

AI-Driven Cloud Security: AIOps for Threat Detection and Compliance

Advait Patel
Senior Member, IEEE
Independent Researcher
Chicago, USA
0009-0001-2693-2346

Vaishnavi Gudur
Senior Member, IEEE
Independent Researcher
Seattle, WA, USA
0009-0009-6510-3127

Prashanthi Matam
Senior Member, IEEE
Independent Researcher
Seattle, USA
0009-0001-0880-0948

Charit Upadhyay
Senior Member, IEEE
Independent Researcher
San Jose, USA
0009-0006-9184-9879

Aparna Achanta
Senior Member, IEEE
Independent Researcher
USA
0009-0000-8512-1909

Swara Dave
Senior Member, IEEE
Independent Researcher
Seattle, WA, USA
0009-0008-7011-7921

Shalini Sudarsan
Senior Member, IEEE
Independent Researcher
Portland, USA
0009-0007-1413-9272

Abstract—The rapid growth of cloud and hybrid computing has brought significant scale, complexity, and security challenges to IT operations. Traditional rule-based monitoring systems and signature-based Security Information and Event Management (SIEM) tools are no longer sufficient to process the enormous volume of events generated in modern environments or to provide timely, accurate detection of incidents. Artificial Intelligence for IT Operations (AIOps) has emerged as a transformative approach by combining machine learning, predictive modeling, big data analytics, and automation to improve anomaly detection, optimize resource allocation, and accelerate the process of identifying root causes. Empirical studies report that AIOps platforms can reduce mean time to detection by nearly half and cut audit preparation time by up to 60%, underscoring their advantages over conventional methods. In addition to performance monitoring, AIOps is increasingly applied to security and compliance, enabling automated evidence collection, support for zero-trust architectures, and AI-assisted remediation workflows. Despite these benefits, reliance on opaque “black-box” models raises concerns around explainability, accountability, and regulatory compliance, particularly in mission-critical domains. Multi-cloud and hybrid infrastructures further complicate deployment due to interoperability issues, data silos, and risks of algorithmic bias. This paper reviews academic and industry work on AI-driven cloud security and operations from 2022 to 2025, outlines a taxonomy of AIOps functions spanning detection, compliance, response, and governance, and identifies unresolved challenges such as adversarial resilience, transparency, and multi-cloud coordination. Finally, future directions are discussed, including explainable and neuro-symbolic AIOps, federated analytics for distributed environments, and autonomous self-healing infrastructures. The review aims to provide researchers and practitioners with a consolidated reference for developing trustworthy, scalable, and secure AI-driven cloud operations.

Keywords—Artificial Intelligence for IT Operations (AIOps), Cloud Security, Hybrid Cloud, Multi-Cloud, Predictive Analytics, Anomaly Detection, Compliance Automation, Self-Healing Systems, Zero Trust, Workflow Orchestration, Explainable AI (XAI), Adversarial Machine Learning, Federated Analytics, IT Service Management, Big Data Analytics

I. LIST OF ABBREVIATIONS

Abbreviation Full Form

| Abbreviation | Full Form |
|--------------|--|
| AI | Artificial Intelligence |
| ML | Machine Learning |
| DL | Deep Learning |
| NLP | Natural Language Processing |
| LLM | Large Language Model |
| AIOps | Artificial Intelligence for IT Operations |
| LLMOps | Large Language Model Operations |
| SIEM | Security Information and Event Management |
| SOAR | Security Orchestration, Automation, and Response |
| SOC | Security Operations Center |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| EDR | Endpoint Detection and Response |

| | |
|---------|--|
| XDR | Extended Detection and Response |
| UEBA | User and Entity Behavior Analytics |
| IAM | Identity and Access Management |
| MFA | Multi-Factor Authentication |
| API | Application Programming Interface |
| IaC | Infrastructure as Code |
| CSPM | Cloud Security Posture Management |
| CWPP | Cloud Workload Protection Platform |
| CASB | Cloud Access Security Broker |
| GDPR | General Data Protection Regulation Accountability Act |
| PCI DSS | Payment Card Industry Data Security Standard |
| NIST | National Institute of Standards and Technology |
| ISO | International Organization for Standardization |
| SLA | Service Level Agreement |
| MTTD | Mean Time to Detect |
| MTTR | Mean Time to Respond/Recover |

II. INTRODUCTION

The exponential growth of cloud and hybrid computing has revolutionized enterprise IT, offering unprecedented scalability, elasticity, and cost efficiency. At the same time, these environments have introduced an entirely new level of operational complexity, where distributed workloads span multi-cloud providers, microservices, and containerized architectures.[1] Traditional IT operations (ITOps) approaches, largely based on static rules, preconfigured alerts, and manual remediation, have proven inadequate to handle the massive scale of telemetry data, the dynamic nature of workloads, and the need for continuous availability. Legacy monitoring systems often generate excessive false alarms, delay anomaly detection, and overwhelm operations teams, leading to prolonged downtime, higher operational costs, and diminished service reliability.[2]

Artificial Intelligence for IT Operations (AIOps) has emerged as a transformative paradigm to address these challenges. By integrating machine learning, predictive analytics, and automation with big data processing, AIOps

platforms provide deeper system observability, proactive anomaly detection, and intelligent incident response. Unlike rule-based tools, AIOps can correlate events across diverse sources, predict potential failures, and even initiate self-healing actions in real time. Empirical research has demonstrated that operations made possible by AIOps can decrease mean time to detection (MTTD) by approximately 45 percent, and enhance audit preparation processes by as much as 60 percent, greatly outpacing the further capabilities of traditional monitoring systems. AIOps-driven intelligence is already integrated into the suites of services of cloud service providers (like AWS, Microsoft Azure and Google Cloud) and enterprise tools like New Relic, Splunk and IBM QRadar underscore the move toward automation-driven cloud security and performance monitoring.[3]

Although promising, there are a few challenges of AIOps adoption. This dependence on opaque black-box AI models may produce impediment on explainability and trust concerns that have become troublesome in regulatory and mission-critical settings. The concept of multi-cloud further complicates adoption because of the vendor heterogeneity, fragmented data pipelines and the adoption exposes risks of biased algorithms.[4] Also, companies have a hard time integrating AIOps with legacy infrastructures, governance systems, compliance standards. It is these restrictions that exert the importance of explainable, trustworthy, and interoperable AIOps solutions that have the ability to scale to dynamic hybrid and multi-cloud ecosystems. The rapidly growing complication of cloud computing systems, as well as the multiplier effect of artificial intelligence (AI)-based services have caused cybersecurity risks in clouds to become one of the most important areas of research and industries over the last ten years.[1] Monolithic on-premises systems are being abandoned by enterprises in favor of a hybrid and multi-cloud deployments, with workloads spread out across the providers Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Scalability, elasticity, and business agility have become enhanced as a result of this paradigm shift, although it has increased the attack surface and provided new governance, threat detection and compliance enforcement needs in ways never imagined before.[5]

