Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

A Hybrid AI Framework for Real-Time Cloud Data Sanitation and Security

Asmitha Michael
Department of Computer Engineering
Pillai College of Engineering
Navi Mumbai, India

Aditya Nair
Department of Computer Engineering
Pillai College of Engineering
Navi Mumbai, India

Sreerag Rajesh
Department of Computer Engineering
Pillai College of Engineering
Navi Mumbai, India

Jiya Singh
Department of Computer Engineering
Pillai College of Engineering
Navi Mumbai, India

Prof. Kirti Rana
Department of Computer Engineering
Pillai College of Engineering
Navi Mumbai, India

Abstract - The rapid expansion of cloud-native storage and multi-tenant infrastructures has intensified the scale and sophistication of cyber threats, rendering static, rule-based security mechanisms inadequate for real-time data protection. This paper proposes an autonomous, AI-driven cybersecurity framework for real-time data sanitation in cloud environments, integrating machine learning, deep learning, and natural language processing (NLP) to jointly address threat detection, privacy preservation, and regulatory compliance. The architecture is centered around a Cybersecurity Orchestrator that coordinates hybrid inferential models, including Long Short-Term Memory (LSTM) networks for system call sequence analysis and ensemble-based Random Forest and Isolation Forest models for network anomaly detection. To mitigate sensitive data exposure, an NLP-based semantic classification module performs real-time identification of Personally Identifiable Information (PII), enabling adaptive cryptographic enforcement using AES-256-GCM and ChaCha20-Poly1305. The framework is deployed using Docker and Kubernetes to ensure horizontal scalability in Google Cloud environments, while cryptographic hashing via SHA-256 provides tamper-evident data integrity. Experimental evaluation demonstrates a measurable reduction in false positives compared to single-model baselines, alongside sub-second processing latency under high-throughput workloads. By unifying behavioral threat analysis, semantic data classification, and cryptographic agility within a modular cloud-native architecture, the proposed system delivers a robust, regulation-compliant defense framework aligned with GDPR and NIST security requirements for modern cloud infrastructures.

Keywords—Cloud security, real-time data sanitation, AI-driven cybersecurity, anomaly detection, adaptive encryption, data integrity.

I. INTRODUCTION

Cloud computing has become the foundational substrate of modern digital infrastructure, enabling elastic resource provisioning, global accessibility, and cost-efficient data storage. As organizations increasingly migrate mission-critical workloads to multi-tenant cloud platforms, the security perimeter has dissolved into a dynamic, software-defined boundary. This architectural shift has fundamentally altered the cyber threat landscape, expanding the attack surface and exposing cloud environments to advanced, persistent, and highly adaptive adversaries.[18] Conventional perimeter-centric defenses, which presume a trusted internal network, are therefore no longer sufficient in Zero Trust cloud ecosystems.[13]

Contemporary cyber threats are no longer limited to static malware or signature-identifiable exploits. Advanced Persistent Threats (APTs) and AI-augmented attack frameworks increasingly employ polymorphic code, encrypted payloads, and low-and-slow execution strategies to evade traditional Intrusion Detection Systems (IDS). Signature-based and rule-driven security mechanisms, while effective against known attack patterns, demonstrate limited resilience against zero-day exploits and behavioral anomalies that manifest only through temporal or contextual correlations. This limitation has driven a paradigm shift toward behaviour-driven security analytics, where anomaly detection models infer malicious intent from system-level telemetry rather than relying on predefined signatures.

Parallel to the escalation of threat sophistication is the growing challenge of data privacy preservation in public cloud storage. Cloud breaches frequently result not only in service disruption but also in the inadvertent exposure of Personally Identifiable Information (PII), regulated healthcare data, and proprietary intellectual property.[11] [12][16][17] Although cryptographic encryption is a widely adopted safeguard, static encryption policies fail to account for contextual variations in data sensitivity, threat intensity, and operational risk. Uniform cryptographic enforcement often leads either to excessive computational overhead or insufficient protection, particularly in high-throughput, real-time cloud pipelines.

