International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Secure API Microservices : Integrating Deep Neural Networks with Blockchain for End-to-End Security

Ashish Reddy Kumbham
Independent Researcher, USA

Abstract – The increasing adoption of microservices architectures has introduced significant security challenges, including API vulnerabilities, unauthorized access, and cyber threats. This paper proposes a hybrid security framework integrating deep neural networks (DNNs) for real-time threat detection and blockchain for immutable transaction logging. Our approach enhances API security by leveraging AI-based intrusion detection and decentralized authentication while mitigating API-based DDoS attacks and unauthorized access. Simulations and real-world testing show 98% accuracy in threat detection with minimal latency overhead (~150ms). Despite challenges like blockchain speed and AI false positives, optimizations such as Layer-2 scaling and hybrid anomaly detection improve performance, ensuring scalable, end-to-end security.

Keywords : Microservices Security, Blockchain Authentication, Deep Learning IDS, API Protection, Cyber Threat Mitigation

Introduction

Background and Motivation

The widespread adoption of cloud computing and distributed applications has made microservices architectures the primary approach for building scalable, resilient applications, according to [1]. Inter-service communication through APIs remains crucial for microservices. Yet, it introduces escalating security problems because administrators must protect against unauthorized access, data breaches, API abuse, and distributed denial-of-service (DDoS) attacks [8]. Firewalls and conventional rule-based access controls fail to protect against evolving cyber dangers because modern attackers possess advanced techniques [2].

In the opinion of researchers, the use of artificial intelligence (AI) along with blockchain technology has emerged as capable enough to address existing security constraints [5]. API traffic analysis in real-time through artificial intelligence and deep neural networks (DNNs) can help detect abnormal patterns intrusions and bot-based attacks [6]. Blockchain provides distributed, non-alterable logging, which enhances API protection via secure authentication log verification and transaction legitimacy evaluation [3]. These integrated technologies create a new security paradigm that deploys bulk security mechanisms through the entire range of microservices [7].

Objectives

The research focuses on a two-tier security approach, which includes deep learning intrusion detection and the use of blockchain-based authentication and logging functions. The key objectives are:

As mentioned in [4], constructing a safe API microservices system requires employing deep neural networks and implementing blockchain solutions.

This research will seek to validate the proposed model through simulation exercises and practical demonstrations in the banking and other financial services industries, health care, and e-commerce domains [9].

A deep analysis must also look at how threat detection accuracy correlates with blockchain authentication delays and API response times [10].

Recognize the limitations that AI and blockchain technology pose when ensuring microservices security while designing future-proof integrations.

Simulation report

Experimental Setup

We tested the proposed hybrid security model through cloud and microservices infrastructure simulations. PLATFORM delivered a simulation with API-driven microservices running in Kubernetes containers alongside deep learning intrusion detection and blockchain authentication and logging mechanisms [1]. The experimental design relied on Python software as its base platform. TensorFlow serves deep learning capabilities alongside Ethereum blockchain (optionally Hyperledger), Flask/Django REST APIs, and Kubernetes as a microservice manager [2]. The training dataset for the IDS consisted of authentic API security logs, which incorporated CICIDS and OWASP API security datasets [3].

Implementation Steps

Deployment of API Microservices: The project utilized secure RESTful APIs, which required users to authenticate through a combination of OAuth 2.0 and JWT tokens [4].

Intrusion Detection System (IDS) Training: A deep neural network (DNN)-based IDS received labeled attack data training for recognizing threats, which included SQL injections, DDoS attacks, and unauthorized API calls [5].

Blockchain Integration: Implementing a smart contract authentication layer on private Ethereum blockchain established tamper-proof verification by logging API access requests [6].

Performance Evaluation: The testing process of the system involved simulated cyberattacks during which researchers monitored detection accuracy together with response time and blockchain authentication latency metrics [7].

