iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** II **Month of publication:** February 2025

DOI: https://doi.org/10.22214/ijraset.2025.66800

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue II Feb 2025- Available at www.ijraset.com

Zero Trust AI Authentication and Blockchain Powered Secure AI

R. K. Poongodi[1], M. Mohan[2], S. Sudharsan[3], C. Vinoth[4]
[1]*M.Tech (IT), Assistant Professor, Department of Cyber Security, Paavai Engineering College (Autonomous), Namakkal, Tamilnadu*
[2, 3, 4]*III Year, Department of Cyber Security, Paavai Engineering College (Autonomous), Namakkal, Tamilnadu*

Abstract: ***The integration of Zero Trust (ZT) security models with Artificial Intelligence (AI) authentication mechanisms, along with the utilization of blockchain technology, offers a novel paradigm for securing digital interactions and data exchanges in increasingly decentralized and complex networks. Zero Trust, a security framework that assumes no implicit trust and enforces strict identity verification, is well-suited for AI-driven authentication systems that require robust, real-time, and adaptive security measures Blockchain technology further enhances this framework by providing a transparent, immutable ledger for logging authentication events, access control decisions, and transactions, ensuring tamper-proof audit trails. Blockchain's decentralized nature also mitigates single points of failure, improving resilience and privacy. When combined, Zero Trust, AI, and blockchain can deliver an advanced, self-evolving security system that both anticipates and responds to new threats with greater precision and efficiency.***

I. INTRODUCTION

As organizations continue to embrace digital transformation and increasingly rely on cloud services, IoT devices, and distributed networks, traditional security models that assume trust within specific perimeters are becoming increasingly inadequate. The concept of *Zero Trust* (ZT) security, which assumes no implicit trust and mandates verification at every point of access, is emerging as a critical approach to safeguarding complex and dynamic environments. In this paradigm, trust is never assumed; instead, verification is continually enforced across all users, devices, and systems.

However, Zero Trust in itself is not sufficient in addressing the complexities of modern security threats. As cyber-attacks become more sophisticated and adversaries increasingly target authentication mechanisms, relying solely on traditional security protocols can expose organizations to significant risks. This is where Artificial Intelligence (AI) and blockchain technologies can play transformative roles, providing real-time adaptability, enhanced decision-making, and immutable security features.AI-powered authentication systems bring an advanced layer of security by continuously assessing access requests based on dynamic factors, such as user behavior, device context, and environmental conditions. These AI-driven solutions can detect anomalies and adaptively enforce security policies, making them highly effective against evolving threats like credential stuffing, phishing, and insider attacks.

II. CONTRIBUTION

Zero Trust is a security framework that assumes no user or device, whether inside or outside the corporate network, should be trusted by default. Instead, trust must be established continuously through various security measures, ensuring that access to resources is tightly controlled.

Blockchain is a decentralized, immutable ledger technology that ensures transparency, security, and trust without the need for a central authority. When combined with AI, blockchain can enhance several aspects of data integrity, privacy, and accountability in AI models and systems

1) Zero Trust's continuous verification of users and devices is enhanced by blockchain's transparency and immutability. Blockchain can verify access control decisions made by AI models, ensuring they cannot be tampered with, while Zero Trust's continuous authentication adds an extra layer of security to blockchain networks.

2) Blockchain allows users to have ownership and control over their data, while Zero Trust AI continuously monitors the security of this data, ensuring that access is only granted to authorized users or devices. Together, they help build more privacy-respecting and secure identity management systems.

A. *Zero Trust AI Authentication*

Zero Trust Security is a cybersecurity model that operates on the principle of "never trust, always verify." In this context, Zero Trust AI Authentication focuses on using AI to enforce strict access controls and authentication protocols, regardless of where the request is coming from (inside or outside the network). Here are the main concepts Every user, device, and application must be authenticated before accessing any resource. AI-driven authentication can use biometric data (facial recognition, fingerprints), behavioral biometrics (keystroke dynamics, mouse movement patterns), or multi-factor authentication (MFA) to verify identities. AI enhances the ability to evaluate the context of access requests. This includes the user's role, location, device security posture, and the time of access. For example, AI might flag a login attempt from a new location or unusual device. Instead of granting permanent access rights, Zero Trust AI Authentication allows dynamic access control based on continuous real-time analysis. If an anomaly is detected (such as unusual behavior), the system might revoke access or request additional authentication.

AI can evaluate risk levels for every action in the system, adjusting security measures based on perceived risk. For instance, accessing sensitive data from a familiar device might require minimal authentication, while access from an unknown device could trigger multi-factor authentication (MFA).

