

Ana Đokić¹
Milan Erić
Milan Čabarkapa
Hana Stefanović

Research paper
DOI – 10.24874/QF.25.060



SECURING INDUSTRIAL DATA: THE ROLE OF BLOCKCHAIN TECHNOLOGY IN INDUSTRIAL AUTOMATION

Abstract: *The ubiquitous and accelerated digitization and integration of information and operational technologies have become a key aspect of modern industrial environments. Through the interconnection and interaction of these technologies, a considerable amount of data is generated, making their protection one of the dominant challenges. This paper aims to explore blockchain technology's role in protecting industrial data in modern industrial environments through a comparison with traditional security systems. The paper focuses on identifying critical processes of industrial automation and exploring how the basic principles of blockchain technology, such as decentralization, immutability and transparency, can contribute to the improvement of industrial data security. A good example of the practical application of blockchain technology can be seen in the case study of the implementation of the IBM Food Trust platform in Walmart's supply chain management, illustrating the benefits, including reduced product tracking time and increased transparency. The qualitative results of this research indicate that blockchain technology can significantly improve industrial data security, but also that there are challenges related to scalability, integration with existing systems and regulatory frameworks.*

Keywords: *blockchain technology, industrial data security, decentralization, transparency, IBM Food Trust*

1. Introduction

In modern industrial environments, manufacturing systems utilize computing resources to transmit real-time data, enabling improved analysis, monitoring, and management of production processes. The digital transformation that facilitates the rapid and efficient exchange of vast amounts of data between different systems brings numerous benefits, including process optimization, predictive maintenance, and enhanced decision-making (Ghani, 2024).

However, as digitalization progresses, industrial control systems are becoming increasingly exposed to sophisticated cyber threats (Tidrea et al., 2019). The consequences of compromised data in industrial automation go beyond financial losses, such as the theft of intellectual property or business secrets and the illegal use of data. They can also result in significant production downtimes, disruption of critical infrastructure, and serious safety risks. These threats necessitate a fundamental shift in the approach to

¹ Corresponding author: Ana Đokić
Email: ana.djokic@its.edu.rs

industrial data protection, through the implementation of advanced security mechanisms (Bernal Bernabé et al., 2024).

This paper identifies critical industrial automation processes, including data collection and management, production line management, and predictive maintenance. These processes rely on the implementation of advanced digital manufacturing technologies such as the Internet of Things (IoT), artificial intelligence (AI), machine learning (ML), and blockchain (Rahman et al., 2024).

The paper explores innovative opportunities for enhancing the security of industrial data through the application of blockchain technology, focusing on its key features: decentralization, immutability, and transparency. A detailed analysis is conducted on the impact of blockchain on data security, its integration with existing systems, and its influence on the efficiency of industrial process management. Understanding these aspects is essential for evaluating the real potential and limitations of blockchain technology in comparison to traditional security systems (Tariq et al., 2019).

The benefits of blockchain, particularly in reducing product traceability time, are illustrated through a case study on the implementation of the IBM Food Trust platform (IBM, 2025) in Walmart's supply chain management.

Qualitative findings from this research emphasize the significant potential of blockchain technology in strengthening industrial data security. At the same time, the study identifies key challenges and limitations related to scalability, integration with legacy systems, and compliance with regulatory frameworks and standards (Jabbar et al., 2020).

Addressing these challenges and developing practical solutions is essential for the continued advancement and adoption of blockchain technology in industrial sectors.

2. Traditional Data Protection Methods and Critical Processes in Industrial Automation

Modern manufacturing processes in industrial systems increasingly rely on automation and interconnectedness through the application of digital technologies, analyzing the impact of digital transformation fundamentally important for understanding and improving industrial efficiency. Industrial automation includes digital tools and systems, such as software, sensors, robots, and automated systems, which enable more efficient production management (Ghani, 2024). By using these technologies, industrial systems become more flexible, reduce costs, and better meet market demands.

However, traditional data management systems, such as encryption, authentication, firewalls, and IPS/IDS solutions, are often inadequate in protecting against modern cyber threats. Their weaknesses include weak authentication, lack of encryption, and insecure communication protocols, which allow for attacks such as unauthorized access and data manipulation (Tidrea et al., 2019). Additionally, reliance on centralized databases increases the risk of data loss due to attacks or failures. The absence of advanced mechanisms for threat detection and response further complicates system protection, while the lack of mechanisms for data integrity can lead to severe operational disruptions (Enemosah, 2024).

