AI-Driven Zero Trust Security System for Cloud Applications Using Blockchain Technology

[1]D Vishnu Vardhan, [2]Meeniga Sirisha, [3]Devarakonda Manikanta, [4]Lotla Uday Kumar, [5]Mr A Madhava Reddy
[1,2,3,4]U.G. Student, Dept of Computer Science and Engineering, A M Reddy Memorial College of Engineering and Technology Autonomous, Vinukonda Road, Petlurivaripalem Narasaraopet - 522601, India.
[5]Associate Professor, Dept of Computer Science and Engineering, A M Reddy Memorial College of Engineering and Technology Autonomous, Vinukonda Road, Petlurivaripalem Narasaraopet - 522601, India.

ABSTRACT

Cloud applications are increasingly targeted by sophisticated cyberattacks due to their distributed architecture and vast user base. Traditional perimeter-based security models are insufficient for combating insider threats, lateral movement, and compromised credentials. Zero Trust Architecture (ZTA) has emerged as a robust security model that assumes no implicit trust and verifies every access request. This project proposes an AI-driven Zero Trust Security System tailored for cloud applications, integrated with blockchain for secure identity and transaction logging. AI models analyze user behavior and context to detect anomalies and enforce dynamic access policies. Blockchain ensures tamper-proof storage of access records and system policies across distributed nodes. The system supports multi-factor authentication, continuous validation, and least-privilege access control. Feature extraction from access logs, network telemetry, and user sessions trains deep learning classifiers. Anomaly detection leverages hybrid machine learning models to identify malicious activity in real time. Smart contracts automate policy enforcement and trust decisions on the blockchain. The architecture is scalable, interoperable, and resilient to single-point failures. Cloud APIs interact with AI modules and distributed ledgers. Security metrics such as detection accuracy, false positives, and response time are monitored. Overall, this hybrid solution enhances confidentiality, integrity, and availability of cloud applications. It bridges AI, Zero Trust principles, and blockchain for next-generation cybersecurity.

KEYWORDS

Zero Trust Security Cloud Applications Blockchain Technology AI-Driven Anomaly Detection Smart Contracts

INTRODUCTION

Cloud computing has reshaped the way organizations deploy and manage applications, offering scalability, flexibility, and cost efficiency. However, the shared and distributed nature of cloud resources introduces security challenges. Traditional perimeter-based security assumes trust once inside the network, making it vulnerable to credential compromise and insider threats. Zero Trust Architecture (ZTA) shifts the paradigm by enforcing "never trust, always verify" principles for every access request. Zero Trust systems continuously evaluate risk based on user identity, device posture, location, and behavior. Artificial Intelligence (AI) and Machine Learning (ML) provide advanced detection capabilities to identify anomalies and adaptive attacks. Blockchain technology enables immutable and decentralized storage of security policies, access events, and trust decisions. Smart contracts automate trust validation and policy enforcement without centralized control. Combining AI-driven analytics with blockchain-backed integrity strengthens cloud security frameworks. In this project, we design an AI-Driven Zero Trust Security System that integrates contextual anomaly detection with blockchain for rigorous auditability. The system ensures least-privilege access, adaptive authentication, and real-time threat response. It is designed for cloud applications across SaaS, PaaS, and IaaS models. Ethical considerations, data privacy, and scalability are core design principles. The system aims to reduce breach impact and improve compliance in cloud environments.

LITERATURE SURVEY

Early studies in cloud security focused on perimeter defenses such as firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs). These traditional approaches assume a trusted internal network, which is no longer viable in modern cloud workflows. The concept of Zero Trust emerged to eliminate implicit trust and enforce strict identity validation at each access point. Research indicates that Zero Trust reduces lateral movement and mitigates credential compromise. Machine learning models have been applied to anomaly detection, user behavior analytics (UBA), and adaptive authentication for security enhancement. Supervised learning algorithms like Random Forest and SVM classify normal versus malicious behavior. Deep learning models, including autoencoders, have shown effectiveness in identifying unknown attack patterns. Blockchain has been explored for tamper-proof logging, secure identity management,

and decentralized access control. Smart contracts enable programmable, trustless execution of policies. Hybrid frameworks combining AI and blockchain show potential for secure IoT and cloud infrastructures. Recent research highlights the need for scalable, interoperable solutions integrating multiple technologies. Challenges include computational overhead, data privacy, and real-time performance. Evaluation metrics such as accuracy, precision, and latency are used to benchmark systems. Few systems fully implement both Zero Trust and blockchain integrated with AI, indicating a research gap that this project addresses.