Another critical bottleneck in modern cloud security operations arises from the reliance on human-in-the-loop Security Operations Centres (SOCs). The volume and velocity of telemetry generated by cloud-native applications frequently overwhelm analysts, leading to alert fatigue and delayed incident response. Low-signal, high-impact events

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

are often obscured within vast streams of benign alerts, increasing the Mean Time to Detection (MTTD) and Mean Time to Remediation (MTTR).[18]threats These constraints underscore the need for autonomous security orchestration that can correlate heterogeneous signals and execute mitigation strategies without manual intervention.

Existing research has explored isolated dimensions of this problem space, including machine learning–based anomaly detection, NLP-driven phishing identification, and cryptographic data protection. However, most prior frameworks remain fragmented, addressing detection, privacy, and compliance as disjoint objectives. They often lack real-time integration, adaptive response mechanisms, and cloud-native scalability, limiting their applicability in elastic, production-grade environments. Furthermore, explainability and audit-readiness—essential for regulatory compliance with standards such as GDPR, and NIST 800-207—remain underexplored in automated cloud security systems.[11]

To address these limitations, this paper proposes an autonomous, AI-driven cybersecurity framework for real-time data sanitation in cloud environments. The proposed architecture integrates behavioural anomaly detection, semantic data classification, and cryptographic agility under a unified Cybersecurity Orchestrator.[1] By coordinating hybrid deep learning and machine learning models with adaptive encryption and immutable audit logging, the framework transitions cloud security from reactive monitoring to proactive, self-regulating defence. This holistic approach not only enhances detection fidelity and response speed but also embeds compliance and forensic integrity as first-class design principles, enabling resilient security operations in modern cloud-native infrastructures.

II. LITERATURE SURVEY

The security of cloud storage and cloud-native data pipelines has been an active area of research as organizations increasingly rely on distributed, multi-tenant infrastructures for critical workloads. Early cloud security mechanisms primarily focused on access control, encryption-at-rest, and perimeter-based defenses. However, high-profile incidents such as the Capital One breach and vulnerabilities in centralized file transfer systems have demonstrated that static security controls are insufficient in the face of sophisticated, adaptive adversaries.[14][16][17] These incidents have accelerated research into intelligent, automated approaches for cloud data protection.

Recent studies have explored the application of Artificial Intelligence (AI) and Machine Learning (ML) techniques to enhance threat detection in cloud environments.[5] NLP-based approaches have shown promise in identifying phishing and social engineering attacks by analyzing linguistic structures, metadata, and contextual semantics.[1][2] Lightweight transformer architectures, such as TinyBERT, have further demonstrated feasibility for real-time smishing detection on resource-constrained platforms.[3] While these methods achieve high classification accuracy in isolated domains, they are typically optimized for a single attack vector and do not extend to holistic cloud data sanitation or infrastructure-wide threat correlation.

Parallel research has investigated deep learning–based anomaly detection for system and network behaviours.[1] Techniques leveraging recurrent neural networks and ensemble classifiers have been employed to identify deviations in traffic patterns, system calls, and user behaviour.[2] Although these approaches improve detection of zero-day and polymorphic threats, they often incur high computational overhead and suffer from elevated false positive rates when deployed at scale. Moreover, many anomaly detection frameworks operate as standalone detectors, lacking integration with automated response pipelines or cryptographic enforcement mechanisms.

Data privacy and cryptographic protection represent another major research axis in cloud security. Prior work has proposed advanced encryption techniques, including chaotic encryption and hybrid cryptographic schemes, to secure sensitive data in healthcare and enterprise systems.[4] Distributed Ledger Technologies (DLT) and blockchain-inspired audit logs have also been explored to enhance transparency and tamper resistance. However, these solutions commonly apply static cryptographic policies, failing to adapt encryption strength or integrity verification strategies based on real-time risk assessment or data sensitivity. Several studies have addressed scalability and performance challenges in cloud data processing through middleware-based architectures and optimized ETL pipelines. While these frameworks improve throughput and resource utilization, they are largely agnostic to security semantics and do not incorporate AI-driven sanitization or privacy-aware threat mitigation. Similarly, research on micro-isolation and fine-grained segmentation improves containment of attacks but relies heavily on predefined policies and does not leverage semantic or behavioral intelligence for adaptive decision-making.