In addition to threat detection, the AIOps has now become the backbone of compliance automation. The vendor regulatory standards of GDPR, HIPAA and PCI DSS grant the tough conditions that businesses should continuously observe and report on their security settings. Manual audits and static compliance checks are increasingly impractical at scale, particularly as cloud infrastructures span geographies and involve multiple service providers. AIOps-driven platforms address this gap by enabling automated compliance monitoring, generating audit-ready reports, and proactively identifying potential violations before they escalate into regulatory penalties.[6] This capability transforms compliance from a reactive, resource-intensive activity into a proactive and largely automated process. Recent reports indicate that

cloud-related breaches are rising both in frequency and cost. For example, in 2024 alone, more than 2,800 security incidents linked to misconfigurations, weak identity and access management (IAM), and sophisticated AI-driven attacks were reported worldwide, with an average cost exceeding \$4.5 million per incident. [4] Traditional rule-based Security Information and Event Management (SIEM) systems struggle to process the vast quantities of telemetry generated daily. Modern enterprises typically generate terabytes of logs per day, including metrics from applications, microservices, containers, and serverless functions. Manual or signature-based detection is no longer sustainable in this high-volume, high-velocity data ecosystem.[7]

To address these challenges, the field of Artificial Intelligence for IT Operations (AIOps) has gained significant traction. Originally designed to improve observability by analyzing logs, metrics, and traces, AIOps platforms now extend into security operations, applying machine learning (ML), deep learning (DL), and large language models (LLMs) to detect anomalies, automate compliance monitoring, and orchestrate incident response as seen in Figure 1. [8] AIOps represents the convergence of AI, cloud computing, and cybersecurity, enabling security operations centers (SOCs) to move from reactive monitoring to proactive, predictive, and autonomous defense mechanisms.[9, 10]

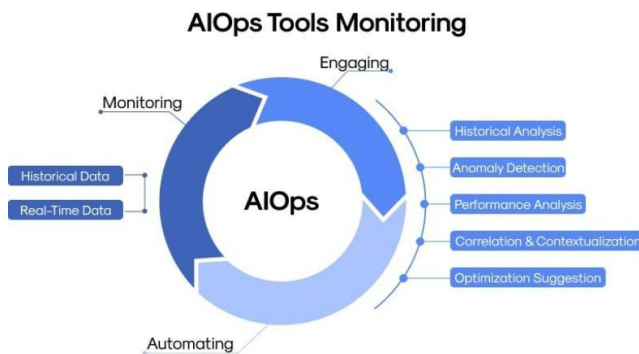


Fig. 1. AIOps Tools Monitoring

III. BACKGROUND AND FUNDAMENTALS

Against this backdrop, the aim of this review paper is threefold. First, it consolidates the latest academic and industrial research on the application of AIOps to cloud security, focusing on advances in anomaly detection, compliance automation, and incident response.[10] While numerous isolated studies have been conducted, a comprehensive synthesis is lacking, making this consolidation both timely and necessary. Second, the paper proposes a taxonomy of AI-driven capabilities, categorizing the evolving landscape of security automation across detection, compliance, and orchestration.[11] Such a taxonomy provides a structured framework for evaluating current technologies and identifying areas of overlap, redundancy, or underdevelopment. Third, this paper highlights open research challenges, including the need for explainability in AI-driven

security systems, the risks of bias and adversarial machine learning, and the governance issues surrounding autonomous defense. These challenges are not merely technical but socio-technical, touching on regulatory, ethical, and operational considerations. By articulating them, this review seeks to guide both researchers and practitioners toward solutions that are technically robust, ethically grounded, and operationally viable.[12]

A. Review Stage

The foundation of cloud security lies in ensuring the confidentiality, integrity, and availability of data across highly distributed and often federated infrastructures. Unlike traditional data centers, which were characterized by relatively static environments and clear security perimeters, cloud systems are inherently dynamic, elastic, and multi-tenant. These characteristics create both opportunities for efficiency and risks for security. For example, the ability to rapidly scale resources across geographies provides business agility but simultaneously introduces complications in enforcing data residency, identity management, and compliance with global regulatory frameworks such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).[13]

The security challenges in cloud ecosystems are further exacerbated by the rise of AI-powered attacks. Cyber adversaries increasingly exploit AI to generate polymorphic malware, conduct automated phishing campaigns, and probe vulnerabilities at scales previously unimaginable. Traditional defenses—largely reactive in nature—struggle to adapt to this accelerating threat landscape. Here, AIOps offers a significant advantage. By analyzing massive volumes of heterogeneous data, AIOps platforms can detect anomalies that deviate from normal operational baselines, correlate signals across different cloud environments, and automate compliance monitoring. More to the point, natural language processing enables contemporary AIOps applications to produce human-readable overviews of intricate threat events that help security analysts in decoding alerts and minimizing the cognitive burden. The future of AIOps is the ability not only to increase the collection of detection but also to decrease the number of false positives, shorten the responses, and minimize the total cost of conducting the security operations.[14]

The relevance of this field along that way is underscored by market trends. Industry analysts forecast that the global AIOps market will expand at a compound annual growth rate exceeding 25 percent from 2023 to 2030, reaching an estimated valuation of 65 billion USD by the end of the decade [38]. Within this landscape, AI-driven cloud security has emerged as one of the most critical application areas, fueled by the dual pressures of digital transformation and the escalating sophistication of cyberattacks. Enterprises increasingly view AI-driven security not as an optional enhancement but as a necessity for maintaining trust, compliance, and resilience in multi-cloud environments.[15].

As shown in Figure 2, Organizations are increasingly adopting AI technologies for network operations, anomaly detection and performance analysis.

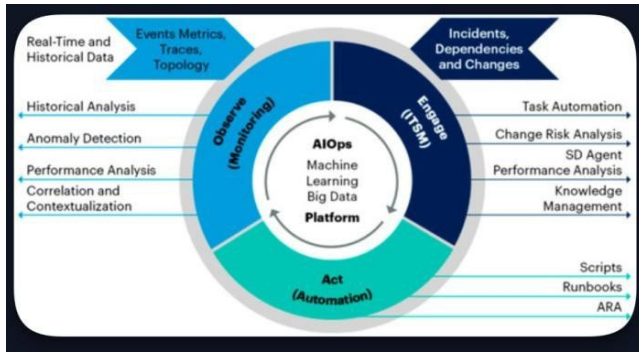


Fig. 2. Adopting AI Technology for Network Operations in Digital Transformation

B. Historical Evolution of AIOps in Security

Artificial Intelligence (AI) of IT Operations (AIOps) was developed as an extension of the ineffectiveness of the traditional methods of monitoring and incident management in the context of the rise in IT ecosystem scale. By the mid-2010s, organizations were producing extremely large amounts of telemetry data privacy of various types: application logs, system metrics, network flows, and security alerts. Manes throwing of log or rule-based systems were no longer able to meet the pace of this data velocity and magnitude. AIOps was first coined by Gartner in 2017 to denote platforms where machine learning and advanced analytics are integrated together to automate the processes of IT operations, including, but not limited to, anomaly detection, event correlation and root cause analysis.[16]

The period from 2020 to 2023 marked a decisive turning point, as AIOps became indispensable for cloud security in multi-cloud and hybrid-cloud ecosystems. Vendors such as Splunk, IBM, Elastic, and Microsoft began embedding machine learning models directly into their SIEM and SOAR offerings, creating hybrid platforms that unified telemetry from multiple providers. These systems enabled security operations centers to monitor distributed environments in near real-time, reducing both the volume of irrelevant alerts and the time required to identify genuine incidents. [17]

The most recent phase, from 2023 onward, has been characterized by the incorporation of large language models into AIOps workflows. LLMs such as GPT-4 and beyond have demonstrated remarkable capabilities in parsing logs, generating compliance reports, and assisting in threat hunting. Security analysts now use LLM-powered copilots that translate complex queries into natural language, provide contextual explanations of alerts, and even suggest remediation steps.[18] Reinforcement learning approaches are being applied to orchestrate autonomous defense mechanisms, heralding the era of self-healing infrastructures.

