Exploring ML Models for Effective Zero Trust Architecture (ZTA) in Cloud-Native Environments (CNEs) for Coarse-Grained Policies

Madhuri Rao[1], Ganesh Khekare[2]

[1] Lincoln University College, Malaysia; [2] Vellore Institute of Technology, Vellore, India

pdf.madhurirao@lincoln.edu.my

Abstract: Cloud Native Environments incorporate Zero Trust Architecture (ZTA) that are mostly static access control rules with coarse grained network segmentations. They are dependent on Role Based Access Control mechanisms which often lead to signature-based intrusion detection systems. They lack the ability to detect behavioral drift and often are characterized with over permissive access mechanisms. Now with microservices, service mesh and Kubernetes, cloud native environments are more dynamic, ephemeral and behavior driven where traditional static ZTA would be inefficient. Machine Learning models could equip ZTA for continuous authentication, context aware authentication, continuous monitoring and least privilege enforcement by enabling behavioral baselining, anomaly detection, risk scoring, bring adaptive policy update and evaluate trust dynamically. In this work we survey and evaluate a proposed Ensemble ML models comprising of LSTM, CNN and SVM that could address these newer challenges posed by microservice and cloud native architectures.

Keywords: Cloud Native Environments (CNE); Zero Trust Architecture (ZTA); Ensemble Machine Learning Model; Long Short-Term Memory (LSTM); Convolutional Neural Network (CNN); Support Vector Machine (SVM)

Introduction

Supervised machine learning models like XGBoost, Support Vector Machine can be used when labelled datasets exists and are effective in detecting known attacks like DoS, R2L, U2R and probe based ZTA attacks. They could classify malicious pod-to-pod traffic and can detect API misuse but, they cannot detect novel attack effectively. Unsupervised learning models like K-Means clustering and isolation forest can detect anomalies in dynamic CNE traffic. They are very suitable for Zero Trust Adaptive models which can identify lateral movement, detect privilege escalation attempts and can also detect unusual service -to-service communications. Deep Autoencoders and Variational Autoencoders that are semi supervised models can be trained on normal behavior only and are suitable for Kubernetes traffic baselining. Reinforcement learning mechanism could enable ZTA [1] for better dynamic policy tuning. However, these models are very difficult to understand and lack of comprehension builds distrust hindering effective use of the system.

Related work

Table 1 shows related work with respect to Zero Trust Architecture. [1] [2] and [3] demonstrate and validate that ensemble methods are more effective than traditional ML models in building effective Zero Trust architecture. The work in [2] is based on IoT intrusions while in [3] Autonomous vehicle security is addressed.

Table 1. Compares this work with the related work or previous research by other researchers

	Application Domain	ML Models	Findings
[1]	Zero Trust Architecture	RF, XGBoost, LR	Ensemble models are more effective for ZTA
[2]	IoT Intrusions detection	SVM, XGBoost,	They validates superior performance of ensemble methods combining multiple classifiers for IoT systems
[3]	Autonomous Vehicle Security	RF, SVM, AdaBoost, XGBoost + LSTM as meta-learner	Ensemble methods are effective in detecting complex cyberattack patterns in consumer CAV environments.
Our work	Cloud Native Environments (CNEs) with microservices and orchestration	Ensemble method with LSTM, CNN and SVM	Ensemble Method comprising if LSTM + CNN+ SVM is effective in devising ZTA for CNEs building coarse grained policies.

Key Contribution

In this study we build an ensemble model comprising of SVM, LSTM and CNN ML models for enabling coarse grained policies in ZTA mechanisms.

Method, Experiments and Results

Single ML models are not as efficient as few combinations that could work more effective as also seen from existing work in ZTA. The proposed model comprises of following steps as depicted in **Figure 1.**

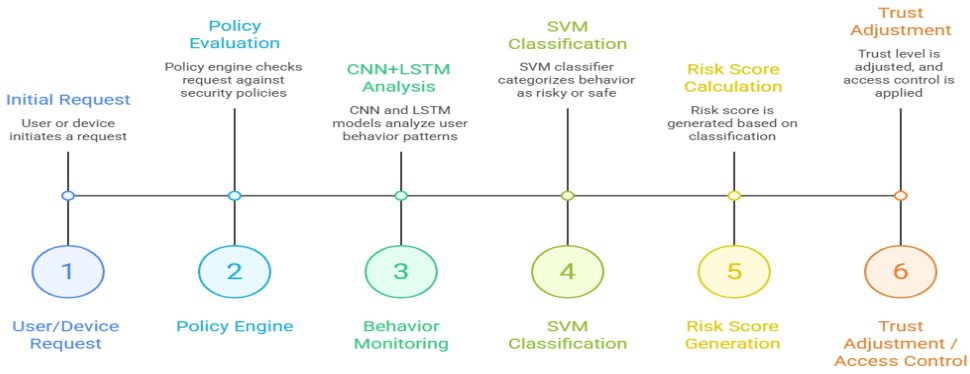

Figure 1: Proposed Ensemble model with (LSTM+CNN+ SVM)

