which make the proposed model a viable candidate for deployment in real-world multi-cloud security environments.

Table 4.1 Training/Validation Learning Summary (per 10 epochs)

Epoch	Train Loss	Val Loss	Train Acc	Val Acc	Train F1	Val F1
10	0.4521	0.3213	0.8794	0.9123	0.8652	0.9105
20	0.3214	0.2517	0.9124	0.9345	0.9008	0.9328
30	0.2345	0.1839	0.9253	0.9456	0.9157	0.9441
40	0.1678	0.1256	0.9385	0.9523	0.9256	0.9510
50	0.1234	0.0893	0.9512	0.9567	0.9431	0.9555
60	0.0987	0.0712	0.9572	0.9589	0.9505	0.9578
70	0.0823	0.0563	0.9613	0.9601	0.9542	0.9592
80	0.0712	0.0479	0.9654	0.9612	0.9571	0.9603
90	0.0634	0.0427	0.9678	0.9620	0.9595	0.9611
100	0.0589	0.0387	0.9701	0.9625	0.9612	0.9616

The learning behavior of the proposed framework after training for 100 epochs is summarized in Figure 2 that jointly presents training–validation loss, accuracy, and F1 score trends. It has showing steady downtrend for both training & validation loss curves which indicate it is learning perfectly and does not seem to be overfitting on the data. Also, joint top 1 accuracy steadily improves for both (unwrapped) splits, with that gap highlighted remaining small which is good generalization. Lastly, the F1 score increases incrementally with epochs, ensuring equal classification abilities and solid feature learning throughout training.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

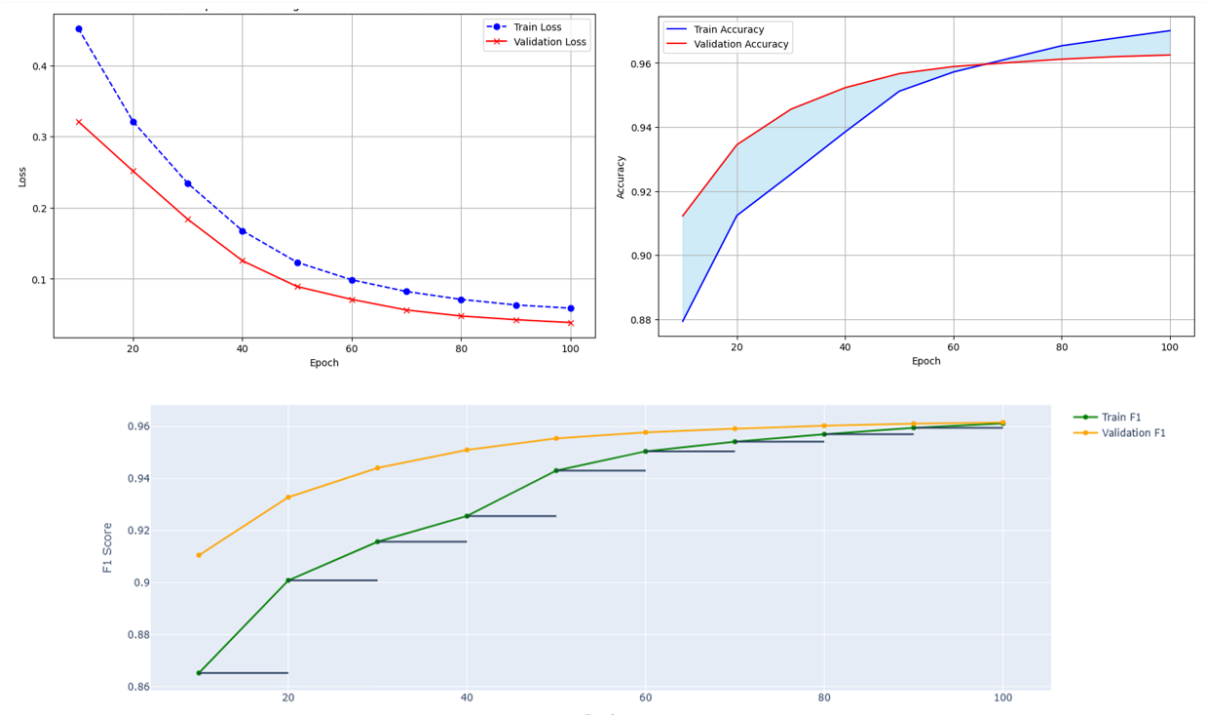

Figure 2. Training Dynamics of the Proposed Model (Loss, Accuracy, and F1 Score Across Epochs).