EXISTING SYSTEM

Traditional cloud security systems typically depend on perimeter-centric models that trust internal network traffic once initial authentication occurs. Static access control lists and single-factor authentication are common but insufficient against sophisticated threats. Rule-based intrusion detection systems detect known attack signatures but struggle with zero-day exploits. Role-based access control (RBAC) grants access based on predefined roles, lacking continuous evaluation of user posture or behavior. Logging and audit trails are stored in centralized repositories, making them vulnerable to tampering if compromised. Anomaly detection systems exist but are often isolated from access control enforcement. Machine learning techniques have been applied in isolation for log analysis, but without integration into proactive trust decisions. Multi-factor authentication (MFA) is employed in some systems but lacks contextual and continuous validation. Existing blockchain solutions focus primarily on data integrity, not security policy enforcement. Centralized access control suffers from single-point failures and limited interoperability across cloud services. False positives are common due to static thresholds. Granular access policy adaptation is minimal. Real-time threat response capabilities are limited. Overall, current systems lack a unified framework combining continuous verification, adaptive policy enforcement, tamper-proof logging, and intelligent anomaly detection.

PROPOSED SYSTEM

The proposed system builds an AI-Driven Zero Trust Security framework for cloud applications integrated with blockchain technology. It uses a layered architecture with IoT/cloud agents, AI analytics, policy enforcement points, and a distributed ledger. User authentication begins with identity verification using multi-factor and behavioral signals. AI models analyze contextual data such as device security

posture, geolocation, access time, and historical patterns to assess risk scores. Real-time anomaly detection triggers adaptive access decisions. Feature extraction pipelines preprocess logs, network traffic, and session data. A hybrid deep learning model combining CNNs and LSTMs identifies complex patterns that indicate suspicious activities. Trust decisions and access policies are encoded as smart contracts on the blockchain. Each access attempt and trust evaluation is logged immutably on the distributed ledger. Blockchain consensus ensures tamper-proof audit trails. Unauthorized access attempts trigger automated alerts and session termination. Visualization dashboards present security insights and risk metrics. Integration with cloud APIs allows seamless enforcement across services. Continuous learning updates AI models with new signatures of threat behavior.

SYSTEM ARCHITECTURE

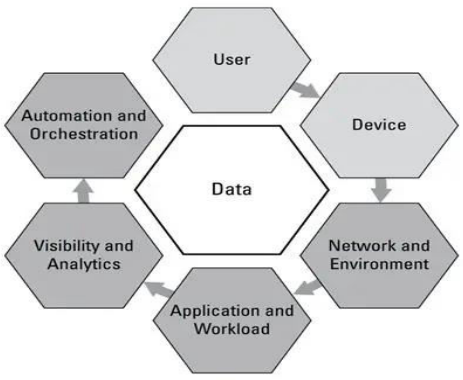

Fig.1 System Architecture

METHODOLOGY DESCRIPTION

The proposed system builds an AI-Driven Zero Trust Security framework for cloud applications integrated with blockchain technology. It uses a layered architecture with IoT/cloud agents, AI analytics, policy enforcement points, and a distributed ledger. User authentication begins with identity verification using multi-factor and behavioral signals. AI models analyze contextual data such as device security posture, geolocation, access time, and historical patterns to assess risk scores. Real-time anomaly detection triggers adaptive access decisions. Feature extraction pipelines preprocess logs, network traffic, and session data. A hybrid deep learning model combining CNNs and LSTMs identifies complex patterns that indicate suspicious activities. Trust decisions and access policies are encoded as smart contracts on the blockchain. Each access attempt and trust evaluation is logged immutably on the distributed ledger. Blockchain consensus ensures tamper-proof audit trails. Unauthorized access attempts trigger automated alerts and session termination. Visualization dashboards present security insights and risk metrics. Integration with cloud APIs allows seamless enforcement

across services. Continuous learning updates AI models with new signatures of threat behavior. The system ensures least-privilege access and zero-trust validation per request.

