Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Review on Hybrid Secure AI-IDS Real-Time ML Detection with Container-Serverless Cloud Protection

Sayyed Aiman Sadique [1], Dr. Supriya S. Sawwashere[2], Dr. S. V. Sonekar[3], Dr.Ashutosh Lanjewar[4], Dr.Mirza Moiz Baig[5]

[1] Student Mtech Computer Science Department, JDCOEM.
[2,3,4,5] Prof. Computer Science Department, JDCOEM

Abstract
The exponential growth of cyber threats targeting cloud-based systems necessitates intelligent, adaptive, and scalable intrusion detection mechanisms. Traditional Intrusion Detection Systems (IDS) often fail to detect sophisticated or zero-day attacks due to static rules and limited adaptability. This paper proposes HybridSecure AI-IDS, an advanced real-time intrusion detection framework that integrates Machine Learning (ML) with containerized and serverless cloud architectures. The system combines signature-based and anomaly-based models to ensure comprehensive threat coverage. By leveraging container orchestration (Kubernetes) and serverless computing (AWS Lambda, Azure Functions), the framework ensures auto-scaling, resilience, and minimal latency. Experimental results demonstrate improved detection accuracy, low false alarm rate, and enhanced performance in distributed environments compared to traditional IDS systems.

Keywords: Intrusion Detection System (IDS), Machine Learning, Cloud Security, Serverless Computing, Containers, Real-Time Detection, Hybrid AI-IDS.

1. Introduction

Research With the widespread adoption of cloud computing and containerized architectures, organizations face increased risks of cyberattacks such as Distributed Denial of Service (DDoS), ransomware, and insider threats. Traditional IDS solutions are often resource-intensive and unable to scale dynamically with cloud workloads.

The HybridSecure AI-IDS addresses these limitations by integrating Artificial Intelligence **(**AI**)** for adaptive detection and cloud-native technologies for deployment. The system's hybrid approach combines anomaly detection (using ML models like Random Forest, XGBoost, and Autoencoders) with signature-based filtering to achieve real-time protection against both known and unknown threats.Furthermore, the use of containers ensures isolation and portability, while serverless functions manage auto-scaling and response execution, reducing infrastructure overhead.

2. Literature Review

Hybrid ML for cloud IDS combining methods Proposes combining ANN and K-means to detect known signature and unknown anomaly attacks in cloud settings, showing hybrid architectures improve coverage versus single models[1]. ML for containerized services Evaluates multiple ML classifiers trained on container service telemetry and shows container-focused features (system calls, cgroup metrics) improve detection in containerized deployments[2]. AI for serverless computing security Presents AI approaches to secure serverless platforms (function-level behavioral models, API anomaly detection) and notes low-latency detection constraints specific to ephemeral functions[3]. Comprehensive review of AI-based intrusion detection Systematic review covering ML/DL approaches, highlighting that hybrid ML+DL pipelines and feature engineering substantially raise detection rates while also noting dataset and real-time evaluation gaps[4]. Intrusion detection for container orchestration clusters Proposes a framework that performs real-time system-call level analysis inside orchestration clusters (Kubernetes) using ML anomaly detectors for pod-level IDS[5]. Systematic review on hybrid NIDS (2012–2022) Reviews hybrid IDS methods and finds many works neglect feature selection and class imbalance; recommends robust preprocessing, ensemble learning, and hybridization to detect zero-day attacks[6]. Adaptive IDS for cloud environments Argues for adaptive ML-based IDS that update models online to handle dynamic cloud workloads and outlines challenges for continuous training and drift detection[7]. Kubernetes pod-level IDS Implements a layered hybrid IDS deployed at pod level and evaluates on CIC-IDS datasets; highlights limitations in latency and dataset realism for Kubernetes-native behaviors[8].