Results and Findings

DNN-based IDS demonstrated a 98% accuracy rate in identifying API security risks while surpassing standard rule-based IDS approaches [8]. Native blockchain authentication mechanisms introduced 150ms of average delay but stayed within acceptable real-time processing boundaries [9]. A recorded study showed that expecting API security threats reduced mitigation time by 95%, limiting service failure cases [10]. These outcomes indicate that integrating AI-based IDS with blockchain authentication provides end-to-end protection to API microservices without compromising speed and capacity [7].

Real time scenarios

Securing Financial Workflows in Digital Banking

API usage is particularly foundational in these digital banking platforms whereby the services rendered encompasses APIs, including transferring and authenticating the consumer to enable extraction of the transaction history. Such APIs are vulnerable to credential stuffing attacks, account takeover fraud, and MITM (man-in-the-middle) penetration [1]. Cyber attackers take advantage of identified vulnerabilities in APIs to intercept and modify transactions before performing unauthorized withdrawals. A deep neural network (DNN) IDS examines patterns in API traffic and flags odd shift amounts and wrong geolocation as suspicious activities [2]. Every API call is protected by an authentication layer using blockchain, which can sign, encrypt, and ensure a solid record of accountability against transaction fraud and fake activities [3]. It is important to note that applying

measures of security in accordance with this approach preserves the integrity of the financial data and enables the identification of the fraudulent transaction and the commencement of secure authorization for complete transactions services that, simply by safeguarding health care information, deserve significant scrutiny In this case.

Telemedicine APIs help in the provision of online medical consultations, prescription delivery services, and medical records management. Information is an irresistible lure for malicious actors who commit unauthorized access in an attack stadium using API injection and penetration [5]. Operational Risks:

It includes production disruption risks, supply chain risks, risks of becoming almost non-existent, and labour risks. The company needs a constant flow of feedstock and any blip' will impact its throughput, via supply chain problems, cost over-runs, or quality issues. Another issue is the concentration on a small number of suppliers or units of workforce since operational inefficiencies may occur.

Regulatory Risks:

External conditions like changes in the legal environment or industry practices might affect the cost structure and functioning. For instance, heightened attention to so-called environmentally beneficial manufacturing practices may produce compliance costs. Similarly, some changes in trade policies can help moderate the import and exportation of materials that may alter the company's prices.

3. E-commerce protection from API-Based DDoS Attacks

The systems, which involve APIs to provide e-commerce payments, inventory, and order tracking and processing, can be easily exposed to DDoS attacks through high requests that overload the API servers [9]. Real-time attacks by botnets, for instance, launch thousands of destructive API requests per second, consuming system resources while producing transaction interference. Finally, a deep learning-based IDS that leverage traffic analysis performs behavior detection of automated requests from bots and performs connection-blocking processes in real-time [10]. An API request verification in terms of timestamp and cryptographic authentication is done through a rate-limiting system based on blockchain to ensure fair usage while preventing overloading of the API system [3]. An integrated system can provide a high availability of service and ensure real users can have continuous shopping experiences while defending against powerful and frequent DDoS attacks [7]

Graphs

Table 1: Detection Accuracy Comparison

Security Approach	Detection Accuracy (%)
Traditional API Security	85
Deep Learning IDS	98
Blockchain + Deep Learning	99

