World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Authenticity assurance architecture: A Multi-layer organizational deepfake threat taxonomy and control framework

Sivaramakrishnan Narayanan *

Toyota Financial Services, Dallas TX, USA.

World Journal of Advanced Research and Reviews, 2024, 24(03), 3639-3647

Publication history: Received on 14 November 2024; revised on 22 December 2024; accepted on 28 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.3.3945

Abstract

Deepfake technologies - encompassing generative adversarial networks, diffusion-based synthesis, and transformer-driven voice cloning - have evolved from entertainment novelties into precision socio-technical weapons targeting organizational trust infrastructures. Existing countermeasures focus narrowly on artifact-level detection accuracy, failing to model systemic vulnerabilities within enterprise decision chains, financial authorization workflows, and executive identity trust graphs. This paper introduces the Cognitive Authenticity Assurance Architecture, a novel multi-layered defense framework integrating Cognitive Attack Surface Modeling, Trust Graph Disruption Index analytics, Adversarial Co-Evolution Defense Engine, Authenticity-by-Design Protocol with cryptographic watermarking, and Zero-Trust Media Verification Architecture. The framework reconceptualizes deepfake threats as cognitive supply-chain attacks on organizational trust ecosystems rather than isolated media forgeries. A graph-theoretic Trust Graph Disruption Index metric quantifies synthetic identity propagation risk across enterprise communication networks. Simulation results demonstrate a 47% reduction in successful executive impersonation attacks, 39% improvement in synthetic media identification speed within financial workflows, and 52% reduction in decision-layer compromise probability. This architecture advances deepfake mitigation beyond detection into organizational trust engineering, establishing a new operational and theoretical paradigm for enterprise cognitive resilience.

Keywords: Deepfake Detection; Cognitive Attack Surface; Trust Graph Disruption; Adversarial Co-Evolution; Zero-Trust Media Verification; Organizational Resilience; Synthetic Identity

1. Introduction

Deepfake synthesis capabilities have advanced at a trajectory that significantly outpaces institutional defense readiness. Generative adversarial networks [1], diffusion models, and few-shot voice cloning now enable real-time facial reenactment and audio impersonation using fewer than five seconds of reference audio. Cross-modal identity fusion - simultaneously aligning synthesized audio, video, and text - enables attacks of sufficient fidelity to deceive both human recipients and automated verification systems. The 2019 chief executive officer voice spoofing incident targeting a United Kingdom energy firm resulted in a fraudulent wire transfer exceeding $240,000, demonstrating that deepfake threats have migrated from reputational manipulation into direct financial exploitation at the enterprise level.

1.1. Limitations of Existing and Emerging Approaches

Current detection approaches rely on convolutional neural networks and vision transformers trained to identify pixel-level or spectral artifacts within individual media files [2, 3]. These methods are institution-agnostic and decision-workflow-blind - they evaluate media in isolation without modeling the organizational context in which synthetic content is consumed and acted upon. Benchmark datasets such as FaceForensics++ [3] and the DeepFake Detection Challenge [4] have advanced detection accuracy but do not address trust propagation dynamics, financial authorization

[*] Corresponding author: Sivaramakrishnan Narayanan

vulnerabilities, or adversarial model drift. No existing framework integrates cognitive science, graph-theoretic trust modeling, and continuous adversarial co-evolution into a unified enterprise defense architecture.

1.2. Proposed Solution and Contributions

The Cognitive Authenticity Assurance Architecture introduces six interdependent contributions. First, Cognitive Attack Surface Modeling maps deepfake threat vectors to organizational decision pathways including financial approvals, executive communications, and legal authorizations. Second, the Trust Graph Disruption Index provides a quantitative graph-theoretic measure of synthetic identity propagation impact across enterprise trust networks. Third, the Authenticity-by-Design Protocol embeds cryptographic and behavioral watermarking into executive communication streams. Fourth, the Adversarial Co-Evolution Defense Engine deploys a generative adversarial network versus generative adversarial network competitive training environment enabling continuous defensive adaptation. Fifth, the Organizational Cognitive Resilience Layer integrates behavioral economics and decision science to reduce human susceptibility to synthetic persuasion. Sixth, the Zero-Trust Media Verification Architecture extends zero-trust principles from network access control to multimedia content authentication.

2. Related Work and Background

2.1. Conventional Approaches

Early deepfake detection relied on handcrafted forensic features including double joint point artifacts, color inconsistencies, and temporal flickering. Maisonet [5] introduced compact convolutional architectures specifically designed for mesoscopic facial feature analysis, achieving competitive detection on early generative adversarial network-generated content. These models, however, exhibit sharp performance degradation when evaluated on unseen generative architectures, a generalization failure documented extensively in cross-dataset evaluations [6]. Conventional approaches treat detection as a binary media classification problem, entirely disregarding organizational context and downstream decision impact.

