IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15681

Cognitive AI for Network Resilience: Integrating Explainable AI and Blockchain for Real-Time Cyber Threat Detection

Rachana V Murthy[1], Amrutha R[2], Ashwitha C Shetty[3], Trupthi J[4], Vinutha N[5]

Assistant Professor, CSE-IoT Cybersecurity with Blockchain, KS Institute of Technology, Bengaluru, India[1]

Student, CSE-IoT Cybersecurity with Blockchain, KS Institute of Technology, Bengaluru, India[2-5]

Abstract: The increasing complexity of cyber threats requires intelligent, adaptive, and transparent security solutions capable of real-time detection and response. This review paper examines the integration of Cognitive Artificial Intelligence (AI), Explainable AI (XAI), and blockchain technology to enhance network resilience against evolving cyberattacks. Recent research on AI-driven threat detection, XAI techniques such as SHAP and LIME, cyber resilience frameworks, and blockchain-based secure logging is analyzed to identify current advancements and research gaps. A conceptual Cognitive AI for Network Resilience (CAINR) framework is proposed, combining deep learning-based threat detection, explainable decision-making, and blockchain-enabled immutable audit trails. The study highlights the strengths and limitations of existing approaches and demonstrates that no single solution currently provides high detection accuracy, interpretability, secure logging, and automated response simultaneously. Future directions, including federated learning and reinforcement learning-based self-healing networks, are discussed. This review provides a foundation for developing trustworthy and resilient next-generation cybersecurity systems.

Keywords: Cognitive AI, Network Resilience, Explainable AI, XAI, Blockchain, Cyber Threat Detection, SHAP, LIME, Intrusion Detection Systems, Machine Learning, Cyber Resilience Framework, Zero-Day Attacks, Industrial IoT, SCADA Security, Threat Intelligence.

I. INTRODUCTION

The digital transformation of critical infrastructure, industrial systems, and organizational networks has dramatically expanded the attack surface available to cyber adversaries. Threats ranging from ransomware and advanced persistent threats (APTs) to distributed denial-of-service (DDoS) campaigns and insider attacks now target systems that underpin national economies, healthcare, transportation, and financial services. Traditional perimeter-based security models and signature-driven intrusion detection systems (IDS) are increasingly inadequate, as they cannot adapt to novel, polymorphic, or zero-day attack patterns.

Cyber resilience has emerged as the governing philosophy for modern security strategy, transcending reactive protection to encompass an organization's ability to prepare, absorb, recover, and adapt in the face of successful intrusions [1]. In parallel, Artificial Intelligence (AI) and Machine Learning (ML) have gained prominence as enabling technologies for automated threat detection, risk classification, and incident response. However, the "black-box" nature of most contemporary AI systems introduces a critical trust gap — security analysts, auditors, and regulators cannot easily validate or explain AI-generated decisions, undermining confidence in automated defenses [2].

Explainable AI (XAI) addresses this gap by providing interpretable rationales for model decisions, enabling human-in-the-loop oversight, reducing false positives, and supporting regulatory compliance [3]. Simultaneously, blockchain technology offers the cybersecurity domain immutable, decentralized, and tamper-proof audit logging capabilities that traditional centralized log management systems cannot provide. The convergence of these three paradigms — Cognitive AI for detection, XAI for transparency, and blockchain for secure accountability — represents a compelling architectural vision for next-generation resilient cybersecurity.

Despite growing individual research threads in each domain, the integrated architecture combining real-time AI-driven threat detection, explainable decision-making, and blockchain-based audit trails remains underexplored. This paper presents a systematic review and synthesis of the relevant literature, identifies critical research gaps, and proposes a conceptual framework — the Cognitive AI for Network Resilience (CAINR) architecture — as a roadmap for future research and implementation.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15681

The remainder of this paper is organized as follows: Section II provides background on fundamental concepts; Section III presents the literature review; Section IV offers comparative analysis; Section V identifies research gaps; Section VI describes the proposed framework; Section VII outlines challenges and future directions; and Section VIII concludes the paper.