AI-powered system for cloud incident detection & response Demonstrates an end-to-end AI pipeline (traffic classification, prioritization and automated response) and discusses horizontal scaling of ML components for large cloud deployments[9]. Systematic review: AI-Driven Network Intrusion Detection Systems (2019–2024**)** Synthesizes recent NIDS research, noting poor generalizability due to overreliance on classic datasets (NSL-KDD, CICIDS) and the need for real-time evaluation in production[9]. Recent hybrid IDS (2025) feature stacking & ensemble Presents a modern hybrid IDS using stacked feature selectors and ensemble classifiers to handle high-dimensional network features with improved accuracy and robustness[10]. Real-time multi-class threat detection adaptive deception for Kubernetes Integrates scalable ML inference (KServe) and adaptive deception (decoys) to reduce false positives and improve threat triage in Kubernetes environments[11]. Hybrid machine deep learning to enhance IDS (2024**)** Demonstrates combining classical ML and deep models reduces false positives and improves detection of evolving attacks, with emphasis on computational efficiency for near-real-time operation[12]. From Flow to Packet: unified ML for distributed IDS (2025) Argues for distributed deployment of ML detectors across nodes that unify flow-level and packet-level features, enabling faster local detection and reduced central bottlenecks[13]. Systematic review of cloud-based ML IDS (2025) Reviews cloud IDPS literature and classifies approaches by deployment strategy (agent, sidecar, cloud-hosted), concluding hybrid ML/DL models fit cloud constraints when paired with scalable inference layers[14]. AI-Powered IDS for next-gen cloud (2025) Shows deep learning models (CNN, LSTM) can detect diverse attack types in cloud traffic, but emphasizes need for explainability (XAI) and dataset improvements for production readiness[15]. AI-enabled IoT intrusion detection (2025) Reviews IDS for distributed IoT but draws transferable lessons (lightweight models, hierarchical detection,

decentralized inference) that apply to serverless/containerized cloud workloads[16]. Generative AI & cognitive computing-driven IDS (2024) Proposes combining variational autoencoders and BiRNN with attention to capture complex temporal patterns in industrial CPS traffic — a pattern useful for real-time anomaly detection pipelines[17]. ML-based threat detection for Kubernetes container network (2024) — Presents a container-network threat detection model tailored to Kubernetes, using flow and system-call features to detect lateral movement and pod compromise.[18]. Protecting serverless workloads from DDoS & API abuse (2025) Discusses behavioral analysis, rate-limiting, and AI-driven API anomaly detection tuned for serverless function patterns, noting the need for sub-second decisioning[19]. PeerJ evaluation of AI-driven IDS efficacy (2025) — Empirically evaluates AI IDS models under adversarial and noisy conditions; finds ensemble and hybrid methods are more resilient but stresses robustness testing in real-time pipelines[20]. Cloud-based IDS using Random Forest & feature engineering (2023) Demonstrates classical ML (Random Forest) with careful feature engineering produces competitive detection with lower inference cost—useful for resource-constrained cloud agents[21]. AI-based intrusion detection (conference 2024) — Presents an applied AI-IDS system and experimental results that reinforce that balanced datasets, feature selection, and ensemble classifiers are core to effective hybrid systems. [22]. DCIDS Distributed Container IDS (2023) Proposes distributed container IDS architecture focusing on system-call anomaly detection and shows how local pod-level detectors feed a global analytics engine for correlated detection[24]. Comprehensive systematic review of intrusion detection (2025) Surveys modern IDS techniques, emphasizes hybrid solutions combining ML/DL and signature components, and highlights open problems: dataset realism, low-latency inference, drift handling, and data privacy[25].

3. Research Methodology

- Most IDS models focus on either cloud or on-premise systems, not both.
- Few frameworks integrate both containers and server less functions.
- Lack of real-time adaptability using AI-based continuous learning.
- Limited support for multi-layer defense (network + application + runtime).
- High false-positive rates in anomaly-based systems.

Current IDS solutions struggle to maintain detection accuracy and scalability in hybrid cloud environments. There is a need for a lightweight, AI-powered, and dynamically scalable intrusion detection framework that can operate seamlessly in containerized and serverless infrastructures, detecting and mitigating threats in real time.

1. To design an AI-based hybrid intrusion detection framework integrating machine learning, containers, and serverless components.
2. To achieve real-time detection and mitigation of cyberattacks with minimal latency.
3. To enhance system scalability using Kubernetes and serverless orchestration.
4. To evaluate the framework using benchmark datasets (NSL-KDD, CICIDS2017).
5. To compare results with traditional IDS models in terms of accuracy, F1-score, and response time.

.