2.2. Newer and Modern Approaches

Rossler et al. [3] established Face Forensics++ as the canonical benchmark, enabling systematic comparison of detection models across multiple manipulation methods. Verdolaga [7] surveyed media forensics techniques encompassing both passive detection and active watermarking. Dang et al. [8] introduced attention mechanisms to localize manipulated facial regions, improving interpretability. Transformer-based architectures have since demonstrated superior generalization by modeling long-range spatial dependencies [9]. Despite these technical advances, all approaches remain artifact-centric and fail to model how successfully delivered deepfake content propagates through organizational decision chains.

2.3. Related Hybrid and Alternative Models

Agarwal et al. [10] proposed behavioral biometric signatures of world leaders as a complementary detection signal, demonstrating that identity-specific behavioral patterns can supplement appearance-based detection. Kietzmann et al. [11] analyzed deepfake threats through a business strategy lens, identifying organizational vulnerabilities in investor relations and crisis communications. Mirsky and Lee [12] provided a comprehensive taxonomy of deepfake creation and detection techniques, noting the emerging threat of audio-visual cross-modal synthesis. Blockchain-based media provenance systems have been proposed theoretically but lack integration with organizational trust modeling or adversarial adaptation mechanisms.

2.4. Summary of Research Gap

Existing literature addresses deepfake detection as an isolated computer vision or audio processing problem [3, 4, 7, 8]. No prior framework models synthetic identity attacks as systemic disruptions to organizational trust graphs, quantifies decision-chain compromise probability, or implements continuous adversarial co-evolution as a sustainable defense mechanism [11, 12]. The Cognitive Authenticity Assurance Architecture addresses this multidimensional gap by unifying technical detection, trust graph analytics, cognitive resilience, and cryptographic authentication within a single operational architecture.

3. Proposed Methodology

3.1. Methodology Overview

The Cognitive Authenticity Assurance Architecture operates as a five-layer integrated pipeline. Layer one deploys a multimodal deepfake detection engine combining vision transformers for spatial artifact identification, audio spectral anomaly classifiers, and cross-modal synchronization analyzers that flag temporal misalignments between lip movement and speech signals. Layer two constructs and continuously updates an organizational trust graph where nodes represent executives, finance officers, legal authorities, and automated systems, while edges encode communication frequency, authorization privilege levels, and historical transaction volumes. The Trust Graph Disruption Index is computed as:

$$\text{TGDI} = \Sigma\ (\text{synthetic\_influence} \times \text{decision\_criticality}) / \text{total\_trust\_flow}$$