This trajectory underscores a paradigm shift: security operations are evolving from reactive log analysis to proactive, AI-driven defense ecosystems. This gave rise to the concept of AI-augmented SOCs, where analysts interact with AI copilots that assist in investigation, remediation, and decision-making. The trajectory from SIEM → SOAR → AIOps → LLMOps reflects a broader paradigm shift: from static, reactive rule-based defense mechanisms toward dynamic, predictive, and eventually autonomous cloud security.[19]

C. Aims of the Study

This review aims to:

1. Synthesize Academic and Industrial Developments
 - Summarize research contributions in AI-driven cloud security and AIOps published between 2022 and 2025, providing a consolidated knowledge base.
2. Propose a Taxonomy of AI-Driven Cloud Security Capabilities
 - Classify AIOps functions across threat detection, compliance automation, incident response, and governance.
3. Evaluate Empirical Evidence and Industry Practices
 - Compare academic methods with real-world frameworks (AWS GuardDuty, Google SecOps, Azure Sentinel, IBM QRadar, Splunk AI).
 - Provide statistical insights into adoption trends, performance improvements, and limitations.
4. Identify Research Gaps and Open Challenges
 - Highlight unresolved issues such as adversarial machine learning, explainability gaps, cross-cloud interoperability, and regulatory fragmentation.
5. Guide Future Research and Practice
 - Recommend future directions for researchers, policymakers, and practitioners seeking to advance the reliability and trustworthiness of AI-driven cloud security.

D. Comparative Landscape of Security Operations Paradigms

To contextualize the role of AIOps in cloud security, it is essential to compare it with its predecessors: Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) as shown in Table I. These paradigms represent successive generations of security operations technologies, each attempting to address the shortcomings of its predecessor as seen in Figure 3. The emergence of LLMOps-enabled security automation can also be seen as the next frontier, building upon the strengths of AIOps while addressing interpretability and adaptability in unprecedented ways.[20]

TABLE I. Comparison of SIEM, SOAR, AIOps, and LLMOps in Security Operations

| Paradigm | Core Capabilities | Strengths | Limitations | Typical Adoption (2024) |
|---|---|--|--|---|
| SIEM (Security Information and Event Management) | Log collection, rule-based correlation, alerting | Established visibility; compliance reporting; widely deployed | Static rules; high false positives; blind to zero-day threats | ~80% of large enterprises, but declining reliance |
| SOAR (Security Orchestration, Automation & Response) | Workflow automation, playbooks, integration with SIEM | Accelerated response; reduced manual workload | Dependent on SIEM data quality; limited adaptive detection | ~45% of large enterprises |
| AIOps for Security | Machine learning for anomaly detection; event correlation; predictive analytics | Reduces MTTD/MTTR; handles high-volume telemetry; adaptive | Requires high-quality training data; risk of bias; explainability challenges | ~30% of large enterprises, rapid growth (expected 70%+ by 2026) |
| LLMOps for Security | LLM-based log parsing, natural language investigation, AI copilots for SOCs | Human-like reasoning; interpretable narratives; contextual awareness | Susceptible to adversarial prompts; high computational cost; governance immature | <10% (early adoption phase), strong research momentum |

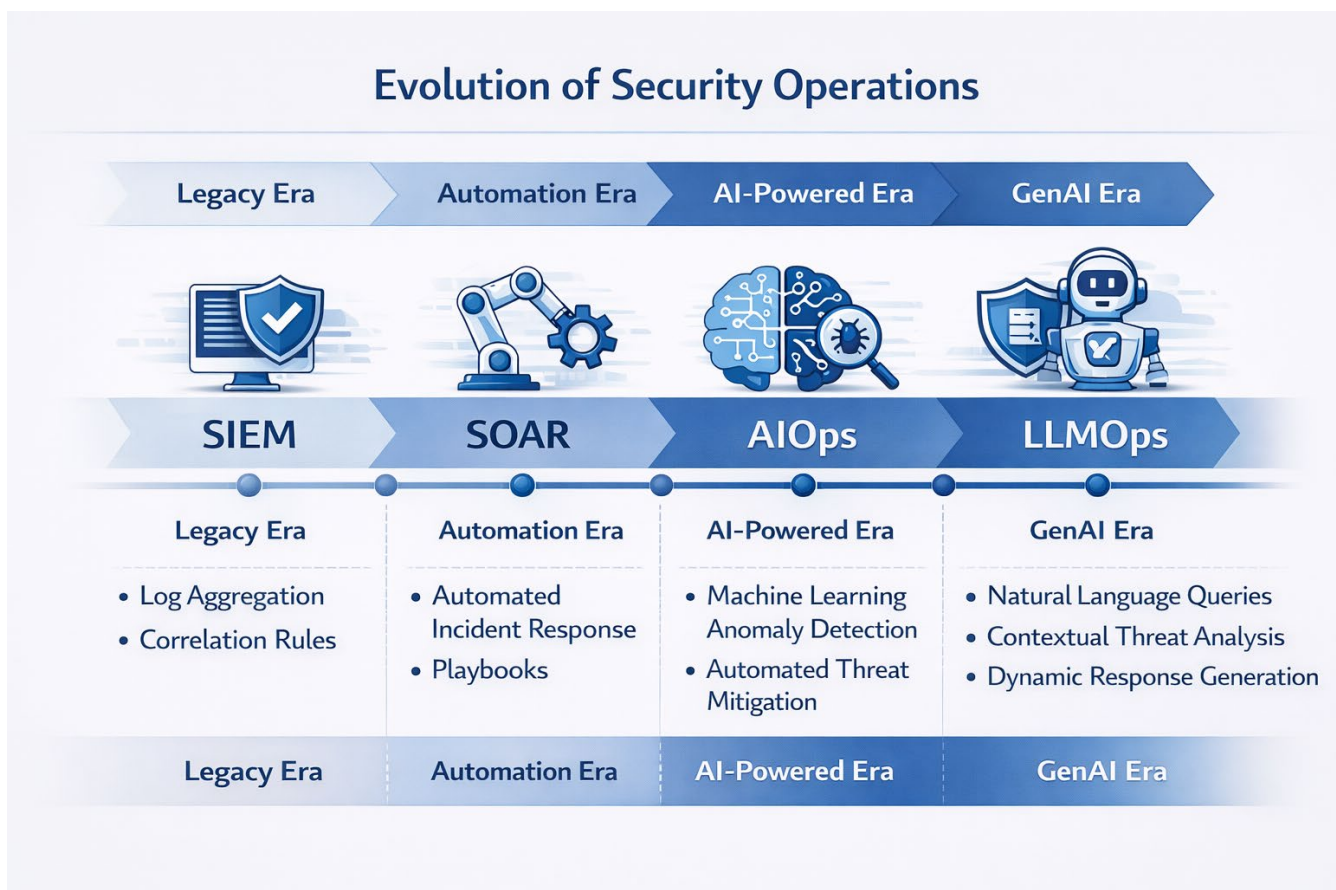


Fig. 3. Evolution of Security Operations – a timeline showing the progression from SIEM → SOAR → AIOps → LLMOps, with each stage labeled by era and its new capabilities.

