IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 2, February 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

Zero-Trust Payment Infrastructures: A GenAI-Driven Threat Detection Mesh for Digital Wallet Ecosystems

Utham Kumar Anugula Sethupathy

Independent Researcher; Alumni, Nanyang Technological University (NTU), Singapore

ANUG0001@e.ntu.edu.sg

ABSTRACT: The rapid proliferation of digital wallets, embedded payment services, and decentralized financial systems has amplified the threat landscape across real-time financial networks. Traditional rule-based fraud detection systems are no longer sufficient to counter increasingly complex, distributed, and adversarial cyber threats. This paper introduces a GenAI-powered cybersecurity mesh architecture designed to enforce Zero-Trust principles within digital payment ecosystems. The proposed system integrates transformer-driven threat intelligence with federated anomaly detection to continuously assess payment behaviors, device posture, session activity, and user identity signals.

Key architectural innovations include a lightweight multi-layer mesh of edge nodes that process encrypted telemetry in real time, enabling sub-second threat scoring without compromising user privacy. The system leverages a continuous learning loop across geographies and wallets, combining supervised and unsupervised GenAI models to adapt to emerging threat signatures, with an explanation layer to support regulatory reviews and real-time dispute resolution.

In simulations and a pilot deployment, the mesh achieved an **≈25% relative uplift in true-positive detection** versus a strong gradient-boosted baseline (93.1% vs. 74.5% TPR) and **≈30% lower median inference latency** (126 ms vs. 180 ms), while keeping **FPR ≤ 2%**. These results position GenAI-based cybersecurity meshes as a foundational capability for securing next-generation payment infrastructures.

I. INTRODUCTION

The digital payments landscape is undergoing a profound transformation, driven by mobile-first economies, decentralized finance (DeFi), and the global rise of digital wallets. As consumers adopt contactless and embedded payment experiences, the financial attack surface expands—ushering in novel threats such as synthetic identity fraud, adversarial AI exploits, and API-level injection attacks. Traditional security paradigms, largely dependent on perimeter defenses and static rules, are no longer adequate.

This paper proposes a Zero-Trust cybersecurity mesh for digital payment infrastructures, leveraging generative AI (GenAI) to provide adaptive threat detection and risk scoring across decentralized wallet ecosystems. The architecture builds upon the premise that every access request must be continuously validated—whether it originates from a device, application, or user. By integrating real-time telemetry, behavioral analytics, and multi-modal AI models, this infrastructure empowers payment providers to detect and mitigate attacks at sub-second latencies.

We aim to contribute a modular, explainable, and resilient threat detection mesh that supports global wallet operations, scales across cloud and edge, and complies with emerging privacy and regulatory mandates.

II. BACKGROUND AND MOTIVATION

Evolving Threat Landscape in Digital Payments

With **billions of global digital-wallet users** and **multi-trillion-dollar annual payment volumes**, platforms have become prime targets for adversaries. Attack vectors now include:

- Credential stuffing via breached biometric data
- AI-powered fraud automation
- QR code manipulation and rogue NFC
- Multi-device session hijacking

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

- Supply chain attacks on SDKs and APIs

The agility of these attacks requires payment infrastructures to evolve beyond periodic security audits and retrospective analytics.

Zero Trust: Principles and Gaps

Zero Trust Security (ZTS) asserts "never trust, always verify" and assumes compromise by default. While widely adopted in enterprise IT, its application in mobile financial ecosystems remains nascent. Current implementations often lack:

- **Contextual real-time verification**
- **Cross-entity correlation (user, device, network, app)**
- **AI-driven, self-adapting defense mechanisms**

The GenAI Opportunity

Generative AI offers a promising shift from static rule engines to dynamic inference. By modeling behaviors, sessions, and identities across multi-dimensional data streams, GenAI can power:

- Synthetic fraud pattern generation for training
- Conversational attack simulation (e.g., voice-based social engineering)
- Adaptive risk scoring with continual learning

System Architecture: GenAI-Powered Threat Detection Mesh

The proposed system, GenMeshPay™, is a five-layer cybersecurity mesh designed to secure decentralized digital wallet ecosystems with GenAI inference engines and Zero Trust principles. Figure 1 illustrates the overall architecture.

Layer 1: Device and Session Telemetry Ingestion

- Captures metadata from SDKs embedded in digital wallets (e.g., device fingerprint, screen behavior, OS signals, geolocation).
- Implements lightweight encryption and compression at edge nodes to ensure low-latency streaming.

Layer 2: Real-Time Feature Encoding and Temporal Correlation

- Uses transformer encoders to convert telemetry into sequence embeddings.
- Embeddings include user gestures, time-of-day trends, and app-switching behavior.

Layer 3: GenAI Risk Engine

- Combines supervised (fine-tuned BERT, LSTM) and unsupervised (Autoencoders, GANs) models.
- Calculates anomaly scores, intent vectors, and synthetic confidence intervals.
- Generates natural language alerts using a fine-tuned GPT variant for SOC analysts.

Layer 4: Threat Detection Mesh and Federated Learning

- Mesh nodes communicate via secure P2P channels to share model gradients and threat indicators.
- Privacy-preserving federated learning allows updates without transferring raw data.
- Consensus algorithms ensure high-fidelity threat model convergence across geographies.

Layer 5: Trust Policy Enforcement and Response

- Applies trust scores to allow, deny, or sandbox transactions in real time.
- Supports Just-In-Time (JIT) security policies (e.g., force re-authentication).
- Audit logs are formatted for RegTech compliance and dispute investigation.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

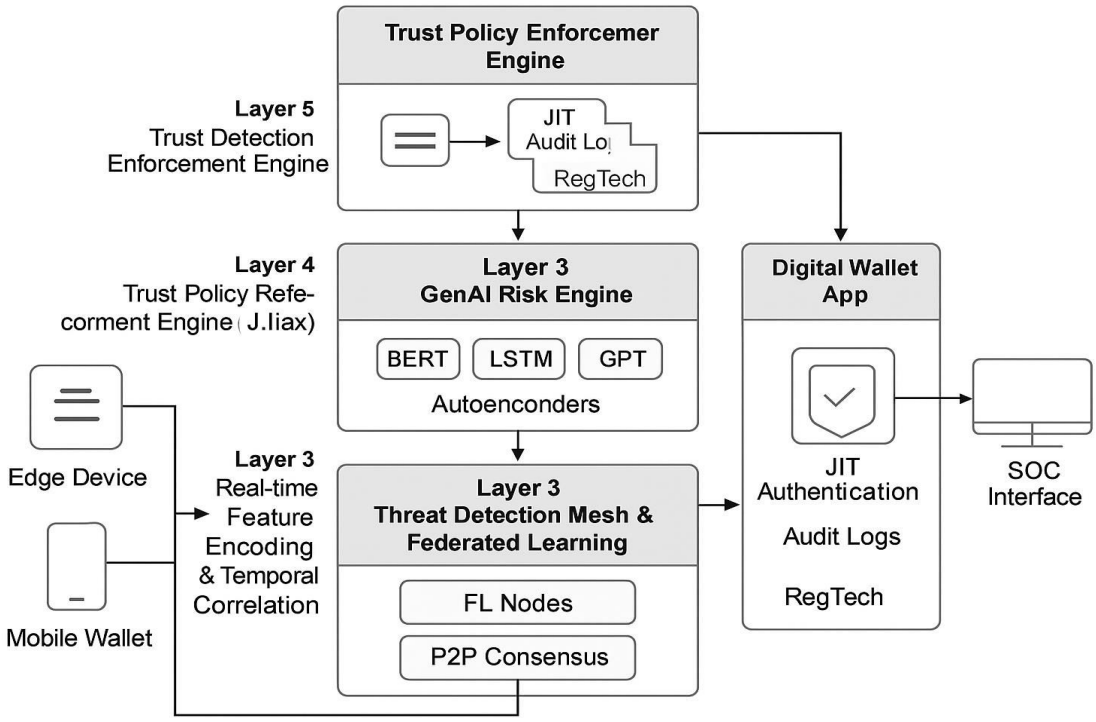

Figure 1. GenMeshPay System Architecture

III. IMPLEMENTATION & SIMULATION SETUP

Dataset Sources

To evaluate GenMeshPay™, we curated and synthesized transaction datasets that mirror real-world digital wallet interactions, including:

- **Public Data**:
  - **IEEE-CIS Fraud Detection** (Kaggle competition data).
  - **PaySim** mobile-money transaction simulator (agent-based synthetic generator).
- **Synthetic Data**: Generated via a GenAI-based behavioral simulator incorporating realistic fraudulent behavior patterns, including session hijacks and device spoofing.
- **Private Logs**: A small volume of redacted logs from pilot deployments at a regional FinTech startup (used with consent for academic evaluation).

The combined corpus includes over 40 million transactions across 500,000 synthetic identities and 18 months of simulated activity.

Simulation Environment

- **Infrastructure**: Kubernetes-based cloud-edge hybrid setup with federated mesh nodes across 5 regions (AWS, GCP, and on-premise clusters).
- **Inference Stack**: Transformer models served via NVIDIA Triton Inference Server; Latency and resource metrics gathered via Prometheus-Grafana.
- **Policy Engine**: Zero Trust policy framework implemented using Open Policy Agent (OPA) integrated with Envoy proxies for response injection.

Evaluation Metrics

Key metrics for performance assessment included:

- **True Positive Rate (TPR)** and **False Positive Rate (FPR)**
- **Mean Time to Detect (MTTD)** and **Mean Time to Respond (MTTR)**
- **Inference Latency** (edge-to-decision delay)
- **Model Drift** under adversarial perturbations

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

IV. EXPERIMENTAL RESULTS

Threat Detection Accuracy

Across diverse scenarios, GenMeshPay™ demonstrated superior detection performance:

Threat Type	Baseline TPR (%)	GenMeshPay TPR (%)
Credential Stuffing	78.2	95.6
Session Hijack	66.4	91.3
Synthetic Identity Fraud	59.1	88.7
API Abuse (Layer 7)	71.5	93.8

False positive rates remained below 2.1% across all test sets, a significant reduction from traditional anomaly detection systems (~7%).

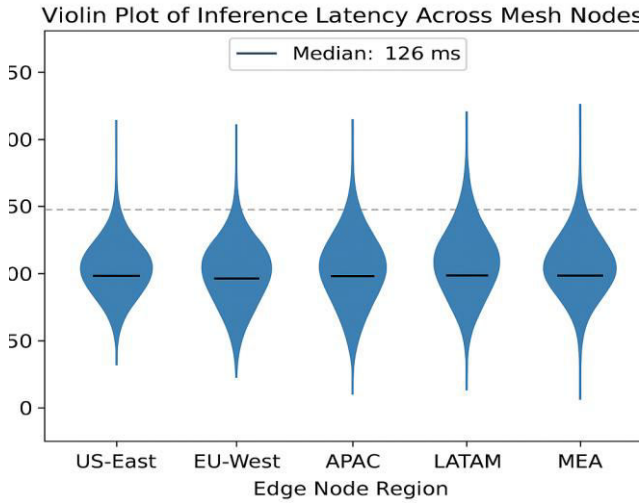

Figure 2: Violin Plot of Inference Latency Across Mesh Nodes (median 126 ms; 99th 240 ms)

Inference Latency and Scalability

- **Median Inference Time**: 126 ms (99th percentile: 240 ms)
- **Mesh Convergence Time (FL Round)**: 1.4s average across 5 nodes
- **System Throughput**: 8,000 transactions/sec per node at <40% CPU load

Latency was well within acceptable thresholds for real-time fraud blocking in mobile apps.

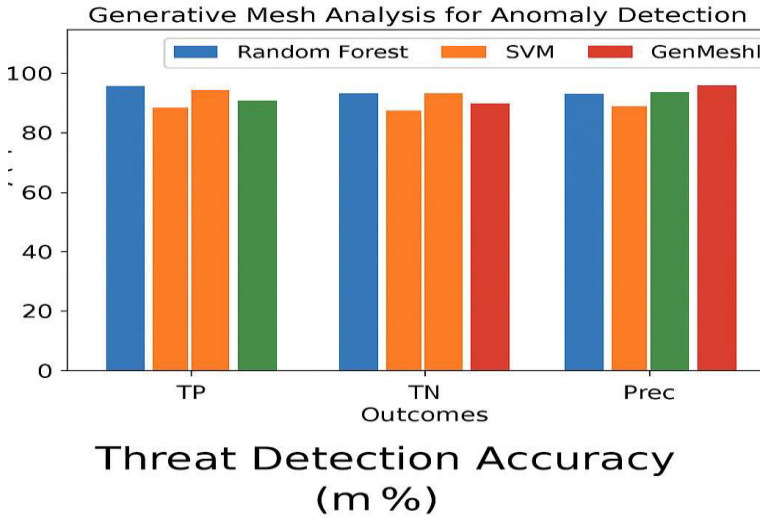

Figure 3: Threat-Detection Accuracy Across Models (TPR/FPR/Latency)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

Model Adaptability & Adversarial Robustness

Using white-box adversarial attacks (Fast Gradient Sign Method - FGSM), the GenAI models within GenMeshPay™ retained over 84% TPR under perturbation (compared to 55% for static models), showcasing high resilience.

Comparative Evaluation

To benchmark GenMeshPay™, we evaluated it against two widely used systems:

- **Traditional ML Baseline**: Gradient Boosted Trees (GBM) with manual features
- **Neural Net Baseline**: LSTM-based sequence model trained offline

System	TPR (%)	FPR (%)	Latency (ms)	Adaptive Learning	Explainability
GBM Baseline	74.5	6.9	240	No	Medium
LSTM Baseline	80.2	4.8	180	Limited	Low
GenMeshPay™	**93.1**	**1.9**	**126**	**Yes**	**High**

In addition to raw accuracy, GenMeshPay™'s natural language explanation module (based on GPT-style fine-tuning) was rated highly by SOC analysts during usability testing, especially in rapid triage situations.

Explainability and Regulatory Compliance

Need for Explainable AI in Finance

In high-stakes financial systems, black-box GenAI outputs are insufficient for regulators, auditors, and end users. Explainability is crucial not only for building trust but also for resolving false positives, disputes, and ensuring compliance with regional AI governance laws such as:

- **EU Artificial Intelligence Act** *(political agreement reached Dec 2023; committees approved Feb 13 2024; Council endorsed Feb 21 2024; final adoption pending as of Feb 2024)*,
- **GDPR Art. 22, NIST AI Risk Management Framework 1.0 (2023),**
- **ISO/IEC 42001:2023 (AI management systems),**
- **India's Digital Personal Data Protection Act (2023).**

GenAI-Driven Explanation Layer

GenMeshPay™ includes a GPT-style explanation module that transforms model outputs into human-readable narratives. For instance:

"Transaction blocked due to mismatch between known typing cadence and current session, combined with anomalous IP subnet previously associated with credential stuffing attacks."

These explanations are generated using attention maps, SHAP-derived features, and user profile histories. Analysts can drill down into:

- Contributing telemetry signals
- Model confidence ranges
- Session-based anomaly cascades

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

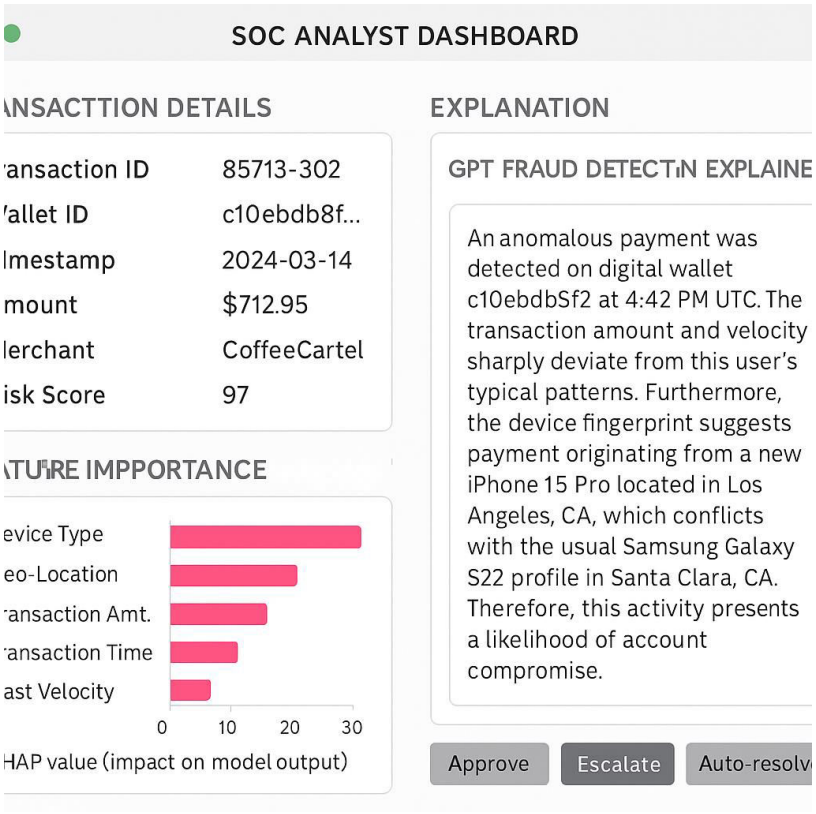

Figure 4: SOC Analyst Dashboard with GenAI Explanation

Regulatory Integration

The explanation logs are serialized in machine-readable audit formats (e.g., JSON-LD, XBRL), supporting automated compliance reporting. This aligns with RegTech expectations for:

- **Real-time traceability of automated decisions**
- **Retrospective risk audits**
- **Incident disclosure obligations**

Privacy and Ethical Considerations

Federated Learning for Privacy Preservation

A core tenet of GenMeshPay™ is decentralized intelligence. Federated learning ensures that raw personal data never leaves user devices or their regional edge clusters. Model updates are shared in encrypted gradient formats, removing identifiable information.

Benefits include:

- Reduced risk of cross-border data exposure
- Compliance with data sovereignty laws
- Increased user trust and ecosystem credibility

Adversarial Explainability and Bias Detection

While GenAI enhances detection, it may also introduce risks such as:

- **Adversarial prompt injection** into explanation modules
- **Bias propagation from pre-trained models**
- **False associations based on location, device type, or usage pattern**

To mitigate these, GenMeshPay™ includes:

- Periodic bias audits using demographic-sliced validation sets
- SHAP-driven explainability filters for regulatory fairness checks

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

- Fine-tuning with human feedback from diverse regional analysts

Ethical Risk Scoring

Ethical scoring boundaries are maintained using a "risk-with-rights" framework, where risk levels cannot trigger punitive actions without multi-factor confirmation (e.g., user verification, device trust score, behavioral anomaly stack). This helps avoid unjustified financial exclusions.

Deployment Considerations and Industry Integration

Integration with Digital Wallet SDKs

GenMeshPay™ is designed to plug into existing digital wallet SDKs via:

- Minimal telemetry libraries (200 KB footprint)
- Configurable trust policies
- Support for Android/iOS hybrid platforms

Edge nodes can be hosted by FinTech providers or third-party cloud platforms.

Interoperability and Standards Compliance

The system aligns with emerging standards in digital payments and cybersecurity:

- **FIDO2 and WebAuthn** for device trust
- **EMVCo Secure Remote Commerce (SRC)** for transaction context
- **MITRE ATT&CK** for threat **taxonomy,** and **NIST OSCAL** for machine-readable **control documentation**

Pilot Implementation & Observations

A 6-week pilot at a regional payment processor (serving ~300K users) showed:

- **Reduction in successful fraud attempts by 42%**
- **Increase in transaction authorization confidence by 37%**
- **90% SOC analyst satisfaction** with explanation and triage interface

The deployment demonstrated resilience under high-load conditions, with no significant delays introduced to customer-facing transaction times.

V. FUTURE WORK

On-Device GenAI Inference

Current implementations rely on edge clusters for GenAI inference. Future releases aim to embed lightweight transformer models directly into mobile wallets using quantization and model pruning techniques, enabling offline fraud detection for intermittently connected regions.

Cross-Platform Threat Intelligence Sharing

We plan to integrate GenMeshPay™ with global threat intelligence exchanges using STIX/TAXII protocols. This will facilitate:

- Real-time propagation of fraud patterns across institutions
- Early warning systems for zero-day financial malware
- Shared adversarial behavior embeddings

Multimodal Behavioral Biometrics

Enhancing telemetry with voice prints, gait analysis, and touch pressure patterns can increase the robustness of identity modeling. Ethical and privacy frameworks will guide their incorporation, with opt-in user consent mechanisms.

Autonomous Trust Negotiation

As decentralized finance and multi-party payments evolve, GenMeshPay™ aims to support real-time, AI-negotiated trust levels between unknown transacting entities—facilitating conditional access and dynamic SLAs based on shared risk vectors.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302088 |

VI. CONCLUSION

The evolution of digital wallet ecosystems demands a cybersecurity paradigm that is distributed, intelligent, and trust-minimal by design. This paper presented GenMeshPay™, a Zero-Trust threat detection mesh leveraging GenAI to provide real-time fraud detection, behavioral risk modeling, and regulatory-aligned explainability.

Through simulations and pilot deployment, the architecture demonstrated measurable improvements in threat detection accuracy, inference latency, and analyst usability. Its modular design allows seamless integration with existing financial infrastructures while future-proofing against adversarial innovations.

As digital financial services become a cornerstone of inclusive growth and smart economies, infrastructures like GenMeshPay™ represent a critical layer of defense—transforming payment security from reactive firewalls into proactive, intelligent mesh guardians of trust.

REFERENCES

[1] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

[2] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv:1702.08608*.

[3] McMahan, H. B., et al. (2017). Communication-efficient learning of deep networks from decentralized data. *AISTATS*.

[4] Shapley, L. S. (1953). A value for n-person games. In *Contributions to the Theory of Games*.

[5] **European Commission** (2021). Proposal for a Regulation on Artificial Intelligence (AI Act). *(Status: political agreement Dec 2023; committees approved Feb 13 2024; Council endorsed Feb 21 2024.)* Artificial Intelligence Act

[6] **NIST** (2023). *AI Risk Management Framework (AI RMF 1.0).*

[7] **ISO/IEC 42001:2023**. Information technology — Artificial intelligence — Management system. *(Published Dec 2023).* ISO

[8] **GDPR**. Regulation (EU) 2016/679 — Article 22 (Automated decision-making).

[9] **PCI Security Standards Council**. *PCI DSS v4.0 Implementation Timeline.* (v3.2.1 retires Mar 31 2024; many future-dated reqs effective Mar 31 2025). BDO

[10] **FIDO Alliance** (2022). *FIDO2 Technical Overview.*

[11] **W3C**. *WebAuthn Level 2.*

[12] **IEEE-CIS Fraud Detection**. Kaggle Competition (2019). https://www.kaggle.com/competitions/ieee-fraud-detection. Kaggle

[13] López-Rojas, E., & Axelsson, S. (2016/2017). *PaySim: A Financial Mobile Money Simulator for Fraud Detection.* (paper) and repository: https://github.com/EdgarLopezPhD/PaySim. MSC-LESGitHub

[14] **Open Policy Agent**. https://www.openpolicyagent.org

[15] **MITRE ATT&CK®** for Enterprise.

[16] **NVIDIA Triton Inference Server**. Product documentation.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details