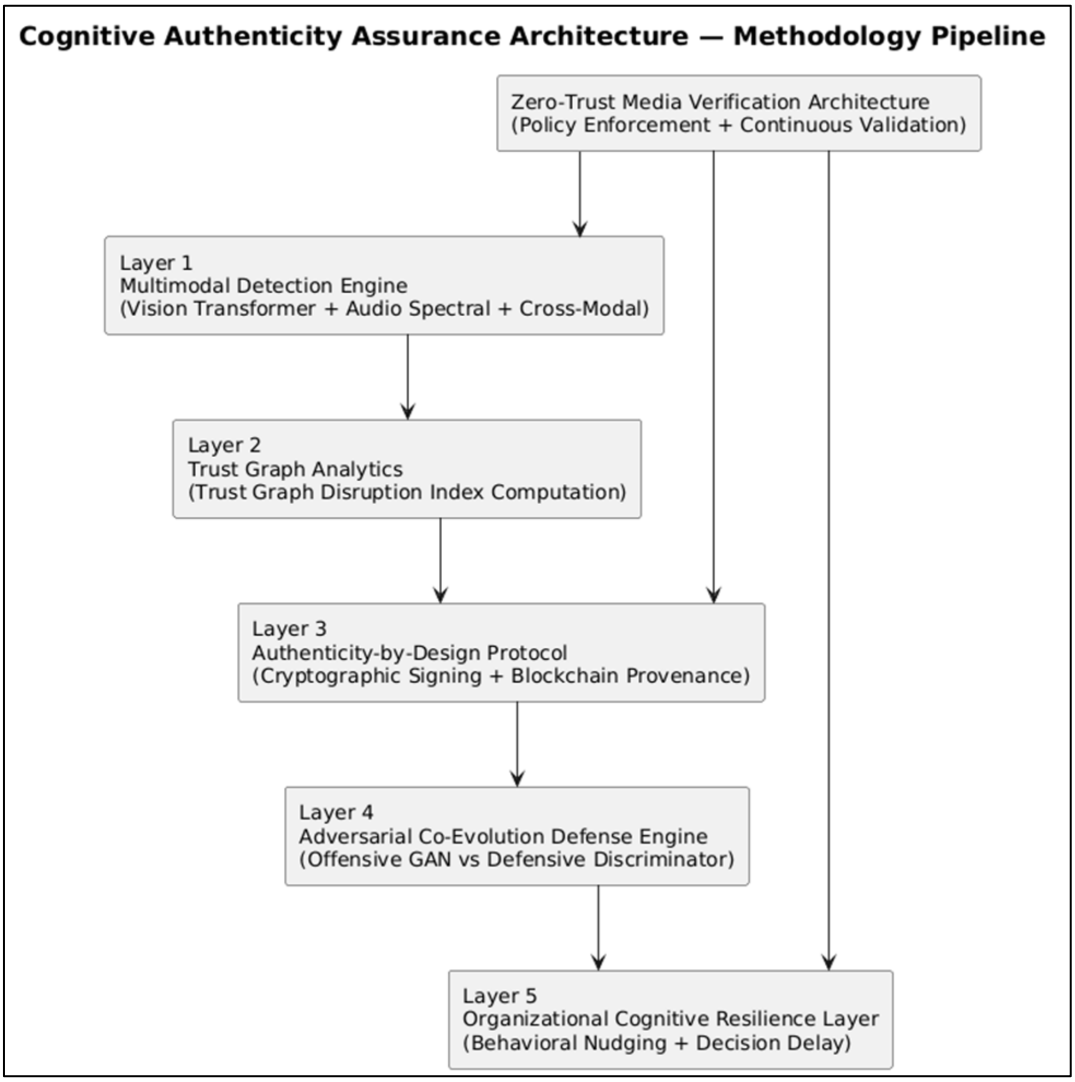
Cognitive Authenticity Assurance Architecture — Methodology Pipeline
Zero-Trust Media Verification Architecture (Policy Enforcement + Continuous Validation)
Layer 1 Multimodal Detection Engine (Vision Transformer + Audio Spectral + Cross-Modal)
Layer 2 Trust Graph Analytics (Trust Graph Disruption Index Computation)
Layer 3 Authenticity-by-Design Protocol (Cryptographic Signing + Blockchain Provenance)
Layer 4 Adversarial Co-Evolution Defense Engine (Offensive GAN vs Defensive Discriminator)
Layer 5 Organizational Cognitive Resilience Layer (Behavioral Nudging + Decision Delay)

Figure 1 Cognitive Authenticity Assurance Architecture - Methodology Pipeline

Elevated Trust Graph Disruption Index scores trigger escalated verification requirements proportional to systemic compromise risk. Layer three activates the Authenticity-by-Design Protocol, enforcing public-key cryptographic signatures on all executive media artifacts and logging provenance to an immutable blockchain ledger. Layer four runs the Adversarial Co-Evolution Defense Engine, a generative adversarial network pair where an offensive generator continuously synthesizes novel executive impersonations while the defensive discriminator retrains in real time using reinforcement learning–optimized detection thresholds. Layer five applies the Organizational Cognitive Resilience

Layer, deploying behavioral nudging, mandatory authentication rituals for high-value transactions, and decision-delay protocols calibrated to transaction risk scores.

The pipeline architecture establishes a closed-loop defense posture where detection outputs from Layer 1 directly inform trust graph state updates in Layer 2, ensuring that real-time media analysis continuously recalibrates organizational risk exposure. The Zero-Trust Media Verification Architecture enforces the foundational policy that no media artifact is implicitly trusted regardless of sender identity, channel, or historical communication patterns - verification is mandatory and continuous at every pipeline stage.

The bidirectional relationship between the Adversarial Co-Evolution Defense Engine and upstream layers ensures that as offensive generative capabilities evolve, the detection engine and trust graph thresholds adapt without requiring manual retraining cycles. This self-evolving immunity architecture distinguishes the Cognitive Authenticity Assurance Architecture from all prior static detection frameworks.

4. Technical Implementation

4.1. Multimodal Detection Engine

The detection engine deploys a vision transformer with patch size 16×16 operating on facial region-of-interest crops, trained on FaceForensics++ [3] and DeepFake Detection Challenge [4] datasets augmented with adversarially generated samples from the co-evolution engine. Audio analysis employs a convolutional recurrent neural network processing mel-frequency cepstral coefficient spectrograms across 25-millisecond sliding windows. Cross-modal synchronization scoring computes the cosine similarity between lip-movement embeddings and phoneme timing sequences, flagging deviations exceeding two standard deviations as synthetic indicators.