II. BACKGROUND AND FUNDAMENTALS

A. Cyber Resilience

Cyber resilience is broadly defined as the ability of an organization, system, or service to anticipate, withstand, recover from, and adapt to adverse conditions caused by cyber-attacks or system failures [1]. Unlike conventional cybersecurity, which primarily focuses on preventing breaches, cyber resilience assumes that breaches will occur and prioritizes continuity of operations, rapid recovery, and systemic learning. The canonical lifecycle comprises four phases: (1) Prepare — risk assessment and defensive configuration; (2) Absorb — resistance and impact limitation during an attack; (3) Recover — restoration of normal operations; and (4) Adapt — integration of lessons learned to strengthen future resilience.

Multiple cyber resilience frameworks (CRFs) have been proposed, with the Cyber Resilience Engineering Framework (CREF) developed by MITRE [1] being the most widely adopted. Other notable frameworks include the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, COBIT, and the CERT-RMM. These frameworks structure resilience goals into measurable objectives and implementable techniques, enabling organizations to systematically assess and improve their security posture.

B. Machine Learning in Cybersecurity

Machine learning has fundamentally altered the threat detection landscape by enabling systems to learn attack patterns directly from data. Supervised learning algorithms such as Random Forest (RF) and Support Vector Machines (SVM) have demonstrated high accuracy in vulnerability classification and intrusion detection tasks. Recent work by Alshahrani and Abu Ghazalah [4] demonstrated that RF achieves 98.38% accuracy on NVD vulnerability data, outperforming SVM (97.50%) in minimizing false negatives for critical risk classes. Deep learning architectures — particularly Convolutional Neural Networks (CNNs) for packet-level traffic analysis and Long Short-Term Memory (LSTM) networks for temporal sequence modeling — further extend detection capabilities to advanced persistent threats and zero-day attack patterns.

C. Explainable Artificial Intelligence (XAI)

XAI refers to a class of AI techniques designed to provide human-interpretable explanations for model decisions [2]. Three foundational mathematical approaches dominate the XAI literature: SHAP (SHapley Additive exPlanations), which assigns each input feature a contribution score derived from cooperative game theory; LIME (Local Interpretable Model-Agnostic Explanations), which approximates complex models locally with interpretable surrogates; and LRP (Layer-wise Relevance Propagation), which backpropagates relevance scores through neural network layers to identify input features driving a prediction. In cybersecurity, XAI enables security analysts to understand why an alert was generated, which features were most indicative of malicious behavior, and how the model should be corrected when errors occur [2][3].

D. Blockchain in Cybersecurity

Blockchain technology provides a distributed, cryptographically secured ledger of records that is tamper-evident and append-only. Key properties relevant to cybersecurity include: decentralization, eliminating single points of failure in log management; immutability, ensuring forensic integrity of security event records; transparency, enabling authorized stakeholders to audit system behavior; and consensus-based verification, which prevents unauthorized modification of stored data. In cyber resilience contexts, blockchain has been explored for SCADA systems [1], supply chain security.

III. LITERATURE REVIEW

This section synthesizes research from the four uploaded primary sources and an extended body of related literature, organized thematically across cyber resilience frameworks, AI-based detection systems, XAI for cybersecurity, and blockchain security applications.

A. Cyber Resilience Frameworks and Strategies

AlHidaifi, Asghar, and Ansari [1] surveyed cyber resilience frameworks (CRFs), identifying the MITRE Cyber Resilience Engineering Framework (CREF) as the most widely adopted model. They highlighted limitations such as the

DOI: 10.17148/IJARCCE.2026.15681

absence of standardized metrics, multi-source data integration, and open-source implementations. The authors recommended integrating MITRE CREF with the NIST Cybersecurity Framework (CSF) for broader applicability.

Bejarano et al. [5] proposed incorporating Machine Learning (ML) into the NIST framework to enhance business continuity, while Hammad et al. [6] introduced an AI-based CRF for critical infrastructure using deep learning and adversarial techniques. Goldman et al. [7] and Rahman et al. [8] focused on supply chain resilience, emphasizing resilience-aware architectures and evidence-based assessment models. Strategic studies by Urciuoli [9], Efthymiopoulos [10], and Conklin [11] stressed that cyber resilience requires both technical safeguards and organizational preparedness.

B. AI and Machine Learning for Threat Detection

Alshahrani and Abu Ghazalah [4] applied Random Forest (RF) and Support Vector Machine (SVM) models to National Vulnerability Database (NVD) data for cybersecurity risk prediction. Their findings showed that Impact and Exploitability are the most influential risk indicators.