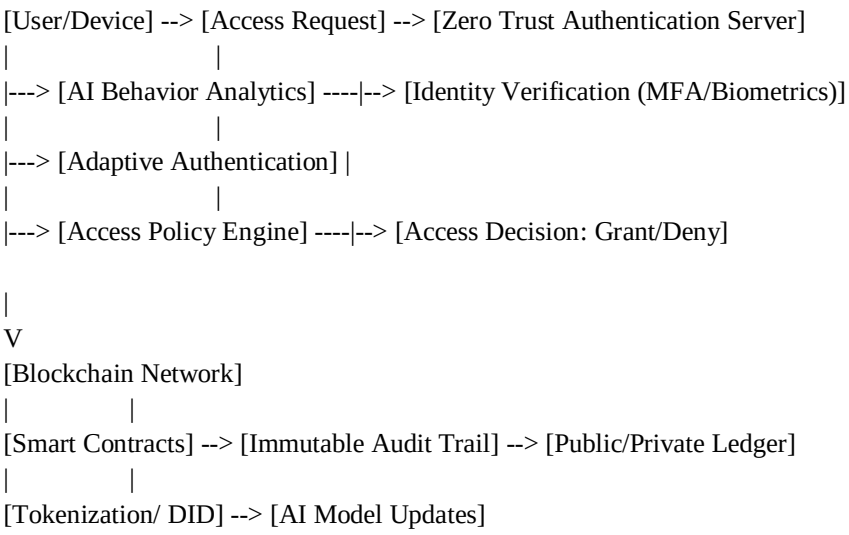
B. *Micro-Segmentation*

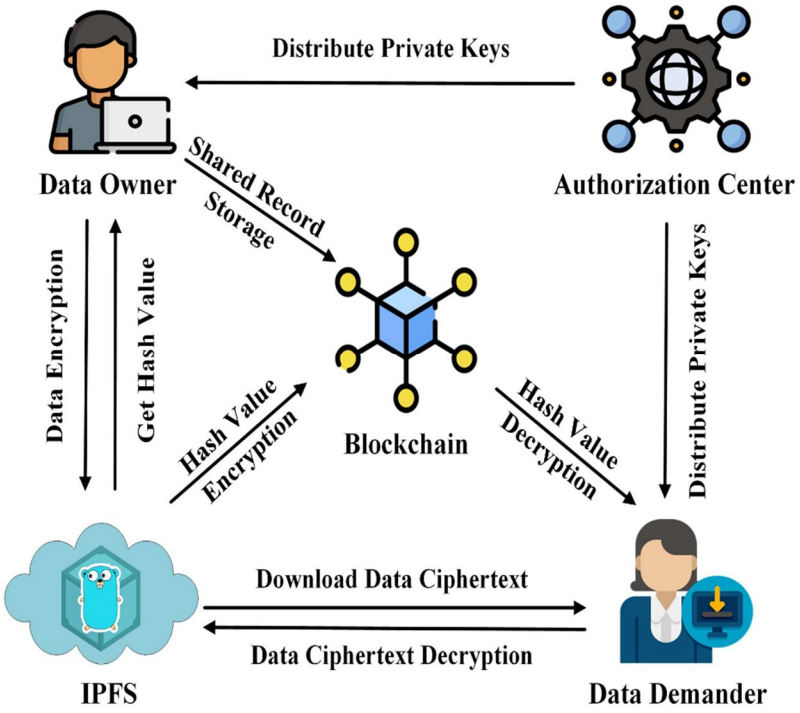
AI-driven Zero Trust approaches often involve segmenting networks into smaller, isolated areas. Each segment requires independent authentication and access control, reducing the risk of lateral movement by attackers within the network. Rather than a one-time authentication check, Zero Trust AI Authentication involves ongoing monitoring. It tracks every action a user performs and can trigger additional checks if behavior patterns change or suspicious activities are detected.

III. BLOCKCHAIN POWERED -AI

Blockchain technology combined with AI introduces a powerful, decentralized model to enhance security, transparency, and data integrity. Blockchain-powered AI refers to the use of blockchain to store and manage data that AI models rely on. It also enables decentralized AI systems where various nodes or parties can collaborate and share AI models or data while maintaining security. In blockchain-powered AI, AI models or datasets can be decentralized, meaning they are distributed across many nodes. This ensures that no single party has complete control, fostering collaboration and reducing the risk of tampering. Blockchain provides a secure, tamper-proof ledger, ensuring that any data used for training AI models is immutable and cannot be altered. This helps to ensure the integrity of the data, which is critical for building trustworthy AI systems. The transparent nature of blockchain allows for clear audit trails of how AI models were trained, what data was used, and how decisions are made. This is crucial for ethical AI, as it allows organizations to explain how their models reach certain outcomes. The transparent nature of blockchain allows for clear audit trails of how AI models were trained, what data was used, and how decisions are made. This is crucial for ethical AI, as it allows organizations to explain how their models reach certain outcomes.