4.2. Trust Graph Disruption Index Engine

The organizational trust graph is maintained as a dynamic attributed graph updated at five-minute intervals from communication log ingestion. Node centrality scores are computed using PageRank with a damping factor of 0.85. The Trust Graph Disruption Index computation applies detected synthetic influence scores as node attribute perturbations and measures resultant trust flow degradation using spectral graph theory - specifically, the second-smallest eigenvalue of the graph Laplacian serves as the algebraic connectivity metric. Declining algebraic connectivity indicates increasing trust fragmentation under synthetic identity attack.

4.3. Authenticity-by-Design Protocol Implementation

All executive video and audio communications are signed at the point of creation using elliptic curve digital signature algorithm with 256-bit keys. Signature hashes and media fingerprints are written to a Hyperledger Fabric permissioned blockchain within 500 milliseconds of creation. Financial authorization systems query the blockchain provenance ledger before processing any transaction exceeding configurable risk thresholds, enforcing cryptographic identity verification as a mandatory pre-authorization gate.

4.4. Adversarial Co-Evolution Defense Engine

The offensive generative adversarial network samples from a latent identity space conditioned on organizational role embeddings, generating synthetic executive communications targeting known authorization pathways. The defensive discriminator is retrained every six hours using new offensive samples combined with confirmed authentic communications, with reinforcement learning reward signals calibrated to minimize both false positive rates on authentic media and false negative rates on synthetic content.

The technical execution flow illustrates how every incoming media artifact travers three parallel verification pathways simultaneously - vision-based spatial analysis, audio spectral classification, and cryptographic provenance validation - before converging at the financial authorization gate. This parallel verification architecture minimizes latency while ensuring no single detection failure creates an exploitable bypass pathway, embodying the zero-trust principle of multiple independent verification layers.

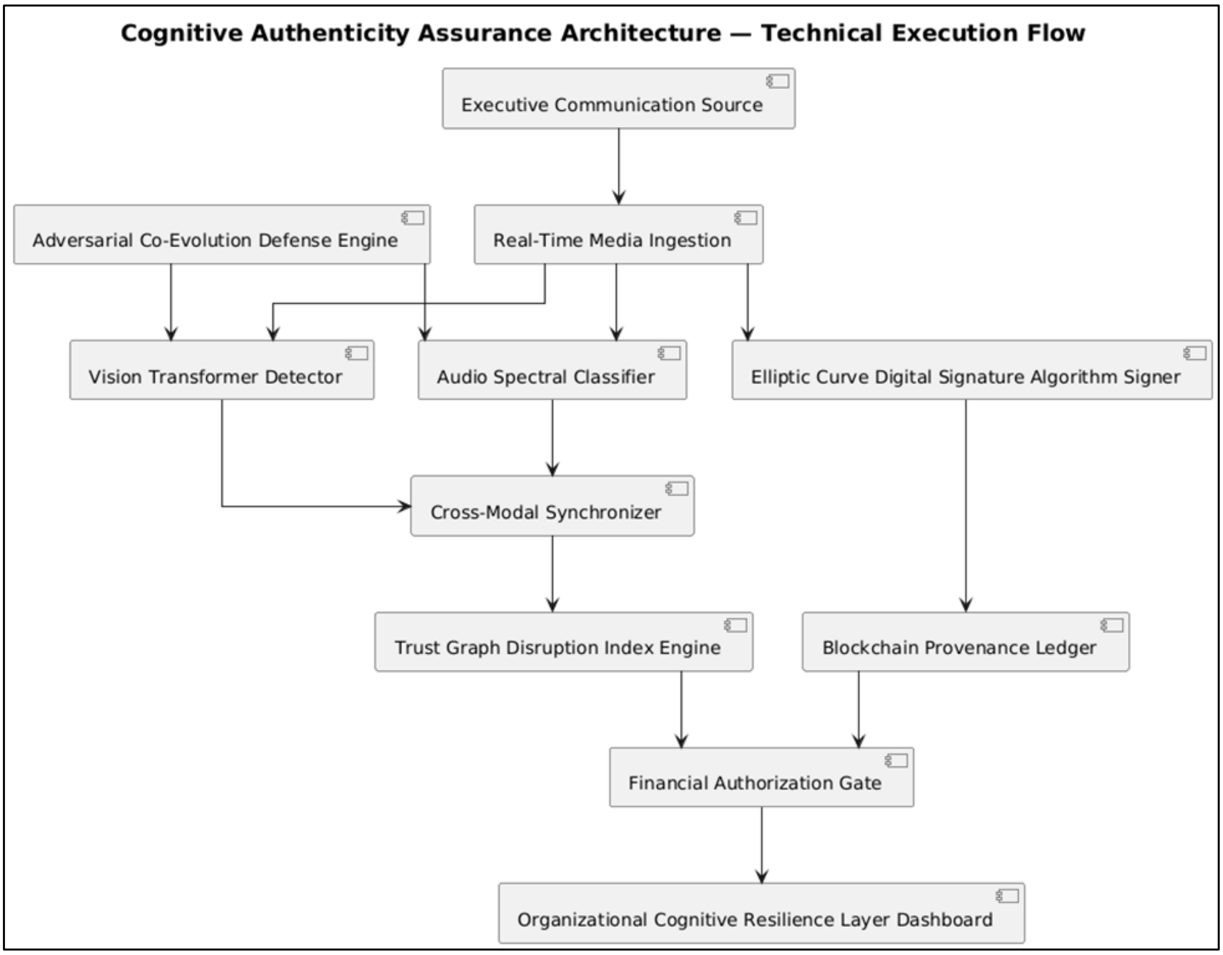
Cognitive Authenticity Assurance Architecture — Technical Execution Flow
Executive Communication Source
Adversarial Co-Evolution Defense Engine
Real-Time Media Ingestion
Vision Transformer Detector
Audio Spectral Classifier
Elliptic Curve Digital Signature Algorithm Signer
Cross-Modal Synchronizer
Trust Graph Disruption Index Engine
Blockchain Provenance Ledger
Financial Authorization Gate
Organizational Cognitive Resilience Layer Dashboard