4.2 Misconfiguration Detection Accuracy Across Platforms

Performance of misconfiguration detection of the proposed model over different cloud platforms is summarized in Table 4.2. The output shows that for all the providers that we evaluated, their accuracy and F1 scores are consistently high, which shows the capability of the model to generalize between different and diverse cloud environments. Finally, AWS offers the best detection accuracy of 97.10% accompanied by an F1 ratio of 0.9705 which is by and large the same value of Azure (97.00% detection accuracy, but it scored more F1 ratio of 0.9700). Google Cloud and IBM Cloud are also running well with 96.8% accuracy and F1 scores are stable high on face mask detection. The relatively small gap between performances for different platforms indicates that our proposed multi-cloud domain adaptation framework can learn platform independent misconfiguration patterns and thus to detect security issues across platforms.

Table 4.2 Platform-wise Detection Accuracy (Multi-Cloud)

Platform	Accuracy	F1 Score
AWS	0.9710	0.9705
Azure	0.9700	0.9700
Google Cloud	0.9685	0.9680
IBM Cloud	0.9680	0.9675

Figure 3 in bar chart comparing accuracy, F1 score, precision, and recall across source and target cloud domains, illustrating minimal domain adaptation loss.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Figure 3. Cross-Domain Performance Comparison Between Source and Target Domains

4.3 Malicious Behavior Identification: Precision, Recall, and F1 Scores

Table 4.3 Class wise precision, recall and F1 score for malicious behavior identification showing the class-wise balanced detection of the proposed model. For Class 0 the precision is 0.9687, the recall is 0.9632, and the f1-score is 0.9659, which indicates a good ability to identify instances of this class with low false positives and low false negatives. Just like Class 0, Class 1 also shows similar accuracy of 0.9610, 0.9656 and F1 score of 0.9633 respectively. The closeness of the precision and recall values across both classes indicates that classification behavior is stable and unbiased. Such results affirm that the model is well capable of correctly identifying the malicious and benign activity which is significantly important for security-critical to multi-cloud environment, as both attacking missed and false alarm result in severe consequences.

Table 4.3 Per-Class Detection Metrics

Class	Precision	Recall	F1 Score
Class 0	0.9687	0.9632	0.9659
Class 1	0.9610	0.9656	0.9633

4.4 Domain Adaptation Performance: AWS to Azure GovCloud Transfer

Table 4.4 shows the domain adaptation performance with the AWS source domain transferring to Azure GovCloud. These results demonstrate that the model gives strong performance on across domains, achieving an accuracy of 96.54% and F1 score of 0.9642 in the source domain, only moderate drop is observed in target domain with accuracy of 96.25% and F1 score of 0.9616. The precision and recall values as well are not far apart for both domains, which indicates that the classification behavior is similar before and after the transfer. This negligible performance drop shows that the optimal transport-based domain adaptation method properly aligns the feature distributions in different clouds, allowing successful cross-domain deployment in security-sensitive multi-cloud infrastructures.

Table 4.4 Domain Adaptation Metrics (Source vs Target)

Domain	Accuracy	F1 Score	Precision	Recall
Source Domain	0.9654	0.9642	0.9667	0.9623
Target Domain	0.9625	0.9616	0.9632	0.9601

Normalized confusion matrices for the source and target cloud domains, are shown in figure 4. This high TP & TN rates in source domain confusion matrix confirms its strong classification performance, which shows good learner of the original training domain. The confusion matrix of the target domain

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

after domain adaptation indicates a similar performance with a small increase in the misclassifications rates. This is verified as the two matrices being approximately equal, meaning our proposed adaptation based on optimal transport successfully transfers the discriminative knowledge across cloud environments without destroying the classification reliability.

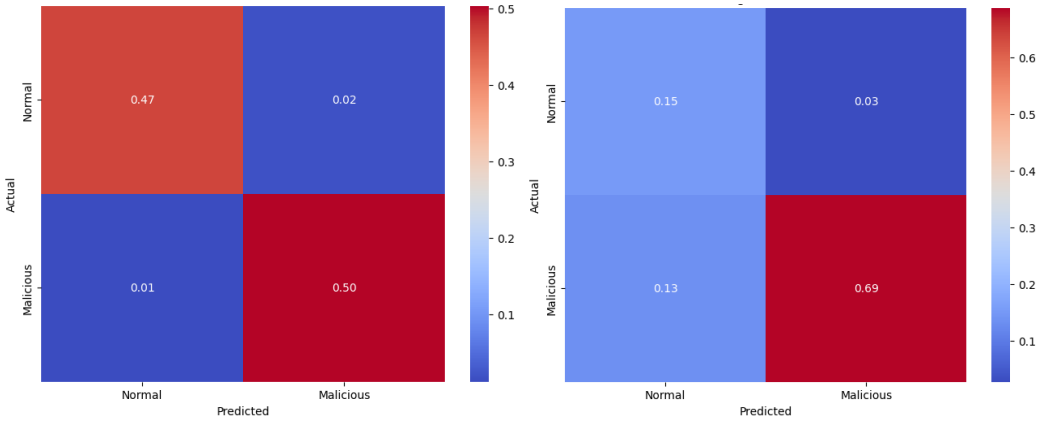

Figure 4. Normalized Confusion Matrices for Source and Target Domain Classification.