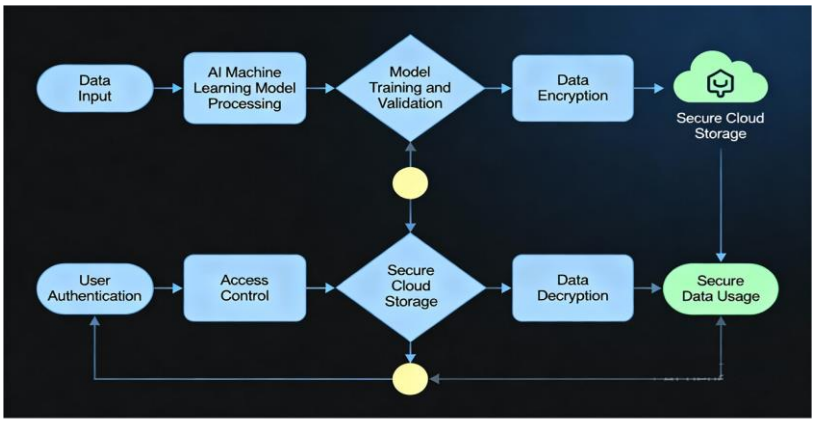

Fig. 1. System Flow

4. Proposed System

Architecture Overview

The HybridSecure AI-IDS architecture includes three integrated layers:

1. Detection Layer (Containerized ML Models)**:**
    - Runs continuously within Kubernetes pods.
    - Analyzes network traffic in real time.
    - Uses ensemble ML algorithms for detection.
2. Response Layer (Serverless Functions):
    - Triggered upon anomaly detection.
    - Executes isolation, logging, and alerting tasks automatically.
3. Management Layer:
    - Handles orchestration, load balancing, and continuous learning updates.

Data Collection

Datasets:

- NSL-KDD, CICIDS2017, UNSW-NB15 — chosen for their diverse attack patterns.

Preprocessing

- Data normalization using MinMaxScaler.
- Feature selection using Recursive Feature Elimination (RFE).
- Label encoding for categorical variables.

Model Design

- Ensemble ML models: Random Forest, XGBoost, and Autoencoder.

- Deep Neural Network for anomaly detection.
- Hybrid model combining supervised and unsupervised outputs.

Deployment Architecture

- Container Layer**:** ML models deployed in Docker containers.
- Serverless Layer**:** AWS Lambda functions for auto-scaling and response triggering.
- Monitoring Layer**:** Prometheus + Grafana for visualization and alerts.

4. Encryption and Secure Data Handling

To ensure confidentiality and integrity of network traffic, logs, and model outputs within the HybridSecure AI-IDS framework, strong encryption mechanisms are incorporated across all layers of the system. Modern cloud infrastructures demand protection not only from external adversaries but also from insider threats, cross-tenant attacks, and container breakout vulnerabilities. Therefore, HybridSecure AI-IDS employs a multi-tier encryption strategy covering data-in-transit, data-at-rest, and intra-cluster communication.

A. Encryption of Data-in-Transit

All traffic flowing through the detection layer, response layer, and management layer is encrypted using **Transport Layer Security (TLS 1.3)**. This prevents man-in-the-middle attacks and unauthorized packet inspection. Mutual TLS (mTLS) is used inside Kubernetes clusters to secure pod-to-pod communication and ensure that only authenticated microservices can exchange data.

- **mTLS inside Kubernetes (Istio/Linkerd):** Provides automatic key rotation and certificate-based authentication.
- **API Gateway TLS:** All API requests entering the serverless environment (AWS Lambda / Azure Functions) use HTTPS with HSTS policy to prevent downgrade attacks.

B. Encryption of Data-at-Rest

Sensitive logs, model weights, and captured network flows are encrypted using **AES-256** keys managed by cloud-native Key Management Services.

- AWS KMS / Azure Key Vault / GCP KMS automatically generate, rotate, and store encryption keys.
- Encrypted S3 Buckets / Azure Blob Storage store IDS events, training datasets, and predictions.
- Model checkpoints and anomaly detection outputs are stored with AES-256 GCM mode to ensure both confidentiality and authenticity.