Several critical processes are essential for the successful implementation of digital manufacturing technologies. One such process is data collection, which involves gathering information from the production environment for decision-making and process optimization. The volume and variety of data create challenges in storage, processing, and analysis, making effective data management critical. The quality of data directly impacts the accuracy of AI and ML models used for predictive maintenance and

production optimization. Open software interfaces, such as APIs, enhance system interoperability, enabling faster and more efficient analysis (Oliveira & Afonso, 2019; Jasim, 2023). Integrating blockchain technology into this process ensures immutability, integrity, and verified provenance of data entering AI and ML models, enabling a transparent and secure flow of information, as well as greater reliability of results and data protection.

Production line management involves monitoring and coordinating all production stages, with Manufacturing Execution Systems (MES) providing real-time insight through data integration from various sources. This approach improves decision-making, increases efficiency, and reduces downtime. Implementing MES systems can be challenging and require significant investments, and successful integration with existing systems is key to maximizing benefits. The integration of Artificial Intelligence (AI) and Machine Learning (ML) allows further optimization of production schedules. At the same time, blockchain plays a crucial role in ensuring the immovable, verified, and immutable record of all activities within the MES system (Wagh, 2024). Blockchain enables transparency and traceability of operations, preventing retroactive data changes, while AI and ML analyze this data to optimize production flows, achieving higher security and efficiency in production management (Ige et al., 2025).

Predictive maintenance uses data analysis and machine learning to identify potential failures before they occur, reducing costs and downtime. The efficiency of predictive models depends on data quality, the accuracy of analysis, and the integration of IoT sensors that enable real-time data collection from equipment (Gama et al., 2022). Blockchain technology ensures secure and decentralized storage of equipment performance data and service interventions, increasing trust in prediction accuracy and minimizing the risk of record manipulation.

By combining AI, ML, and blockchain, reliable predictive maintenance based on secure, verified data is enabled, increasing the accuracy of predictions and improving system efficiency (Rahman et al., 2024).

3. Blockchain Technology and Industrial Data Security

Blockchain technology, originally associated with cryptocurrencies, offers a new approach to data security that addresses many challenges specific to modern industrial systems (Chen et al., 2024). With its inherent security features, blockchain technology provides a promising solution for protecting critical information, including intellectual property, manufacturing processes, and supply chains, which are frequent targets of cyberattacks. At its core, blockchain functions as a distributed, immutable ledger that records transactions securely and transparently (Al-Jaroodi & Mohamed, 2019), with each transaction cryptographically secured and linked to the previous one, making alterations impossible without leaving a visible trace (Hammoudeh, 2021). This immutability ensures data integrity and provides a high level of trust among all entities, including users, validators, and applications utilizing blockchain technology (Justinia, 2019).

The key principles of this technology, decentralization, immutability, and transparency, enable a high level of security and data integrity in industrial applications (Habib et al., 2022). Figure 1 illustrates how the interconnected principles of blockchain technology contribute to meeting the specific security, operational, and integration requirements of modern industrial systems.

The graphical representation illustrates how the listed principles relate to the specific advantages they support, emphasizing the role of blockchain as a technology with the potential to substantially improve the security and reliability of digitized industrial systems (Rahman et al., 2024).

Decentralization removes the need for a central authority, which enhances fault tolerance, improves resilience against failures, and reduces reliance on intermediaries. Key advantages of a decentralized approach include the use of distributed ledgers, increased resistance to cyberattacks, and secure data storage that avoids single points of failure (Tariq et al.,

2019). Immutability ensures the integrity of data through cryptographically linked blocks, along with mechanisms such as tamper detection, audit trails, and verification of authenticity. These features support consistent and verifiable transaction records, further strengthening trust in blockchain-based systems (Tariq et al., 2019).

