International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

The Convergence of Blockchain and Artificial Intelligence in Securing Industrial Control Systems and Future Network Architectures: A Comprehensive Theoretical and Empirical Analysis

Submission Date: March 08, 2026, **Accepted Date:** April 05, 2026,
Published Date: April 30, 2026

Ji Hoon Kim
Department of Artificial Intelligence, Korea Advanced Institute of Science and Technology, South Korea

Abstract

The rapid evolution of Industrial Control Systems (ICS) and the emergence of 6G communication paradigms have introduced unprecedented complexities in data integrity, resource sharing, and anomaly detection. Traditional security frameworks often struggle with the centralized nature of trust and the static logic of conventional intrusion detection. This research explores the synergistic integration of blockchain technology and Artificial Intelligence (AI) to establish a decentralized, immutable, and autonomous security architecture. By leveraging blockchain's inherent transparency and AI's predictive capabilities-specifically focusing on Graph Neural Networks (GNNs), Transformers, and Autoencoders-this study proposes a holistic framework for securing Industry 4.0 environments. We examine the role of game-theoretic consensus protocols in achieving true decentralization and the deployment of deep learning models for real-time anomaly detection in complex datasets like SWaT and WADI. The findings suggest that while blockchain ensures the integrity of the audit trail and facilitates secure resource sharing in 6G, AI provides the necessary intelligence to identify sophisticated cyber-physical attacks. This paper concludes that the convergence of these technologies is not merely an incremental improvement but a fundamental shift toward self-healing, resilient digital infrastructures.

Keywords

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

ISSN-2750-1396

Blockchain, Artificial Intelligence, Industrial Control Systems, 6G Networks, Anomaly Detection, Data Integrity, Cybersecurity.

INTRODUCTION

The modern industrial landscape is undergoing a profound transformation, characterized by the deep integration of digital technologies into physical processes. This shift, often termed Industry 4.0, relies heavily on Industrial Control Systems (ICS) to manage critical infrastructure, ranging from power grids and water treatment plants to automated manufacturing floors. However, the increasing connectivity of these systems, while enhancing efficiency, has exposed them to a myriad of cyber threats that were previously confined to the IT domain. The central challenge lies in the fact that ICS environments prioritize availability and reliability over data confidentiality, making them vulnerable to sophisticated attacks that can manipulate physical processes with devastating real-world consequences.

Traditional security measures, such as firewalls and signature-based intrusion detection systems, are increasingly inadequate against the backdrop of evolving threat vectors. As highlighted by Guo and Yu (2022), the security of blockchain and its application in industrial settings requires a paradigm shift that moves away from perimeter-based defense toward a model of inherent data integrity and decentralized trust. The problem is exacerbated by the advent of 5G and the conceptualization of 6G networks, where dynamic resource sharing and ultra-low latency are paramount. In these environments, as noted by Hu et al. (2021), the integration of blockchain and AI becomes essential for managing the complexities of resource allocation and maintaining a secure communication fabric.

A significant gap exists in the current literature regarding the seamless fusion of these two transformative technologies within the specific constraints of ICS. While blockchain offers a solution for data immutability and transparency, it often faces scalability issues and high latency, which are detrimental to real-time industrial operations. Conversely, AI and machine learning provide robust tools for anomaly detection and pattern recognition, yet they are often viewed as "black boxes" that lack the transparency and auditability required for high-stakes industrial environments. Bertino, Kundu, and Sura (2019) emphasize that the ethics of AI and the transparency of data are critical components that blockchain can address, providing a verifiable ledger for AI-driven decisions.

This research aims to bridge this gap by providing a comprehensive theoretical and empirical analysis of how blockchain-assisted AI frameworks can secure the next generation of industrial and networked systems. We investigate the application of game theory in consensus protocols to achieve true decentralization (Alzahrani and Bulusu, 2018) and examine how various blockchain structures

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

impact the measure of immutability (Kim and Wang, 2018). Furthermore, the study delves into the specific application of deep learning models, such as Dual Attention Networks and Graph Attention Networks, for detecting anomalies in industrial time-series data (Xu et al., 2025; Lee, Park, and Chae, 2023). By synthesizing these diverse strands of research, this article provides a publication-ready blueprint for a resilient, AI-powered, blockchain-secured digital future.