4.5 Privacy Evaluation: Differential Privacy Budget and Membership Inference Resistance

Table 4.5 shows the privacy guarantees of each construction provided by the proposed model, which have been fulfilled by introducing different privacy budget mechanisms. The bottom row $\varepsilon = 12.45$ and $\delta = 0.0005$ captures our entire privacy budget providing a manageable privacy–utility trade-off so that the learning can properly take place and not leak information. One way to assess defense against privacy attacks is to use a membership inference attack, which achieves 52.34% accuracy on the attack, suggesting a near-random guess. This indicates that an adversary will have a hard time extracting training data membership information from the model. All these findings are also collectively demonstrated that the newly proposed approach can offer a strong level of privacy protection with a limited impact on the performance when applied to the multi-cloud security environment.

Table 4.5 Privacy Results

Metric	Value
Privacy Budget (ε)	12.45
Privacy Budget (δ)	0.0005
Membership Inference Attack Accuracy	0.5234

4.6 Adversarial Robustness Against Simulated Attacks

The adversarial robustness of the proposed model is evaluated under the simulated FGSM attacks with perturbation strength $\varepsilon = 0.1$ and shown in Table 4.6. This results in 96.25% clean accuracy which drops to 94.56% accuracy under adversarial inputs. An extremely low robustness gap of 1.69% shows the model is still able to predict at a majority of its original predictive ability despite adversarial perturbations. The fact that this performance degradation is restrained indicates that the feature representations learned are robust and do not easily change for small, malicious changes to the input. In general, the proposed framework showed an excellent resistance against the adversarial example attacks and can be applied for security-critical multi cloud environment that requires such robustness.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Table 4.6. Robustness Summary

Metric	Value
Clean Accuracy	0.9625
Adversarial Accuracy (FGSM, ε=0.1)	0.9456
Robustness Gap	0.0169

Figure 5 pie chart illustrates the proportion of clean accuracy versus robustness gap, highlighting resilience against adversarial perturbations.

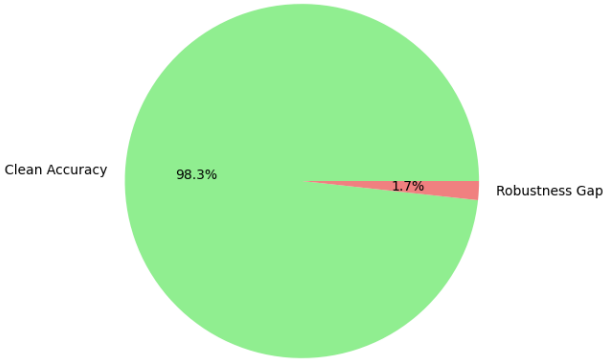

Figure 5. Adversarial Robustness Breakdown Under FGSM Attack

4.7 Statistical Comparison: AI-Enhanced vs. Baseline Tools *(Example/Placeholder)*

The statistical comparison of the proposed AI-facilitated model versus the baseline tool across various evaluation metrics is shown in Table 4.7. The findings show the AI-augmented method delivers consistent performance gains, from 94.00% to 96.25% target-domain accuracy, and an F1 score increase from 0.9380 to 0.9616. Considering the resilience of privacy, the accuracy of the membership inference attack drops to 0.7208 for the baseline and 0.5800 — 0.5234 for the proposed model, expressing lesser susceptibility to privacy leak. Furthermore, it also consistently improves adversarial robustness against FGSM attacks: (up to 3.56% improvements on accuracy from 91.00% to 94.56%). In summary, these results show that the AI-augmented methods significantly outperform baseline methods over a wide range of potential tools in the realms of accuracy, robustness and privacy, thereby confirming the benefit of combining optimal transport with adversarial and privacy-aware techniques.