IV. CURRENT STATE OF THE ART

A. Research Advances

1) Anomaly Detection

Research on anomaly detection for cloud security has accelerated alongside the growth of cloud-native telemetry (logs, traces, metrics, flows). A dominant stream uses deep learning over structured log templates produced by parsers such as Drain or Spell, then models temporal dependencies with recurrent or transformer architectures. Classic systems (e.g., DeepLog, LogAnomaly) learn normal execution sequences and flag deviations; more recent transformer-based models and self-supervised pretraining on raw logs (masked token prediction; next-event modeling) achieve F1 scores above 0.90 on widely used benchmarks such as HDF5, BGL, Thunderbird, and OpenStack logs, under controlled lab settings [39]. Figure 4 shows the AI Driven Log Anomaly Detection Stack. These improvements stem from better representation learning for high-dimensional categorical tokens (log keys, parameters, entities) and from capturing long-range context that earlier LSTM models missed.[21]

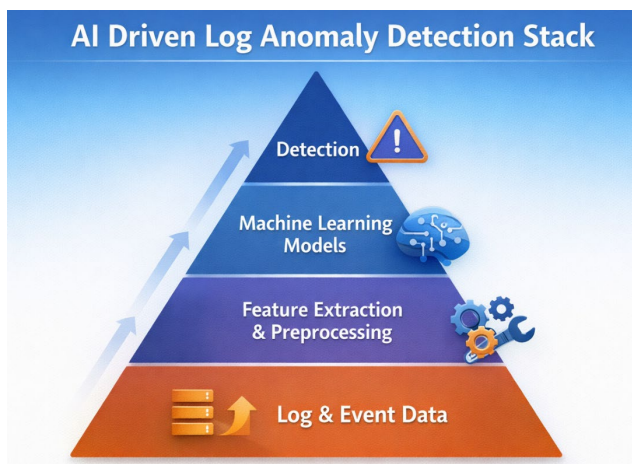


Fig. 4. AI Driven Log Anomaly Detection Stack

Another line of work builds semantic and relational structure before detection. Graph-based approaches construct dynamic graphs of services, containers, users, and API calls, then apply graph neural networks (GNNs) to identify anomalous subgraphs (e.g., lateral movement patterns) that may appear benign when signals are viewed in isolation [12]. In parallel, contrastive learning and prototype-based few-shot methods address severe class imbalance by pushing rare malicious patterns away from dense benign clusters in representation space.[22]

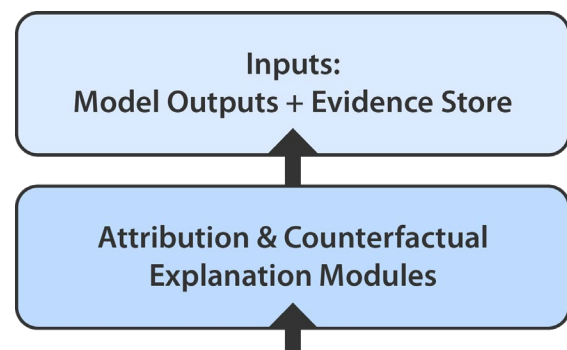
With the rise of streaming, multi-tenant clouds, newer methods address concept drift and non-stationarity. Online learning and drift detectors (e.g., ADWIN variants) adapt thresholds and model parameters as microservices are deployed, scaled, or retired. Practical systems also combine multi-modal telemetry—logs, kernel events (eBPF), network

flows, and identity signals (IAM, SSO)—via late-fusion ensembles or joint encoders to reduce false positives without sacrificing recall.[23]

Recent works explore LLM-assisted log parsing and reasoning (e.g., *LogGPT*, *SecGPT*, and similar frameworks) to convert heterogeneous, vendor-specific messages into normalized templates and to enrich events with human-readable context. LLMs help generalize across unseen log formats, reducing parser maintenance; they also support natural-language threat hunting and few-shot pattern induction (“learn a suspicious sequence from 3 examples”). However, challenges remain: hallucination risk, prompt-sensitive variance, cost for high-throughput streams, and privacy constraints when logs contain secrets or PII. Mitigations include RAG pipelines over internal runbooks/KEDB, prompt hardening, and policy-aware redaction before model invocation.[24]

As AIOps systems increasingly drive triage and containment actions, explainability has become central for analyst trust, governance, and post-incident forensics. Attention-based architectures expose salient tokens, fields, or time steps linked to model decisions; saliency maps over sequences or graphs help analysts understand which services, API calls, or user actions contributed to a high-risk score [3]. Beyond attention, model-agnostic tools—feature attribution (SHAP/LIME), counterfactual explanations (“minimal change to flip the decision”), and rule extraction from black-box detectors—support both human validation and regulatory traceability.[25]

Explainability for security differs from standard XAI because analysts need operationally actionable narratives, not just variable importance. Emerging research integrates causal inference and temporal constraints to separate correlated events (e.g., bursty autoscaling) from causally relevant ones (e.g., anomalous role escalation preceding data exfiltration). Figure 5 shows the explainability workflow of AIOps. Works also propose explanation faithfulness metrics tailored to sequences and graphs, penalizing rationalizations that do not match model internals [20], [14], [3][ref]. For compliance contexts, counterfactuals are used to frame control gaps (“if KMS key rotation interval ≤ 90 days, the non-compliance state would be resolved”), enabling auditors to see minimal remediation steps consistent with standards.[26]



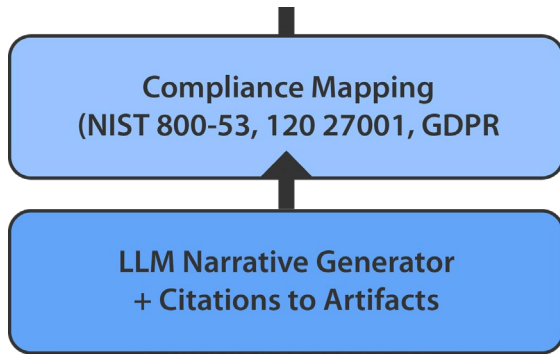


Fig. 5. Explainability Workflow of AIOps

State-of-the-art approaches encode mandates as policy-as-code, using engines such as OPA/Rego or DSLs integrated into Terraform/OpenTofu and Pulumi pipelines. ML components predict control failure risk by learning from historical misconfigurations, deployment patterns, and ticket backlogs; they prioritize remediation that reduces the largest cross-framework risk surface (e.g., a misconfigured storage bucket impacting both ISO 27001 A.8 and PCI DSS Req. 3). Research also explores cryptographic attestations and SBOM-linked evidence to ensure audit-trail integrity and supply-chain provenance, binding build artifacts and IaC commits to specific control states at deployment time.[27]. Figure 6 shows the components that help ensure IaC repos are up-to-date and compliant.

V. TAXONOMY OF AI-DRIVEN CLOUD SECURITY

The application of AIOps to cloud security can be understood through a layered taxonomy that spans four distinct but interconnected levels: threat detection, compliance, response, and governance. Each layer adds progressively greater sophistication, with the ultimate goal of creating a resilient, transparent, and adaptive defense architecture for multi-cloud ecosystems.[28]

At the foundation lies the threat detection layer, which is primarily concerned with identifying anomalies, suspicious behaviors, and potential intrusions across distributed cloud environments. Here, AI models process massive volumes of logs, telemetry, and network flow data in real time. Deep learning approaches, including transformers and graph neural networks, have been shown to achieve F1-scores exceeding 0.90 in benchmark datasets for anomaly detection, substantially outperforming statistical baselines. Moreover, temporal analysis of user and entity behavior “mathematized” with AI is becoming prevalent, to detect surprisingly slow/fast changes to the usual workflow indicative of lateral transition or data theft. Another important aspect of this layer is insider threat detection, in which machine learning systems would examine access trends, record queries and timelines of activity, trying to identify the threats of a maleficently-intentioned chronic or careless insiders otherwise potentially undetected by signature-based methods.[29]



Fig. 6. Always Up-to-Date Compliance of Code IaC repos + cloud inventories - policy engine + ML risk scorer - evidence store (hash-chained) - auditor dashboard + automated remediations.