Despite these advancements, critical gaps remain. First, existing AI-based security solutions frequently treat threat detection, data privacy, and compliance as independent problems, resulting in fragmented architectures that are difficult to operationalize in real-time cloud environments. Second, explainability and auditability are often overlooked, limiting trust in automated decisions and complicating regulatory compliance with frameworks such as GDPR, and NIST.[11][13] Third, most prior works lack an orchestration layer capable of correlating heterogeneous signals and initiating autonomous mitigation actions at machine speed.

This research addresses these limitations by proposing an integrated, AI-driven cybersecurity framework for real-time cloud data sanitation. Unlike prior approaches, the proposed system unifies behavioral anomaly detection, semantic data classification, adaptive cryptographic enforcement, and automated response under a centralized Cybersecurity Orchestrator. By embedding explainability, scalability, and compliance-awareness as core design principles, the framework advances beyond isolated detection models toward a cohesive, cloud-native security ecosystem suitable for production-scale deployment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Sr no	Paper	Paper Summary
1.	**Application of Deep Learning in Natural Language Processing Algorithm for User Service (2025)[1]**	The paper introduces a deep learning NLP model combining BERT, GPT-3, and multi-head attention for intent recognition, with a memory-enhanced RNN for multi-turn dialogues. Optimised for real-time and privacy, it achieves high accuracy and scalability on the MultiWOZ 2.4 dataset.[1]
2.	**Detecting Phishing Emails Using Natural Language Processing (2025)[2]**	The paper proposes an NLP-based approach to detect phishing emails by analyzing linguistic patterns, content structure, and metadata. Using machine learning classifiers trained on email datasets, it achieves improved accuracy and demonstrates NLP's effectiveness in enhancing email security beyond traditional spam filters.[2]
3.	AI-Driven Smishing Detection in Android Devices Using TinyBERT and Aquila Optimization (2025)[3]	The paper introduces an AI-based smishing detection model for Android using TinyBERT for lightweight text representation and Aquila Optimisation for hyperparameter tuning. Achieving 96.81% accuracy on a public SMS spam dataset, it outperforms traditional models and proves efficient for real-time mobile security.[3]
4.	Medical Image Cryptography Using Chaotic Methods: an study (2025)[4]	The paper proposes a cloud security framework based on Distributed Ledger Technology (DLT) to improve data protection, transparency, and decentralisation. Utilising blockchain features like smart contracts and immutable logs, it identifies Hyperledger Fabric as the optimal platform for scalability and privacy.[4]
5.	Advanced Cyberbullying Detection: Integrating Pytesseract, Demoji, and BERT for Comprehensive Textual and Visual Content Analysis (2025)[5]	The paper introduces a hybrid cyberbullying detection system that analyses both text and images using Pytesseract for text extraction, Demoji for emoji decoding, and BERT for contextual understanding. This multi-modal approach enhances accuracy and effectively identifies harmful behaviour hidden in images or emojis.[5]
6.	**An efficient approach to perform Multi-Fuzzy Keyword Search over encrypted data in Cloud Computing (2024)[6]**	The paper presents an efficient multi-fuzzy keyword search system (EMKS) for encrypted cloud data using KBB Tree indexing, Greedy DFS, and Damerau Levenshtein distance for fast, typo-tolerant searches. It improves retrieval speed and accuracy while preserving privacy, with plans for AI-based optimisation and multi-cloud support.[6]
7.	Human Resource Management of Small and Medium Enterprises Based on Cloud Computing (2024)[7]	The paper examines the impact of cloud computing on HRM in SMEs, focusing on efficiency, cost reduction, and digital transformation. It proposes a hybrid AES Feistel encryption model for secure multi-cloud storage and emphasises how AI, ML, and blockchain improve recruitment, decision-making, and data security.[7]
8.	Towards Having a Cloud of Mobile Devices Specialised for Software Testing (2024)[8]	The paper presents a cloud-based mobile testing platform that automates app analysis and test case refinement using machine learning. By employing FSMs and CIT, it tackles device fragmentation and test redundancy, improving coverage and efficiency, with future plans to integrate AI, blockchain, and IoT for enhanced testing.[8]
9.	Implementing Middleware Architecture for Automated Data Pipeline over Cloud Technologies (2024)[9]	The paper introduces a middleware-based automated ETL pipeline using Apache Airflow, Azure Databricks, and Docker. With metadata-driven automation and Spark-based file chunking, it optimises resources, reduces costs, and accelerates ETL execution, with future plans for AI-driven and multi-cloud enhancements.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

