INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 13, issue 03 (2026)

The Convergence of Blockchain and Deep Learning in Securing Cyber-Physical Systems and FinTech Infrastructures: A Multidimensional Analysis of Threats, Mitigation, and Future Paradigms

Eugiene J. Montgomery
Global Institute for Cyber Security Research, University of Melbourne, Australia

Abstract: The rapid digitalization of critical infrastructures and financial services has necessitated a paradigm shift in cybersecurity strategies. Cyber-Physical Systems (CPS), the Internet of Medical Things (IoMT), and Financial Technology (FinTech) platforms are increasingly susceptible to complex vulnerabilities that transcend traditional security boundaries. This research provides an exhaustive investigation into the integration of Blockchain and Deep Learning-specifically Transformer-CNN frameworks and Auto-Encoders-to mitigate emerging threats such as data injection, man-in-the-middle attacks, and sophisticated fraud. By synthesizing current literature on Industrial Control Systems (ICS) and SCADA vulnerabilities, the paper establishes a theoretical foundation for decentralized, cognitively autonomous security architectures. The study explores the efficacy of multilevel intrusion detection, trusted token authentication, and post-quantum blockchain considerations. Findings indicate that while Deep Learning offers superior anomaly detection in high-dimensional time-series data, Blockchain provides the immutable ledger necessary for decentralized trust. The convergence of these technologies facilitates a self-healing security ecosystem capable of addressing the challenges of multi-cloud environments and real-time digital payment fraud. The paper concludes with a critical assessment of the trade-offs between system performance and cryptographic robustness in the era of software-defined networks.

Keywords: Cyber-Physical Systems, Blockchain, Deep Learning, FinTech Security, Anomaly Detection, Industrial Control Systems, Data Privacy.

Introduction

The modern technological landscape is defined by the seamless integration of computational algorithms and physical processes, a phenomenon broadly categorized as Cyber-Physical Systems (CPS). From smart power grids and automated manufacturing to the intricate networks of the Internet of Medical Things (IoMT), these systems form the backbone of contemporary civilization. However, as noted in the comprehensive reviews provided by MDPI (2025), this connectivity introduces a vast attack surface, rendering critical infrastructures vulnerable to an array of cyber threats that were previously inconceivable. The transition from isolated industrial loops to networked environments has exposed legacy systems, such as Supervisory Control and Data Acquisition (SCADA) networks, to vulnerabilities that traditional firewalls and signature-based detection systems can no longer adequately address.

The complexity of these threats is multifaceted. In the realm of industrial transformation, security and privacy issues are not merely technical glitches but represent existential threats to public safety and economic stability (Anusha et al., 2023). Attacks against Industrial Control Systems (ICS) often target the very intersection of the digital and physical, where a single packet manipulation can result in catastrophic physical damage (Makrakis et al., 2021). Real-life security incidents have demonstrated that the fragility of critical infrastructure is a global concern, requiring a deeper technical analysis of how incidents unfold and how they can be preempted (IEEE, 2025).

In parallel, the financial sector has undergone a radical transformation through the rise of FinTech. Digital wallets, mobile payment systems, and decentralized finance (DeFi) platforms have democratized access to capital but have also invited sophisticated fraud mechanisms. The integration of blockchain and FinTech offers significant opportunities for enhancing transaction security, yet it also introduces new challenges regarding performance, scalability, and the security of the underlying consensus mechanisms (Gupta & Dhillon, 2020; Castillo, 2021). The challenge lies in creating a system that is both secure and efficient enough to handle the millisecond-latency requirements of modern digital payments.

Despite significant advancements, a literature gap remains in the holistic integration of cognitive autonomy and decentralized trust. Most current research focuses either on machine learning for anomaly detection or blockchain for data integrity. There is a pressing need for a unified framework that utilizes deep learning for "intelligence" and blockchain for "truth." This research addresses this gap by analyzing how blockchain-assisted deep learning models-particularly those utilizing Transformer-CNN architectures-can provide real-time fraud detection and robust defense for CPS (Fnu et al., 2026). By examining the latest trends in cloud computing and software-defined networks, this paper elucidates the path forward for securing the digital age.

Methodology

The methodology employed in this research is rooted in a systematic qualitative and theoretical synthesis of current state-of-the-art security architectures. The study begins by deconstructing the architectural vulnerabilities of CPS and FinTech platforms. This involves a technical analysis of real-life security incidents to identify common attack vectors such as distributed denial-of-service (DDoS), false data injection attacks (FDIA), and unauthorized access through compromised SCADA nodes (IEEE, 2025; Yang et al., 2021).