Wang et al. [1] developed an explainable intrusion detection system using SHAP, while Karn et al. [3] used SHAP and LIME to detect cryptomining attacks in Kubernetes environments. Baryannis et al. [4] examined the trade-off between predictive accuracy and interpretability, finding that interpretable models are often preferred despite lower accuracy. Aguilar et al. [5] proposed interpretable decision-tree autoencoders for anomaly detection in industrial environments.

For Industrial Control Systems (ICS), Haque et al. [6] introduced a resilience assessment framework based on the Analytical Hierarchy Process (AHP), while Li et al. [7] demonstrated that software diversification strategies can reduce the risk of zero-day attack propagation.

C. Explainable AI for Cybersecurity

Rjoub et al. [2] provided a comprehensive survey of XAI in cybersecurity, mapping XAI techniques to security applications such as intrusion detection, access control, authentication, privacy, and trust management. They also identified key evaluation criteria including transparency, understandability, responsibility, and autonomy.

Among post-hoc explanation methods, SHAP is widely adopted due to its consistency and ability to provide both local and global explanations. LIME offers efficient local explanations, whereas Layer-wise Relevance Propagation (LRP) is particularly suitable for deep neural networks. In contrast, inherently interpretable models such as decision trees and rule-based systems provide transparency but may sacrifice predictive performance.

The TRUST XAI framework [8] improves explanation reliability in Industrial IoT environments using statistical analysis and mutual information, while xAI-GAN [9] combines saliency maps, LIME, and DeepSHAP to enhance both model explainability and training effectiveness.

D. Blockchain and Distributed Security

Birnbaum et al. [2] demonstrated that blockchain combined with virtualization can significantly improve SCADA security by reducing the impact of cyberattacks. Kim and Kim [12] validated a blockchain-based customs clearance system using the MITRE ATT&CK framework, achieving improved operational efficiency while maintaining resilience against cyber threats.

Salutina et al. [11] emphasized that cybersecurity must combine technological safeguards with governance mechanisms such as regulation, staff training, auditing, and international cooperation. Their risk-management lifecycle closely aligns with cyber resilience principles.

E. Real-Time Monitoring and Threat Intelligence

Research by the Ponemon Institute [3] identified automation as a key factor in reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). AI-driven analytics, orchestration platforms, and Security Information and Event Management (SIEM) systems form the foundation of modern threat intelligence architectures.

CyGraph [4], developed by MITRE, enhances cyber resilience by correlating multi-source security events into a unified dependency model, enabling both proactive and reactive defense strategies. Additionally, threat modeling approaches such as STRIDE and PASTA have proven effective for cyber resilience assessment, while Microsoft's five-phase threat

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15681

modeling process provides a practical framework for identifying and mitigating security risks across enterprise and industrial environments.

Author(s) / Paper	Year	Methodology	Dataset / Domain	Key Findings	Limitations
G. Rjoub et al., *A Survey on Explainable Artificial Intelligence for Cybersecurity*	2023	Systematic survey of XAI techniques in cybersecurity	Cybersecurity, Network Security, Threat Detection	XAI improves transparency, trust, and interpretability of AI-based security systems.	Lack of standardized XAI frameworks and limited real-world deployment.
M. Mishra et al., *AI for Cybersecurity Threat Detection: A Machine Enabled Computing Perspective*	2025	AI, Deep Learning, Reinforcement Learning, Anomaly Detection	Cyber Threat Detection	AI significantly improves threat prediction, anomaly detection, and automated response.	Ethical concerns, model bias, and explainability challenges remain unresolved.
S. Dwivedi et al., *Artificial Intelligence in Cyber Defense: A Study of Modern Security Solutions*	2025	Machine Learning, Deep Learning, IDS, Automated Incident Response	Cyber Defense Systems	AI enhances intrusion detection and automated response mechanisms.	Vulnerable to adversarial attacks and requires large volumes of quality data.
D. I. Christine and M. Thinyane, *Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries*	2020	Comparative analysis of national cybersecurity strategies	National Cybersecurity and Resilience	Countries with mature cybersecurity programs exhibit stronger resilience frameworks.	Limited operational implementation of resilience strategies in many countries.
T. Y. Salutina et al., *Cybersecurity Risk Management and Monitoring of Digital Development*	2024	Risk assessment and monitoring framework	Digital Enterprises and Organizations	Effective risk management improves cybersecurity posture and business continuity.	Focuses on organizational policies rather than advanced AI-based defense mechanisms.
T. Munusamy and T. Khodadadi, *Enhancing Cyber Resilience Management*	2023	Exploratory analysis of resilience attributes	Cyber Resilience Management	Identifies seven resilience attributes: Readiness, Reliability, Resistance, Rebound, Robustness, Reflectiveness, and Rationale.	Conceptual framework lacks empirical validation in operational environments.
A. Hoenig et al., *Explainable AI for Cyber-Physical Systems:*	2024	Comprehensive review of XAI in CPS	Cyber-Physical Systems (CPS)	XAI enhances trust, accountability, cybersecurity, and resilience in CPS.	Lack of standardized evaluation metrics and practical implementations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15681