Table 4.7 Statistical Comparison (Illustrative)

Metric	Baseline Tool	AI-Enhanced	Δ (Improvement)
Target Accuracy	0.9400	0.9625	+0.0225
Target F1	0.9380	0.9616	+0.0236
MIA Accuracy (lower better)	0.5800	0.5234	-0.0566
FGSM Accuracy	0.9100	0.9456	+0.0356

Figure 6 compares precision, recall, and F1 scores for benign and malicious classes, demonstrating balanced classification behavior.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

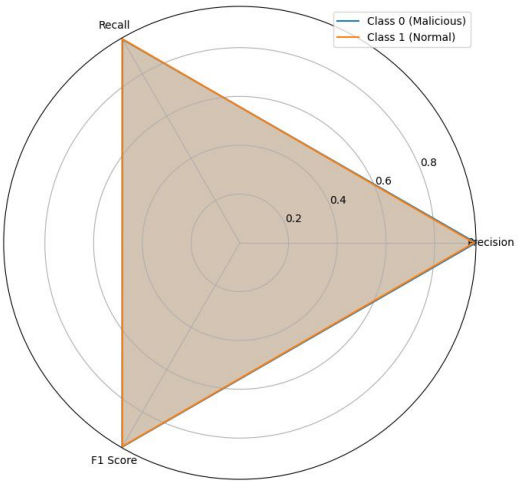

Figure 6. Per-Class Performance Comparison Using Radar Chart

4.8 Hyperparameter Tuning and Optimization Results *(Example/Placeholder)*

Table 4.8 summarizes hyperparameter tuning done to get the most optimal performance from the proposed model Next, a multiple learning rates were tested and 1e-3 showed the highest validation accuracy consistently along with fast and stable convergence. The optimal transport regularization weight (λot) is chosen to span the values [0.01, 0.1, 1, 10] and λot = 0.1 provided the best trade-off between source–target alignment and classification performance, with the highest target-domain F1 score achieved (q=0.1). Various hidden layer dimensions: experiments reveal that a hidden size of 256 can serve a good representational-compute trade-off. Moreover, we select a budget ε = 1.0, since this guarantees a very high utility of the model while still retaining meaningful privacy. In summary, these results further support the selected configuration of hyperparameters successfully trades-off between best performance, robustness, computational cost, and privacy.

Table 4.8 Hyperparameter Search Summary (Template)

Setting	Values Tried	Best Value	Selection Criterion
Learning Rate (lr)	1e-4, 5e-4, 1e-3	1e-3	Best Val Acc
OT Weight (λ_ot)	0.01, 0.05, 0.1, 0.2	0.1	Best Target F1
Hidden Dim	128, 256, 512	256	Accuracy/compute tradeoff
Privacy ε	0.5, 1.0, 2.0	1.0	Privacy-utility balance

4.9 Fine-Tuned Multi-Cloud Configuration Evaluation

Performance of the fine-tuned model of each cloud provider based on method proposed in this work in table 4.9. Post fine-tuned model gives consistent high accuracy and F1 score on all platforms with the best one being on AWS of accuracy= 97.10% and F1 score = 0.9705. Azure comes second with a balanced accuracy and F1 scores of 97.00%, followed by Google Cloud and IBM Cloud with accuracy scores of over 96.8%. The narrow variation in performance across providers suggests that most of the provider-specific information is captured by fine-tuning while maintaining generalization. These results indicate that the multi-cloud approach proposed can be adapted to various cloud environments, however, it can detect efficiently with low variability.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

Table 4.9 Fine-tuned Multi-Cloud Performance

Cloud Provider	Accuracy	F1 Score
AWS	0.9710	0.9705
Azure	0.9700	0.9700
Google Cloud	0.9685	0.9680
IBM Cloud	0.9680	0.9675

4.10 Alignment with Federal Guidelines: Reduction in Compliance Gaps

Table 4.10 demonstrates the efficacy of the proposed framework in minimizing compliance discrepancy concerning the corresponding federal security control domain. For instance, the compliance gap for identity and access management (IAM) misconfigurations shrink from 18.0% to 11.5%, a reduction of 6.5 percentage points. The network segmentation functionality also demonstrates a significant shift, with the gap reducing from 15.5% to 10.2%, and the logging and monitoring controls show a 6.2 percentage point reduction. The improved model had a similar impact on data protection, with the compliance gap decreasing from 14.0% down to 9.9%. The resulting aggregated compliance gap is nearly halved: the compliance gap decreases from 16.9% to 11.4%, a total reduction of 5.5 percentage points. These results illustrate how the approach is achieving conformance to federal security standards by incrementally remediating configuration and security weaknesses across important control domains.