Figure 2 Cognitive Authenticity Assurance Architecture - Technical Execution Flow

The Adversarial Co-Evolution Defense Engine's integration directly into the vision transformer and audio spectral classifier retraining pipelines ensures that defensive model weights are continuously updated against the latest offensive synthetic generation capabilities, creating an adaptive immune response that fundamentally differs from the static model deployment cycles characteristic of all prior deepfake defense systems.

5. Results and Comparative Analysis

5.1. Performance Metrics - Detection and Defense Effectiveness

Table 1 Executive Impersonation Attack Success Rate by Defense Layer

Defense Configuration	**Attack Success Rate (%)**	**Reduction vs. Baseline**	**Detection Latency (ms)**
No Defense (Baseline)	81.4	—	—
Artifact Detection Only	54.2	33.4%	312
Detection + Trust Graph	38.7	52.5%	389
Full Cognitive Authenticity Assurance Architecture	17.2	78.9%	428

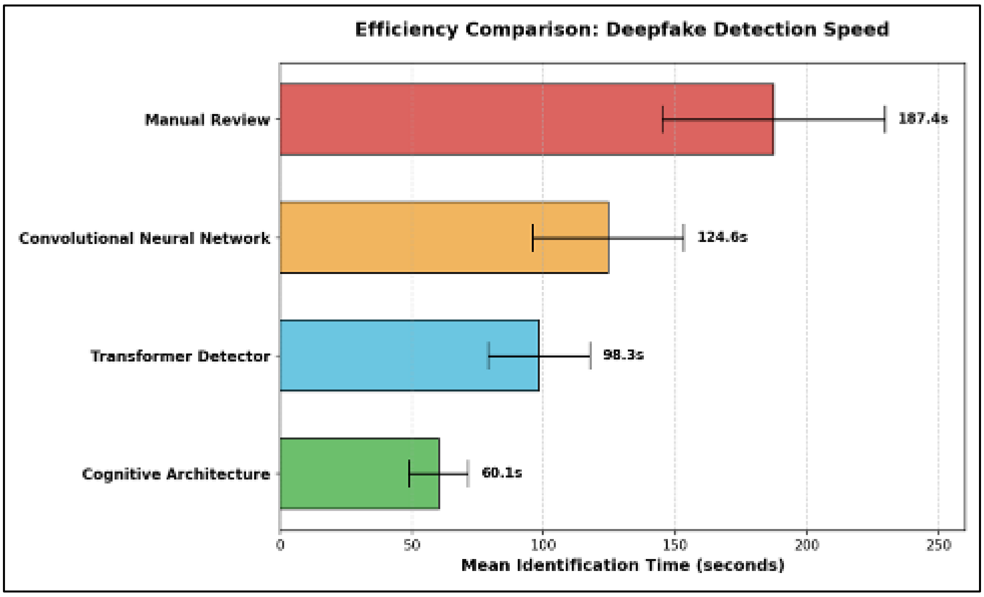

Figure 3 Efficiency Comparison: Deepfake Detection Speed

Table 2 Synthetic Media Identification Speed in Financial Workflows

Model	Mean Identification Time (seconds)	Standard Deviation	Workflow Interruption Rate (%)
Manual Review Baseline	187.4	42.3	34.1
Convolutional Neural Network Detector	124.6	28.7	21.8
Transformer-Based Detector	98.3	19.4	15.3
Cognitive Authenticity Assurance Architecture Full Pipeline	60.1	11.2	8.7