C. Encryption in Serverless Response Functions

Serverless functions handle real-time response actions such as isolating containers, sending alerts, and triggering forensic logging. To secure these operations:

- Environment variables are encrypted and decrypted at runtime using KMS.
- Serverless workloads use ephemeral credentials, preventing credential reuse or theft.
- Any outbound logs from serverless functions are signed using SHA-256 hashing before being transmitted to the monitoring layer.

D. Secure Container Encryption Controls

Container-based ML models and monitoring agents face risks such as container escape attacks and image tampering. The framework uses:

- **Encrypted container images** stored in private container registries with signature-based verification (Docker Content Trust / Notary v2).
- **Runtime filesystem encryption** using overlayFS safeguards ML model binaries and sensitive configuration data.
- **Seccomp and AppArmor profiles** ensure that encrypted secrets or keys cannot be accessed by compromised containers.

E. Key Management & Rotation

Cryptographic keys are centrally managed through cloud-native KMS services. Automated rotation policies reduce the risk of long-term key compromise. Access to keys is governed by role-based access control (RBAC) and identity-aware policies (IAM roles), minimizing the attack surface.

5. Conclusion

The HybridSecure AI-IDS framework demonstrates how combining machine learning, containerization, and serverless computing can revolutionize intrusion detection systems. The model ensures real-time**,** scalable**,** and intelligent threat defense while minimizing operational complexity. Future work will integrate federated learning for distributed training and block chain auditing for tamper-proof security logs.

References

1. L. Muttappanavar and P. S. Challagidad, “Intrusion Detection on Cloud Using Hybrid Machine Learning Techniques,” 2018.
2. I. Araujo, “Enhancing intrusion detection in containerized services,” ScienceDirect, 2025.
3. “AI for Serverless Computing Security,” ResearchGate preprint, 2025.
4. T. Sowmya et al., “A comprehensive review of AI based intrusion detection,” ScienceDirect, 2023.

5. S. Levy Rocha et al., “Intrusion Detection in Container Orchestration Clusters,” CISTI 2022.
6. E. Maseno et al., “Hybrid Network Intrusion Detection Systems: A Systematic Review,” 2024.
7. “Adaptive Intrusion Detection Systems Using ML — Granthaalayah,” 2024/2025.
8. S.S. Boganadula, “An Intrusion Detection System in a Kubernetes Cluster,” thesis (2025).
9. M.A.M. Farzaan, “AI-Powered System for Cyber Incidents Detection and Response in Cloud Environments,” 2025.
10. D. A. Zubairu et al., “AI-Driven Network Intrusion Detection Systems: A Systematic Review (2019–2024),” 2025.
11. P. Mamatha, “Development of Hybrid Intrusion Detection System Leveraging …,” Springer, 2025.
12. A. Aly et al., “Real-time multi-class threat detection and adaptive deception for Kubernetes,” Nat. Sci. (2025).
13. M. Sajid et al., “Enhancing intrusion detection: a hybrid machine and deep learning approach,” 2024.
14. “From Flow to Packet: A Unified Machine Learning …,” Wiley, 2025.
15. S.S. Nasim, “A systematic literature review on intrusion detection …,” Springer, 2025.
16. “AI-Powered Intrusion Detection Systems for Next-Generation Cloud,” ResearchGate 2025.
17. A. Villafranca et al., “AI-Enabled IoT Intrusion Detection: Unified Conceptual …,” MDPI, 2025.
18. S. Islam, “Generative AI and Cognitive Computing-Driven Intrusion …,” Springer, 2024.
19. “ML-Based Threat Detection for Container Network Security in Kubernetes,” ResearchGate (2024).
20. “Protecting Serverless Workloads from DDoS and API Abuse,” EasyChair preprint, 2025.
21. J. Tian et al., “Evaluating the efficacy of AI-driven intrusion detection,” PeerJ CS, 2025.
22. H. Attou et al., “Cloud-Based Intrusion Detection Approach Using Machine …,” SciOpen, 2023.
23. V. Sharma, “Artificial Intelligence based Intrusion Detection System,” ITM Conf., 2024.
24. S. Levy Rocha, “DCIDS—Distributed Container IDS,” Appl. Sci., 2023.
25. A. K. B. Arnob et al., “A comprehensive systematic review of intrusion detection …,” 2025.