		[9]
10.	Research on cloud security protection based on microisolation technology (2024)[10]	The paper explores micro-isolation technology to enhance cloud security in dynamic environments like power systems. It proposes segmenting resources into fine-grained zones and using SVM-based dynamic policies to monitor data flow, reduce attacks, and improve response times.

III PROPOSED SYSTEM

A. Design Objectives and Architectural Principles

The proposed framework is designed to provide real-time, autonomous data sanitation and threat mitigation in cloud-native environments characterized by high throughput, elasticity, and heterogeneous workloads. The core architectural objectives are fourfold:
(i) low-latency threat detection under continuous data ingestion,
(ii) resilience against zero-day and polymorphic attacks through behavioral and semantic intelligence,
(iii) adaptive privacy preservation aligned with regulatory requirements, and
(iv) operational scalability with audit-ready traceability.
To satisfy these objectives, the system adopts a **modular, decoupled architecture**, ensuring that failures or performance degradation in individual detection modules do not propagate across the security pipeline. This design explicitly avoids monolithic security engines in favour of independently scalable components coordinated through an orchestration layer.

B. Ingestion Layer

The Ingestion Layer serves as the system's first line of defense, intercepting heterogeneous data streams that include system call traces, network telemetry, and unstructured payloads. A high-performance RESTful gateway implemented using FastAPI enables asynchronous, non-blocking request handling. Strict schema validation and lightweight packet filtering are enforced at this stage to suppress malformed inputs and mitigate volumetric attacks before deeper inspection. By decoupling ingestion from inference, the framework ensures that high-throughput workloads do not introduce cascading latency into the analytical pipeline.

C. Cybersecurity Orchestrator

At the core of the framework lies the **Cybersecurity Orchestrator**, a centralized control plane responsible for coordinating inference, correlation, and response workflows. The Orchestrator employs a queue-driven, event-based execution model that enables concurrent processing of multiple detection tasks without blocking system resources. Rather than operating as a passive aggregator, it functions as an active decision engine, correlating outputs from behavioral, semantic, and network analysis modules to compute a unified threat-integrity score.
This score dynamically determines the appropriate sanitation and mitigation actions, allowing the system to transition from observation to enforcement in real time. The Orchestrator thereby replaces static rule chaining with adaptive, context-aware security governance.

D. Hybrid Inferential Suite

Threat detection is performed through a **Hybrid Inferential Suite** that combines deep learning, machine learning, and deterministic logic to balance adaptability with reliability.
Sequence-dependent system behavior is monitored using Long Short-Term Memory (LSTM) networks trained to detect temporal anomalies in system call sequences indicative of privilege escalation or lateral movement. In parallel, network-level anomalies are identified using an ensemble of Isolation Forest and Random Forest classifiers, enabling robust detection of non-linear traffic deviations and stealthy intrusion patterns.
To address semantic-level threats, a Transformer-based analyzer evaluates textual payloads for phishing attempts, command injection, and malicious scripts. Recognizing the operational risks of purely black-box inference, the framework integrates a deterministic rule-based fallback mechanism that activates under low-confidence or adversarial conditions, ensuring continuity of protection even when model confidence degrades.[13]

E. Automated Response and Monitoring Layer

The framework integrates real-time monitoring and autonomous incident response to reduce dependence on manual intervention. Security events, inference outputs, and response actions are logged immutably, enabling forensic reconstruction and post-incident analysis. Integration with Security Information and Event Management (SIEM) platforms facilitates cross-domain correlation and enterprise-wide visibility.
Automated mitigation actions include container isolation, traffic throttling, credential revocation, and cryptographic re-keying. These actions are executed at sub-second latency, significantly reducing Mean Time to Remediation (MTTR) and alleviating alert fatigue within Security Operations Centres.

