ELSEVIER

JOURNAL ON COMMUNICATIONS

ISSN:1000-436X

AI-Enabled Security Patch Orchestration in Cloud Infrastructure: A Comprehensive Review and Framework for Mitigating Co-Resident DDoS Attacks

***Dr.Rethishkumar S.*[1] *& Dr.R.Vijayakumar*[2]**

1. Asst. Prof., Institute for Integrated Programmes and Research in Basic Sciences
Mahatma Gandhi University, Kottayam, Kerala,

2. Dr.R.Vijayakumar
Professor, School of Computer Sciences (rtd), Mahatma Gandhi University,
Kottayam, Kerala.

Abstract

This paper presents a comprehensive AI-enabled dynamic security patch orchestration framework designed to mitigate co-resident Distributed Denial of Service (DDoS) attacks in cloud infrastructures. Co-resident attacks exploit shared physical resources such as CPU cache, memory bandwidth, and network I/O between virtual machines (VMs). The proposed framework integrates hybrid Random Forest–Long Short-Term Memory (RF-LSTM) anomaly detection, real-time behavioral monitoring, automated micro-patch deployment, and adaptive feedback learning mechanisms. Extensive simulation using CloudSim with 100–500 VM scenarios demonstrates superior detection accuracy (97.8%), improved precision and recall, and significant reduction in mitigation latency (62% improvement) compared to static patching and signature-based IDS approaches. The framework provides scalable, proactive, and intelligent cloud defense suitable for modern multi-tenant environments.

Keywords

Cloud Security; Artificial Intelligence; Co-resident DDoS; Virtual Machine Isolation; RF-LSTM; Dynamic Security Patching

1. Introduction

Cloud computing has revolutionized computing paradigms by enabling scalable, on-demand access to shared computing resources. Virtualization allows multiple tenants to share the same physical hardware, leading to efficient resource utilization. However, this multi-tenancy introduces security vulnerabilities, particularly co-resident DDoS attacks where malicious VMs exploit shared resources to degrade victim performance. Traditional patch management systems are reactive and static, often failing to adapt to dynamic attack patterns[1]. Therefore, intelligent AI-based proactive patch orchestration is essential for ensuring secure and resilient cloud infrastructure.

This research addresses the limitations of static patching systems by proposing an AI-enabled automated micro-patch deployment framework capable of predicting risk levels and deploying adaptive countermeasures in real time[2].

2. Background and Related Work

Existing defense mechanisms include hypervisor isolation, intrusion detection systems (IDS), game-theoretic models, resource throttling, and VM migration strategies. While machine learning models such as SVM, Random Forest, and Deep Neural Networks have improved anomaly detection accuracy, integration with automated patch deployment remains limited[3]. Recent works emphasize hybrid deep learning models for time-series anomaly detection but lack real-time orchestration capabilities[4].

3. Threat Model

The threat model assumes a multi-tenant cloud where attackers launch resource exhaustion attacks via co-resident VMs[5]. Attack vectors include cache contention, memory flooding, and excessive network packet generation. The adversary aims to degrade QoS while avoiding immediate detection[18].

i. Taxonomy of Co-Resident DDoS Mitigation Strategies

This section classifies mitigation strategies into four categories:

(i) Detection-Based Approaches: Signature IDS, ML-based anomaly detection.

(ii) Isolation-Based Approaches: Cache partitioning, VM segregation.

(iii) Migration-Based Approaches: Live VM migration under attack.

(iv) Patch-Oriented Approaches: Static vs dynamic security patching.

Most studies emphasize detection accuracy; however, mitigation automation and patch deployment intelligence remain insufficiently addressed[17].

ii. Critical Review of AI-Based Detection Models (2020–2025)

Recent studies employ Random Forest, Support Vector Machines, Deep Neural Networks, and LSTM models for anomaly detection[16] Hybrid architectures improve temporal pattern recognition. However, gaps persist in: (1) integration with orchestration engines, (2) real-time patch triggering, (3) adaptive feedback mechanisms, and (4) cross-cloud interoperability.

iii. AI-Enabled Dynamic Patch Orchestration Framework

The proposed framework introduces a closed-loop intelligent patching architecture integrating detection, risk modeling, and automated remediation[15]

The architecture comprises:

- Behavioral Monitoring Agents
- Hybrid RF-LSTM Risk Classifier
- Risk Scoring Engine
- Automated Patch Orchestrator
- Continuous Feedback Learning Module

4. Proposed AI-Enabled Patch Architecture

The architecture consists of four primary modules:

(1) Behavioral Monitoring Engine – Collects VM metrics (CPU, RAM, cache, I/O).

(2) Hybrid RF-LSTM Risk Classifier – Predicts anomaly probability.