Author(s) / Paper	Year	Methodology	Dataset / Domain	Key Findings	Limitations
Issues and Challenges					
R. Alghanmi et al., *HuntSmart: Hypothesis-Driven Threat Hunting Using GenAI*	2025	SecureBERT, Generative AI, MITRE ATT&CK mapping	Cyber Threat Intelligence (CTI)	Automates TTP extraction, hypothesis generation, and threat prioritization.	Dependent on quality of CTI data and GenAI-generated outputs may require validation.
K. Ahi and S. Valizadeh, *LLMs and Generative AI in Cybersecurity and Privacy*	2025	Survey of LLMs, GenAI, XAI, and defensive strategies	AI-driven Cybersecurity	LLMs provide both offensive and defensive cybersecurity capabilities.	High risk of AI-generated malware and misuse of generative models.
A. Kumar and K. Guleria, *Leveraging Machine Learning Algorithms for Threat Detection*	2024	Logistic Regression, Decision Tree, and Random Forest	AI-Enhanced Cybersecurity Dataset	Random Forest achieved the highest accuracy and effectiveness in threat detection.	Limited evaluation on real-time large-scale network environments.
H. Lee et al., *SoK: Demystifying Cyber Resilience Quantification in CPS*	2022	Systematization of cyber resilience metrics	Cyber-Physical Systems	Proposes resilience quantification using R4 metrics (Robustness, Rapidity, Redundancy, and Resourcefulness).	Cyber resilience measurement remains immature and lacks universal metrics.
V. P. S. and M. J. Nene, *Zero-Knowledge Range Proofs and Blockchain Integration for Enhancing SCADA Data Security*	2025	Hyperledger Fabric and Zero-Knowledge Proofs (Bulletproofs)	SCADA Systems	Blockchain and ZKRP improve integrity, privacy, and tamper resistance of industrial systems.	Additional computational overhead and scalability concerns for large deployments.

IV. RESEARCH GAPS IDENTIFIED

The systematic review of existing literature reveals the following critical research gaps in the current state of cybersecurity and network resilience research:

A. Lack of Integrated Architectures

While individual components — AI detection, XAI transparency, and blockchain logging — have been studied in isolation, there is a significant absence of unified architectural frameworks that coherently combine all three. The majority of reviewed papers address at most two of these three dimensions, leaving the integration challenge largely unaddressed. Specifically, the feedback loop between XAI explanations, blockchain-logged incidents, and adaptive ML model retraining has not been formally studied.

B. Opacity of AI Decision-Making in Production Systems

Despite the growing body of XAI research, Rjoub et al. [2] observe that XAI deployment in live cybersecurity operations remains limited. Most enterprise security platforms still rely on black-box ML models, creating accountability gaps that are increasingly problematic under emerging AI governance regulations. The accuracy-interpretability trade-off, while acknowledged, lacks principled resolution in high-stakes real-time detection scenarios.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15681

C. Centralized Log Management Vulnerabilities

Traditional SIEM systems and centralized log repositories represent high-value targets for sophisticated adversaries. Altering or destroying logs is a documented attacker technique for covering intrusion evidence. Current literature offers limited exploration of blockchain-anchored SIEM integration, despite blockchain's well-demonstrated tamper-resistance properties.