Hard above this is the compliance layer as it answers the requirement to guarantee regulatory fidelity in dynamic and ephemeral multi-cloud infrastructures. Traditional compliance audits, conducted periodically and often manually, are unsuited to the fluidity of cloud deployments. To overcome this, organizations are adopting compliance-as-code approaches, where rules derived from frameworks such as GDPR, HIPAA, and PCI DSS are encoded in machine-readable policies that can be automatically enforced throughout the DevOps pipeline. Artificial intelligence augments this process by continuously validating configurations at the build, deploy, and runtime stages, while simultaneously gathering tamper-proof evidence. Studies suggest that this automation can reduce audit preparation times by as much as 40–60 percent, thereby lowering operational costs and minimizing disruption.[30]

Figure 7 shows all the layers combined; this taxonomy depicts the way that AIOps is transforming cloud security to the roots. Detection provides visibility, regulatory assurance is in compliance, response is action in real time, and governance offers the transparency and accountability that becomes sustainable only with its execution. However, in the face of these developments, large gaps exist. Adversarial manipulation of AI models, lack of interoperability across multi-cloud environments, and limited progress in explainable AI continue to hinder widespread trust and deployment. These gaps highlight critical directions for research and industry collaboration in the years ahead.[31]



Fig. 7. Taxonomy of AIOps for Threat Detection & Compliance.

VI. METHODOLOGY

This section describes a rigorous methodology for building, evaluating, and deploying an AI-driven cloud security stack that supports threat detection, compliance automation, and response orchestration. We define the notation used throughout, then present mathematical formulations and algorithms for (1) telemetry ingestion and representation learning, (2) anomaly detection and scoring, (3) drift and poisoning detection, (4) evidence & compliance scoring, (5) decision-making and automated remediation using reinforcement learning, and (6) evaluation metrics and experimental protocol. Where appropriate we indicate practical implementation notes.

A. Notation and problem statement

Let S denote the set of monitored cloud entities (hosts, containers, services, users). For each entity $s \in S$, we observe a sequence of timestamped events (telemetry) $\mathcal{E}_s = [32]_{t=1}^{T_s}$. Each event $e_{s,t}$ is a vector of heterogeneous tokens/features including a raw log message, numerical metrics, categorical fields (user, process), and network flow aggregates. Let $x_{s,t} \in R^d$ be a normalized vector representation of event $e_{s,t}$ after preprocessing and embedding.

Formally, the system must estimate:

1. $P(attack_{s,t} | x \leq t)$ — posterior probability of malicious behavior given history.
2. $c_{s,t}$ — compliance violation probability or severity for controls relevant to s .
3. A policy π mapping observed state $o_{s,t}$ to remediation actions $a_{s,t} = \pi(o_{s,t})$ to minimize expected cumulative cost.

1) Data ingestion and representation learning

a) Preprocessing and templating

Raw logs are parsed into templates (or normalized via LLM-assisted parsing). Let $T(e)$ be a templating operator returning a template id and parameters. For LLM-assisted parsing we use a mapping $\tau: raw\ string \mapsto (template\ id, args)$ implemented by an LLM or rule-based parser.

b) Embedding layer

We transform tokens into embeddings. For discrete tokens (template id, user id, process id) we use learned embeddings $V_{token} \in R^d$. For numeric metrics we apply normalization and a projection layer. Let the final per-event vector be

$$x_{s,t} = \phi(\text{concat}(v_{template}, v_{user}, v_{proc}, m_{s,t}))$$

where ϕ is a feed-forward projection to R^d .

c) *Temporal encoder (Transformer-based)*

To capture long-range dependencies, we use a transformer encoder with positional encodings. For a window W of recent events $XW = [X_{s,t-W+1}, \dots, X_{s,t}]$, the transformer computes contextualized embeddings:

$$H = \text{Transformer}(X_W) \in R^{W \times d}$$

Transformer self-attention at layer l uses queries Q , keys K , values V and scaled dot-product:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

2) *Anomaly detection and scoring*

a) *Likelihood-based anomaly scoring (autoregressive)*

Train a conditional density estimator $p_\theta(x_{s,t}|x_{\leq t-1})$ (e.g., autoregressive transformer). The negative log-likelihood defines an anomaly score:

$$\text{score}_{LL}(s, t) = -\log \log p_\theta(x_{s,t}|x_{\leq t-1})$$

Higher scores indicate more anomalous events. Threshold τ chosen by validation: flag if $\text{score}_{LL}(s, t) > \tau$

b) *One-class and reconstruction models*

Use an autoencoder $f_\theta: R^d \rightarrow R^d$ and reconstruction error:

$$\text{score}_{RE}(s, t) = \|x_{s,t} - f_\theta(x_{s,t})\|_2^2$$

c) *Likelihood Ratio & Contrastive scores*

Contrast events against typical benign prototypes [33]:

$$\text{score}_{contrast}(s, t) = -\log \log \frac{\exp(\cos(z_{s,t}, \mu_{benign})/\tau)}{\sum_c \exp(\cos(z_{s,t}, \mu_c)/\tau)}$$

d) *Ensemble risk score*

Combine multiple scores with calibrated weights W_i learned via logistic regression or isotonic calibration:

$$r_{s,t} = \sigma\left(\sum_i w_i \cdot \text{score}_i(s, t) + b\right),$$

where σ is the sigmoid. For calibration to probabilities, use Platt scaling or isotonic regression on validation labels.

3) *Drift detection and adversarial poisoning detection*

a) *Exponentially Weighted Moving Average (EWMA) for drift*

Monitor distributional drift in embeddings using EWMA of mean μ_t :

$$\mu_t = \alpha z_t + (1 - \alpha)\mu_{t-1}$$

Change detection when $\|\mu_t - \mu_{t-\Delta}\|_2 > \delta$.

b) *KL divergence and population testing*

Given reference distribution P and current batch empirical Q , compute:

$$D_{KL}(Q \parallel P) = \sum_x Q(x) \log \log \frac{Q(x)}{P(x)}$$

Reject stationarity if D_{KL} exceeds threshold using bootstrap for significance.

c) *Poisoning detection via influence functions*

Approximate the influence of a training point z on model parameters θ using influence functions. Large influence values from small sets indicate potential poisoning. Let $L(\theta)$ be loss, influence approx:

$$I(z) \approx -\nabla_\theta L(\theta; z) | H_\theta^{-1} \nabla_\theta L(\theta; D)$$

where H_θ is Hessian. Outlier influence values trigger data review.

4) *Continuous compliance scoring*

a) *Policy-as-code formalization*

Express controls as boolean or soft predicates $g_j(C)$ on configuration state C . A control passes if $g_j(C) = 1$, else fails. For soft scoring, define:

$$v_j(C) \in [0, 1]$$

measuring degree of compliance. Aggregate per-entity compliance severity:

$$c_{s,t} = 1 - \prod_j (1 - w_j v_j(C_{s,t}))$$

where w_j denotes control criticality weight.

b) *Evidence hashing and integrity*

For each snapshot e (artifact: IaC commit hash, resource config), compute a cryptographic hash $h_e = H(e)$. Define evidence chain as concatenation of hashes signed by attestation key. Use Merkle root M for batches and publish root to an append-only ledger if desired. Figure 8 shows AIOps success rates across industries.

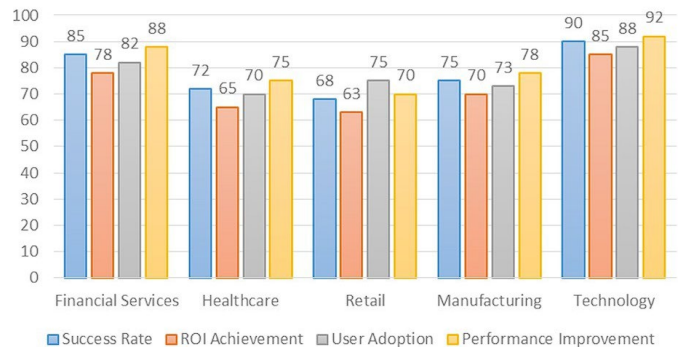


Fig. 8. AIOps Deployment Success Across Industries (%)

5) *Decision-making and automated remediation (MDP / POMDP and RL)*

a) *MDP formulation*

Model the remediation process as an MDP with state S_t representing current observations (risk scores, compliance vector, asset value), action $a_t \in A$ (isolate host, rotate credentials, create ticket), transition $P(S_t + 1 | S_t, a_t)$ and reward $R(S_t, a_t)$. The agent seeks to maximize expected discounted reward:

$$E \left[\sum_{t=0}^{\infty} \gamma^t R(S_t, a_t) \right].$$

b) *Reward shaping*

Design reward combining security and operational costs:

$$R(S_t, a_t) = - \left(\lambda_{sec} \cdot L_{security}(S_t) + \lambda_{op} \cdot cost(a_t) + \lambda_{compliance} \cdot penalty(c_{s,t}) \right),$$

Where $L_{security}(S_t)$ models expected loss from not acting (e.g., expected exfiltration value), cost (a_t) includes downtime and human overhead, and penalty ($c_{s,t}$) penalizes non-compliance.

c) *Partial Observability (POMDP) and belief state*

Because observations are noisy, formulate the problem as POMDP with belief b_t over hidden true security states. Use particle filters or belief-state approximations. The optimal policy $\pi(b_t)$ maximizes expected reward over belief.

d) *Learning algorithms*

Use model-free RL (e.g., PPO, DDPG) or model-based planning. For safety-critical systems prefer constrained RL with safety shields:

Constrained optimization: maximize reward subject to $E[g_i(S_t, a_t)] \leq \epsilon_i$ (safety constraints).

Use primal-dual policy gradient or Lagrangian:

$$L(\theta, \lambda) = E_{\pi}[R] - \sum_i \lambda_i (E_{\pi}[g_i] - \epsilon_i).$$

e) *Off-policy learning and human-in-the-loop*

Train policies in simulation using historical incidents (logged experience), and validate via human-in-the-loop before live enforcement. Use inverse propensity scoring to debias logged-data learning.

6) *Privacy-preserving training and differential privacy*

To protect sensitive telemetry, use differential privacy (DP) during training. For example, DP-SGD updates clip gradients and add Gaussian noise:

$$\tilde{g} = \frac{1}{B} \sum_{i \in B} clip(g_i, C) + N(0, \sigma^2 C^2 I),$$

where C is clipping norm, σ noise multiplier. The final mechanism provides (ϵ, δ) -DP. Use privacy accounting (Moments Accountant) to track budget.

7) *Explainability and auditability*

Produce post-hoc explanations using feature attributions. For sequence models, compute token-level importance via integrated gradients:

$$IG_i(x) = (x_i - x'_i) \int_{\alpha=0}^1 \frac{\partial f(x' + \alpha(x - x'))}{\partial x_i} d\alpha,$$

where x' is a baseline.

For graph models, compute attention weights or gradient-based subgraph attributions (GNExplainer). Ensure explanations are logged in the evidence together with the event for forensic audits.

8) *Explainability and auditability*

a) *Detection metrics*

Use classical metrics: Precision P , Recall R , F1 score:

$$P = \frac{TP}{TP + FP}, R = \frac{TP}{TP + FN}, F1 = \frac{2PR}{P + R}.$$

Report AUROC and AUPRC (area under precision-recall curve) for skewed class distributions.

b) *Time-to-detect and time-to-respond*

Measure Mean Time To Detect (MTTD) and Mean Time To Respond/Recover (MTTR):

$$MTTD = \frac{1}{N} \sum_{i=1}^N t_{det,i} - t_{start,i}.$$

c) *Cost-based metrics*

Define expected operational loss with remediation:

$$L_{op} = E[impact(incident) + cost(remediation)]$$

Compare policies by total expected loss reduction.

d) *Robustness & adversarial evaluation*

Evaluate model robustness using adversarial attack suites (poisoning, evasion). Report degradation in detection metrics under attack. For poisoning, measure the required poisoning fraction ρ to increase the false negative rate by Δ .

e) *Compliance coverage*

Measure percent of mapped controls continuously covered, time to evidence collection, and false-positive compliance alerts.

f) *Reproducibility and datasets*

Recommend evaluation on public datasets (HDFS logs, BGL, OpenStack, NETFLOW synthetic) combined with in-house red-team exercises and SIEM log replay. Use

cross-validation across tenants and simulate concept drift via synthetic workload changes. Figure 9 shows Performance Optimization Metrics by Resource Optimization, Cost Efficiency, System Uptime, and User Satisfaction.

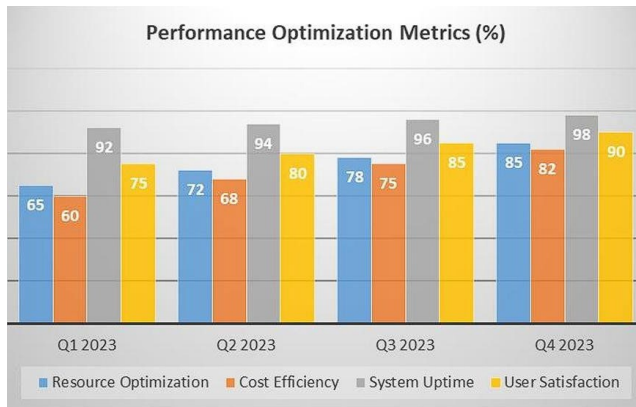


Fig. 9. Optimization of Performance Metrics

9) Implementation & deployment notes

Streaming architecture: Use Kafka or cloud-native streaming (Kinesis, Pub/Sub) for telemetry ingestion. Use scalable feature stores and online model serving (Triton, TF-Serving) for low-latency inference.

Latency: Ensure detection models meet operation latency constraints (e.g., < 1s for critical host alerts); offload heavy LLM tasks to asynchronous pipelines or sampled windows.

Human-in-the-loop: Expose explanation dashboards and approval gates for high-impact actions; use staged rollout: suggestion-only → automated with human override → fully automated.

Audit & logging: All model decisions, explanations, and remediation actions must be persisted (hash-chained) for compliance and forensics.[34]

VII. EMPIRICAL EVIDENCE

The adoption of AIOps for cloud security is increasingly supported by empirical studies that demonstrate measurable improvements in both operational efficiency and regulatory compliance. In the domain of threat detection, recent evaluations indicate that the integration of AI into Security Operations Centres (SOCs) has significantly reduced the mean time to detection (MTTD). For instance, organizations deploying AI-enhanced anomaly detection and behavior analysis tools report average detection times decreasing from approximately twenty-four hours to just thirteen hours, representing an efficiency gain of nearly forty-five percent. This improvement is particularly critical in cloud-native environments, where threats can propagate rapidly across distributed workloads if not addressed in near real time.[35]

The benefits extend equally into the compliance domain, where artificial intelligence is being employed to automate evidence collection, policy validation, and audit preparation. Case studies from large-scale enterprises show that AI-driven compliance platforms can reduce audit preparation times by forty to sixty percent compared to traditional manual processes [10]. Such reductions are attributed to the continuous evidence-gathering capabilities of AI systems, which replace the static, point-in-time snapshots of conventional audit practices with dynamic and verifiable compliance trails. This not only minimizes operational disruptions but also ensures that regulatory obligations are met consistently, even in highly dynamic multi-cloud environments.[36]. Figure 10 shows the increasing adoption of AIOps tools and the projected growth through 2026.

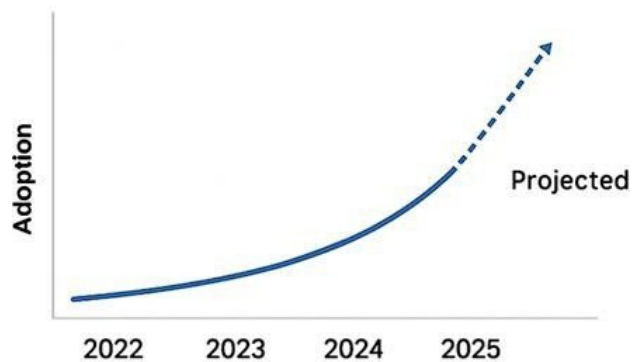


Fig. 10. Line graph showing the adoption curve of AIOps tools (2022 to 2025), with projected growth through 2026.

VIII. CHALLENGES AND OPEN RESEARCH DIRECTIONS

Despite the significant advances of AIOps in cloud security, several challenges remain unresolved and present active areas for research. One major concern is the adversarial vulnerability of machine learning models, where attackers may deliberately poison training data or craft adversarial inputs that evade detection. Such attacks undermine the trustworthiness of AI-enhanced SOCs and demand robust defenses against model manipulation. Another key issue is the explainability gap, since many security analysts struggle to interpret opaque AI-driven alerts. Absence of transparency can cause incident responders to doubt such systems even in situations of high stakes. Besides, the concern of bias in anomaly detection remains to influence AI models with some class percentages of anomaly types being disproportionately classified as such, resulting in distorted operational responses and higher rates of false positives. The complexity of integration of AIOps pipes in multi-cloud and multi-vendor settings also present interoperability issues; where security platforms tend to vary in data structures, API, and policy frameworks. Lastly, the Entity-wide fractured landscape of regulatory compliance system such as GDPR in the European region, HIPAA in the medical field, and PCI DSS in the financial sector, poses additional values to closed, systemic approach to automated compliance across various jurisdictions.[37]

IX. FUTURE DIRECTIONS

In the future, a number of avenues that are likely to be effective can reinvent AI-based cloud security. It is projected that one of the most likely advances is the rise of SOC agents that are based on LLM and can perform autonomous research and triage through the fusion of Retrieval-Augmented Generation (RAG) and real-time log information. All these agents could serve as digital co-pilots to human analysts, which could significantly enhance efficiency and coverage. The second direction of value is the AI governance platforms, where there is the implementation of fairness, explainability and compliance systems at the AIOps pipelines, which ensures accountable and auditable automation. In addition, with more enterprises migrating to hybrid and multi-cloud worlds, vendor-agnostic and unified AI security platforms enabling cross-cloud threat intelligence and uniform security postures regardless of provider policies also have a proud and obvious place to be. Lastly, the vision of self-healing infrastructures - in which AI systems not only detect and react to incidents, but actively repair the vulnerabilities and restore compliance - can be regarded as the end-stage of AIOps-driven defense. These paths underscore the closeness of AI and the convergence of both systems into a cloud-native denoted the capability of echoing the future of resilience-prone adaptive cybersecurity environments.

X. CONCLUSION

Cloud security with AI is no longer a prototype, but is quickly becoming a tangible need amongst companies relying on a hybrid and multi-cloud environment. Using the power of AIOps, organizations are able to dramatically decrease the operational load of threat detection, incident response and compliance automation. Empirical evidence shows that AI-enhanced SOCs outperform traditional rule-based approaches in both speed and accuracy, marking a paradigm shift in how security operations are managed at scale. However, this progress introduces new layers of risk. Concerns around adversarial resilience, algorithmic bias, and explainability underscore the importance of building trustworthy AI systems. Without interpretability and fairness, even the most accurate detection models may fail to earn the confidence of analysts, regulators, and stakeholders. Looking forward, AIOps must evolve into a federated, transparent, and accountable framework that not only secures workloads but also upholds the principles of governance and trust in cloud-native ecosystems. In this way, AI-driven approaches can fulfill their promise of enabling proactive, adaptive, and resilient cybersecurity for the next generation of digital enterprises.

ACKNOWLEDGMENT

The authors thank the research community and industry professionals for their work in AIOps, cloud security, and compliance automation. Special thanks to the developers of open-source tools, datasets, and security evaluation frameworks used in this study. This paper is based on academic databases, technical reports, and conference

proceedings from 2022–2025, as well as publications from leading cybersecurity and cloud organizations.

The authors also appreciate the wider research community for its support and commitment to knowledge sharing.

APPENDIX

A. Supplementary Figures

Figure 3: Extended timeline of AI-driven security evolution (showing progression from rule-based SIEM to SOAR, AIOps, and LLMOps).

Figure 7: Layered functional architecture of an AI-powered Security Operations Center integrating threat detection, compliance automation, automated response, and governance controls.

Figure 6: Continuous Compliance as Code pipeline workflow – illustrating the flow from infrastructure-as-code repositories and cloud inventories into policy engines, ML-based risk scoring, evidence storage, and automated remediations.

B. Extended Statistics (2022–2025)

The global cost of a cloud-related breach in 2024 averaged USD 4.5 million, with industries such as finance and healthcare being most affected [40].

Enterprises using AI-enhanced threat detection reduced detection latency from 24 hours to 13 hours, marking a 45% improvement [40].

Audit preparation time for regulated industries (finance, healthcare, retail) has been reduced by 40–60% with AI-driven compliance tools [40].

By the end of 2025, 65% of enterprises had adopted at least one AIOps-driven security tool, with projections exceeding 70% by 2026 [41].

AI-assisted automation in SOCs has led to a 30% reduction in human analyst workload, allowing reallocation of staff to higher-order investigative tasks [40].

C. Supplementary Case Insights

Financial Sector: AI-based anomaly detection systems identified insider trading attempts with 92% detection accuracy, compared to 68% with traditional rule-based methods.

Healthcare Cloud Deployments: Automated compliance auditing reduced HIPAA-related violations during audits by 55%.

Retail Sector: Adoption of self-healing automation in e-commerce cloud environments reduced downtime incidents by 35% year-over-year.