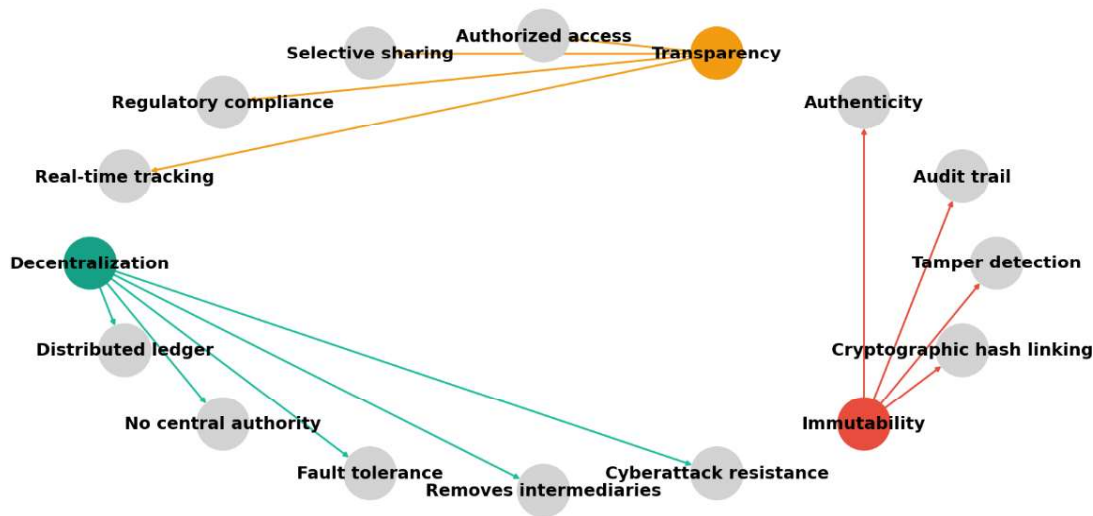


Figure 1. Key principles of blockchain technology

Transparency enables relevant stakeholders to access data while maintaining access control through mechanisms such as selective sharing and authorized access. This feature supports improved compliance with regulatory requirements and facilitates real-time process monitoring, thereby increasing the overall efficiency of industrial supply chains (Tariq et al., 2019).

4. Case Study

This case study analyzes a pioneering implementation of blockchain technology in the complex supply chain management operations of Walmart. The main focus is on the technological foundation of the IBM Food Trust platform (IBM, 2025), which enables the execution of this initiative. It serves as an excellent example to illustrate

the benefits of digital technologies in addressing complex challenges in modern industry.

4.1. Technological Foundation of the IBM Food Trust Platform

The IBM Food Trust platform employs a permissioned blockchain, giving access only to pre-approved participants, which strengthens data security and control within the supply chain (Michael et al., 2020). The distributed nature of the platform ensures data transparency and immutability, making it virtually impossible to alter information once recorded (Shankaran, 2024). Integration with Walmart’s systems began with pilot programs that facilitated problem identification and process optimization (Kumar et al., 2024). In addition to

significant changes in existing data collection, processing, and sharing protocols, as well as organizational restructuring, the integration process required employee training, ensuring smooth assimilation with existing systems (Shankaran, 2024).

4.2. Data Management

Data entry into the IBM Food Trust blockchain involved meticulous recording of key information at various stages of the supply chain (Shankaran, 2024), including origin, transportation, and storage conditions (Anjum et al., 2024). Data automation through IoT devices enabled accuracy, while manual entry was employed for information not capturable via sensors and tracking tags (Chigilipalli et al., 2023). Upon entry, data were verified to ensure accuracy before being permanently written to the blockchain. The immutability of the blockchain, enabled by cryptographic mechanisms such as hashing and digital signatures, prevents unauthorized data modifications (Shankaran, 2024; Kumar et al., 2024). Each block is cryptographically linked to the previous one, preventing tampering and ensuring system integrity. Digital signatures authenticate the data, and timestamps provide an exact record of the moment of entry, thereby increasing transparency and accountability (Kumar et al., 2024).

4.3. Traceability and Integration

One of the key advantages of the IBM Food Trust platform is its ability to enable real-time tracking of products throughout the entire supply chain, providing detailed insight into product movement from the farm to retail shelves (Shankaran, 2024; Anjum et al., 2024). This system allows for accurate identification of product location and status, which is essential for swift responses to issues such as contamination or delays, thereby reducing losses and protecting consumer safety (Anjum et al., 2024). Compared to traditional methods, which did

not support real-time tracking, IBM Food Trust represents a significant advancement. The integration of this platform into Walmart's complex supply chain system required coordination with numerous suppliers and partners, as well as substantial modifications to existing data management and business process systems (Michael et al., 2020; Shankaran, 2024; Kumar et al., 2024). The process involved adapting IT infrastructure and building consensus among all stakeholders, underscoring the importance of collaboration and planning to maximize the benefits of the new platform, minimize the risk of losses, and protect Walmart's corporate reputation.

4.4. Implementation Outcomes

The implementation of blockchain at Walmart significantly reduced product traceability time from six days to nearly real-time, just a few seconds, which is crucial for rapidly addressing food safety concerns. This accelerated response decreases the risk of contamination spread, reduces the scale of product recalls and financial losses, and enhances supply chain efficiency by lowering waste and improving environmental sustainability (Shankaran, 2024).