D. Insufficient Real-Time Detection Capability

Many evaluated ML and XAI methods are validated on static benchmark datasets rather than streaming, high-velocity network traffic. The latency introduced by SHAP computations or blockchain consensus mechanisms can be prohibitive for sub-second response requirements in SCADA, power grid, and financial trading environments. Real-time performance validation under adversarial conditions is largely absent from the reviewed literature.

E. Limited Adaptability Against Zero-Day and Evolving Attacks

Static trained models suffer performance degradation against concept drift — the gradual evolution of attack patterns over time. Reinforcement learning-based adaptive detection is promising [12] but computationally expensive and difficult to stabilize in dynamic environments. Few reviewed frameworks incorporate mechanisms for continuous model updating without full retraining, a critical requirement for practical deployment.

F. Privacy and Federated Learning Gaps

Cyber threat intelligence sharing across organizations is constrained by privacy, competitive, and regulatory concerns. Federated learning frameworks that enable collaborative model training without raw data exchange are emerging but remain underexplored in the cyber resilience context. The intersection of federated XAI and distributed blockchain logging is an entirely open research area [2].

G. Inadequate ICS and CPS Coverage

Industrial Control Systems, Cyber-Physical Systems, and IoT environments present unique constraints — limited computational resources, legacy protocol dependence, and high availability requirements — that render general-purpose cybersecurity solutions inapplicable. The reviewed literature identifies this as a consistently underserved domain, particularly regarding XAI explainability in resource-constrained embedded systems.

V. PROPOSED REVIEW INSIGHTS: THE CAINR CONCEPTUAL FRAMEWORK

Based on the synthesis of reviewed literature and identified gaps, this paper proposes the Cognitive AI for Network Resilience (CAINR) framework, a conceptual integrated architecture designed to address the limitations of existing approaches. CAINR is structured around four interconnected functional layers.

A. Layer 1: Real-Time Threat Detection (Cognitive AI Engine)

The detection layer employs a hybrid deep learning architecture combining CNN modules for spatial feature extraction from packet payloads and network flow representations, with LSTM networks for capturing temporal attack progression sequences. This ensemble approach enables detection of both instantaneous anomalies and persistent, slow-burn APT campaigns. For structured vulnerability data, Random Forest classifiers — validated by Alshahrani and Abu Ghazalah [4] at 98.38% accuracy — serve as high-speed risk classifiers. Continuous learning mechanisms using streaming data adapters (Apache Kafka or similar) enable the detection engine to update incrementally, reducing performance degradation from concept drift.

B. Layer 2: Explainability and Decision Transparency (XAI Gateway)

Every detection alert generated by the Cognitive AI Engine is passed through an XAI Gateway before reaching human analysts or automated response systems. SHAP is applied for global model interpretation and feature attribution at the organizational level, while LIME provides fast local explanations for individual incident alerts. LRP is reserved for deep neural network components requiring neuron-level attribution. The XAI Gateway generates human-readable natural language summaries of each decision using the nine desirability criteria framework proposed by Rjoub et al. [2]:

C. Layer 3: Blockchain-Anchored Immutable Audit Trail

All security events, XAI-generated explanations, analyst actions, and automated responses are hashed and written to a permissioned blockchain ledger (e.g., Hyperledger Fabric) as tamper-proof records. The blockchain layer serves three distinct security functions: (1) forensic integrity — ensuring that incident logs cannot be altered post-hoc by adversaries or insider threats; (2) cross-organizational threat intelligence sharing — enabling secure, verifiable sharing of anonymized threat indicators without revealing sensitive network topology; and (3) compliance and auditing — providing regulators,