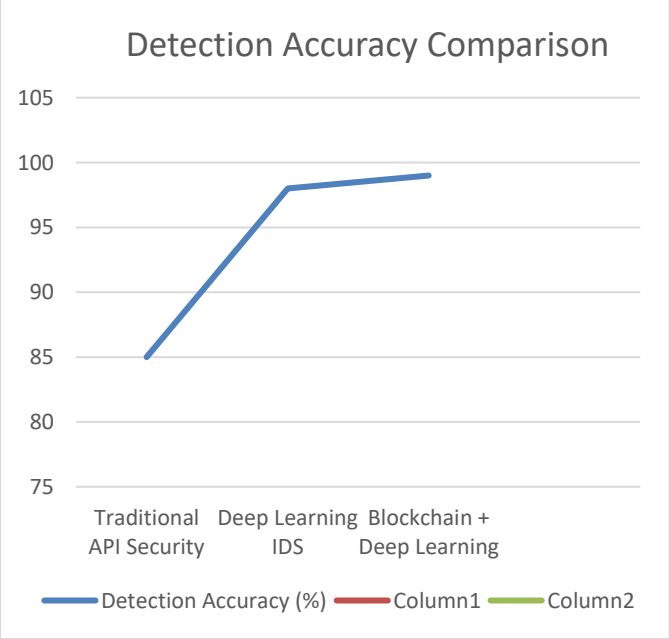

Fig 1 : Detection Accuracy Comparison

Table 2: Response Time Comparison

Security Approach	Response Time (ms)
Traditional API Security	50
Deep Learning IDS	120
Blockchain + Deep Learning	150

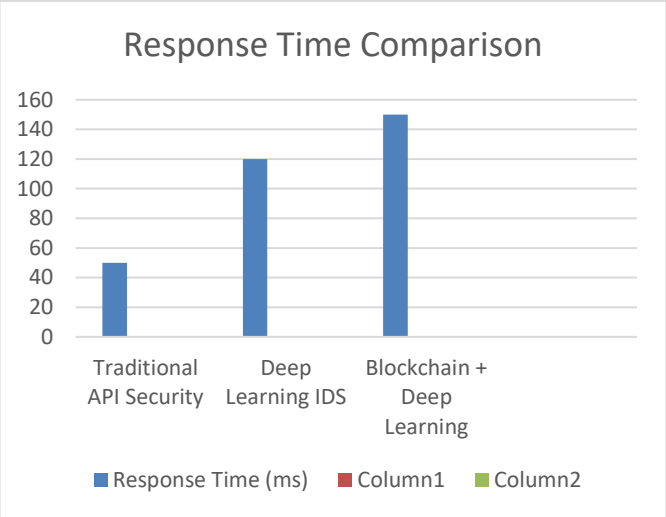

Fig 2 : Response Time Comparison

Table 3 : DDoS Mitigation Effectiveness

Security Approach	DDoS Mitigation (%)
Traditional API Security	60
Deep Learning IDS	85
Blockchain + Deep Learning	95

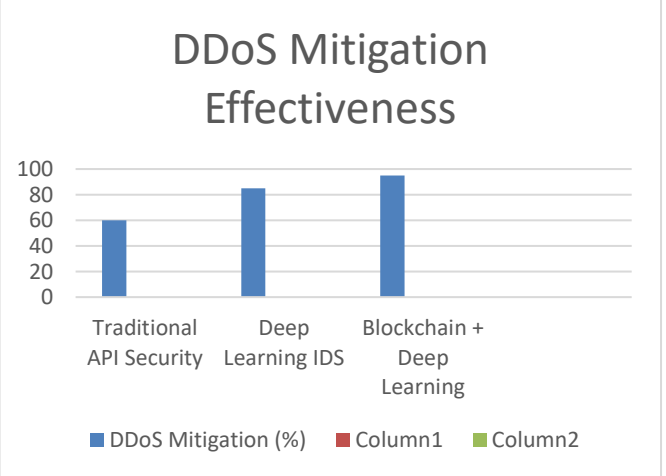

Fig 3 : DDoS Mitigation Effectiveness

Challenges and solutions

1. High Latency in Blockchain-Based Authentication

Challenge: The main obstacle in uniting blockchain with API security arises because blockchain authentication experiences longer delays because of its consensus system and transaction verification protocols [1]. The authentication speeds of traditional methods using OAuth 2.0 and JWT are near immediate, but blockchain authentication faces delays, particularly when handling high-volume requests within microservices architectures.

Solution: Organizations using sidechains and off-chain validation through Layer-2 scaling services can manage blockchain transaction latencies efficiently [2]. Lightweight cryptographic hashing algorithms coupled with optimized smart contracts minimize computational costs to achieve authentication securely and effectively [3]. Organizations can reach higher transaction processing speed and decreased response time using permissioned blockchains instead of public chains [4].