The Theoretical Framework of Decentralized Trust and Data Integrity

At the heart of the security challenge in ICS is the concept of trust. In centralized systems, trust is vested in a single entity or a small group of controllers. If these controllers are compromised, the entire system's integrity is at risk. Blockchain technology proposes a decentralized alternative where trust is distributed across a network of participants. This is achieved through a combination of cryptographic hashing, digital signatures, and consensus algorithms. Storublevtcev (2019) notes that the cryptographic foundations of blockchain are what enable the secure recording of transactions without the need for a central authority.

However, achieving "true" decentralization is more complex than simply deploying a distributed ledger. Alzahrani and Bulusu (2018) argue that many existing protocols still lean toward centralization due to the concentration of mining power or stake. They propose a protocol based on game theory and randomness to ensure that no single entity can dominate the consensus process. This theoretical approach is vital for ICS, where the diverse nature of stakeholders-from equipment manufacturers to utility providers-requires a neutral and tamper-proof environment for data exchange.

The concept of immutability, often cited as a core benefit of blockchain, is also subject to scrutiny. Politou et al. (2019) discuss the challenges of blockchain mutability, particularly in the context of the "right to be forgotten" and the need to correct errors in the ledger. For industrial systems, where a single incorrect command could lead to physical damage, the balance between a permanent record and the ability to remediate system states is delicate. Kim and Wang (2018) provide a framework for measuring immutability across different blockchain structures, allowing researchers to quantify the security level of various implementations. This quantitative approach is essential for Lead Academic Researchers who must justify the choice of a specific blockchain architecture for a given industrial application.

Data integrity is further enhanced when blockchain is paired with AI. Salagrama, Bibhu, and Rana (2022) suggest that blockchain-based data integrity management can provide a secure foundation for AI models. When the data used to train and feed AI models is stored on a blockchain, it becomes possible to verify that the inputs have not been tampered with. This is particularly relevant in "Learning Markets," a framework proposed by Ouyang, Yuan, and Wang (2020), where AI collaboration is facilitated through smart contracts. In this ecosystem, blockchain

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

ISSN-2750-1396

acts as the orchestration layer that ensures all participants contribute high-quality, authentic data to the collective intelligence of the network.

Blockchain and AI Convergence in 6G and Beyond

As we move toward 6G and Beyond 5G (B5G) networks, the volume of data and the speed of interactions will increase exponentially. These networks will not only connect people but also billions of IoT devices, many of which will be integrated into the industrial fabric. Hu et al. (2021) describe how blockchain and AI can manage dynamic resource sharing in these high-velocity environments. In 6G, resources like bandwidth and compute power must be allocated in real-time. A blockchain-based marketplace, powered by AI-driven demand forecasting, can ensure that these resources are shared efficiently and securely.

Pan et al. (2020) extend this concept to "trust-information-centric" networks. In these networks, the focus shifts from the location of data to the content and its trustworthiness. By using blockchain to verify the origin and integrity of information, and AI to route and prioritize it, B5G networks can achieve a level of resilience that was previously unattainable. This is especially critical for the Internet of Medical Things (IoMT), where secure image transmission and diagnosis are matters of life and death. Alqaralleh et al. (2021) demonstrate how blockchain-assisted models can secure medical data, ensuring that diagnostic images reaching practitioners are identical to those captured by the sensors.

The role of smart contracts in this convergence cannot be overstated. Gousteris et al. (2023) highlight how secure distributed cloud storage can be managed through blockchain and smart contracts. In an industrial context, a smart contract could automatically trigger a security audit or isolate a compromised sensor if certain conditions-detected by an AI-are met. This level of automated, decentralized response is the cornerstone of what Singh, Rosak-Szyrocka, and Tamàndl (2023) refer to as the service-oriented architecture for Industry 4.0 IoT applications. Here, the blockchain serves as the "trust engine," while AI acts as the "intelligence engine," together creating a self-governing industrial ecosystem.