Discussions

CNN enables effective feature extraction as given by Eq.(1)

$$H_{CNN} = ReLU\ (W\ x\ X\ +\ b) \qquad \text{Eq.(1)}$$

LSTM enables temporal modelling explained as per Eq. (2)

$$h_t = LSTM\ (x_t\ , h_{t-1}) \qquad \text{Eq.(2)}$$

Feature fusion as performed in the next step before giving input to the SVM classifier which is based on Eq.(3).

$$F\ =\ concat\ (\ H_{CNN}\ , h_t\ ) \qquad \text{Eq.(3).}$$

SVM brings about margin based classification and its decision is based as per Eq.(4).

$$y = sign\ (\ W^T\ F\ +\ b) \qquad \text{Eq.(4)}$$

Conclusions

1. Problem statement Addressed/ Motivation

   The aim of the research work here was to design and evaluate an Ensemble based ML model for Zero Trust behavioral enforcement in cloud native environments as they can dynamically adapt access decisions based on computed risk scores derived from network flow data.

2. Method used

   In this work we explore CIC-IDS2017 dataset with an ensemble ML model comprising of SVM+LSTM+ CNN for developing coarse grained policies for ZTA in CNEs. The CIC-IDS2017 dataset contains packet level data with 80+ features.

3. Key findings

   The proposed Ensemble model comprising of CNN+ LSTM + SVM provides output that has three coarse grained policy levels as depicted in Figure 1.

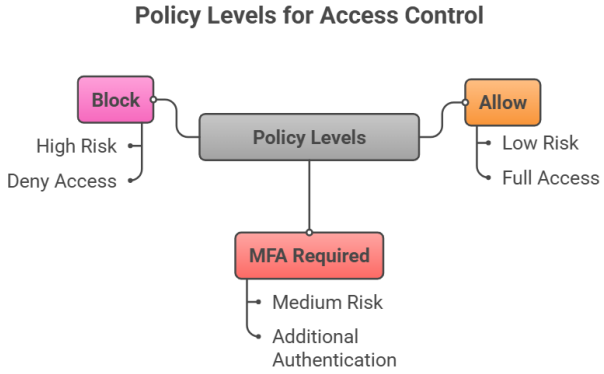

Figure 1: Coarse grained policy levels attained

The model can also show which features have an important role in creating these policy levels. Allow policy is based on a risk score between 0-30 and typical characteristics include high device compliance, normal login patterns, no previous violations, and appropriate access times. This enables full access and normal monitoring is performed further. MFA Required decision is taken when the risk score is between 31-70 with key determining Characteristics as moderate compliance issues, unusual geolocation, slightly anomalous behavior and 1-2 previous violations. With MFA challenges monitoring is increased. When the risk score is between 71 -100, decision to Block is taken caused by critical compliance failures, multiple failed attempts, high-risk geolocation or abnormal attack patterns if detected. In such case access to the resources is denied and incident response is triggered.

4. Limitations of the work and future work that should be carried

The proposed framework demonstrates the feasibility of integrating Ensemble based ML with risk scoring within a Zero Trust enforcement. However, the study deals with dataset that captures static enterprise traffic and lacks cloud-native telemetry data. Future work aims to include real-time streaming data with adaptive reinforcement learning-based policy optimization and explore Explainable AI (XAI) mechanisms to enhance trust and deployment realism.

References

1. V. M. Zanpure, "Improving Zero Trust Architecture with Machine Learning: Automatic Threat Detection using Network Traffic Analysis," *2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, Chennai, India, 2025, pp. 1-6, doi: 10.1109/RMKMATE64874.2025.11042837.
2. N. U. Sama, S. Ullah, S. M. A. Kazmi, M. Mazzara, “Cutting-Edge Intrusion Detection in IoT Networks: A Focus on Ensemble Methods”, vol. 13, pp. 8375 – 8392, 2025. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10744011
3. I. Ahmad, U. A. Mughal, L. Yang, Y. Alkhrijah, A. Almadhor, M. A. Alawad, "Intelligent Ensemble Learning Framework for Intrusion Detection in Consumer Connected and Autonomous Vehicles," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 4, pp. 12437-12448, Nov. 2025, doi: 10.1109/TCE.2025.3619781