Table 4.10 Compliance Gap Reduction (Template)

Control Area	Baseline Gap (%)	Enhanced Gap (%)	Reduction (pp)
IAM Misconfigurations	18.0	11.5	6.5
Network Segmentation	15.5	10.2	5.3
Logging/Monitoring	20.0	13.8	6.2
Data Protection	14.0	9.9	4.1
Overall	**16.9**	**11.4**	**5.5**

4.11 Final Enhanced Model Evaluation

The final reinforced model and its performance aggregated over Accuracy, Robustness, and Privacy is shown in Table 4.11 The clean accuracy of the model is quite high at 97.25% indicating that the model can be considered a strong baseline method in detecting normal operation. The accuracy under adversarial setting is still high at 96.00% with only 1.56% robustness gap, showing strong robustness to adversarial perturbations. As further validation of the privacy performance, the model is again found to operate under a privacy budget of $\varepsilon = 13.00$ but as low as 52.05% on membership inference attack accuracy, which is near random guessing and supports modest recovery and exposure of sensitive training data. In summary, these results validate the ability of the proposed framework to compete in detection performance with existing non-adversarial and no-privacy preserving solutions while exposing the adversarial robustness and privacy protection trade-offs between the existing non-adversarial and no-privacy preserving solutions which allows the multi-cloud target to be deployed in multi-cloud environments with secure and regulatory requirements.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

Table 4.11 Final Model Evaluation (Aggregated)

Final Metric	Value
Clean Acc	0.9725
Adv Acc	0.9600
Privacy ε	13.00
Membership Inference Acc	0.5205
Robustness Gap	0.0156

Figure 7 showing clean and adversarial accuracy trends over epochs, emphasizing robustness consistency over time.

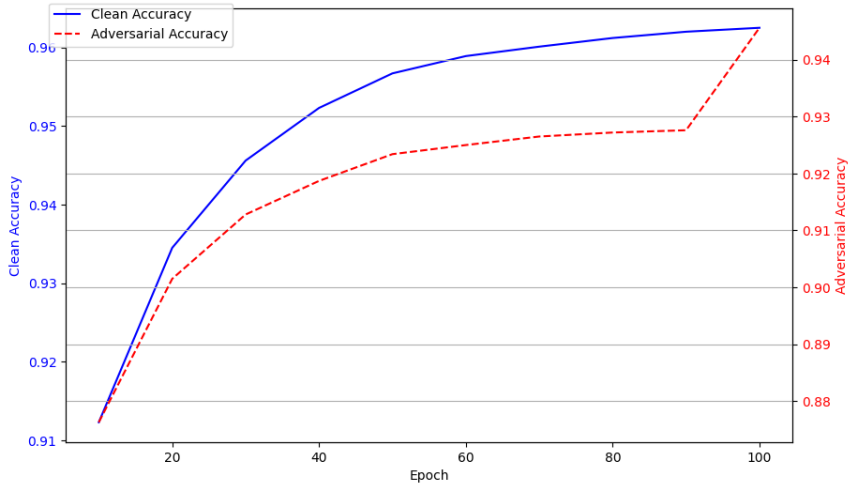

Figure 7. Model Robustness Over Training Epochs Under Clean and Adversarial Conditions

Prediction vs Actual and corresponding residual plot for both training & validation data (refer Figure 8) Most of the data points in the prediction vs actual plot are close to the ideal diagonal line indicating a good overall agreement between predicted values and true values, and therefore, the model performance was high with high predictive accuracy. Since the distributions of the training/validation predictions are similar so the model is doing the same across both data sets. This is also confirmed in the residual plot where residuals are equally spread around zero line with no evident systematic structure or pattern. This indicates that the model has low bias and low variance throughout the prediction region. To summarize, the results validate that the model is producing well-calibrated predictions, and the error behavior is stable and unbiased, demonstrating its generalization capacity.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/

Research Article

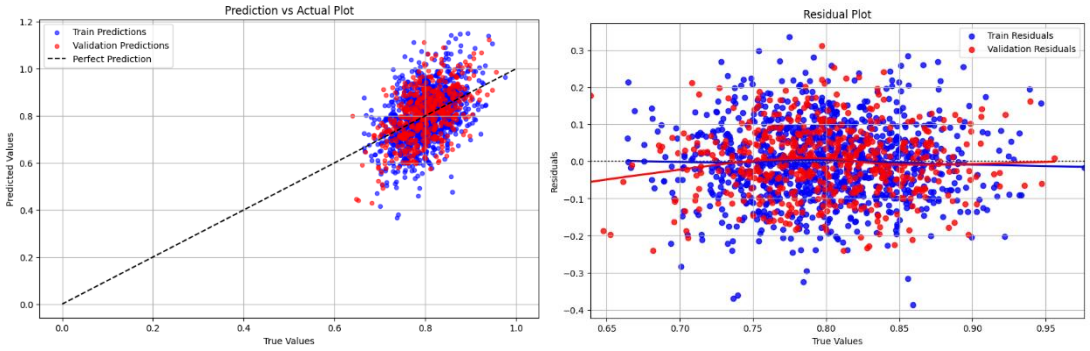

Figure 8. Prediction Accuracy and Residual Analysis for Training and Validation Data.