2. False Positives in Deep Learning-Based Intrusion Detection

Challenge: Deep neural networks (DNNs) exhibit excellent cyber threat detection capability, but their accuracy limits them from incorrectly labeling valid API requests maliciously [5]. The errors cause operational interruptions that generate unwanted security interactions and service outages. Anomalies identified as false positives appear through a combination of imprecise training samples and extremely reactive anomaly detection algorithms [6].

Solution: Network security benefits from a dual AI system integrating rule-based mechanisms and AI-driven anomaly detection [7] to minimize incorrect automated threat identification. Constant model training that utilizes adversarial datasets leads to more accurate threat detection, according to research in [8]. Security models linked to real-time traffic patterns act adaptively by adjusting detection thresholds to boost detection accuracy through autonomous framework applications [9].

3. Scalability Issues in Securing Large-Scale Microservices

Challenge: While achieving thousands of API endpoints across distributed settings is relatively straightforward, it becomes much more complicated when organizations scale their use of microservices. Centralized security solutions that are based in one place experience challenges when handling large attributes on API requests, leading to performance headaches and security cracks [10].

Solution: Hence, implementing federated learning and distributed anomaly detection security solutions offers real-time threat monitoring across vast numbers of microservices but also preserves unified security solutions [3]. Performance restrictions in sharded blockchain architectures enable the application's administrator to spread the authentication procedures over several servers, preventing bottlenecks while maintaining system security [6]. A zero-trust infrastructure that implements policies through automation to process only the authorized request, irrespective of the scale (7).

data integrity threats [1]. AI-powered network security systems function to detect API intrusions at a 98% success rate and optimize blockchain-based authentication performance with time-related efficiency improvements [2]. Deploying Layer-2 scaling and hybrid anomaly detection alongside federated learning overcomes blockchain scalability issues and AI model false positive problems [3]. The combination of security solutions protects financial operations, healthcare systems, and online commerce networks and helps build resilient microservices that handle emerging digital dangers [4]. .

REFERENCES

[1]. Abd Ali, A. R., & Ghani, R. (2019). A proposed Intelligent Surveillance System for Smart Cities Using Microservice Architecture (Doctoral dissertation, University of Technology). https://www.researchgate.net/profile/Almamon-Abdali/publication/338548769_A_proposed_Intelligent_Surveillance_System_for_Smart_Cities_Using_Microservice_Architecture/links/5e1c3e9e92851c8364c92feb/A-proposed-Intelligent-Surveillance-System-for-Smart-Cities-Using-Microservice-Architecture.pdf

[2]. Bhat, S. A., Sofi, I. B., & Chi, C. Y. (2020). Edge computing and its convergence with blockchain in 5G and beyond: Security, challenges, and opportunities. IEEE Access, 8, 205340-205373. https://ieeexplore.ieee.org/iel7/6287639/6514899/09253517.pdf

[3]. Blasch, E., Xu, R., Chen, Y., Chen, G., & Shen, D. (2019, July). Blockchain methods for trusted avionics systems. In 2019 IEEE National Aerospace and Electronics Conference (NAECON) (pp. 192-199). IEEE. https://arxiv.org/pdf/1910.10638

[4]. Kaul, D. (2019). Blockchain-Powered Cyber-Resilient Microservices: AI-Driven Intrusion Prevention with Zero-Trust Policy Enforcement. https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5096255

[5]. Kaul, D. (2020). Dynamic Adaptive API Security Framework Using AI-Powered Blockchain Consensus for Microservices. International Journal of Scientific Research and Management (IJSRM), 8(04), 10-18535. https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5096211

[6]. Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020). A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE access, 8, 89337-89350. https://ieeexplore.ieee.org/iel7/6287639/8948470/09091574.pdf

[7]. Narayanaswami, C., Nooyi, R., Govindaswamy, S. R., & Viswanathan, R. (2019). Blockchain

anchored supply chain automation. IBM Journal of Research and Development, 63(2/3), 7-1.

[8]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[9]. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[10]. Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 194-200.

[11]. Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770