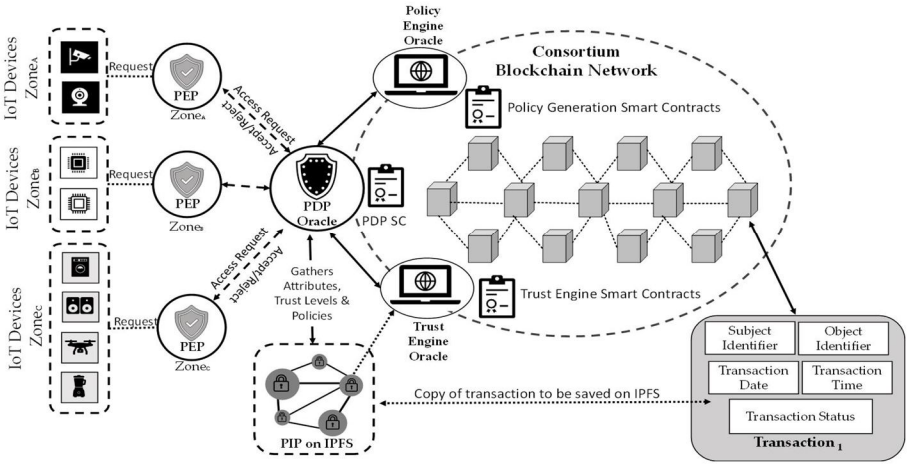
A. *Working Model*





B. A Blockchain Based Zero-Trust Access Control

Zero-Trust Security is a cybersecurity model that assumes that no entity (user, device, or network) is inherently trusted, whether inside or outside the organization's network perimeter. This model typically involves continuous authentication, least-privilege access, and real-time monitoring to ensure that only authorized individuals and systems can access resources. blockchain technology, with its decentralized, immutable, and transparent features, can significantly enhance the Zero-Trust model. By using blockchain for access control, organizations can provide stronger security, auditability, and accountability, especially in distributed and dynamic environments. Blockchain can store cryptographic proofs of identity in a decentralized manner. Instead of relying on traditional password-based authentication or centralized identity stores, users could have a private key stored on the blockchain, ensuring that only the rightful user can authenticate their access. The blockchain network could also facilitate multi-factor authentication (MFA) by verifying attributes from multiple decentralized sources, ensuring that only users with the correct set of attributes can gain access.



Permissions can be dynamically adjusted based on real-time factors like user behavior, device health, and geolocation. The access request is verified against the smart contract policies.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue II Feb 2025- Available at www.ijraset.com

C. Real-Time Use Case Of Zero-Trust Ai Authentication And Blockchain-Powered Secure Ai

The integration of Zero-Trust Security, AI Authentication, and Blockchain technologies is a game-changer for modern cybersecurity, providing enhanced security, scalability, and trust in AI-based systems. Below are some real-time usage scenarios where these technologies can be effectively utilized.

Use Case: Real-Time Access Management in Enterprises

1) Scenario: In a large organization, employees access sensitive data or systems based on roles, time of access, and contextual factors (e.g., device health, location, behavior). AI-based authentication continuously monitors user behavior and validates identity.

2) Real-Time Features:

- Behavioral Biometrics: AI can analyze typing patterns, mouse movements, or other biometrics (e.g., facial recognition, voice recognition) in real-time to confirm the identity of the user.
- Continuous Authentication: Even after login, AI monitors ongoing user behavior for signs of anomaly (e.g., logging in from an unusual location or accessing unauthorized files). If an anomaly is detected, it can trigger a re-authentication request or lock access.
- Blockchain: Once the user is authenticated, the access request, authentication event, and any changes in access rights are recorded immutably on a blockchain, providing an auditable trail for compliance and security monitoring.

D. Blockchain-Powered Secure AI for Data Privacy and Integrity

AI models require vast amounts of data for training and real-time decision-making. Blockchain helps ensure the security and integrity of AI data by providing tamper-proof storage and validation mechanisms. This also addresses concerns about data privacy and auditability in regulated industries.