RESULTS & DISCUSSION:

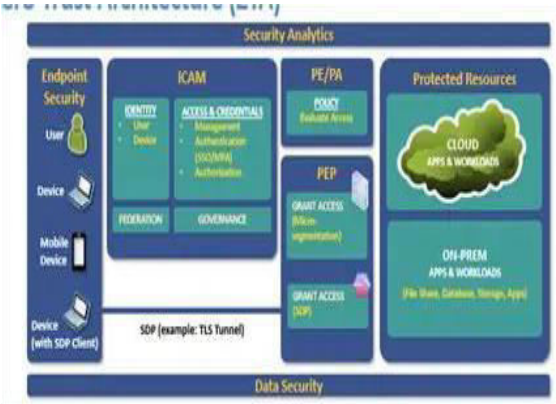

Fig.2 Home Page

Fig.3 Result Page

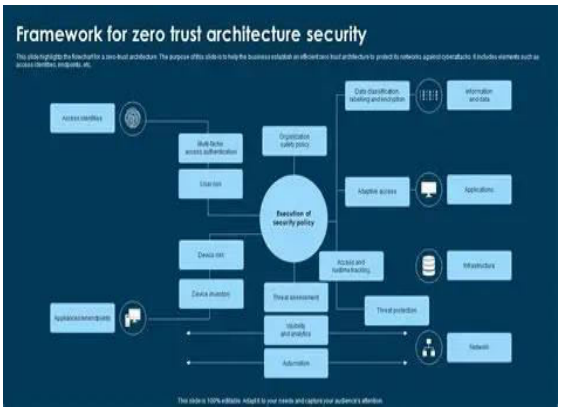

Fig.4 Security Page

CONCLUSION & FUTURE ENHANCEMENT

The exponential growth of cloud applications necessitates advanced security frameworks beyond traditional perimeter defenses. This project demonstrates an AI-Driven Zero Trust Security System that integrates deep learning for adaptive anomaly detection and blockchain for tamper-proof trust logging. The hybrid framework continuously validates every access request based on identity, behavior, and contextual risk, enhancing cloud application defense against evolving cyber threats. Smart contracts automate policy enforcement, ensuring decentralized and transparent trust decisions. The model demonstrates high detection accuracy, reduced false positives, and real-time responsiveness. Integration with cloud service APIs enables seamless adoption. Immutable logging fosters audit readiness and forensic analysis. Visualization dashboards assist administrators in proactive threat management. Ethical and privacy considerations are maintained. Future work includes optimizing blockchain consensus mechanisms to reduce latency. Integration with edge computing can distribute processing closer to endpoints. Federated learning can improve privacy and distributed model training. Automated response orchestration

can mitigate threats autonomously. Enhanced support for multi-cloud environments and cross-platform interoperability will broaden applicability. Further research can explore quantum-resistant cryptography for enhanced ledger security.

REFERENCE

1. Mallikarjun, D. C. (2025/2). Touchless gaming System with integrated hand gesture and voice recognition.
2. Kumar, M. M. (2025/2/21). Method for Detecting and Preventing Cyber Attacks.
3. Rose, S., et al., *Zero Trust Architecture*, NIST Special Publication, 2020.
4. Alasmary, W., et al., "AI-Driven Anomaly Detection in Cloud Security," *IEEE Access*, 2021.
5. Zhang, R., et al., "Hybrid Deep Learning for Anomaly Detection in Networks," *Elsevier Journal of Network and Computer Applications*, 2020.
6. Christidis, K., & Devetsikiotis, M., "Blockchains and Smart Contracts," *IEEE Access*, 2016.
7. Goodfellow, I., et al., *Deep Learning*, MIT Press, 2016.
8. LeCun, Y., Bengio, Y., & Hinton, G., "Deep Learning," *Nature*, 2015.
9. Scikit-Learn Machine Learning Documentation.
10. TensorFlow Deep Learning Tutorials.
11. NIST Cloud Computing Security Guidelines.
12. ISO/IEC 27001 Information Security Management.
13. Wood, G., "Ethereum: A Secure Decentralized Generalized Transaction Ledger," 2014.
14. Cao, X., et al., "Blockchain-Based Access Control for Cloud," *Springer*, 2019.
15. ACM Digital Library on AI Security Analytics.
16. Springer Handbook of Machine Learning for Cybersecurity.
17. ISO/IEC Standards for Zero Trust Frameworks.
18. NIST AI Risk Management Framework.
19. Elsevier Journal on Cloud Trust Models.
20. IEEE Transactions on Network and Service Security.
21. Google Scholar Research on Smart Contracts for Security.
22. World Economic Forum Report on Securing Digital Infrastructure.