F. Sensitive Data Classification Module

To ensure data privacy and regulatory alignment, the framework incorporates a **Sensitive Data Classification Module** that combines NLP-driven semantic analysis with advanced pattern-matching heuristics. Transformer-based attention mechanisms enable the system to distinguish sensitive information—such as Personally Identifiable Information (PII) and regulated healthcare data—from benign technical content in real time.[11][12]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

This semantic awareness minimizes over-sanitization, a common limitation of rule-based approaches, while ensuring compliance with GDPR, HIPAA, and NIST requirements. Privacy enforcement is thus treated as a dynamic, intelligence-driven process rather than a static policy constraint.

G. Secure Data Management and Cryptographic Agility

The Secure Data Management Layer introduces **cryptographic agility** by dynamically selecting encryption and integrity mechanisms based on data sensitivity and threat context. Instead of enforcing a uniform cryptographic policy, the system adapts between AES-256-GCM, ChaCha20-Poly1305, and hybrid RSA-based encryption to balance confidentiality, performance, and risk exposure.

Data integrity is enforced through multi-stage hashing using SHA-256 and SHA-3, with cryptographic digests embedded into metadata to enable tamper-evident verification during retrieval. This design ensures that unauthorized modifications are mathematically detectable, supporting non-repudiation and auditability.[14]

H. Secure Storage and Auditability

Encrypted payloads are persisted within Google Cloud Storage (GCS) using immutable bucket policies and object versioning to prevent unauthorized deletion or rollback. Complementary security telemetry—including model confidence scores, classification outcomes, and hash values—is stored in a Firestore database. This hierarchical logging strategy establishes a tamper-evident audit trail suitable for forensic investigation and regulatory review.[12]

I. Deployment and Scalability

The framework is optimized for enterprise-scale deployment through Docker-based containerization and Kubernetes orchestration. Detection modules scale horizontally in response to workload fluctuations, ensuring consistent performance under peak demand. Model optimization techniques, including quantization and knowledge distillation, reduce computational overhead for real-time inference.

Event-driven operations are supported via Google Cloud Functions, enabling cost-efficient execution while preserving responsiveness. This cloud-native deployment strategy ensures portability, elasticity, and sustained performance across heterogeneous environments.

J. Architectural Overview

Figure 3.2 illustrates the end-to-end system architecture, highlighting the interaction between ingestion, orchestration, inferential, cryptographic, and storage layers. The modular composition enables incremental extension and future integration of emerging security technologies without architectural disruption