A primary focus of the methodology is the evaluation of Deep Learning (DL) strategies for anomaly detection. We examine the utility of Auto-Encoders in learning the "normal" operational states of industrial sensors. By training these models on vast datasets of time-series information, we can identify deviations that indicate either system failure or malicious intervention (MDPI, 2025; Luo et al., 2021). The methodology further explores the application of multilevel intrusion detection approaches (Ling et al., 2025), which categorize threats at the network, transport, and application layers, thereby reducing the false-positive rates that often plague traditional machine learning models.

The integration of Blockchain technology is analyzed through the lens of decentralized authentication and non-repudiation. We evaluate various consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), to determine their suitability for high-stakes industrial environments where latency is a critical factor (Gervais et al., 2016). The research investigates the use of "Trusted Token Authentication Services" (TTAS) as a means of securing SCADA networks within energy management systems, replacing static passwords with dynamic, blockchain-verified tokens (Yang et al., 2021).

Furthermore, the methodology incorporates a detailed analysis of the Transformer-CNN framework for real-time fraud detection in digital payments. Unlike standard neural networks, the Transformer architecture utilizes self-attention mechanisms to weigh the importance of different transactions in a sequence, while the CNN component extracts local spatial features from transaction metadata (Fnu et al., 2026). This dual-pronged approach is evaluated against traditional fraud detection methods to measure improvements in speed and accuracy. Finally, the study considers the legal and regulatory frameworks surrounding blockchain, arguing for standardized protocols to facilitate cross-border security cooperation (Hammi et al., 2022).

Theoretical Elaboration: The Nature of Modern Cyber Threats

To understand the necessity of combined blockchain and deep learning solutions, one must first appreciate the sophistication of modern cyber vulnerabilities. As detailed in recent comprehensive reviews (MDPI, 2025), vulnerabilities in cyber-physical systems often stem from the "air-gap" myth-the belief that because a system is not directly connected to the public internet, it is safe. Stuxnet and subsequent attacks proved that physical access points, maintenance ports, and supply chain compromises provide ample entry for malicious code. In the context of the Internet of Medical Things (IoMT), these vulnerabilities take on a biological dimension. Compromised medical devices, such as insulin pumps or pacemakers, can be manipulated via cyber-physical attacks, leading to direct harm to patients (Anusha et al., 2023).

The threats are not merely external. Insider threats and misconfigured multi-cloud environments provide fertile ground for data breaches. Mohammad (2021) emphasizes that as organizations migrate their critical data to the cloud, the traditional perimeter defense model collapses. Encryption techniques and access control mechanisms must evolve to be data-centric rather than network-centric. The complexity of these environments is further increased by Software-Defined Networking (SDN), which, while offering flexibility, introduces a centralized controller that acts as a "single point of failure" or a high-value target for attackers (Hassan et al., 2019).

In the FinTech sector, the threats are primarily driven by economic incentives. Digital wallets like MOMO face constant pressure from phishing, social engineering, and technical exploits targeting the mobile interface (Tran, 2020). E-commerce security challenges often involve the interception of payment tokens or the creation of fraudulent accounts

using stolen identities (Osita et al., 2022). These attacks are increasingly automated, utilizing botnets and basic AI to probe for weaknesses in transaction logic. Therefore, the defense must also be automated and intelligent, leading to the necessity of deep learning-based models for cognitive autonomy (Purdue, 2025).

The Role of Deep Learning in Anomaly Detection

Deep learning represents the "brain" of the modern security architecture. Traditional Intrusion Detection Systems (IDS) rely on pre-defined signatures-essentially a database of known attack patterns. However, modern attackers utilize "zero-day" exploits that have no signature. This is where anomaly detection becomes vital. By using neural networks to model the "steady state" of a system, any deviation can be flagged as a potential threat (IEEE, 2025).

Auto-Encoders are particularly effective for this task. An Auto-Encoder is a type of neural network that learns to compress input data into a lower-dimensional representation and then reconstruct it back to the original form. When the network is trained only on "normal" operational data, its ability to reconstruct "anomalous" data is poor. This reconstruction error serves as a high-fidelity signal for detecting subtle anomalies in complex CPS environments (MDPI, 2023). For example, in a water treatment plant, an Auto-Encoder might monitor the relationship between pump speed, flow rate, and chemical levels. A hacker attempting to slowly increase chemical dosage would be detected because the resulting data pattern would differ from the "compressed" logic learned by the model.