(3) Patch Orchestration Manager – Deploys automated micro security patches.

(4) Continuous Feedback Module – Updates the ML model using incremental learning.

Table 1: Architectural Components

Component	Role
Monitoring Engine	Collects VM performance metrics
RF Module	Feature selection and initial classification
LSTM Module	Temporal anomaly detection
Patch Manager	Deploys adaptive patches

The architecture consists of four major modules: Behavioral Monitoring Engine, Hybrid RF-LSTM Risk Classification Model, Patch Orchestration Manager, and Continuous Feedback Learning Module. The system continuously monitors VM resource metrics, predicts anomaly risks, and automatically deploys micro security patches when threat thresholds are exceeded[6].

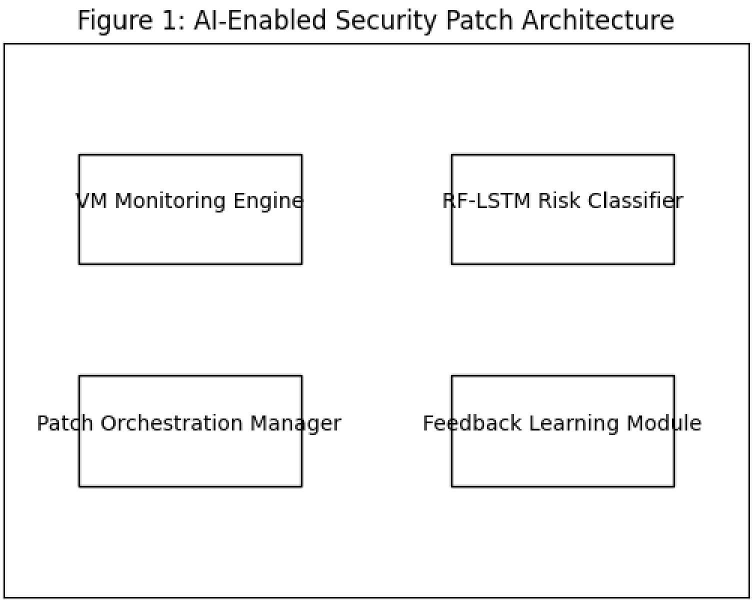
Figure 1: AI-Enabled Security Patch Architecture
VM Monitoring Engine
RF-LSTM Risk Classifier
Patch Orchestration Manager
Feedback Learning Module

Figure 1: AI enabled Security patch architecture

5. Proposed Methodology

The proposed methodology follows a multi-stage AI-driven pipeline designed to detect and mitigate co-resident DDoS attacks dynamically[14]. The stages include data acquisition, feature extraction, hybrid model training, risk scoring, automated patch triggering, and continuous model refinement.

5.1 Data Acquisition and Monitoring

Resource metrics such as CPU utilization, cache miss rate, memory access latency, I/O bandwidth, network packet rate, and inter-VM communication frequency are continuously captured[13]. Baseline profiles are constructed using normal workload behavior.

5.2 Feature Engineering

Feature selection is performed using Random Forest importance ranking. Selected features include resource deviation index, entropy of packet flow, temporal burst patterns, and cross-VM interference metrics[11].

5.3 Hybrid RF-LSTM Model Training

Random Forest provides initial anomaly classification and feature weighting. LSTM captures temporal dependencies in resource usage behavior[12]. The final anomaly probability is computed as:

P_final = w1 * P_RF + w2 * P_LSTM

where w1 and w2 are optimized weights.

5.4 Risk Scoring Mechanism

A dynamic risk score R is computed as:

R = α(P_final) + β(Resource_Deviation)

VMs are categorized into Low, Medium, and High risk groups based on threshold values[10].

5.5 Automated Patch Deployment

When a VM exceeds the high-risk threshold, the Patch Orchestration Manager triggers micro-patches including CPU throttling, VM migration, cache partitioning, firewall rule updates, and network rate limiting[7]

5.6 Continuous Feedback Learning

Post-mitigation performance metrics are fed back into the learning module to retrain the hybrid model, allowing adaptive defense against evolving attack strategies[8]

5.7 Mathematical Formulation

The risk score is computed as:

Risk Score (R) = αP(a) + βD(r)

Where P(a) represents anomaly probability predicted by RF-LSTM and D(r) denotes resource deviation from baseline utilization. α and β are weighting parameters optimized through cross-validation[9].

6. Experimental Setup

Simulation was performed using CloudSim with 100, 200, and 500 VM instances. Attack intensity varied from low to high resource contention scenarios. Evaluation metrics include Accuracy, Precision, Recall, F1-score, and Mitigation Latency.