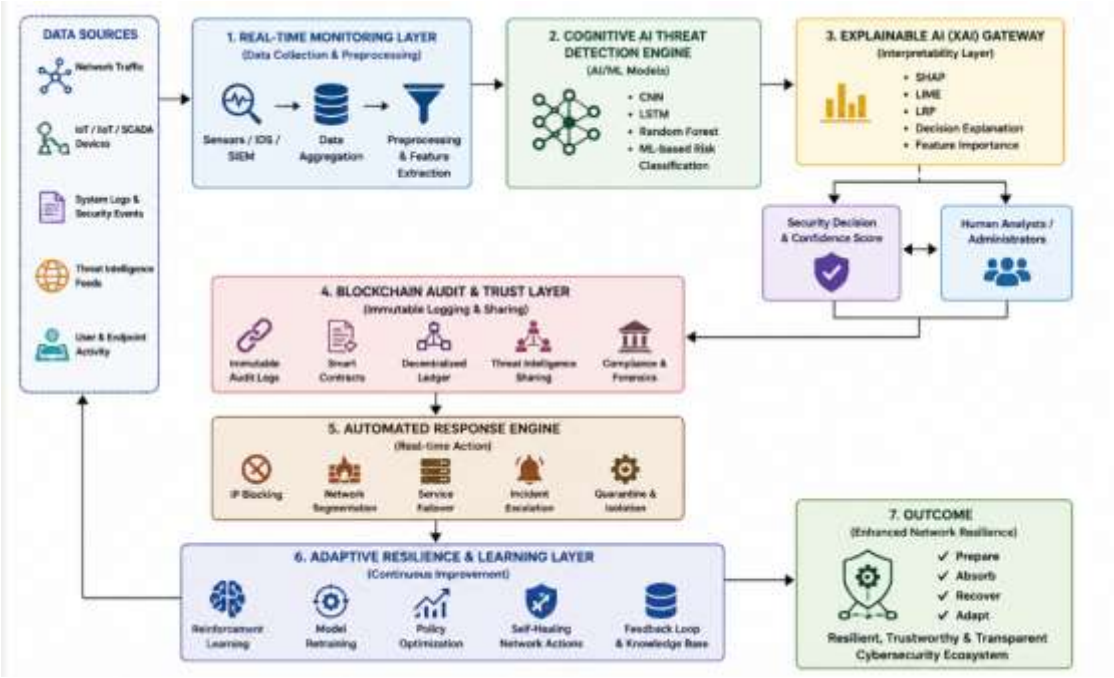
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15681

auditors, and incident response teams with a verifiable, chronologically ordered record of all security decisions. Smart contracts automate log validation and enforce retention policies, while federated access control ensures organizational privacy.



D. Layer 4: Automated Response and Adaptive Resilience

The response layer implements the cyber resilience lifecycle (Prepare-Absorb-Recover-Adapt) through a reinforcement learning-based policy engine. Drawing on the ETTR controller approach for microgrid resilience [5] and SDN-based recovery for power systems [6], the response engine selects optimal countermeasures from a policy library based on threat classification, impact assessment, and current network state. Automated responses include network segmentation, IP blocking, service failover activation, and alert escalation to human operators for high-uncertainty scenarios. The adaptation component continuously updates both the detection ML models and the response policy based on blockchain-logged incident outcomes, closing the cyber resilience feedback loop.

E. Framework Workflow

The CAINR workflow operates as follows: (1) Network sensors and SIEM collectors feed real-time event streams to the Cognitive AI Engine; (2) the engine classifies events and generates risk scores; (3) the XAI Gateway enriches each classification with feature attribution explanations and confidence estimates; (4) all events and explanations are written to the blockchain audit trail; (5) high-confidence threats trigger automated response actions via the policy engine; (6) low-confidence and novel events are escalated to human analysts with XAI-generated context; (7) analyst decisions and outcomes are logged to blockchain; and (8) the adaptation module updates models and policies based on accumulated experience. This loop embodies the Prepare-Absorb-Recover-Adapt resilience lifecycle at an operational cadence.

VI. CONCLUSION

This review paper presents a comprehensive synthesis of research at the intersection of Cognitive AI, Explainable Artificial Intelligence (XAI), blockchain technology, and cyber resilience. The reviewed literature on cyber resilience frameworks, ML-based intrusion detection, XAI methodologies, SCADA/ICS security, and blockchain auditing demonstrates substantial progress within individual domains, while significant integration gaps remain.A key finding is that no existing solution simultaneously provides high-accuracy real-time threat detection, interpretable decision-making, tamper-proof audit logging, and adaptive response capabilities. While ML-based systems achieve detection accuracies exceeding 98%, they often lack transparency. XAI techniques improve interpretability but remain limited in real-world deployment, whereas blockchain-based logging ensures forensic integrity but is rarely integrated with AI-driven cybersecurity frameworks.To address these challenges, the proposed CAINR framework integrates deep learning-based threat detection, SHAP/LIME-powered explainability, permissioned blockchain audit trails, and reinforcement learning-

DOI: 10.17148/IJARCCE.2026.15681

based adaptive response. This architecture operationalizes the cyber resilience lifecycle—Prepare, Absorb, Recover, and Adapt—while maintaining human oversight through transparent decision explanations.