Use Case: Secure and Transparent AI Model Training in Healthcare

1) Scenario: A healthcare provider uses AI to predict patient outcomes based on historical medical data. Blockchain ensures that the data used to train the AI model is authentic, secure, and only accessible by authorized personnel.

2) Real-Time Features:

- Data Provenance: Blockchain ensures that any data fed into the AI system is traceable and authentic. For instance, data from medical records or sensors is hashed and stored on a blockchain, so stakeholders can verify its integrity in real time.
- Smart Contracts for Data Access Control: Smart contracts enforce strict access controls, granting or denying access to patient data based on predefined criteria. For example, a doctor can access only specific patient records related to their department. If access conditions are met, blockchain logs the transaction.
- AI Model Transparency: Blockchain records not only the data used to train the model but also the parameters and decisions made by the model. This creates transparency in AI decision-making, critical for explaining decisions in healthcare and other high-stakes industries.

IV. CONCLUSION

Despite the significant benefits, implementing a Zero-Trust AI authentication system combined with blockchain does come with challenges. These include integration with legacy systems, scalability concerns, and the computational cost associated with real-time AI processing and blockchain consensus mechanisms. However, the ongoing advancements in AI models, blockchain scalability solutions and cloud-native technologies offer promising avenues to overcome these obstacles. Zero-Trust AI Authentication and Blockchain-Powered Secure AI together provide a robust framework to address the evolving cybersecurity needs of modern organizations. By leveraging these technologies, businesses can not only protect critical data and systems but also build trust with their users, ensure compliance, and future-proof their digital infrastructure in an increasingly interconnected and threat-prone world.