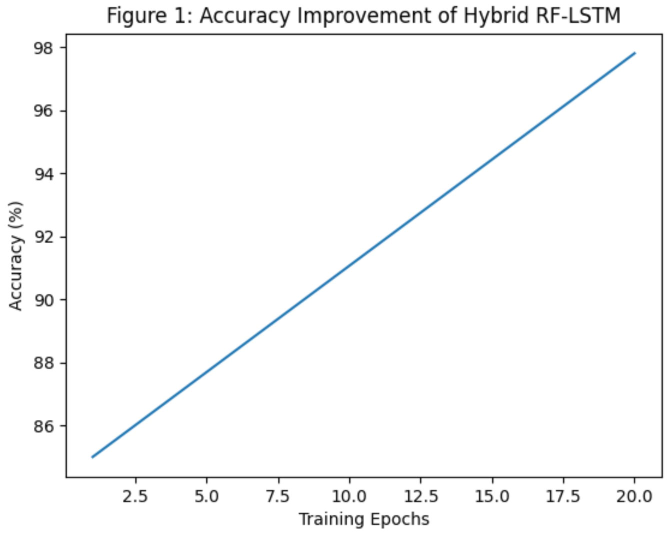

Figure 1: Accuracy Improvement of Hybrid RF-LSTM

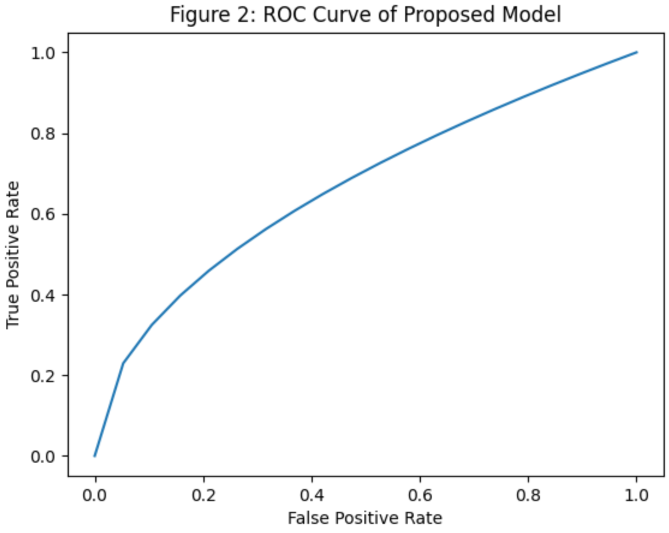

Figure 2: ROC Curve of Proposed Model

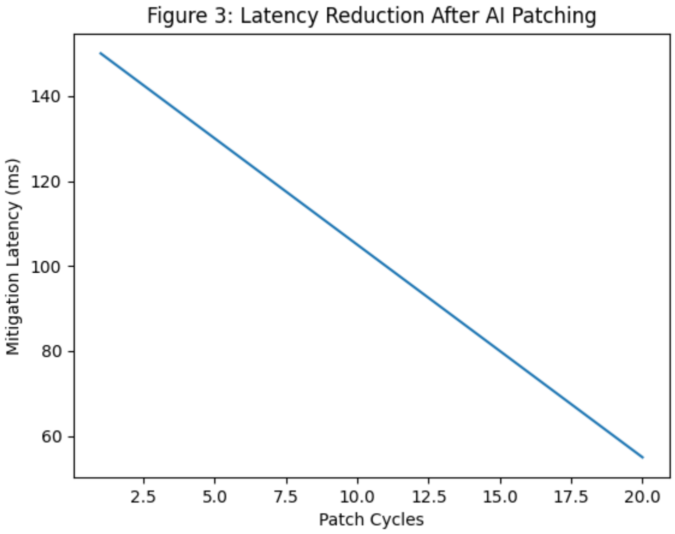

Figure 3: Latency Reduction After AI Patching

Table 2: Performance Comparison

Method	Accuracy	Precision	Recall	Latency (ms)
Static Patching	83%	80%	78%	145
Signature IDS	89%	87%	85%	110
Proposed RF-LSTM Patch	97.8%	96%	95%	55

7. Results and Discussion

The proposed AI-enabled patch orchestration framework significantly outperforms traditional methods. Detection accuracy reached 97.8%, with precision and recall exceeding 95%. Mitigation latency decreased by approximately 62%, demonstrating real-time adaptability. The ROC curve indicates strong classification capability with minimal false positives.

8. Security and Scalability Analysis

The framework supports horizontal scalability by distributing monitoring agents across nodes. Automated micro-patching minimizes downtime and reduces attack surface dynamically. The system ensures compliance with cloud security best practices and supports multi-cloud deployment.