The integration of smart contracts into the blockchain platform automated processes such as payment execution, document verification, and compliance checks, thereby reducing manual labor, increasing accuracy, and improving operational efficiency (Kumar et al., 2024; Anjum et al., 2024). Blockchain's immutability ensured transparency, as all participants had access to tamper-proof data, reducing disputes and enhancing collaboration among partners while enabling consumers to access product origin information (Shankaran, 2024; Kumar et al., 2024).

Blockchain's security features mitigated the risk of data manipulation, thereby enhancing system integrity and fostering trust among stakeholders, which in turn reduced the risk

of financial loss (Shankaran, 2024; Kumar et al., 2024). Its distributed architecture improved system resilience to attacks and reduced dependence on a central authority, further increasing transparency and accountability within the network (Michael et al., 2020).

4.5. Case Study Conclusion

Walmart's approach to adopting the IBM Food Trust platform demonstrates the potential of blockchain technology in optimizing supply chains. The initiative delivered improvements in key areas: reduced product tracking time, process automation, enhanced data integrity, increased transparency, food safety, and reduced risks of undesirable activities (Shankaran, 2024). However, the implementation also highlighted challenges such as scalability, interoperability between different blockchain platforms, and the need for broader industry adoption. Future research should focus on addressing these challenges and developing new blockchain applications in supply chain management (Shankaran, 2024; Kumar et al., 2024).

Despite these challenges, the success of Walmart's initiative provides valuable insights and serves as a case study for other organizations seeking to adopt blockchain technology to optimize their supply chain operations (Shankaran, 2024). The experience gained through this implementation may help shape future strategies and support the integration of blockchain across various industries.

5. Comparative Analysis

Traditional data management systems in industrial automation often fail to provide adequate protection against modern cyber threats, as many of them were designed before cybersecurity became a critical component of digital infrastructure. As a result, these systems lack features that are now considered fundamental to secure

architectures (Tidrea et al., 2019). Vulnerabilities are typically found in areas such as weak authentication, insecure communication protocols, lack of encryption, and reliance on centralized databases. Additionally, many systems do not possess mechanisms for real-time attack detection and response, nor do they guarantee data integrity, making them susceptible to information tampering and operational disruptions (Enemosah & George, 2024).

In today's industrial environment, increasing pressure from regulatory bodies to establish robust protection systems further complicates the situation. Legal and regulatory frameworks often require the implementation of specific security controls, including encryption methods and incident response protocols. Non-compliance with these standards can lead to severe consequences, ranging from financial penalties to reputational damage (Ghani, 2024). In this context, comparing existing solutions with emerging technologies such as blockchain becomes essential for evaluating the potential to enhance data protection in the industrial sector.

To visualize the extent to which various methods address security challenges in industrial automation, Figure 2 presents a comparative analysis of the key characteristics of traditional (Pfleeger & Pfleeger, 2007) and blockchain-based approaches. The diagram compares both approaches across several dimensions, including data security, decentralization, attack resilience, confidentiality, implementation costs, scalability, system integration, and capabilities for traceability and auditing.

Based on the presented diagram, the advantages and limitations of different data protection methods in the context of industrial automation are observable. As shown, blockchain technology stands out particularly in the categories of decentralization, attack resilience, data

integrity, and capabilities for traceability and auditing, significantly outperforming traditional methods, which tend to be weaker in these areas. Techniques such as encryption and authentication still hold a critical position in ensuring trust within communication channels, while data backup and recovery remain essential for business continuity, especially in cases of data loss or

corruption (Latif et al., 2021).

However, in categories such as scalability and interoperability with other systems, blockchain presents moderate challenges, indicating that its implementation must be carefully planned according to the specific needs and architecture of a given system (Pieroni et al., 2020).