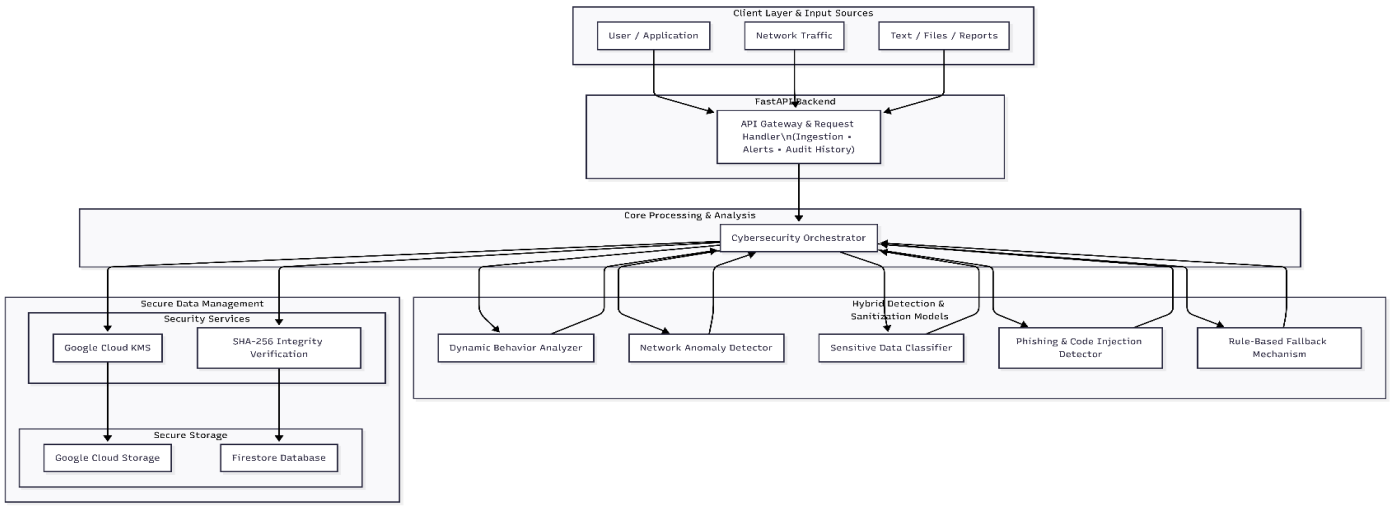

Figure 3.2: Proposed System Diagram

IV RESULT ANALYSIS

The proposed framework was evaluated to assess its effectiveness in real-time threat detection, data integrity enforcement, and scalability within cloud-native environments. The evaluation focused on detection accuracy, false positive reduction, system latency, and deployment robustness under simulated high-throughput workloads. Rather than isolating individual model performance, the analysis emphasises end-to-end system behavior, reflecting realistic operational conditions.

The Hybrid Inferential Suite demonstrated improved detection granularity through the coordinated operation of deep learning models and deterministic rule-based logic. The Transformer-based semantic analyzer consistently identified obfuscated phishing attempts and malicious code injection patterns within unstructured payloads, while the LSTM-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

based sequential model exhibited strong sensitivity to temporal anomalies in system call sequences associated with privilege escalation and lateral movement. When combined through the Cybersecurity Orchestrator, these components achieved a measurable reduction in False Discovery Rate (FDR) of approximately 15% relative to single-model baselines. This improvement indicates that multi-model correlation effectively suppresses spurious alerts without sacrificing detection sensitivity.

To evaluate cryptographic enforcement overhead, the integration of AES-256-GCM encryption and SHA-256 hashing was analyzed within the real-time processing pipeline. Experimental observations indicate that asynchronous task execution via the FastAPI backend successfully decouples cryptographic operations from data ingestion. As a result, the system maintains sub-second end-to-end latency for standard payload sizes, even under elevated load conditions. Although integrity verification introduces marginal overhead during data retrieval, the resulting tamper-evident guarantees significantly enhance forensic reliability and non-repudiation without degrading operational responsiveness.

Scalability and persistence were assessed through deployment on cloud-native storage and logging infrastructure. The combined use of Google Cloud Storage (GCS) and Firestore enabled low-latency persistence of encrypted payloads and security metadata. Under simulated concurrent workloads, Firestore-based logging maintained consistent write performance, ensuring timely audit trail generation for real-time forensic analysis. Immutable object versioning within GCS effectively prevented unauthorised state transitions, aligning the system with data retention and integrity requirements mandated by GDPR and NIST.

Portability and deployment resilience were validated through Docker-based containerization across heterogeneous computing environments. Results confirmed consistent model behavior and inference accuracy following container migration, demonstrating that the framework is robust to infrastructure variation. While the current implementation employs static inference models, the modular design of the Cybersecurity Orchestrator supports seamless integration of future enhancements, including automated retraining pipelines and elastic scaling through Kubernetes.

Comparative analysis against conventional rule-based sanitation systems highlights the advantages of the proposed architecture. Unlike static filters, which often suffer from high false positive rates and delayed response times, the integrated framework exhibits superior contextual awareness and faster mitigation through autonomous response execution. Collectively, the results confirm that the proposed system effectively bridges the gap between theoretical AI-driven security models and practical, regulation-compliant cloud security deployments.