However, time-series data in CPS and FinTech is often non-linear and highly volatile. Simple neural networks struggle with long-term dependencies. This has led to the adoption of Deep Learning for time-series forecasting, which allows systems to predict future states and identify anomalies when the actual state deviates from the prediction (Big Data, 2025). Furthermore, cognitive autonomy in autonomous systems requires the model to not only detect an attack but to understand its context. Deep learning models for cybersecurity intelligence allow autonomous vehicles or drones to distinguish between a sensor malfunction and a malicious spoofing attack (Purdue, 2025).

Blockchain as a Decentralized Trust Mechanism

If deep learning is the "intelligence," blockchain is the "integrity." The fundamental challenge in decentralized systems is achieving "Consensus"-a way for all participants to agree on the state of the ledger without a central authority. Bonneau et al. (2015) outlined the early challenges of Bitcoin and cryptocurrencies, noting that the security of the system depends on the economic cost of an attack. In a blockchain, every transaction is cryptographically linked to the previous one, creating an immutable chain.

For FinTech and digital payments, blockchain eliminates the "double-spending" problem and provides a transparent audit trail. Castillo (2021) argues that blockchain's primary contribution to cybersecurity is the decentralization of data. In a traditional centralized database, an attacker who gains administrative access can alter or delete records without detection. In a blockchain, altering a single record would require the re-computation of all subsequent blocks across a majority of the network nodes, an act that is computationally and economically unfeasible for most adversaries (Gervais et al., 2016).

In Industrial Internet of Things (IIoT) environments, blockchain can be used to secure device identities. Instead of a central server verifying every sensor, the sensors can use a blockchain-based authentication service. Yang et al. (2021) demonstrated that using a Trusted Token Authentication Service (TTAS) significantly reduces the risk of unauthorized commands being sent to SCADA controllers. Each command is signed and verified against a blockchain, ensuring that even if an attacker gains access to the network layer, they cannot issue valid control commands without the corresponding cryptographic tokens.

The Convergence: Blockchain-Assisted Transformer CNNs

The cutting edge of this field is the integration of these two technologies into a single framework. Fnu et al. (2026) proposed a "Blockchain-Assisted Transformer CNN Framework" specifically designed for real-time digital payment fraud detection. This approach addresses the limitations of both technologies when used in isolation. Blockchain provides the secure data source-a decentralized ledger of all past transactions-ensuring that the training data for the AI has not been tampered with.

The Transformer component of the model uses self-attention mechanisms to analyze the temporal relationships between transactions. For example, if a user typically makes small purchases in London and suddenly initiates a large transfer from a new device in a different country, the self-attention layer will highlight this anomaly by comparing it to the user's

historical transaction "attention" map. Simultaneously, the CNN component processes the metadata-IP addresses, device fingerprints, and geographic data-extracting spatial features that indicate a fraudulent setup.

This convergence also solves the "Black Box" problem of AI. One of the major criticisms of deep learning in security is the lack of transparency; it is often difficult to explain why a model flagged a certain event as an attack. By recording the AI's decision-making parameters and the raw data inputs on a blockchain, organizations can perform a "security audit" of the AI itself. This ensures that the system is not only autonomous but also accountable (Kuznetsov et al., 2024).

Results

The synthesis of empirical data across the cited studies reveals several critical findings regarding the efficacy of integrated security models. In CPS environments, the transition to multilevel intrusion detection has resulted in a marked decrease in false-positive rates. Ling et al. (2025) found that by segmenting the detection process-first filtering common network noise and then applying deep learning to the remaining suspicious packets-system accuracy improved by over 15% compared to single-layer models.

In the FinTech sector, the implementation of blockchain-assisted fraud detection has shown significant promise in reducing the "time-to-detection." Traditional bank fraud detection can take hours or even days to confirm a suspicious pattern. However, the Transformer-CNN framework, when operating on a high-performance blockchain, can identify and block fraudulent transactions in sub-second intervals (Fnu et al., 2026). The use of optimal feature selection-identifying the most relevant data points for the model-was shown to be a critical factor in maintaining this speed without sacrificing security.

Regarding SCADA and industrial security, the results of implementing Trusted Token Authentication (TTAS) were particularly noteworthy. In simulated attacks on energy management systems, the TTAS prevented 100% of unauthorized command injections, even when the attacker had successfully breached the primary network perimeter (Yang et al., 2021). This confirms that moving trust to a decentralized token-based system is far more effective than relying on the inherent security of the communication protocol itself.