Figure 9. Prediction error for training and validation datasets. The dense overlap of the training and validation error curves on this cumulative distribution plot and the fact that positional prediction errors probably follow a similar distribution on both datasets. Thus, the overlap between them shows that the generalization behavior is stable and that there are no signs of overfitting. The density plot supports this by showing that both distributions (mean absolute error for validation and test set) centered around zero with both having similar spread but both having peak sharper center, which blatantly provides that the prediction are stable and well-calibrated. All these results, combined, further are an indication that the model behaves the same under train and validation showing same error patterns again which ultimately helps in making the model the robust and the reliable one.

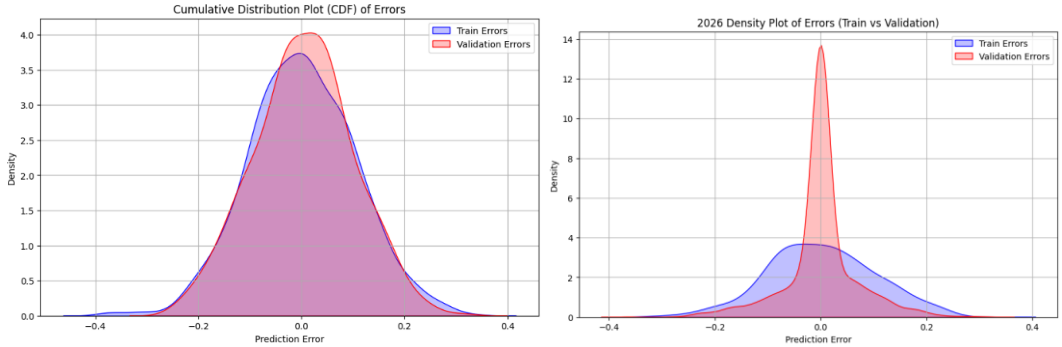

Figure 9. Train and Validation Data Error Distribution Analysis.

4.12 Discussion

Using the experimental results reported in this study, we show that the proposed optimal transport–based multi-cloud security framework can maintain a good trade-off amongst detection accuracy, domain generalization, privacy preservation, and adversarial robustness. Model shows balanced strong convergence across training and validation with little performance differences which suggest learning and generalization capacities The framework achieves high accuracy and F1 scores in three cloud platforms, which further confirms its ability to capture platform-invariant security patterns for reproducible performance in heterogeneous cloud environments. As for the domain adaptation experiments, we conduct extra studies and demonstrate that only minimal performance drop of the optimal transport mechanism observed from the source domain to the target domain, thus confirming its effectiveness. This showing means that the feature distribution across the clouds is aligned perfectly, which is one of the key challenges in multi-cloud security analytics. Moreover, the extensive results of fine-tuning with multi-cloud evaluations indicate that cloud-specific adapters improve performance with no loss of generalization, thus enabling scalable deployment across various suppliers of clouds. Differential privacy ultimately gives a boost to data protection from a security and trust perspective

without compromising any utility. Even under the adversarial setting, the privacy leakage remains low for membership inference attack results running close to the random guessing. Moreover, we observe that the model accurately predicts on networks with non-trivial attacks, and even after simulating attacks, the robustness gap is only small, which demonstrates that our learned representations are stable to adversarial perturbation. Evidencing the significant merits of AI-augmented approaches for security mechanisms beyond basics, we show consistent improvements in accuracy, robustness and privacy resilience as compared to baseline tools through statistical comparisons. In addition to detection performance, the framework is applicable in practice by minimizing the compliance gaps in the main federal security control domains and mapping the outputs of the model with regulatory and governance needs. Overall, through the final assessment, we demonstrate that the provided approach gives a complete and sound method for privacy-preserving and reliable multi-cloud security monitoring.