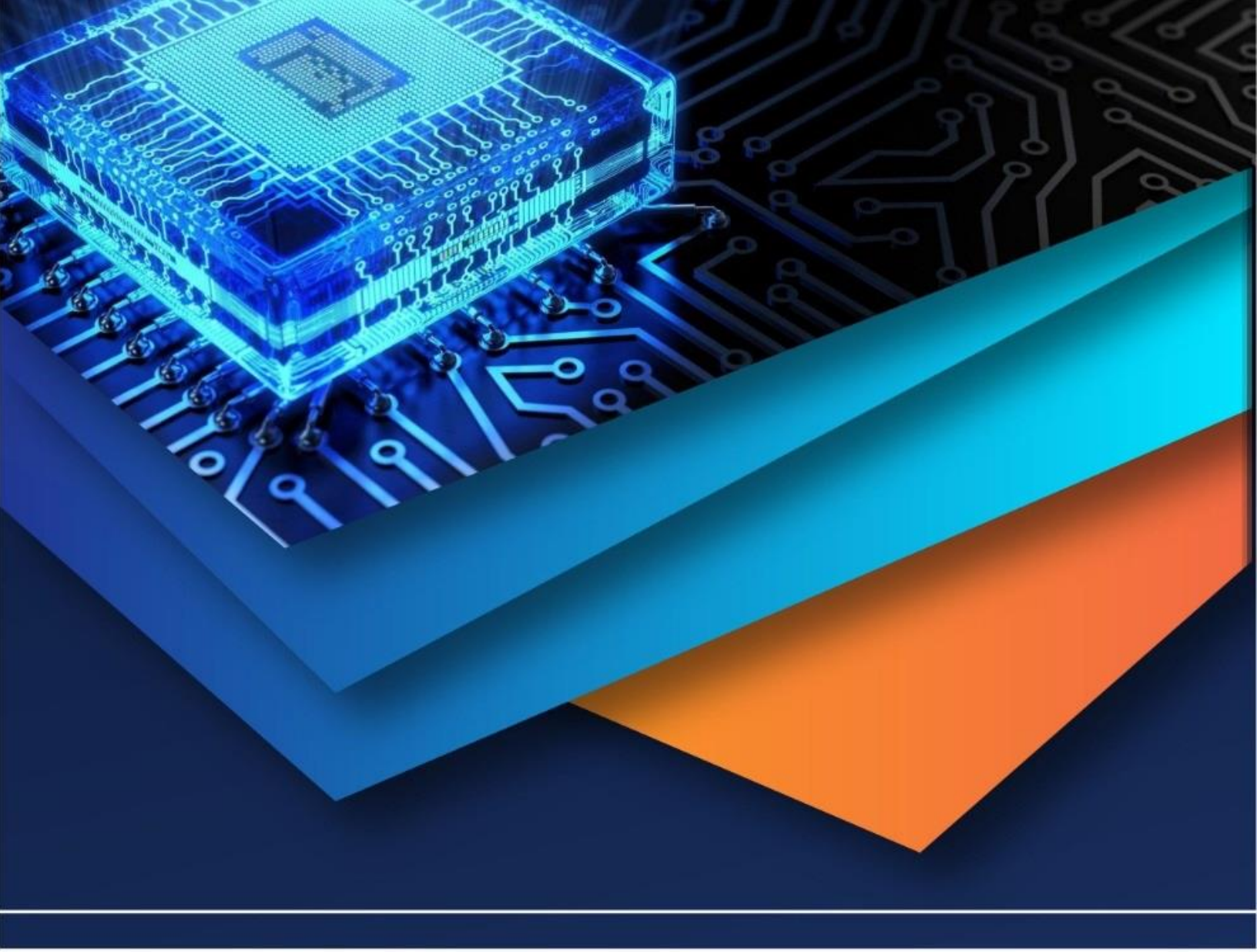
V. ACKNOWLEDGEMENT

First and foremost, I would like to acknowledge the researchers, practitioners, and thought leaders whose extensive work in Zero-Trust security, AI-driven authentication, and blockchain technology have laid the foundation for this study.

Their pioneering research and contributions have provided critical insights into how these technologies can be integrated to create secure, scalable, and transparent systems. I would also like to thank the academic and industry organizations that have developed key frameworks, standards, and guidelines, such as the National Institute of Standards and Technology (NIST) for their publication on Zero-Trust architectures and the European Union Blockchain Observatory for their continuous research on blockchain and AI.

REFERENCES

[1] Dharminder G. Dhingra & Wiley (2021). Discusses the integration of blockchain with AI for secure, privacy-preserving systems, including Zero-Trust access control.
[2] Abhishek Sharma, Sandeep Kumar, Pradeep Kumar & Springer (2021). Focuses on securing blockchain systems with AI, exploring Zero-Trust models and AI-based authentication methods.
[3] Kshema Iyer, Sudhir Bhatnagar & Wiley (2021). A practical guide that explores blockchain and AI, detailing applications for security, identity management, and Zero-Trust security.
[4] Dan O'Farrell, Andrew McKinney (2021). A practical guide on implementing Zero-Trust security in the enterprise, exploring the integration of AI and blockchain for better access control and trust management.
[5] Evan Gilman, Doug Barth & O'Reilly Media (2020). Provides practical insights into Zero-Trust models, including AI-driven authentication and integration with blockchain for enhanced security.
[6] Leslie F. Sikos & Springer (2020). A deep dive into AI in cybersecurity, covering Zero-Trust and AI-driven authentication systems, and touching on blockchain applications.
[7] Arshdeep Bahag ,Vijay Madisetti& VPT (2020). A practical guide on how blockchain can secure AI models and implement Zero-Trust security principles in real-world applications.
[8] Bhavesh R. Patel (2020). A hands-on guide that combines AI and blockchain, focusing on Zero-Trust and secure AI authentication solutions.
[9] Imran Bashir (2020). Covers blockchain fundamentals and its integration with AI for building Zero-Trust and secure AI systems.
[10] M. J. McMillan & Routledge (2020). Focuses on blockchain applications in financial services and explores how Zero-Trust principles and AI can be applied in financial AI security systems.
[11] Muhammad Ali Babar, Amit Kumar & Springer (2020). This book discusses how blockchain and AI can be used together to secure digital systems in Industry 4.0, with a focus on Zero-Trust models for security.
[12] Primavera De Filippi, Aaron Wright & Harvard University Press (2018). While focusing on legal aspects, the book also explores blockchain's role in securing AI models and enhancing Zero-Trust security.
[13] Kai-Fu Lee & Houghton Mifflin Harcourt (2018). While focused on AI, this book touches on the need for secure AI systems, which could benefit from Zero-Trust security models and blockchain integration.
[14] Daniel Drescher & Springer (2017). A simple introduction to blockchain, exploring its potential to support secure AI systems, Zero-Trust security, and access management.
[15] Tiana Laurence & Wiley (2017). A beginner-friendly guide to blockchain, which also discusses how blockchain can enhance AI security and be applied in Zero-Trust systems.
[16] Don Tapscott, Alex Tapscott & Penguin (2016). Discusses how blockchain is transforming industries, including its potential for enhancing AI security and supporting Zero-Trust models.
[17] Brian Russell, Drew Van Duren & Syngress (2016). The application of Zero-Trust security frameworks for IoT systems, incorporating AI and blockchain for securing devices and data flows.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY