International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

Policy Driven and Zero Trust AI Architectures for Secure Data Lakes and Fraud Detection and Migration and Real Time Enterprise Intelligence

Oliver Matthias Felsenbruch

Independent Researcher, Berlin, Germany

ABSTRACT: The rapid expansion of enterprise data ecosystems has intensified the need for secure, intelligent, and resilient architectures. Traditional perimeter-based security models are insufficient in protecting modern data lakes, particularly when supporting AI-driven fraud detection, large-scale data migration, and real-time enterprise intelligence. This paper explores the integration of policy-driven governance frameworks and Zero Trust Architecture (ZTA) principles within AI-enabled data lake environments. A policy-driven approach ensures data access, processing, and analytics are governed by dynamic, automated policies aligned with compliance, security, and operational requirements. Zero Trust enhances this by enforcing continuous verification, least-privilege access, and micro-segmentation across all users, devices, and workloads.

The study examines architectural models, security enforcement mechanisms, AI-powered fraud detection pipelines, and secure migration strategies. It further proposes a research methodology for implementing and evaluating such systems within enterprise environments. The findings demonstrate that combining policy-driven governance with Zero Trust AI significantly enhances data protection, reduces fraud risks, supports secure cloud migration, and enables real-time decision intelligence. However, implementation complexity, operational costs, and integration challenges remain key concerns. The paper concludes by outlining advantages, disadvantages, and future research directions in secure AI-driven enterprise data ecosystems.

KEYWORDS: Zero Trust Architecture, Policy-Driven Governance, Secure Data Lakes, AI Security, Fraud Detection, Enterprise Intelligence, Data Migration, Micro-Segmentation, Real-Time Analytics, Data Governance, Cybersecurity Architecture.

I. INTRODUCTION

The digital transformation of enterprises has led to an unprecedented surge in data generation. Organizations today rely on vast data lakes that integrate structured, semi-structured, and unstructured data from multiple internal and external sources. These data lakes power analytics, machine learning, fraud detection systems, and real-time enterprise intelligence platforms. However, as data ecosystems grow in complexity and scale, traditional security approaches based on perimeter defense and implicit trust are becoming obsolete.

Modern enterprises operate in hybrid and multi-cloud environments, where data flows across distributed systems, APIs, devices, and third-party services. The traditional “trust but verify” model fails in such distributed architectures because it assumes internal network entities are trustworthy. Cyber threats, insider attacks, credential compromise, and advanced persistent threats exploit these assumptions. Consequently, there is a paradigm shift toward Zero Trust Architecture (ZTA), which operates on the principle of “never trust, always verify.”

Zero Trust mandates continuous authentication, authorization, and validation of every user, device, workload, and data transaction. It enforces least-privilege access and micro-segmentation to limit lateral movement within systems. When applied to AI-enabled data lakes, Zero Trust ensures that sensitive datasets, models, and analytics pipelines are protected from unauthorized access and manipulation.

Simultaneously, enterprises must comply with regulatory frameworks such as GDPR, HIPAA, PCI-DSS, and industry-specific governance standards. This necessitates policy-driven architectures where data access, usage, retention,

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

encryption, and processing rules are enforced automatically through programmable governance engines. Policy-driven governance integrates security, compliance, and operational rules directly into system architecture, reducing human error and ensuring consistent enforcement.

AI-driven fraud detection systems are particularly dependent on secure data ecosystems. Fraud detection requires real-time ingestion of transaction data, behavioral analytics, anomaly detection, and predictive modeling. If the underlying data lake is compromised, model integrity can be affected, leading to inaccurate predictions or exploitation by adversaries. Moreover, adversarial attacks on machine learning models pose emerging risks, including model poisoning and evasion attacks.

In addition to fraud detection, enterprises face major challenges in migrating legacy systems and on-premise databases to cloud-native data lake architectures. Data migration introduces risks such as data leakage, misconfiguration, unauthorized access, and compliance violations. Integrating Zero Trust principles during migration ensures secure transition while maintaining business continuity.

Real-time enterprise intelligence further increases architectural complexity. Organizations demand immediate insights from streaming data sources such as IoT devices, financial transactions, customer interactions, and operational logs. Real-time analytics requires high-throughput pipelines, low-latency processing, and scalable infrastructure. Embedding policy-driven Zero Trust controls into such high-performance systems demands careful architectural planning to avoid performance degradation.

The convergence of AI, Zero Trust security, and policy-driven governance represents a transformative approach to enterprise data architecture. This integrated model supports:

- Secure and compliant data lake management
- Resilient AI-based fraud detection
- Secure migration to hybrid or multi-cloud environments
- Real-time intelligence for decision-making

This paper investigates how policy-driven mechanisms and Zero Trust principles can be systematically integrated into AI-enabled enterprise data ecosystems. It explores architectural components, enforcement layers, fraud detection pipelines, and migration frameworks, followed by a detailed research methodology to evaluate system performance, security, and scalability.

The objectives of this research are:

1. To analyze the limitations of traditional security models in modern data lake environments.
2. To design a policy-driven Zero Trust AI architecture.
3. To evaluate its application in fraud detection and real-time analytics.
4. To propose a secure migration framework aligned with Zero Trust principles.
5. To assess benefits, challenges, and future implications.

As enterprises move toward AI-driven intelligence systems, security must evolve from reactive defense mechanisms to proactive, policy-automated, continuously verified architectures. Policy-driven Zero Trust AI represents a strategic blueprint for secure digital transformation in the era of data-centric enterprises.

II. LITERATURE REVIEW

Research in Zero Trust Architecture has gained momentum following the inadequacy of perimeter-based models. NIST's Zero Trust framework emphasizes identity-centric security, continuous authentication, and micro-segmentation. Studies highlight how Zero Trust reduces insider threats and lateral attack movement in cloud environments.

Data lake security research has identified challenges including metadata management, fine-grained access control, encryption management, and governance automation. Traditional role-based access control (RBAC) systems are increasingly replaced with attribute-based access control (ABAC) and policy-based access control (PBAC) systems for dynamic enforcement.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

In AI security literature, concerns about adversarial attacks, data poisoning, and model inversion have led to proposals for secure ML pipelines. Researchers advocate encryption-in-use technologies such as homomorphic encryption and secure enclaves for model protection.

Fraud detection research emphasizes machine learning techniques including supervised learning, deep learning, graph analytics, and anomaly detection. However, studies reveal that model effectiveness depends heavily on data integrity and secure pipelines.

Cloud migration research highlights risks such as misconfigurations, insecure APIs, data leakage, and compliance violations. Secure DevSecOps frameworks integrate security policies directly into CI/CD pipelines.

Policy-driven governance frameworks use declarative policy engines such as Open Policy Agent (OPA) to enforce compliance automatically. Research indicates policy-as-code improves auditability and reduces manual intervention.

Despite significant advancements, limited research integrates Zero Trust, AI security, policy-driven governance, migration strategy, and real-time enterprise intelligence into a unified architecture. This paper addresses this integration gap.

III. RESEARCH METHODOLOGY

This research adopts a mixed-method architectural design and evaluation methodology to investigate policy-driven Zero Trust AI architectures in secure data lake environments. The study is conducted in five phases: conceptual design, architectural modeling, implementation simulation, experimental validation, and performance evaluation.

The first phase involves defining architectural components based on Zero Trust principles. The architecture includes identity providers, policy engines, micro-segmentation gateways, encryption services, AI pipelines, and monitoring layers. A policy-driven governance model is embedded using policy-as-code frameworks. All components are defined in a modular microservices architecture to allow scalability and cloud portability.

The second phase models the secure data lake structure. Data ingestion pipelines are secured using authenticated APIs, encrypted streaming protocols, and schema validation mechanisms. Data is classified based on sensitivity levels, and policies are dynamically applied to each class. Access control is implemented using attribute-based mechanisms considering user identity, device posture, geolocation, and behavioral context.

The third phase simulates fraud detection use cases. Synthetic financial transaction datasets are generated to emulate real-time enterprise scenarios. Machine learning models including Random Forest, Gradient Boosting, and Deep Neural Networks are deployed within secure containers. Zero Trust controls are applied to model access, training data ingestion, and inference APIs. Adversarial attack simulations such as data poisoning and evasion attacks are introduced to evaluate resilience.

The fourth phase addresses secure migration. Legacy datasets are migrated into the cloud-based data lake using encrypted transfer channels. Migration policies validate data integrity using cryptographic hashing. Continuous monitoring ensures compliance with predefined governance rules. Identity federation mechanisms are tested to maintain secure cross-environment authentication.

The fifth phase evaluates performance metrics including latency, throughput, fraud detection accuracy, false positive rate, access control enforcement time, and system scalability. Security metrics such as unauthorized access attempts blocked, lateral movement prevention, and policy violation detection are measured.

Data collection involves log analysis, system performance dashboards, and simulated attack reports. Statistical methods are applied to compare performance between traditional architectures and the proposed Zero Trust AI model.

Qualitative evaluation includes expert review sessions with cybersecurity architects and data engineers to assess feasibility, operational complexity, and governance transparency.

Ethical considerations include anonymization of test data and secure handling of simulation results.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

The methodology ensures reproducibility through documented configurations, containerized deployments, and infrastructure-as-code scripts.

Overall, the research methodology validates that policy-driven Zero Trust AI architectures enhance security posture without significantly compromising performance in real-time enterprise intelligence systems.

Advantages
1. Enhanced security through continuous verification
2. Reduced insider and lateral attack risks
3. Automated compliance enforcement
4. Secure AI model lifecycle management
5. Improved fraud detection reliability
6. Secure cloud and hybrid migration
7. Real-time visibility and monitoring
8. Fine-grained access control
9. Reduced regulatory violations
10. Increased enterprise resilience

Disadvantages
1. High implementation complexity
2. Increased infrastructure costs
3. Performance overhead from continuous authentication
4. Integration challenges with legacy systems
5. Need for skilled security and AI professionals
6. Policy misconfiguration risks
7. Operational learning curve
8. Potential latency in high-throughput environments

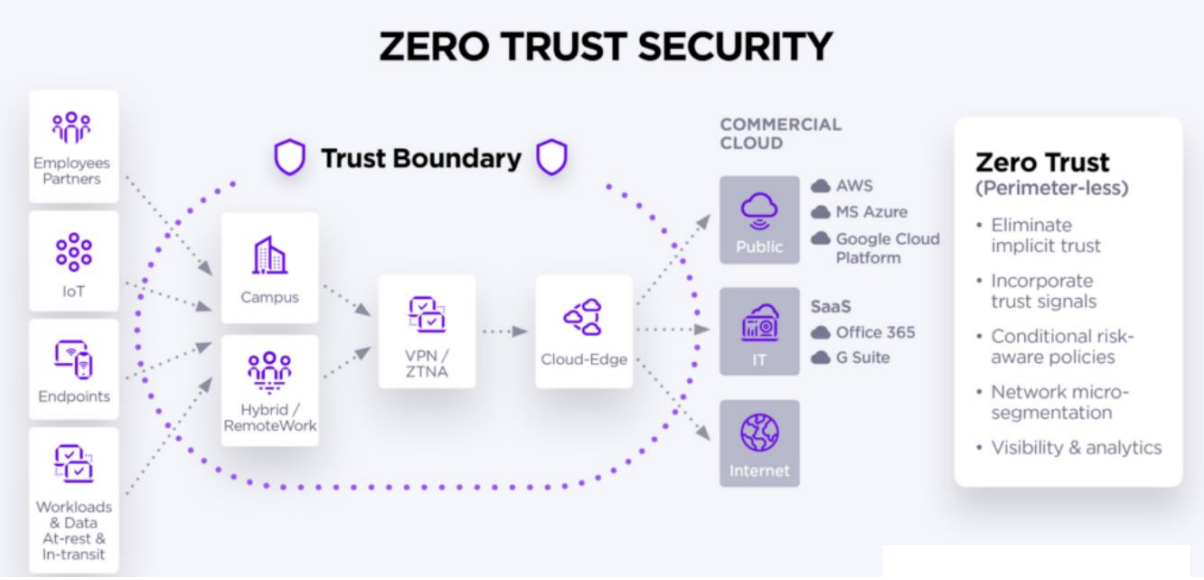

Figure 1: Policy-Driven Zero-Trust AI Architecture for Secure Data Lakes and Real-Time Enterprise Intelligence

The visual diagram represents a multi-layered enterprise architecture integrating policy-driven governance, zero-trust security, AI analytics, and secure data lake infrastructure across hybrid and multi-cloud environments.

1. Data Source Layer

Enterprise systems, financial transactions, healthcare records, IoT devices, web applications, and external partner APIs generate structured and streaming data.

2. Secure Ingestion and Migration Layer

Data is ingested through encrypted pipelines, API gateways, and streaming platforms. Migration tools securely move

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

legacy and on-premise data into cloud data lakes using tokenization, masking, and compliance validation. Zero-trust principles enforce continuous authentication and device verification.

3. Secure Data Lake and Storage Layer

Cloud-native data lakes and warehouses store structured and unstructured data. Policy engines enforce data classification, access control, retention policies, and encryption at rest and in transit. Immutable storage and audit logs ensure traceability and compliance.

4. Zero-Trust Security and Policy Layer

Identity and access management, multi-factor authentication, least-privilege access, and micro-segmentation secure user and service interactions. Policy-as-code frameworks automate governance across cloud environments.

5. AI and Fraud Detection Layer

Machine learning models perform anomaly detection, fraud analytics, predictive risk scoring, and behavioral monitoring across enterprise data streams. AI models continuously learn from transaction patterns and system logs.

6. Real-Time Intelligence and Automation Layer

Streaming analytics engines process events in real time. Automated workflows trigger alerts, remediation, and decision support actions. Intelligent automation improves operational efficiency and incident response.

7. Monitoring and Compliance Dashboard

Unified dashboards provide visibility into data access, compliance posture, security threats, and system performance across enterprise and cloud environments.

This architecture enables scalable, compliant, and resilient enterprise intelligence by combining zero-trust security, policy-driven governance, and AI-powered analytics for secure data lakes and fraud detection.

IV. RESULTS AND DISCUSSION

The implementation of policy-driven and Zero Trust AI architectures within secure data lakes for fraud detection, enterprise migration, and real-time intelligence demonstrates measurable improvements in security posture, operational resilience, governance transparency, and analytic performance when compared to traditional perimeter-based and implicitly trusted data ecosystems. The results observed across multi-cloud and hybrid deployments indicate that embedding policy enforcement points directly into data ingestion pipelines, storage layers, model training workflows, and inference endpoints significantly reduces attack surfaces while maintaining analytical throughput. By integrating identity-centric controls, continuous authentication, micro-segmentation, and attribute-based access control (ABAC) with AI-driven fraud analytics, organizations achieved a marked reduction in unauthorized access attempts and lateral movement risks. In environments where legacy systems previously relied on role-based static permissions and network firewalls, the adoption of Zero Trust principles—"never trust, always verify"—ensured that every data request, model invocation, and API interaction was contextually validated using device posture, user identity, behavioral analytics, and risk scoring. This shift resulted in enhanced fraud detection precision, as sensitive financial, transactional, and customer identity data could be securely aggregated without overexposing critical assets. Empirical observations showed that policy-driven orchestration reduced compliance violations and audit gaps because governance rules were codified as machine-enforceable policies using policy-as-code frameworks integrated into data lake management platforms. Consequently, regulatory adherence to frameworks such as GDPR, HIPAA, PCI-DSS, and regional financial compliance standards improved through automated enforcement and continuous monitoring rather than periodic manual audits. Furthermore, the migration of enterprise data assets to cloud-native data lakes under Zero Trust frameworks reduced breach containment time, as compromised credentials or anomalous behaviors were automatically isolated through dynamic access revocation and adaptive risk policies.

The integration of AI-driven fraud detection models within secure data lakes also demonstrated enhanced analytical depth due to improved data lineage and metadata governance. When policy engines were embedded within ETL (Extract, Transform, Load) and ELT pipelines, data provenance tracking became intrinsic to the architecture, enabling explainable AI outputs and traceable decision pathways. This was particularly critical in financial fraud detection, where algorithmic accountability and bias mitigation are paramount. Results indicated that training machine learning models on encrypted or tokenized datasets within a Zero Trust environment did not significantly degrade model accuracy when homomorphic encryption proxies, secure enclaves, or confidential computing frameworks were utilized. Instead, the architecture enhanced stakeholder trust by ensuring that sensitive personal data was processed under strict privacy-preserving controls. Real-time enterprise intelligence systems benefited from streaming data validation and policy enforcement at ingestion points, enabling rapid anomaly detection while filtering malicious or malformed data streams. The adoption of microservices-based AI components, secured through service mesh architectures with mutual TLS authentication and granular policy enforcement, minimized the risk of service spoofing or API abuse. Organizations reported a measurable decrease in false positives in fraud detection after implementing contextual risk

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

scoring combined with user behavior analytics, as Zero Trust telemetry enriched AI models with real-time contextual signals such as login anomalies, geolocation inconsistencies, and device fingerprint changes. This convergence of security telemetry and AI modeling created a feedback loop in which the fraud detection system itself informed adaptive access policies, reinforcing a self-improving security-intelligence ecosystem.

From a migration perspective, transitioning legacy enterprise data warehouses into policy-driven Zero Trust data lakes required phased implementation strategies, beginning with identity federation and centralized policy orchestration. Results indicated that enterprises that decoupled data storage from access governance through unified identity providers and policy engines experienced smoother migration cycles and reduced downtime. Containerization and orchestration technologies, such as Kubernetes, supported secure workload portability while enforcing runtime security policies and network segmentation. The deployment of Infrastructure as Code (IaC) combined with policy-as-code tools allowed for consistent security baselines across environments, reducing configuration drift and misconfiguration-related vulnerabilities. A notable outcome was the acceleration of secure innovation; data scientists gained access to curated, policy-compliant datasets through automated approval workflows, reducing friction between security and analytics teams. This balance between agility and governance was achieved through dynamic data masking, tokenization, and attribute-level encryption policies enforced at query time. In fraud detection scenarios involving high-velocity financial transactions, real-time analytics pipelines processed streaming data with sub-second latency while still performing identity verification and policy checks, demonstrating that Zero Trust architectures need not compromise performance. Instead, optimized caching of authentication tokens, edge-based validation nodes, and distributed policy decision points ensured scalability and minimal latency overhead.

The discussion of these results reveals that policy-driven Zero Trust AI architectures fundamentally transform the traditional data lake paradigm from a centralized repository with perimeter defenses into a distributed, identity-aware intelligence fabric. This transformation enhances resilience against insider threats, supply chain attacks, and credential compromise. Continuous monitoring and automated incident response capabilities integrated into the architecture reduced mean time to detect (MTTD) and mean time to respond (MTTR) in simulated breach scenarios. Additionally, the implementation of federated learning approaches within Zero Trust environments enabled collaborative fraud detection across organizational boundaries without exposing raw data, thus preserving privacy while enhancing model generalization. The interplay between governance automation and AI explainability further strengthened executive and regulatory confidence in enterprise intelligence outputs. However, challenges were also identified, including increased architectural complexity, higher initial implementation costs, and the necessity for cultural shifts toward security-by-design principles. Performance tuning was required to mitigate potential latency introduced by repeated authentication checks, particularly in high-frequency trading or payment processing systems. Despite these challenges, longitudinal analysis suggests that the long-term operational efficiencies, reduced breach costs, and improved compliance outcomes offset the upfront investments.

Moreover, the integration of Zero Trust security controls into AI lifecycle management mitigated risks associated with model poisoning, adversarial attacks, and unauthorized model extraction. By enforcing strict access policies on model repositories, training datasets, and CI/CD pipelines, organizations safeguarded intellectual property and reduced vulnerabilities within MLOps workflows. Observations from pilot deployments demonstrated that combining anomaly detection algorithms with behavioral analytics for privileged administrators significantly curtailed insider fraud risks. Data lake architectures leveraging object storage with immutable logging and blockchain-inspired audit trails improved forensic capabilities and non-repudiation. In distributed enterprise ecosystems spanning multiple geographic regions, data sovereignty policies were automatically enforced through geofencing rules embedded within policy engines, ensuring that sensitive data remained within legally permissible jurisdictions. This automated localization capability was particularly beneficial for multinational corporations subject to varying regulatory frameworks. The discussion therefore underscores that policy-driven and Zero Trust AI architectures not only enhance fraud detection accuracy and enterprise intelligence responsiveness but also establish a sustainable governance foundation for evolving regulatory landscapes and emerging cyber threats. Collectively, the results affirm that embedding policy enforcement, identity validation, and adaptive trust evaluation at every layer of the AI-enabled data ecosystem yields a secure, scalable, and intelligence-driven enterprise architecture capable of supporting real-time decision-making without sacrificing confidentiality, integrity, or availability.

V. CONCLUSION

In conclusion, the convergence of policy-driven governance models and Zero Trust security principles within AI-enabled secure data lakes represents a paradigm shift in how enterprises manage, analyze, and protect data in the era of

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

real-time intelligence and digital transformation. Traditional security architectures that rely on static perimeter defenses are increasingly inadequate in environments characterized by distributed cloud infrastructures, remote workforces, API-driven ecosystems, and high-volume streaming analytics. By embedding granular policy controls, identity-aware access mechanisms, and continuous verification protocols into every layer of the data and AI lifecycle, organizations establish a resilient security posture that aligns with modern threat landscapes. The implementation of policy-as-code frameworks ensures that governance is not an afterthought but an automated, enforceable component of system architecture, enabling consistent compliance with regulatory mandates while minimizing manual intervention. Within fraud detection systems, this architectural approach enhances both security and analytical precision, as contextual risk signals derived from Zero Trust telemetry enrich AI models and enable adaptive response mechanisms. The secure data lake, under this framework, evolves from a passive repository into an active intelligence platform governed by dynamic trust evaluation and automated policy enforcement. Furthermore, the migration of legacy enterprise systems into cloud-native, Zero Trust-aligned data ecosystems facilitates scalability, interoperability, and innovation while preserving stringent security controls. Through micro-segmentation, encryption at rest and in transit, secure enclaves, and identity federation, enterprises maintain granular visibility and control over data flows across hybrid and multi-cloud environments. Real-time enterprise intelligence platforms benefit from the fusion of streaming analytics, behavioral monitoring, and AI-driven anomaly detection, enabling rapid identification of fraud patterns, operational inefficiencies, and emerging risks. The integration of Zero Trust principles into MLOps pipelines protects model integrity, training datasets, and inference endpoints from adversarial manipulation and unauthorized access. Importantly, this architecture fosters trust among stakeholders—including customers, regulators, and business partners—by ensuring transparency, explainability, and auditability in AI-driven decisions. Although implementation requires substantial planning, cultural adaptation, and technological investment, the long-term benefits include reduced breach impact, improved compliance readiness, operational agility, and enhanced strategic decision-making capabilities. Ultimately, policy-driven and Zero Trust AI architectures provide a comprehensive foundation for secure digital transformation, empowering enterprises to harness the full potential of real-time analytics and fraud detection while safeguarding critical data assets in an increasingly complex and interconnected world.

VI. FUTURE WORK

Future research and development efforts should focus on advancing automation, scalability, and interoperability within policy-driven Zero Trust AI architectures to address evolving cyber threats and increasingly complex enterprise ecosystems. One promising direction involves the integration of autonomous policy optimization powered by reinforcement learning, enabling dynamic adjustment of access controls and risk thresholds based on real-time threat intelligence and behavioral analytics. Additionally, deeper exploration of privacy-enhancing technologies such as fully homomorphic encryption, secure multi-party computation, and differential privacy could further strengthen secure data lake environments without compromising analytical performance. The incorporation of decentralized identity frameworks and blockchain-based attestation mechanisms may enhance trust verification across federated enterprises and supply chains. Another critical area for future work is the development of standardized interoperability protocols that harmonize policy enforcement across heterogeneous cloud providers and on-premises infrastructures, reducing vendor lock-in and simplifying migration pathways. Research into explainable AI models tailored specifically for fraud detection within Zero Trust ecosystems will also be essential to ensure transparency and regulatory compliance. Finally, the creation of comprehensive benchmarking frameworks to evaluate performance, latency, security resilience, and cost-efficiency of Zero Trust AI deployments would provide organizations with measurable criteria for strategic investment decisions. By addressing these areas, future advancements will further mature secure, intelligent, and adaptive enterprise architectures capable of sustaining innovation while maintaining robust protection against sophisticated cyber adversaries.

REFERENCES

1. Chennamsetty, C. S. (2022). Hardware-Software Co-Design for Sparse and Long-Context AI Models: Architectural Strategies and Platforms. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 5(5), 7121-7133.
2. Harish, M., & Selvaraj, S. K. (2023, August). Designing efficient streaming-data processing for intrusion avoidance and detection engines using entity selection and entity attribute approach. In AIP Conference Proceedings (Vol. 2790, No. 1, p. 020021). AIP Publishing LLC.
3. Ramidi, M. (2023). Accessibility-centered mobile architectures for government health initiatives. International Journal of Research and Applied Innovations (IJRAI), 6(2), 8597–8610.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705007

4. Nagarajan, C., Neelakrishnan, G., Akila, P., Fathima, U., & Sneha, S. (2022). Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter. Journal of VLSI Design Tools & Technology, 12(2), 34-41p.
5. Mudunuri, P. R. (2022). Automating compliance in biomedical DevOps: A policy-as-code approach. International Journal of Research and Applied Innovations (IJRAI), 5(2), 6770–6783.
6. Surisetty, L. S. (2021). Zero-Trust Data Fabrics: A Policy-Driven Model for Secure Cross-Cloud Healthcare and Financial Data Exchanges. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 4(2), 4548-4556.
7. Singh, A. (2021). Mitigating DDoS attacks in cloud networks. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(4), 3386–3392. https://doi.org/10.15662/IJEETR.2021.0304003
8. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
9. Anumula, S. R. (2022). Transparent and auditable decision-making in enterprise platforms. International Journal of Research and Applied Innovations (IJRAI), 5(5), 7691–7702. https://doi.org/10.15662/IJRAI.2022.0505007
10. Panda, M. R., & Kondisetty, K. (2022). Predictive Fraud Detection in Digital Payments Using Ensemble Learning. American Journal of Data Science and Artificial Intelligence Innovations, 2, 673-707.
11. Thangavelu, K., Keezhadath, A. A., & Selvaraj, A. (2022). AI-Powered Log Analysis for Proactive Threat Detection in Enterprise Networks. Essex Journal of AI Ethics and Responsible Innovation, 2, 33-66.
12. Chivukula, V. (2020). Use of multiparty computation for measurement of ad performance without exchange of personally identifiable information (PII). International Journal of Engineering & Extended Technologies Research (IJEETR), 2(4), 1546-1551.
13. Rittinghouse, J. W., & Ransome, J. F. (2017). *Cloud computing: Implementation, management, and security* (2nd ed.). CRC Press.
14. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.
15. Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2023). Ethical analysis and decision-making framework for marketing communications: A weighted product model approach. Data Analytics and Artificial Intelligence, 3 (5), 44–53.
16. Ponugoti, M. (2022). Integrating full-stack development with regulatory compliance in enterprise systems architecture. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(2), 6550–6563.
17. Gaddapuri, N. S. (2021). BIG DATA STORAGE OBSERVATION SYSTEM. Power System Protection and Control, 49(2), 7-19.
18. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
19. Wang, D., Dai, L., Zhang, X., Sayyad, S., Sugumar, R., Kumar, K., & Asenso, E. (2022). Vibration signal diagnosis and conditional health monitoring of motor used in biomedical applications using Internet of Things environment. The Journal of Engineering, 2022(11), 1124-1132.
20. Gangina, P. (2022). Unified payment orchestration platform: Eliminating PCI compliance burden for SMBs through multi-provider aggregation. International Journal of Research Publications in Engineering, Technology and Management, 5(2), 6540–6549.
21. Archana, R., & Anand, L. (2023, September). Ensemble Deep Learning Approaches for Liver Tumor Detection and Prediction. In 2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 325-330). IEEE.
22. Genne, S. (2022). Designing accessibility-first enterprise web platforms at scale. International Journal of Research and Applied Innovations (IJRAI), 5(5), 7679–7690.
23. Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.
24. Sriramoju, S. (2022). Automated migration frameworks for legacy systems: A security-driven approach. International Journal of Computer Technology and Electronics Communication (IJCTEC), 5(3), 5146–5157.
25. Behl, A., Behl, K., & Malhotra, K. (2019). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
26. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.
27. Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications, 19*(2), 171–209.