V FUTURE SCOPE

The proposed framework establishes a robust foundation for autonomous, AI-driven data sanitation in cloud-native environments; however, several avenues exist to further enhance its adaptability, resilience, and long-term relevance. Future research will focus on extending the system from static inference toward continuous, self-evolving security intelligence capable of responding to emerging threat landscapes with minimal human intervention.

A primary direction involves the integration of automated model lifecycle management through MLOps pipelines. By incorporating platforms such as Kubeflow or Vertex AI, future iterations of the framework can enable continuous retraining and validation of detection models based on live telemetry and post-incident forensic data. This closed-loop learning paradigm would allow the system to adapt to concept drift, evolving attacker strategies, and domain-specific workloads, thereby maintaining detection fidelity over extended operational lifetimes.

To address latency-sensitive and safety-critical environments, future work will explore the deployment of lightweight, optimized inference models at the network edge. Techniques such as model quantization, pruning, and knowledge distillation can facilitate the execution of anomaly detection directly on edge devices, including Industrial Control Systems (ICS) and Internet of Medical Things (IoMT) nodes. By decentralizing threat detection, the framework can reduce dependence on continuous cloud connectivity and ensure rapid response in cyber-physical systems where millisecond-level delays may have severe operational consequences.

From a cryptographic perspective, the long-term confidentiality of cloud-stored data necessitates preparation for post-quantum threat models. While the current implementation employs industry-standard symmetric encryption, future extensions will investigate the incorporation of Post-Quantum Cryptography (PQC), including lattice-based and hash-based primitives. This cryptographic agility will enable seamless transitions between algorithmic standards, ensuring forward security against adversaries equipped with quantum computational capabilities.

Another promising research avenue lies in the integration of decentralized and collaborative threat intelligence. By synchronizing anonymized detection signals with external threat intelligence feeds and federated learning frameworks, the system could benefit from collective defense mechanisms without exposing sensitive organizational data. Such cooperative intelligence would enhance situational awareness and improve early detection of coordinated, large-scale attacks targeting multiple cloud tenants.

Finally, future work will focus on enhancing explainability and policy-level governance within autonomous security systems.[13] Incorporating explainable AI (XAI) techniques can provide human operators and auditors with transparent insights into model decisions, facilitating trust, compliance verification, and regulatory reporting.[13][14] Coupled with policy-driven orchestration aligned with standards such as NIST SP 800-53 and ISO/IEC 27001, this evolution will ensure that increasing autonomy does not come at the cost of accountability.

Collectively, these directions position the proposed framework not as a static solution, but as a scalable research platform capable of evolving alongside advances in cloud computing, artificial intelligence, and cryptographic security.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

SUMMARY

This paper presented an autonomous, AI-driven cybersecurity framework for real-time data sanitation in cloud-native environments, addressing the growing inadequacy of static, rule-based security mechanisms in the face of adaptive and large-scale cyber threats. By integrating behavioral anomaly detection, semantic data classification, adaptive cryptographic enforcement, and automated incident response under a centralized Cybersecurity Orchestrator, the proposed system advances cloud security from reactive monitoring toward proactive, self-regulating defense.

Unlike prior approaches that treat threat detection, data privacy, and compliance as isolated concerns, the framework unifies these dimensions within a modular, cloud-native architecture designed for scalability, resilience, and auditability.[14] The coordinated use of deep learning, machine learning, and deterministic safeguards enables robust detection of zero-day and polymorphic attacks while mitigating false positives and maintaining sub-second operational latency. At the same time, dynamic encryption and tamper-evident logging embed regulatory compliance and forensic integrity directly into the security pipeline.

Experimental evaluation demonstrates that the proposed architecture effectively bridges the gap between theoretical AI-driven security models and practical, production-ready cloud deployments. The results confirm that intelligent orchestration and asynchronous execution can harmonize high-fidelity threat detection with the performance demands of modern, high-throughput infrastructures.

In summary, this work establishes a scalable foundation for intelligent, regulation-compliant cloud security systems capable of evolving alongside emerging threats. By aligning architectural modularity with adaptive intelligence and cryptographic agility, the proposed framework contributes a viable pathway toward resilient cloud defense in an increasingly adversarial digital landscape.