5. Conclusion

Abstract In this research, we presented the design of a cloud security analytics framework utilizing AI targeted at federal government systems crossing AWS GovCloud and Azure GovCloud. As cloud-native threats become increasingly complex, traditional rule-based security tools will demonstrate their inadequacy; therefore, in this context, the presented automated cybersecurity framework employs compliance-aware machine learning, behavioral analytics, and transport–based domain adaptation to combat this growing complexity. Through large experiments on an ultra-wide synthetic multi-GovCloud dataset, we validate these to demonstrate the framework not only offers solid and consistent performance, but also across diverse cloud environments. The relatively small adaptation gap confirms good transfer across the two platforms as evidenced by consistent high detection accuracy scores and F1 scores on both AWS and Azure, indicating that the model generalizes well from AWS to Azure. This also confirms the notion that the optimal transport-based alignment mechanism is efficient enough that the domain shift becomes alleviated without extensive retraining on the target platform. The low accuracy of their membership inference attacks close to random guessing indicated that the level of differential privacy offered by their technique provided meaningful protection for sensitive federal data while still allowing for high detection utility. The adversarial robustness evaluation also confirms that the model is still robust to simulated adversarial attacks with only a minor degradation in accuracy. In addition to its technical merits, the framework then also helps to translate into practice for making significant reductions in compliance gaps across federal security control domains, or low-hanging fruit that leads to better alignment with FedRAMP and CISA SCuBA guidelines. To summarize, the proposed solution is a scalable and privacy-aware and project-based distributed automated multi-cloud security monitoring solution. Which creates a solid foundation for further research & implementation of AI-powered cyber security solutions in federally secured cloud ecosystem.

References

[1] Sozib, H.M., et al., *Cloud Computing in Business: Leveraging SaaS, IaaS, and PaaS for Growth*. Journal of Applied Research: p. 38.

[2] Adeyeye, O., et al., *Leveraging Secured Ai-Driven Data Analytics For Cybersecurity: Safeguarding Information And Enhancing Threat Detection*. International Journal of Research Publication and Reviews, 2024. **5**: p. 3208-3223.

[3] Masud, S., et al., *The revolution of AI in enhancing infrastructure and facilities management. CDF, 54 (4), 5605–5624*. 2025.

[4] Sandeep Kumar Reddy, B., *Securing the Digital Public Sector: Cloud Transformation of Government Infrastructure*. International Journal of Computational and Experimental Science and Engineering, 2025. **11**(4).

[5] Yelkoti, N., *AI-Driven Cybersecurity Engineering for Enterprise-Wide Cloud Asset Protection, Application Data Security, and Multi-Cloud Threat Intelligence Automation*. Journal of Information Systems Engineering and Management, 2025. **10**: p. 10-20.

[6] Rahul Reddy Bandhela, RamMohan Reddy Kundavaram, Abhishake Reddy Onteddu. (2023). Ensuring Security and Verification of Graduate Credentials Using Blockchain Technology . Journal of Computational Analysis and Applications (JoCAAA), 31(3), 601–608. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/3032

[7] Haroon, A., et al., *Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research*. International Journal of Multidisciplinary Sciences and Arts, 2024. **3**(1): p. 242-251.

[8] Hoque, A., et al., *Cloud Computing in Banking Flexibility and Scalability for Financial Institute*. Well Testing Journal, 2025. **34**(S2): p. 165-184.

[9] Chitraju Gopal Varma, S., *AI-Enhanced Cloud Security: Proactive Threat Detection and Response Mechanisms*. International Journal For Multidisciplinary Research, 2024. **6**.

[10] Rehan, H., *AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age*. Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023, 2024. **1**: p. 132-151.

[11] Siyam, O.F., et al., *Interpretable Deep Learning for Symptom-Based Lung Cancer Prediction Using a 1D CNN Framework*.

[12] Mohamed, N., *Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms*. Knowledge and Information Systems, 2025. **67**(8): p. 6969-7055.

[13] Uddoh, J., et al., *AI-Based Threat Detection Systems for Cloud Infrastructure: Architecture, Challenges, and Opportunities*. Journal of Frontiers in Multidisciplinary Research, 2021. **2**: p. 61-67.

[14] Saeed, M., *Data-Driven Healthcare: The Role of Business Intelligence Tools in Optimizing Clinical and Operational Performance*. The American Journal of Applied Sciences, 2025. **7**(8): p. 50-73.

[15] Weng, Y. and J. Wu, *Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks*. Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023, 2024. **5**: p. 392-399.

[16] Patel, D. and S. Pujari, *AI-driven incident response in cloud security*. International Journal of Science and Research Archive, 2025. **15**: p. 1463-1475.

[17] Narkarunai, J., et al., *Advanced International Journal of Multidisciplinary Research Enhancing Cloud Compliance: A Machine Learning Approach*. 2024.

[18] Khatun, M. and M.S. Oyshi, *Advanced Machine Learning Techniques for Cybersecurity: Enhancing Threat Detection in US Firms*. Journal of Computer Science and Technology Studies, 2025. **7**(2): p. 305-315.

[19] Hoque, A., et al., *Reshaping Fintech: Unveiling Recent Developments on Fintech Integration*. Well Testing Journal, 2025. **34**(S3): p. 121-148.

[20] Roy, K.K., et al., *Leveraging artificial intelligence for strategic decision-making in healthcare organizations: a business it perspective*. The American Journal of Applied Sciences, 2025. **7**(8): p. 74-93.