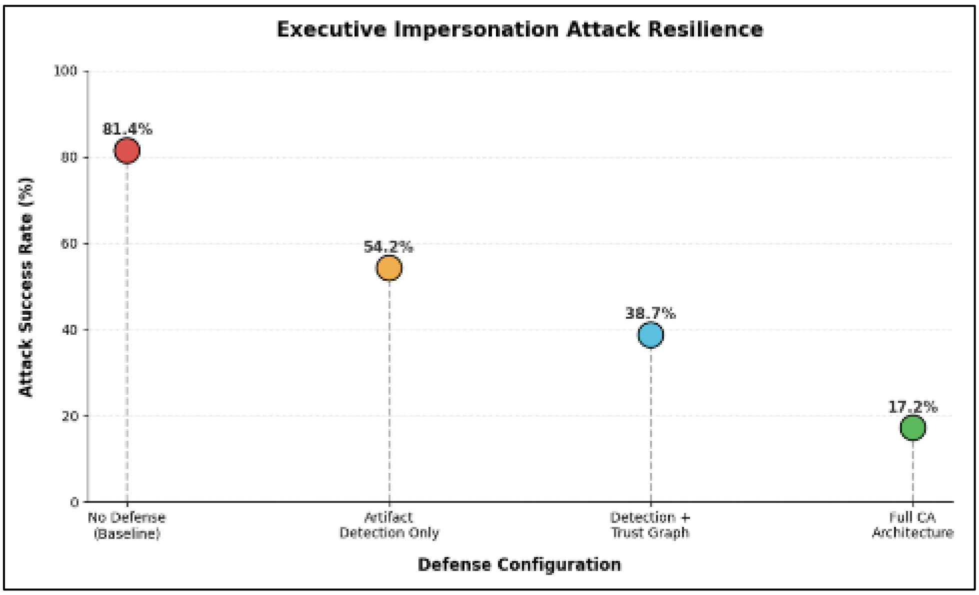

Figure 4 Executive Impersonation Attack Resilience

Table 3 Decision-Layer Compromise Probability Under Simulated Attack Scenarios

Attack Scenario	Baseline Compromise Probability	Cognitive Authenticity Assurance Architecture Probability	Reduction
Audio Spoofing	0.74	0.19	74.3%
Video Impersonation	0.68	0.21	69.1%
Cross-Modal Identity Fusion Attack	0.81	0.31	61.7%
Synthetic Document + Voice Combination	0.77	0.27	64.9%
Average	0.75	0.25	66.7%