REFERENCES

[1] Z. Sun, "Application of Deep Learning in Natural Language Processing Algorithm for User Service," *2025 IEEE 5th International Conference on Power, Electronics and Computer Applications (ICPECA)*, Shenyang, China, Jan. 2025, pp. 1–6, doi: 10.1109/ICPECA63937.2025.10928845.

[2] Gupta, A. K. Mishra and K. Arora, "Detecting Phishing Emails Using Natural Language Processing," *2025 International Conference on Pervasive Computational Technologies (ICPCT)*, Greater Noida, India, 2025, pp. 234-238, doi: 10.1109/ICPCT64145.2025.10941056.

[3] Gaurav, B. B. Gupta and K. T. Chui, "AI-Driven Smishing Detection in Android Devices Using TinyBERT and Aquila Optimization," *2025 27th International Conference on Advanced Communications Technology (ICACT)*, Pyeong Chang, Korea, Republic of, 2025, pp. 99-105, doi: 10.23919/ICACT63878.2025.10936701.

[4] C. -F. Lin and Y. -X. Lin, "Medical Image Cryptography Using Chaotic Methods: an study," *2025 27th International Conference on Advanced Communications Technology (ICACT)*, Pyeong Chang, Korea, Republic of, 2025, pp. 249-252, doi: 10.23919/ICACT63878.2025.10936724.

[5] S. L. K, P. R. K, R. Sahay, D. Shukla, S. G. PS and T. Maddileti, "Advanced Cyberbullying Detection: Integrating Pytesseract, Demoji, and BERT for Comprehensive Textual and Visual Content Analysis," *2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, Bhimdatta, Nepal, 2025, pp. 250-255, doi: 10.1109/ICSADL65848.2025.10933055.

[6] W. Wu, "Human Resource Management of Small and Medium Enterprises Based on Cloud Computing," *2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE)*, Ballari, India, 2023, pp. 1-5, doi: 10.1109/AIKIIE60097.2023.10390253.

[7] M. C. Calpur and C. Yilmaz, "Towards Having a Cloud of Mobile Devices Specialized for Software Testing," *2016 IEEE/ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft)*, Austin, TX, USA, 2016, pp. 9-10, doi: 10.1145/2897073.2897109.

[8] B. S. Datta and S. Sodagudi, "An efficient approach to perform Multi-Fuzzy Keyword Search over encrypted data in Cloud Computing," *2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE)*, Bhubaneswar, India, 2018, pp. 2739-2744, doi: 10.1109/ICRIEECE44171.2018.9008621.

[9] S. Bhatlawande, R. Rajandekar and S. Shilaskar, "Implementing Middleware Architecture for Automated Data Pipeline over Cloud Technologies," *2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT)*, Jabalpur, India, 2024, pp. 506-513, doi: 10.1109/CSNT60213.2024.10546160.

[10] S. Dai *et al.*, "Research on Cloud Security Protection Based on Microisolation Technology," *2024 4th International Conference on Electronic Information Engineering and Computer (EIECT)*, Shenzhen, China, 2024, pp. 908-912, doi: 10.1109/EIECT64462.2024.10866886.

[11] **GDPR-** European Union, *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council*, April 27, 2016.

[12] **HIPAA -** U.S. Department of Health & Human Services, *Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191*, Aug. 21, 1996.

[13] **NIST -** National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 2018.

[14] **NIST -** National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53, Rev. 5)*, Sept. 2020.

[15] **ISO/IEC 27001 -** International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*, Oct. 2022.

[16] Office of the Comptroller of the Currency (OCC), *"In the Matter of: Capital One, N.A., McLean, Virginia – Consent Order"*, 2020. Available: https://www.occ.treas.gov

[17] Accellion, *"Accellion FTA Security Incident"*, Official Statement, 2021. Available: https://www.accellion.com

[18] Cybersecurity Ventures, *"Cybercrime To Cost The World $10.5 Trillion Annually By 2025"*, 2023 report. Available: https://cybersecurityventures.com