The review highlights the need for future cybersecurity solutions that combine intelligent detection, explainable decision-making, and immutable accountability. Such integration is essential for building trustworthy, resilient, and adaptive network security systems capable of addressing next-generation cyber threats.

REFERENCES

[1] G. Rjoub, J. Bentahar, O. Abdel Wahab, R. Mizouni, A. Song, R. Cohen, H. Otrok, and A. Mourad, "A Survey on Explainable Artificial Intelligence for Cybersecurity," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 5115–5140, Dec. 2023, doi: 10.1109/TNSM.2023.3282740.

[2] M. Mishra, R. Bokka, R. R. Pradhan, and K. Agrawalla, "AI for Cybersecurity Threat Detection: A Machine Enabled Computing Perspective," in *Proc. International Conference*, 2025, pp. 202–206.

[3] S. Dwivedi, N. Varish, and Priyanka, "Artificial Intelligence in Cyber Defense: A Study of Modern Security Solutions," in *2025 International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI)*, 2025, pp. 813–818, doi: 10.1109/IC3ECSBHI.2025.XXXXXXX.

[4] D. I. Christine and M. Thinyane, "Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries," in *2020 IEEE Intl Conf. on Dependable, Autonomic and Secure Computing, Pervasive Intelligence and Computing, Cloud and Big Data Computing, and Cyber Science and Technology Congress (DASC-PICom-CBDCom-CyberSciTech)*, 2020, pp. 71–78, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00027.

[5] T. Y. Salutina, G. P. Platunina, and I. A. Frank, "Cybersecurity, Risk Management and Monitoring of Digital and Infocommunication Development of the Company," in *2024 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, 2024, pp. 1–5, doi: 10.1109/EMCTECH63049.2024.10741653.

[6] T. Munusamy and T. Khodadadi, "Enhancing Cyber Resilience Management: Exploring Attributes in the Context of Security and Resilience," in *2023 IEEE 30th Annual Software Technology Conference (STC)*, 2023, pp. 2–7, doi: 10.1109/STC58598.2023.00006.

[7] A. Hoenig, K. Roy, Y. T. Acquaah, S. Yi, and S. S. Desai, "Explainable AI for Cyber-Physical Systems: Issues and Challenges," *IEEE Access*, vol. 12, pp. 73113–73140, 2024, doi: 10.1109/ACCESS.2024.3395444.

[8] R. Alghanmi, S. Kulaibi, J. Alghamdi, E. Bahashwan, and A. Aeshmawi, "HuntSmart: Hypothesis-Driven Threat Hunting Using GenAI," in *2025 International Conference on Innovation in Artificial Intelligence and Internet of Things (AIIT)*, 2025, doi: 10.1109/AIIT63112.2025.11082910.

[9] K. Ahi and S. Valizadeh, "Large Language Models (LLMs) and Generative AI in Cybersecurity and Privacy: A Survey of Dual-Use Risks, AI-Generated Malware, Explainability, and Defensive Strategies," 2025.

[10] A. Kumar and K. Guleria, "Leveraging Machine Learning Algorithms for Threat Detection Using AI-Enhanced Cybersecurity Datasets," in *Proc. 2024 4th International Conference on Technological Advancements in Computational Sciences*, 2024, pp. 483–488.

[11] H. Lee, S. Kim, and H. K. Kim, "SoK: Demystifying Cyber Resilience Quantification in Cyber-Physical Systems," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2022, pp. 178–183.

[12] V. P. S. and M. J. Nene, "Zero-Knowledge Range Proofs and Blockchain Integration for Enhancing SCADA Data Security," in *2025 International Conference on Data Science, Agents, and Artificial Intelligence (ICDSAAI)*, Chennai, India, Mar. 2025, pp. 1–6.