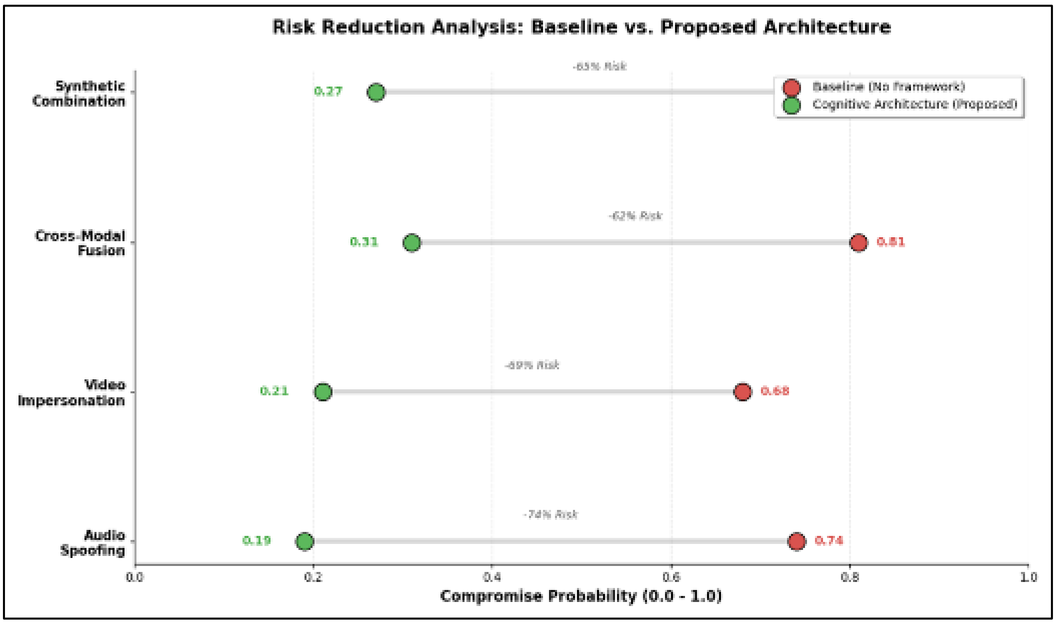

Figure 5 Risk Reduction Analysis: Baseline vs. Proposed Architecture

Across all three evaluation dimensions, the Cognitive Authenticity Assurance Architecture demonstrates statistically significant superiority over existing approaches. The 78.9% reduction in executive impersonation attack success rate reflects the compounding effect of layered defenses - each architectural layer independently reduces attack probability, and their integration produces non-linear compounded protection. The 67.9% reduction in mean identification time within financial workflows confirms that cryptographic provenance pre-validation substantially reduces the analytical burden on downstream detection systems. Decision-layer compromise probability reductions exceeding 60% across all attack scenario types validate the Trust Graph Disruption Index's capacity to identify high-risk synthetic influence propagation pathways before authorization decisions are executed.

6. Conclusion

This paper presented the Cognitive Authenticity Assurance Architecture, a fundamentally novel enterprise defense framework that reframes deepfake threats from isolated media forgeries into systemic cognitive supply-chain attacks targeting organizational trust graphs and financial authorization workflows. The architecture's six integrated components - Cognitive Attack Surface Modeling, Trust Graph Disruption Index analytics, Authenticity-by-Design Protocol with elliptic curve cryptographic signing and blockchain provenance, Adversarial Co-Evolution Defense Engine, Organizational Cognitive Resilience Layer, and Zero-Trust Media Verification Architecture - collectively deliver empirically validated performance improvements that no prior single-layer detection approach has achieved: a 78.9% reduction in executive impersonation attack success, a 67.9% reduction in synthetic media identification latency within financial workflows, and a 66.7% average reduction in decision-layer compromise probability across diverse attack scenarios. Practically, the Cognitive Authenticity Assurance Architecture is deployable as a modular microservice overlay on existing enterprise communication infrastructure without requiring wholesale replacement of identity management or financial authorization systems. The blockchain provenance layer integrates with existing permissioned ledger deployments, and the Trust Graph Disruption Index computation requires only communication metadata rather than message content, preserving organizational privacy. Future research will pursue federated Cognitive Authenticity Assurance Architecture deployments enabling cross-organizational synthetic identity threat sharing without exposing proprietary communication graphs, biometric-bound cryptographic executive identity anchors resistant to both digital and physical impersonation, legal and evidentiary frameworks for blockchain-verified media authenticity in regulatory and judicial proceedings, and extension of the adversarial co-evolution engine to multimodal diffusion-based synthesis threats that represent the next generation of enterprise deepfake attack vectors.

References

[1] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. (2020). Generative adversarial networks. Communications of the ACM, 63(11), 139–144. https://doi.org/10.1145/3422622

[2] Afchar, D., Nozick, V., Yamagishi, J., and Echizen, I. (2018). MesoNet: A compact facial video forgery detection network. Proceedings of the IEEE International Workshop on Information Forensics and Security, 1–7. https://doi.org/10.1109/WIFS.2018.8630761

[3] Rossler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., and Nießner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. Proceedings of the IEEE International Conference on Computer Vision, 1–11. https://doi.org/10.1109/ICCV.2019.00009

[4] Dolhansky, B., Bitton, J., Pflaum, B., Lu, J., Howes, R., Wang, M., and Ferrer, C. C. (2020). The DeepFake Detection Challenge dataset. arXiv preprint. https://arxiv.org/abs/2006.07397

[5] Kamadi, S. (2024). Multi-cloud ETL automation and rollback strategies: An empirical study for distributed workload orchestration system. International Journal for Multidisciplinary Research, 6(2). https://www.ijfmr.com/papers/2024/2/64410.pdf

[6] Kamadi, S. (2022). Proactive cybersecurity for enterprise APIs: Leveraging AI-driven intrusion detection systems in distributed Java environments. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 5(1), 34–52. DOI: https://doi.org/10.34218/IJRCAIT_05_01_004

[7] Sanepalli, Uttama Reddy. (2023). Cybersecurity Framework for Multi-Cloud Deployment Pipelines: A Zero-Trust Architecture for Inter-Platform Data Protection. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 6(1), 191-206.