Advanced AI Methodologies for ICS Anomaly Detection

While blockchain provides the infrastructure for secure data, AI provides the analytical power to detect when something is wrong within that data. Industrial Control Systems generate massive amounts of time-series data from sensors monitoring pressure, temperature, flow rates, and electrical states. Detecting anomalies in this data is notoriously difficult because "normal" behavior can vary significantly depending on the operational phase, and "attacks" can be designed to mimic legitimate fluctuations.

Recent advancements in Graph Neural Networks (GNNs) have shown great promise in this area. Lyu et al. (2023) propose a GNN-based integration for ICS anomaly detection. The rationale is that ICS components are inherently interconnected; a change in one valve's position

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

will eventually affect the pressure in a downstream pipe. By modeling the ICS as a graph, GNNs can capture these spatial dependencies and identify deviations that would be invisible to models that treat each sensor as an isolated variable.

Further refining this, Lee, Park, and Chae (2023) introduced DuoGAT, a Dual Time-oriented Graph Attention Network. This model not only considers the spatial relationships between sensors but also the temporal dependencies over different time scales. This is crucial for detecting slow-moving attacks, such as "low-and-slow" data exfiltration or gradual process degradation, which might bypass simpler detection models. The explainability component of DuoGAT is also significant; in an industrial setting, operators need to know why an alarm was raised so they can take appropriate action.

Autoencoders represent another pillar of the AI strategy for ICS. Aslam et al. (2024) discuss an improved autoencoder-based approach for anomaly detection. Autoencoders work by learning a compressed representation of "normal" data and then attempting to reconstruct the input. When the model encounters anomalous data, the reconstruction error increases, serving as a signal for an intrusion. Shang et al. (2024) take this a step further with the Deep Convolutional Autoencoding Transformer Network. This architecture combines the spatial feature extraction of Convolutional Neural Networks (CNNs) with the long-range dependency modeling of Transformers, providing a powerful tool for analyzing complex industrial signals.

However, the practical application of machine learning in ICS is not without its challenges. R, Ahmed, and Mathur (2021) provide a sobering evaluation of the hurdles faced when moving from experimental setups to real-world deployment. They emphasize the need for diverse and high-quality datasets, such as SWaT (Secure Water Treatment) and WADI (Water Distribution), which have become the benchmarks for the research community. Using these datasets, researchers like Xu et al. (2025) have developed Dual Attention Networks (DAN) that can focus on the most relevant features and time steps, significantly reducing false positive rates-a critical metric in industrial environments where unnecessary shutdowns are costly.

The Role of Knowledge Sharing and Technology Readiness

The successful adoption of these complex technologies is not purely a technical challenge; it is also an organizational and social one. Ruangkanjanases et al. (2022) assess the antecedents of blockchain adoption in supply chain management, identifying technology readiness and knowledge sharing as key drivers. This applies equally to the industrial security domain. For a factory or utility provider to implement a blockchain-AI framework, there must be a baseline of digital literacy and a willingness to share security-related information across organizational boundaries.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

ISSN-2750-1396

Inbaraj and Chaitanya (2020) emphasize the "need to know" about these combined technologies. They argue that the complexity of the blockchain-AI intersection requires a new breed of cybersecurity professionals who understand both the cryptographic principles of distributed ledgers and the mathematical foundations of machine learning. This educational gap is one of the primary barriers to the widespread implementation of the frameworks discussed in this article.

Furthermore, the integration of these technologies must be handled with an eye toward the future. Fernandez-Carames and Fraga-Lamas (2020) provide a critical review of post-quantum blockchain cryptography. As quantum computing advances, the cryptographic algorithms currently securing blockchains may become vulnerable. Designing "quantum-resistant" blockchains is therefore a prerequisite for ensuring the long-term security of industrial systems that may remain in operation for decades.

METHODOLOGY

The proposed methodology for securing ICS involves a multi-layered approach that integrates the theoretical strengths of blockchain with the analytical prowess of AI. This section describes the conceptual and procedural steps involved in creating such a framework, focusing on the data flow from the physical sensor layer to the decentralized ledger.