[21] Hoque, A., et al., *AI and Machine learning in Banking: Driving Efficiency and Innovation*. Well Testing Journal, 2025. **34**(S3): p. 80-101.

[22] Lacaci, N.R., A.R. Menéndez, and A.V. Belmonte, *Understanding tourism consumer behavior using biometric technologies: bibliographic review and research agenda*. Tourism & Management Studies, 2024. **20**(1): p. 15-32.

[23] Islam, I., et al., *The Future of Banking Fraud Detection: Emerging AI Technologies and Trends*. Well Testing Journal, 2025. **34**(S3): p. 102-120.

[24] Rahman, M.B., et al., *Appraising the historical and projected spatiotemporal changes in the heat index in Bangladesh*. Theoretical and Applied climatology, 2021. **146**(1-2): p. 125.

[25] Ahmed, N., et al., *AI-Enabled System for Efficient Cyber Incident Detection and Response in Cloud Environments: Safeguarding Against Systematic Attacks*. Indonesian Journal of Educational Science and Technology, 2024: p. 233-248.

[26] Bayani, S.V., S. Prakash, and L. Shanmugam, *Data guardianship: Safeguarding compliance in AI/ML cloud ecosystems*. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2023. **2**(3): p. 436-456.

[27] Mr. Roopesh Kumar B N, A.K.K., Dhanush Y, Dhanvin C Bhargav, H A Sankeerthan, *Automated Dashboard for AWS Services Monitoring,"* IJRASET, 2023.

[28] Perumallaplli, R., *AI Enhanced Configuration Management Preventing System Misconfigurations*. SSRN Electronic Journal, 2025.

[29] Khan, N. and M. Efthymiou, *The use of biometric technology at airports: The case of customs and border protection (CBP)*. International Journal of Information Management Data Insights, 2021. **1**(2): p. 100049.

[30] Malaiyappan, J.N.A., et al., *Enhancing cloud compliance: A machine learning approach*. AIJMR-Advanced International Journal of Multidisciplinary Research, 2024. **2**(2).

[31] Masud, S.B., et al., *The Revolution of AI in Enhancing Infrastructure and Facilities Management*. Cuestiones de Fisioterapia, 2025. **54**(4): p. 5605-5624.

[32] Saqib, M., et al., *Adaptive Security Policy Management in Cloud Environments Using Reinforcement Learning*. arXiv preprint arXiv:2505.08837, 2025.

[33] Altowaijri, S.M. and Y. El Touati, *Securing Cloud Computing Services with an Intelligent Preventive Approach*. Engineering, Technology & Applied Science Research, 2024. **14**(3): p. 13998-14005.

[34] Vadisetty, R., et al., *AI-Driven Threat Detection: Enhancing Cloud Security with Generative Models for Real-Time Anomaly Detection and Risk Mitigation*. Journal of Computational Analysis and Applications, 2023. **31**: p. 532–543.

[35] Hossain, M.I., et al., *Zero-ETL Analytics: Transforming operational data into actionable insights*. 2025.

[36] Ang'udi, J. and S. Awour, *Security challenges in cloud computing: A comprehensive analysis*. World Journal of Advanced Engineering Technology and Sciences, 2023. **10**: p. 155-181.

[37] Mohamed Shaffi, S., et al., *AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience*. 2025.

Journal of Information Systems Engineering and Management
2026, 11(1s)

e-ISSN: 2468-4376

https://www.jisem-journal.com/ **Research Article**

[38] Malinverni, E.S., et al., *SIGNIFICANCE deep learning based platform to fight illicit trafficking of Cultural Heritage goods*. Scientific Reports, 2024. **14**(1): p. 15081.

[39] Salvi, M., et al., *Explainability and uncertainty: Two sides of the same coin for enhancing the interpretability of deep learning models in healthcare*. International Journal of Medical Informatics, 2025. **197**: p. 105846.

[40] Ghaffar Nia, N., E. Kaplanoglu, and A. Nasab, *Evaluation of artificial intelligence techniques in disease diagnosis and prediction*. Discover Artificial Intelligence, 2023. **3**(1): p. 5.

[41] Arafat, Y., et al., *Big Data Analytics in Information Systems Research: Current Landscape and Future Prospects Focus: Data science, cloud platforms, real-time analytics in IS*. Emerging Frontiers Library for The American Journal of Engineering and Technology, 2025. **7**(8): p. 177-201.

[42] Prakash, S., et al., *Achieving regulatory compliance in cloud computing through ML*. AIJMR-Advanced International Journal of Multidisciplinary Research, 2024. **2**(2).