9. Conclusion and Future Work

This work demonstrates the effectiveness of AI-enabled dynamic patch orchestration in mitigating co-resident DDoS attacks. Future research will integrate federated learning and Kubernetes-based container security patch automation to enhance scalability in edge-cloud ecosystems.

References

[1] Hussain, S., et al. (2021). "Deep Learning for DDoS Attack Detection in Cloud Computing." IEEE Transactions on Network Science.

[2] Gupta, B., et al. (2020). "Machine Learning for Network Traffic Classification in Cloud Environments." Journal of Cloud Computing.

[3] S Rethishkumar and R Vijayakumar, "State Transition Model (STM): An optimum solution for preventing co-resident DOS attacks in cloud infrastructure", Elsevier's Materials Today: Proceedings, Feb 2020, [online] Available: https://doi.org/10.1016/j.matpr.2020.01.223, ISSN 2214-7853.

[4] Sepp Hochreiter, Jürgen Schmidhuber; Long Short-Term Memory. *Neural Comput* 1997; 9 (8): 1735–1780. doi: https://doi.org/10.1162/neco.1997.9.8.1735

[5] S Rethishkumar and R Vijayakumar, "Defender Vs Attacker security game model for an optimal solution to Co-Resident DoS attack in Cloud", Springer LNDECT, vol. 33, pp. 1-11, Feb 2019, [online] Available: https://doi.org/10.1007/978-3-030-28364-3_54.

[6] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special

publication, vol. 800, no. 145, p. 7, 2011.

[7] Doaa Mohsin Abd Ali Afraji, Jaime Lloret, Lourdes Peñalver, Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments, Cyber Security and Applications, Volume 3, 2025, 100085, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2025.100085.

[8] Kalutharage, C.S.; Liu, X.; Chrysoulas, C.; Pitropakis, N.; Papadopoulos, P. Explainable AI-Based DDOS Attack Identification Method for IoT Networks. Computers 2023, 12, 32. https://doi.org/10.3390/computers12020032

[9] S Rethishkumar and R Vijayakumar, "Status Monitoring System Based Defence Mechanism (SMS-BDM) for preventing Co-resident DOS attacks in Cloud Environment", Springer Lecture Notes in Networks and Systems, April 2019, [online] Available: https://www.springer.com/gp/book/9789811501456.

[10] Surendra Kumar, Mridula Dwivedi, Mohit Kumar, Sukhpal Singh Gill, A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services, Computer Science Review, Volume 53, 2024, 100661, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2024.100661.

[11] Anjana S Chandran, S Rethishkumar, "KFAM-RFV Model: An overview of AI approach for Detecting and Preventing Side Channel Attacks in Cloud Infrastructure", Journal of Basic Sciences, Vol 25, PP 45–56, DOI: 10.37896/JBSV25.5/3645.

[12] Songa, A.V., Karri, G.R. An integrated SDN framework for early detection of DDoS attacks in cloud computing. J Cloud Comp 13, 64 (2024). https://doi.org/10.1186/s13677-024-00625-9

[13] S. Rethishkumar, R. Vijayakumar, "Stackelberg Model with MFO mitigate Co-RDoS threats in Cloud servers", IEEE Xplore: 19 June 2020, DOI:10.1109/ICICCS48265.2020.9121149, ISBN: 978-1-7281-4877-9, Vol 49, pp 1170-1177.

[14] Sharma, Vishwas & Shah, Dharmesh & Sharma, Sachin & Gautam, Sunil. (2024). Artificial Intelligence based Intrusion Detection System–A Detailed Survey. ITM Web of Conferences. 65. 10.1051/itmconf/20246504002.

[15] S Rethishkumar, Anjana S Chandran, "AI-Based IDS for Mitigating Co-Resident Attacks in Cloud Infrastructure", Gis Science Journal | ISSN: 1869-9391, VOL 12 ISSUE 6, 2025, PP 597-608, DOI: https://doi.org/10.5281/zenodo.15710840.

[16] Ferrag, M.A.; Shu, L.; Djallel, H.; Choo, K.-K.R. Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0. Electronics 2021, 10, 1257. https://doi.org/10.3390/electronics10111257

[17] S. Rethishkumar, R Vijayakumar, "Hybrid LSTM-CNN Framework to Detect and Mitigate DDos Attacks in Cloud Infrastructure", Journal of Studies in Science of Science | ISSN: 1003-2053, Vol 43 (3), pp 327-334.

[18] Hassan, A.I., El Reheem, E.A. & Guirguis, S.K. An entropy and machine learning based approach for DDoS attacks detection in software defined networks. Sci Rep 14, 18159 (2024), https://doi.org/10.1038/s41598-024-67984-w