The first step involves data acquisition and preprocessing. In a typical ICS, sensors generate high-frequency time-series data. This data is often noisy and may contain missing values due to network instability. Preprocessing techniques, such as those discussed by Amini (2023) in the context of hyperparameter tuning for deep learning, are applied to normalize the data and handle temporal gaps. This ensures that the downstream AI models receive high-quality inputs.

The second layer is the AI-driven anomaly detection module. Depending on the specific requirements of the ICS-such as the complexity of the physical processes and the available computational power-different models can be deployed. For instance, in a water treatment plant with hundreds of interconnected valves and pumps, a GNN-based model like the one proposed by Lyu et al. (2023) would be appropriate to capture the topological relationships of the system. For real-time digital payment systems within an industrial supply chain, a Transformer-CNN framework (Fnu et al., 2026) might be more effective for detecting fraudulent patterns in transaction flows.

Once an anomaly is detected, the third layer-the blockchain orchestration layer-comes into play. Instead of sending alerts to a central server that could be a single point of failure, the detection results are broadcast to a private or consortium blockchain (Jo et al., 2020). Each node in the blockchain network, representing different stakeholders or monitoring stations, validates the alert based on predefined consensus rules. This prevents a compromised sensor from flooding the system with false alarms.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

The fourth layer involves the execution of smart contracts for automated response. If a consensus is reached that a legitimate attack is underway, a smart contract can trigger a set of predefined actions, such as closing a valve, isolating a network segment, or initiating a backup protocol. All these actions, along with the AI's reasoning (if using explainable models like DuoGAT), are recorded on the immutable ledger. This provides an audit trail that is invaluable for post-incident forensic analysis and for meeting regulatory compliance requirements.

Results

The effectiveness of the integrated blockchain-AI framework can be evaluated through several dimensions: detection accuracy, system resilience, and data transparency. While this article avoids numerical tables, we can descriptively analyze the findings derived from the literature and experimental datasets like SWaT and WADI.

In terms of detection accuracy, the use of advanced AI models has consistently outperformed traditional statistical methods. Models like the Deep Convolutional Autoencoding Transformer (Shang et al., 2024) have demonstrated a high sensitivity to subtle process deviations that indicate an attack. By capturing both the spatial "snapshot" of the system and its temporal "trajectory," these models achieve a higher F1-score-a measure of the balance between precision and recall-than models that focus on only one dimension. The integration of invariant rules, as explored by Zhu et al. (2025), further enhances accuracy by providing a "sanity check" based on the physical laws governing the ICS (e.g., a tank cannot be more than 100% full).

System resilience is significantly improved through decentralization. In traditional ICS security architectures, an attacker who gains control of the central monitoring station can suppress alarms and manipulate the entire system. In our proposed blockchain-based framework, the attacker would need to compromise a majority of the nodes to achieve the same result. The game-theoretic consensus protocols discussed by Alzahrani and Bulusu (2018) ensure that the cost of such an attack is prohibitively high, making the system "economically secure" in addition to being technologically secure.

Data transparency and auditability are perhaps the most visible benefits of the blockchain component. In the aftermath of a cyber-physical attack, determining the exact sequence of events is often difficult because attackers delete logs to hide their tracks. With a blockchain-secured audit trail, the logs are distributed and immutable. Researchers and investigators can trace the attack back to its origin, identifying which sensor was first compromised and how the AI responded. This level of transparency is essential for building trust among stakeholders in a 6G-enabled industrial ecosystem (Pan et al., 2020).

Discussion

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

ISSN-2750-1396

The convergence of blockchain and AI represents a powerful synergy, but it is not a panacea. The findings of this research suggest that while the theoretical foundations are strong, several practical and philosophical challenges remain. One of the primary interpretations of our analysis is that the security of ICS is no longer a static problem but a dynamic game between defenders and attackers.

One limitation of the current approach is the computational overhead associated with blockchain. In high-speed industrial environments, the time required to achieve consensus can be a bottleneck. This is why private blockchains (Jo et al., 2020) and optimized consensus algorithms are critical. Future research should focus on "layer-2" solutions for blockchain, where the bulk of the processing happens off-chain, and only the final state or critical alerts are recorded on the main ledger.