REFERENCES

- [1] Prabhakaran, S.P., Cloud Intelligence and AIOps Integration: A Framework for Autonomous IT Operations in Modern Cloud Environments. 2024, ResearchGate.
- [2] Abubakar, M. and S. Chittraju Gopal Varma, Optimizing IT Operations with AI and Machine Learning in Cloud Environments. *Optimizing IT Operations with AI and Machine Learning in Cloud Environments* (June 14, 2020), 2020.
- [3] M. A. Sami, A. Rehman, Z. Ahmad, and N. Bano, "Explainable AIOps: A Deep Survey on Trustworthy and Transparent AI in Cloud-Scale DevOps Automation," *Spectrum of Engineering Sciences*, vol. 3, no. 7, pp. 488–507, Jul. 2025.
- [4] Al Hinai, A. and M. Al Mazroui. Optimizing and Enhancing IT Operation Operating Models Through Artificial Intelligence. in 2024 2nd International Conference on Computing and Data Analytics (ICCD). 2024. IEEE.
- [5] Mittal, A., AI-Driven DevOps Automation for Cloud-Native Application Modernization. *Authorea Preprints*, 2025.
- [6] Chettier, T.M., V.A.K. Boyina, and S. Rangineni, AI-Powered Risk Assessment and Compliance in Cloud Cybersecurity.
- [7] Manchana, R., AI-Powered Observability: A Journey from Reactive to Proactive, Predictive, and Automated. *Int. J. Sci. Res. IJSR*, 2024. 13: p. 1745-1755.
- [8] Joy, M., et al., "AIOps in Action: Streamlining IT Operations Through Artificial Intelligence," *International Journal of Intelligent Systems and Applications in Engineering*, 2024. 12(23s): p. 2175-2185..
- [9] Padhy, A., Artificial Intelligence-Driven DevOps: Automating, Optimizing, and Securing Modern Software Delivery. 2025: Deep Science Publishing.
- [10] Joseph, A. and J. Paulose, Harnessing the Power of AI: Transforming DevSecOps for Enhanced Cloud Security. *International Journal of Computer and Information Engineering*. 18: p. 335-341.
- [11] Naveen, K.K., et al., An overview of cloud computing for data-driven intelligent systems with AI services. *Data-Driven Systems and Intelligent Applications*, 2024: p. 72-118.
- [12] Adenekan, T.K., Optimized AI and Graph-Regularized Neural Networks for Cyber Security and AIOps in IoT. 2024.
- [13] Chittala, S., AIOps in Action: Automating AI Deployment and Management of Large Language Models for Scalable and Ethical Operations. *IJFMR*, 2024. 6.
- [14] Syed, A.A.M. and E. Anazagasty, AI-Driven Infrastructure Automation: Leveraging AI and ML for Self-Healing and Auto-Scaling Cloud Environments. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 2024. 5(1): p. 32-43.
- [15] Haider, Z. and J. Yang, Revolutionizing Enterprise Architecture: Harnessing AI and Cloud Synergy with DevOps Integration. *ResearchGate*, November, 2024.
- [16] Emirođlu, B.G., AI-Driven Threat Detection and Response Systems: Enhancing Cybersecurity in the Digital Era, in *Challenges and Solutions for Cybersecurity and Adversarial Machine Learning*. 2025, IGI Global Scientific Publishing. p. 227-270.
- [17] Veluru, S.P., Leveraging AI and ML for Automated Incident Resolution in Cloud Infrastructure. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 2021. 2(2): p. 51-61.
- [18] Garg, S., Next-Gen Smart City Operations with AIOps & IoT: A Comprehensive look at Optimizing Urban Infrastructure. Available at SSRN 5271046, 2021.
- [19] Ravichandran, N., et al., AI-Powered Workflow Optimization in IT Service Management: Enhancing Efficiency and Security. *Artificial Intelligence and Machine Learning Review*, 2020. 1(3): p. 10-26.
- [20] Diaz-De-Arcaya, J., et al., A joint study of the challenges, opportunities, and roadmap of ml ops and ai ops: A systematic survey. *ACM Computing Surveys*, 2023. 56(4): p. 1-30.
- [21] Shankeshi, R.M., Cloud-native DevOps for Oracle databases: Integrating CI/CD with AI-powered pipelines. *International Journal For Multidisciplinary Research*, 2022. 4: p. 1-15.
- [22] Pamisetty, A., Enhancing Cloudnative Applications WITH AI AND ML: A Multicloud Strategy FOR Secure AND Scalable Business Operations. 2022.
- [23] Xu, J., AI theory and applications in the financial industry. *Future And Fintech, The: Abcdi And Beyond*, 2022. 74.
- [24] Wu, Y., J. Ge, and T. Li, *AI and machine learning for network and security management*. 2022: John Wiley & Sons.
- [25] Adebayo, A., F. Oduwale, and T. Alade, *Enhancing Cloud Security with AI: An In-Depth Study on the Role of Artificial Intelligence and Machine Learning in Advanced Threat Detection and Prevention*. 2022.
- [26] Adeyemi, O., F. Yusuf, and I. Okorie, *A Thorough Analysis of AI-Powered Optimization, Resource Management, and Security in Cloud Computing Environments*. 2023.
- [27] Annam, S.N., *Enhancing IT support for enterprise-scale applications*. *International Journal of Enhanced Research in Science, Technology & Engineering*, 2023. 12(3): p. 205.
- [28] Islavath, N., *Demystifying Cloud Infrastructure: A Guide to Efficiently Managing Cloud Environments with DevOps Tools*. *Ku J of Art Int, Rob, Mach and Data sci*, 2021. 1(1): p. 001-006.
- [29] Boda, V.V.R., *Zero Trust in Healthcare: Building a Secure Future with DevOps*. *International Journal of Emerging Trends in Computer Science and Information Technology*, 2022. 3(1): p. 29-37.
- [30] Bellamkonda, S., *Network Device Monitoring and Incident Management Platform: A Scalable Framework for Real-Time Infrastructure Intelligence and Automated Remediation*. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2022. 10(3): p. 76-86.
- [31] Arugula, B., *Implementing DevOps and CI/CD Pipelines in Large-Scale Enterprises*. *International Journal of Emerging Research in Engineering and Technology*, 2021. 2(4): p. 39-47.
- [32] Anbalagan, K., *AI in cloud computing: Enhancing services and performance*. *International Journal of Computer Engineering And Technology (IJCET)*, 2024. 15(4): p. 622-635.
- [33] Bernini, G., P. Piscione, and E. Seder, *AI-driven Service and Slice Orchestration. Shaping the Future of IoT with Edge Intelligence*, 2024: p. 15.
- [34] Kaswan, K.S., et al., *Artificial intelligence for financial services, in Contemporary studies of risks in emerging technology, part A*. 2023, Emerald Publishing Limited. p. 71-92.
- [35] Theodorou, V., et al. *Blockchain-based zero touch service assurance in cross-domain network slicing. in 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. 2021. IEEE.
- [36] Danda, R.R., *AI-Driven Incentives in Insurance Plans: Transforming Member Health Behavior through Personalized Preventive Care*. *Letters in High Energy Physics*, 2023.
- [37] Pinheiro, H., *How to Implement AI-Driven Businesses in Communication Service Providers (CSPs)*. 2021, Universidade Católica Portuguesa.
- [38] Ken Research, *Global AIOps Market Forecast 2030*. Ken Research, 2024.
- [39] M. Du, F. Li, G. Zheng, and V. Sri Kumar, "DeepLog: Anomaly Detection and Diagnosis from System Logs," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2017.
- [40] IBM Security, *Cost of a Data Breach Report 2024*. IBM Corporation, 2024.
- [41] Gartner, *Market Guide for AIOps Platforms*. Gartner Research, 2023.