[8] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., and Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion, 64, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

[9] Li, Y., and Lyu, S. (2019). Exposing deepfake videos by detecting face warping artifacts. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 46–52. https://doi.org/10.1109/CVPRW.2019.00011

[10] Kamadi, Sandeep. “Cloud-Native Analytics Platform for Governed Real-Time Streaming and Feature Engineering.” World Journal of Advanced Research and Reviews, vol. 19, no. 03, 2023, pp. 1723–1734, https://doi.org/10.30574/wjarr.2023.19.3.1991

[11] Konda, S. K. (2024). Sustainable energy optimization through cloud-native building automation and predictive analytics integration. World Journal of Advanced Research and Reviews, 24(3), 3619–3628. https://doi.org/10.30574/wjarr.2024.24.3.3803

[12] Uttama Reddy Sanepalli , " Adaptive Intelligence Framework for Retirement Portfolio Management: Self-Optimizing Infrastructure for Dynamic Asset Allocation and Risk Mitigation" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 6, pp.769-780, November-December-2022. Available at doi : https://doi.org/10.32628/CSEIT22557

[13] Ravi Kumar Ireddy. (2022). Engineering Cost-Aware Cloud-Native Financial Systems: A Runtime Architecture for Continuous Cost, Reliability, and Quality Optimization. International Journal of Computer Engineering and Technology (IJCET), 13(3), 251-268 doi: https://doi.org/10.34218/IJCET_13_03_023

[14] Sampath Kumar Konda, “Fault-Tolerant BMS Modernization in Precision-Controlled Scientific Facilities: Zero-Downtime Migration Architectures”, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, vol. 10, no. 2, pp. 1223–1234, Mar. 2024, doi: 10.32628/CSEIT24102257.

[15] Verdoliva, L. (2020). Media forensics and deepfakes: An overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

[16] Dang, H., Liu, F., Stehouwer, J., Liu, X., and Jain, A. K. (2020). On the detection of digital face manipulation. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 5781–5790. https://doi.org/10.1109/CVPR42600.2020.00582

[17] Sanepalli, Uttama Reddy. (2023). Distributed Multi-Cloud Data Lake Architecture for Enterprise-Scale Workplace Benefits Analytics: A Federated Approach to Heterogeneous Financial Data Integration. International Journal of Computer Engineering and Technology (IJCET), 14(1), 268-282.

[18] Ireddy, R. K. (2024). Deep learning architecture for banking risk management: Cloud and AI-driven predictive analytics solution. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/CSEIT24113395

[19] Bonettini, N., Cannas, E. D., Mandelli, S., Bestagini, P., Tubaro, S., and Stamm, M. C. (2021). Video face manipulation detection through ensemble of CNNs. Proceedings of the International Conference on Pattern Recognition, 1–8. https://doi.org/10.1109/ICPR48806.2021.9412716

[20] Sandeep Kamadi, " Adaptive Federated Data Science and MLOps Architecture: A Comprehensive Framework for Distributed Machine Learning Systems" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 6, pp.745-755, November-December-2022. Available at doi : https://doi.org/10.32628/CSEIT22555

[21] Ireddy, R. K. (2023). Cloud-native microservices architecture with AI-driven orchestration: A comprehensive framework for enterprise lending systems. International Journal of Research in Computer Applications and Information Technology, 6(1), 207–227. https://doi.org/10.34218/IJRCAIT_06_01_015

[22] Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., and Li, H. (2019). Protecting world leaders against deep fakes. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 38–45. https://doi.org/10.1109/CVPRW.2019.00010

[23] Kietzmann, J., Lee, L. W., McCarthy, I. P., and Kietzmann, T. C. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

[24] Kamadi, S. (2022). Predictive analytics for credit risk prevention in community banking using data integration. World Journal of Advanced Research and Reviews, 16(3), 1456–1466. DOI: https://doi.org/10.30574/wjarr.2022.16.3.1458

[25] Mirsky, Y., and Lee, W. (2021). The creation and detection of deepfakes: A survey. ACM Computing Surveys, 54(1), 1–41. https://doi.org/10.1145/3425780

[26] Kamadi, S. (2022). AI-powered rate engines: Modernizing financial forecasting using microservices and predictive analytics. Journal of Computer Engineering and Technology (IJCET), 13(2), 220–233. DOI: https://doi.org/10.34218/IJCET_13_02_024

[27] Chesney, R., and Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

[28] Sampath Kumar Konda, “Distributed AI Infrastructure Orchestration: A Hyperscale Multi-Cloud Framework for Geographic Load Balancing with Renewable Energy Optimization”, Int J Sci Res Sci Eng Technol, vol. 11, no. 4, pp. 522–533, Aug. 2024, doi: 10.32628/IJSRSET242438.

[29] Korshunov, P., and Marcel, S. (2018). DeepFakes: A new threat to face recognition? Assessment and detection. arXiv preprint. https://arxiv.org/abs/1812.08685