Furthermore, the review of wireless sensor network (WSN) coverage optimization via machine learning indicated that security is often a trade-off with energy efficiency (Annals of Operations Research, 2023). However, by using deep learning to predict sensor failures and potential attack paths, network longevity was increased by 20% while simultaneously improving the detection of physical tampering. These results suggest that the integration of intelligence into the network layer does not necessarily lead to resource exhaustion if the models are properly optimized.

Discussion

While the integration of Blockchain and Deep Learning offers a formidable defense, the "Discussion" must address the significant hurdles to widespread adoption. The foremost challenge is the "Trilemma" of blockchain: balancing security, scalability, and decentralization. High-frequency digital payment systems require thousands of transactions per second (TPS). Most public blockchains cannot yet support this volume without centralization or significant latency (Gervais et al., 2016). Therefore, many industrial applications are forced to use private or consortium blockchains, which, while faster, reintroduce certain elements of centralized risk.

The second major challenge is the computational cost of Deep Learning. Training Transformer models requires immense GPU power and vast amounts of data. In an IoMT context, where devices are often battery-powered and have limited processing capabilities, running complex neural networks locally is impossible. This necessitates "Edge Computing" architectures where the processing is done at a nearby gateway, but this introduces its own set of security vulnerabilities during the data transfer process (Hassan et al., 2019).

There is also the emerging threat of "Adversarial Machine Learning." Attackers are now using their own AI models to "probe" a defense AI, finding the specific edge cases that allow an attack to pass undetected. If an attacker knows that a system uses an Auto-Encoder for anomaly detection, they can design "adversarial noise"-slight manipulations of the data that are invisible to the human eye but cause the neural network to misclassify the attack as normal behavior (MDPI, 2023).

Ethical and regulatory considerations also loom large. As Hammi et al. (2022) point out, the global nature of blockchain conflicts with national data sovereignty laws, such as the GDPR in Europe. The "right to be forgotten" is fundamentally at odds with the "immutability" of a blockchain. Furthermore, as AI takes over autonomous security decisions, questions

of liability arise. If an AI-driven security system erroneously shuts down a power grid during a perceived attack, who is responsible? The developer of the AI, the operator of the grid, or the entity that provided the training data?

Finally, the specter of Quantum Computing threatens the very foundations of current cryptographic standards. Most blockchains rely on Elliptic Curve Cryptography (ECC), which can be broken by a sufficiently powerful quantum computer. While post-quantum blockchain research is underway, the migration of existing infrastructures to quantum-resistant algorithms will be a massive undertaking (Castillo, 2021).

Future Scope and Recommendations

The future of cybersecurity lies in the evolution of "Proactive and Predictive" systems. Rather than reacting to an attack, future architectures will use deep learning to simulate millions of potential attack scenarios in a "Digital Twin" environment, identifying vulnerabilities before they exist in the real world. Blockchain will evolve into a more fluid "Distributed Ledger Technology" (DLT) capable of supporting cross-chain interoperability, allowing a medical device on one network to securely communicate with a hospital database on another without manual intervention.

For researchers and practitioners, the following recommendations are provided:

1. Prioritize Explainable AI (XAI): Move away from "black box" models. Security operators must be able to understand the "why" behind an AI's alert to make informed decisions.

2. Standardize Blockchain Protocols: To achieve the vision of a global, secure FinTech ecosystem, industry-wide standards for blockchain interoperability and smart contract auditing must be established (Hammi et al., 2022).

3. Invest in Edge-Based Security: As IoT and IoMT grow, the focus must shift to securing the "Edge." Lightweight deep learning models and efficient consensus mechanisms for low-power devices are critical.

4. Prepare for Quantum Sovereignty: Organizations should begin auditing their cryptographic assets and planning for a transition to lattice-based or other quantum-resistant encryption methods.

Conclusion

The battle for cybersecurity in the age of Cyber-Physical Systems and FinTech is an escalating arms race. As this research has demonstrated, the vulnerabilities of our critical infrastructures are deep and systemic, ranging from the physical manipulation of industrial sensors to the complex fraud mechanisms of digital wallets. However, the convergence of Deep Learning and Blockchain provides a sophisticated and resilient counter-measure.

By utilizing Deep Learning-particularly Auto-Encoders and Transformer-CNN frameworks-we can achieve a level of cognitive autonomy that allows systems to detect and respond to threats in real-time. By anchoring these intelligent systems in the decentralized trust of Blockchain, we ensure that the data they process and the decisions they make are immutable, transparent, and beyond the reach of a single point of failure.

While significant challenges remain-ranging from the scalability trilemma to the threat of adversarial AI and quantum computing-the path forward is clear. The integration of "Intelligence" and "Integrity" is not merely an option but a necessity. As we move toward 2030 and beyond, the resilience of our global society will depend on our ability to build these self-healing, decentralized, and cognitively autonomous security ecosystems. The digital age promises unparalleled progress, but only if it is built upon a foundation of absolute and verifiable security.

References

1. Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. A Comprehensive review on cybersecurity issues and their mitigation measures in FinTech. 2024.

2. Annals of Operations Research. Machine learning for coverage optimization in wireless sensor networks: a comprehensive review. 2023.

3. Anusha, R., Vijayashree, J., Jayashree, J., & Yousuff, M. CPS Support IoMT Cyber Attacks, Security and Privacy Issues and Solutions. Cyber-Physical Systems for Industrial Transformation, CRC Press. 2023.

4. Big Data. Deep Learning for Time Series Forecasting: A Survey. 2025.

5. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., & Felten, E. Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy. 2015.

6. Castillo, A. Blockchain and Cybersecurity in Fintech: Enhancing Transaction Security in the Digital Age. Journal of Cybersecurity Research, 18(3), 101-118. 2021.

7. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. On the security and performance of proof of work blockchains. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

8. Gupta, M., & Dhillon, G. Blockchain and Fintech: Security Challenges, Opportunities, and Future Directions. Journal of Financial Technology, 12(2), 45-63. 2020.

9. Hammi, A., Jinugu, A., Bouaoud, M., Hefnawy, A., & Bouras, A. Blockchain technology regulation: time for standardized frameworks. Blockchain Driven Supply Chains and Enterprise Information Systems. Springer International Publishing. 2022.

10. Han, S., M. Xie, H.-H. Chen, & Y. Ling. Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges. IEEE Syst. J., 8 (4). 2014.

11. Hassan, W., Chou, T. S., Li, X., Appiah-Kubi, P., & Tamer, O. Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks. Int J Inf & Commun Technol. 2019.

12. IEEE Access. Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. 2021.

13. IEEE Journals & Magazine. Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. 2025.

14. IEEE Xplore. A Review of Neural Networks for Anomaly Detection. 2025.

15. Kumar, S., Lim, W. M., Sivarajah, U., & Kaur, J. Artificial intelligence and blockchain integration in business: trends from a bibliometric-content analysis. Information Systems Frontiers, 25(2), 871-896. 2023.

16. Kuznetsov, A., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access. 2024.

17. Ling, J., L. Zhang, C. Liu, G. Xia, & Z. Zhang. Machine Learning-Based Multilevel Intrusion Detection Approach. Electronics, 14 (2). 2025.

18. Luo, Y., Y. Xiao, L. Cheng, G. Peng, & D. Yao. Deep Learning-based Anomaly Detection in Cyber-physical Systems: Progress and Opportunities. ACM Comput Surv, 54 (5). 2021.

19. Makrakis, G.M., C. Kolias, G. Kambourakis, C. Rieger, & J. Benjamin. Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. IEEE Access, 9. 2021.

20. MDPI Electronics. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. 2025.

21. MDPI Electronics. A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. 2025.

22. MDPI Mathematics. Auto-Encoders in Deep Learning-A Review with New Perspectives. 2023.

23. Mohammad, N. Enhancing Security and Privacy in Multi-Cloud Environments: A Comprehensive Study on Encryption Techniques and Access Control Mechanisms. International Journal of Computer Engineering and Technology (IJCET), 12, 51-63. 2021.

24. Osita, G. C., Chisom, C. D., Okoronkwo, M. C., Esther, U. N., & Vanessa, N. C. Application of Emerging Technologies in Mitigation of e-Commerce Security Challenges. CCU J. Sci, 2. 2022.

25. Purdue University. Deep Learning Based Models for Cognitive Autonomy and Cybersecurity Intelligence in Autonomous Systems. 2025.

26. Sancho Larraz, J., García Moros, J., & Alesanco Iglesias, Á. Design and evaluation of novel authentication, authorization and border protection mechanisms for modern information security architectures. Doctoral dissertation, Zaragoza University. 2021.

27. Tran, T. M. A. Mobile Payment Security: A case study of Digital Wallet MOMO. 2020.

28. Yaga, D., Mell, P., Roby, N., & Scarfone, K. Blockchain Technology Overview. National Institute of Standards and Technology. 2018.

29. Yang, Y. S., Lee, S. H., Chen, W. C., Yang, C. S., Huang, Y. M., & Hou, T. W. TTAS: Trusted token authentication service of securing SCADA network in energy management system for industrial Internet of Things. Sensors, 21(8). 2021.