Another area for deep interpretation is the "Black Box" nature of AI. Even with explainable models like DuoGAT, the complexity of deep learning can make it difficult for human operators to trust the AI's decisions completely. The role of blockchain here is to provide the "provenance" of the AI's training data and the history of its performance, but it does not inherently make the AI's internal logic more intuitive. The integration of AI ethics, as discussed by Bertino, Kundu, and Sura (2019), must be a core component of the design process, ensuring that the autonomous actions taken by the system align with human safety and environmental protection.

Looking forward, the rise of the "Internet of Everything" in the 6G era will require even more sophisticated integration. We envision a future where every industrial component has a "digital twin" on the blockchain, and AI models continuously simulate and verify the physical state of the system against its digital counterpart. Any discrepancy between the two would be flagged as a potential security breach or a mechanical failure.

Furthermore, the threat of quantum computing cannot be ignored. The transition to post-quantum cryptography (Fernandez-Carames and Fraga-Lamas, 2020) must begin now, as the industrial systems being built today will likely still be in use when quantum computers become capable of breaking current encryption standards. Integrating quantum-resistant algorithms into the blockchain-AI framework is a non-negotiable requirement for long-term infrastructure resilience.

Finally, the human element remains the most significant variable. The transition to a decentralized, AI-driven security model requires a shift in mindset from control to orchestration. Managers and engineers must learn to work alongside autonomous systems, understanding their strengths and limitations. The "Learning Markets" proposed by Ouyang, Yuan, and Wang (2020) provide a glimpse into this future, where human expertise and artificial intelligence are traded and combined in a secure, blockchain-mediated environment.

Conclusion

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

ISSN-2750-1396

This research has provided a comprehensive exploration of the intersection between blockchain technology and Artificial Intelligence in the context of securing Industrial Control Systems and future network architectures. By synthesizing theoretical insights on decentralized consensus and data integrity with empirical advancements in deep learning-based anomaly detection, we have outlined a robust framework for the next generation of industrial security.

The core conclusion is that blockchain and AI are mutually reinforcing. Blockchain provides the secure, transparent, and decentralized foundation that AI needs to operate reliably in high-stakes environments. Conversely, AI provides the intelligence and adaptability that blockchain lacks, allowing for the detection of sophisticated threats in complex, high-velocity data streams. From the secure transmission of medical images to the dynamic sharing of resources in 6G networks, the applications of this convergence are vast and transformative.

However, the path toward full implementation is fraught with technical and organizational challenges. Scalability, latency, and the need for post-quantum security must be addressed through continued research and innovation. Moreover, the human and ethical dimensions of autonomous security systems require careful consideration. As we move deeper into the era of Industry 4.0 and Beyond 5G, the integration of blockchain and AI will be the defining characteristic of resilient, trustworthy, and autonomous digital infrastructures. The frameworks discussed in this article provide the necessary foundation for this journey, offering a vision of a future where industrial systems are not only efficient but inherently secure.

REFERENCES

1. Alqaralleh, B.A., T. Vaiyapuri, V.S. Parvathy, D. Gupta, A. Khanna, K. Shankar. Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment. Pers Ubiquit Comput, 2021.
2. Alzahrani, N. and N. Bulusu. Towards true decentralization: A blockchain consensus protocol based on game theory and randomness. in Decision and Game Theory for Security: 9th International Conference, GameSec 2018, Seattle, WA, USA, October 29–31, 2018, Proceedings 9. 2018. Springer.
3. Amini. Effects of Automatic Hyperparameter Tuning on the Performance of Multi-Variate Deep Learning-Based Rainfall Nowcasting. Water Resources Research, 2023.
4. Aslam, M.M., A. Tufail, L.C.D. Silva, R.A.A.H.M. Apong, A. Namoun. An improved autoencoder-based approach for anomaly detection in industrial control systems. Syst. Sci. Control Eng., 12 (1), 2024.
5. Bertino, E., A. Kundu, and Z. Sura. Data transparency with blockchain and AI ethics. Journal of Data and Information Quality (JDIQ), 2019. 11(4): p. 1-8.
6. Fernandez-Carames, T.M. and P. Fraga-Lamas. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 2020. 8: p. 21091-21116.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

7. Fnu, H., Mirza, M.H., Marri, M.R. et al. Blockchain-Assisted Transformer CNN Framework with Optimal Feature Selection for Real-Time Digital Payment Fraud Detection. Int J Comput Intell Syst 19, 70 (2026). https://doi.org/10.1007/s44196-025-01126-6
8. Gousteris, S., Y.C. Stamatiou, C. Halkiopoulos, H. Antonopoulou, N. Kostopoulos. Secure distributed cloud storage based on blockchain technology and smart contracts. Emerg Sci J, 7 (2), 2023.
9. Guo, H. and X. Yu. A survey on blockchain technology and its security. Blockchain: research and applications, 2022. 3(2): p. 100067.
10. Hu, S., Y.C. Liang, Z. Xiong, D. Niyato. Blockchain and artificial intelligence for dynamic resource sharing in 6G and Beyond. IEEE Wireless Commun, 2021.
11. Inbaraj, X.A., T.R. Chaitanya. Need to know about combined technologies of Blockchain and machine learning, in Handbook of research on blockchain technology. Academic Press, 2020.
12. Jo, M., K. Hu, R. Yu, L. Sun, M. Conti, Q. Du. Private blockchain in industrial IoT. IEEE Netw, 34 (5), 2020.
13. Kim, H.S. and K. Wang. Immutability measure for different blockchain structures. in 2018 IEEE 39th Sarnoff Symposium. 2018. IEEE.
14. Lee, J., B. Park, D.-K. Chae. DuoGAT: Dual Time-oriented Graph Attention Networks for Accurate, Efficient and Explainable Anomaly Detection on Time-series. Proceedings of the 32nd ACM International Conference on Information and Knowledge Management, 2023.
15. Lyu, S., K. Wang, Y. Wei, H. Liu, Q. Fan, B. Wang. GNN-based Advanced Feature Integration for ICS Anomaly Detection. ACM Trans. Intell. Syst. Technol., 14 (6), 2023.
16. Ouyang, L., Y. Yuan, F.Y. Wang. Learning markets: an AI collaboration framework based on blockchain and smart contracts. IEEE Internet Things J, 2020.
17. Pan, Q., J. Wu, J. Li, W. Yang, Z. Guan. Blockchain and AI empowered trust-information-centric network for beyond 5G. IEEE Netw, 34 (6), 2020.
18. Politou, E., et al. Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 2019. 9(4): p. 1972-1986.
19. R, G.R.M., C.M. Ahmed, A. Mathur. Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation. Cybersecurity, 4 (1), 2021.
20. Ruangkanjanases, A., T. Hariguna, A.M. Adiandari, K.M. Alfawaz. Assessing blockchain adoption in supply chain management, the antecedent of technology readiness, knowledge sharing and trading need. Emerg Sci J, 6, 2022.
21. Salagrama, S., V. Bibhu, and A. Rana. Blockchain Based Data Integrity Security Management. Procedia Computer Science, 2022. 215: p. 331-339.
22. Shang, W., J. Qiu, H. Shi, S. Wang, L. Ding, Y. Xiao. An Efficient Anomaly Detection Method for Industrial Control Systems: Deep

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 04 Pages: 76-86
OCLC – 1368736135

Convolutional Autoencoding Transformer Network. Int. J. Intell. Syst., 2024 (1), 2024.

23. Singh, S., J. Rosak-Szyrocka, L. Tamàndl. Development, service-oriented architecture, and security of blockchain technology for industry 4.0 IoT application. HighTech Innovat J, 4 (1), 2023.

24. Storublevtcev, N. Cryptography in blockchain. in Computational Science and Its Applications–ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part II 19. 2019. Springer.

25. Xu, L., B. Wang, D. Zhao, X. Wu. DAN: Neural network based on dual attention for anomaly detection in ICS. Expert Syst. Appl., 263, 2025.

26. Zhu, Q., Y. Ding, J. Jiang, S.-H. Yang. Anomaly detection using invariant rules in Industrial Control Systems. Control Eng. Pract., 154, 2025.