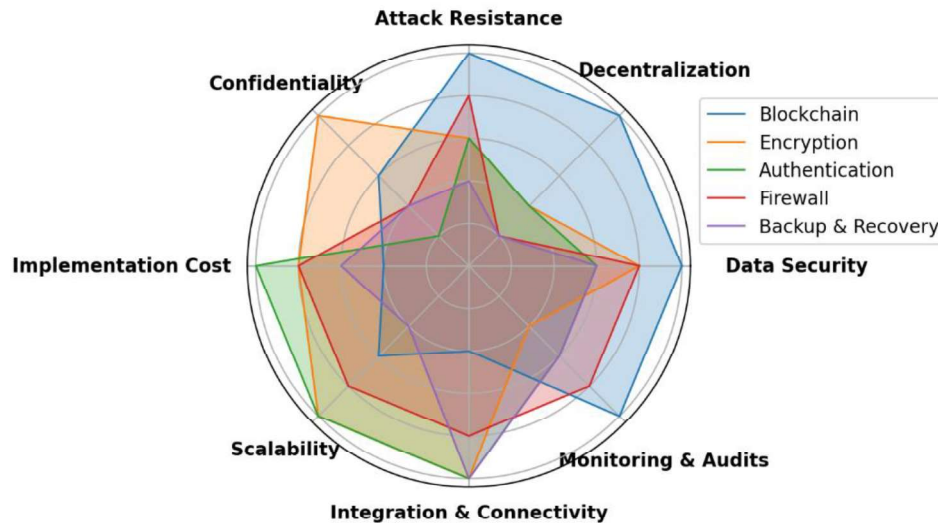


Figure 2. Comparative performance analysis of security methods across various criteria

This comparison explains the main features of each method and points to how they can complement one another through the combined use of different technologies. In modern industrial systems, achieving effective data protection increasingly depends on hybrid approaches, with blockchain acting not as a substitute, but as a key part of improving existing solutions. The qualitative findings confirm that timely adaptation of emerging technologies, such as blockchain, is essential to meet growing demands for security, transparency, and regulatory compliance. Therefore, Figure 2 serves not only as an overview of current technologies but also as a strategic roadmap for future decision-making in the digital transformation of industrial systems.

6. Conclusion

Blockchain technology shows significant potential in enhancing the protection of industrial data by offering decentralized, immutable, and transparent mechanisms that enable greater system resilience against unauthorized access, manipulation, and data loss. The implementation of automated security procedures further contributes to reducing reliance on manual processes and increasing operational efficiency.

The case study of the IBM Food Trust platform, used within Walmart's supply chain, illustrates how blockchain can improve traceability, integrity, and trust in industrial data flows. This specific application highlights blockchain's ability to address the limitations of traditional protection models, particularly in

environments requiring high levels of reliability and auditability.

However, technical and regulatory barriers still limit broader adoption. Challenges such as scalability, interoperability, energy efficiency, and misaligned regulatory frameworks pose serious issues, especially in the context of industrial automation that requires real-time data processing and stringent security standards. For example, the high energy consumption often associated with certain blockchain platforms can be a barrier to mass adoption in industrial systems that demand efficiency and low resource consumption.

Further development of this technology requires focused research toward achieving a balance between security, privacy, and performance. Special attention should be given to the development of interoperable solutions, energy-efficient consensus protocols, and alignment with regulatory standards. If these challenges are successfully addressed, blockchain technology could become a key pillar in the transformation of digital security for industrial systems, enabling more stable, secure, and transparent ecosystems for managing industrial processes and data.

References:

- Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access*, 7, 36500–36515. <https://doi.org/10.1109/access.2019.2903554>
- Anjum, A., Maheen, R., Nida, S., Maniyar, T. N., & Khan, Z. M. (2024). Traceability of fruits and vegetables agricultural products using blockchain. *International Journal for Multidisciplinary Research (IJFMR)*, 6(3), May–June. <https://doi.org/10.36948/ijfmr.2024.v06i03.19943>
- Bernal Bernabé, J., Cánovas, J. C., Hernández-Ramos, J., Torres Moreno, R., & Karmeta, A. (2024). Privacy-preserving solutions for blockchain: Review and challenges. *International Journal of Advanced Research*, 9(2), 359–361. <https://doi.org/10.21474/IJAR01/12455>
- Chigilipalli, B. K., Karri, T., Chetti, S. N., Bhiogade, G., Kottala, R. K., & Cheepu, M. (2023). A review on recent trends and applications of IoT in additive manufacturing. *Applied System Innovation*, 6(2), 50. <https://doi.org/10.3390/asi6020050>
- Chen, H., Wei, N., Wang, L., Mobarak, W. F. M., Albahar, M. A., & Shaikh, Z. A. (2024). The role of blockchain in finance beyond cryptocurrency: Trust, data management, and automation. *IEEE Access*, 12, 64861–64885. doi: 10.1109/ACCESS.2024.3395918
- Enemosah, A., & George, I. O. (2024). Cloud security frameworks for protecting IoT devices and SCADA systems in automated environments. *World Journal of Advanced Research and Reviews*, 22(3), 2232–2252. <https://doi.org/10.30574/wjarr.2024.22.3.1485>
- Gama, J., Ribeiro, R. P., & Veloso, B. (2022). Data-driven predictive maintenance. *IEEE Intelligent Systems*, 37(4), 27–29. <https://doi.org/10.1109/MIS.2022.3167561>
- Ghani, A. S. (2024). Revolutionizing supply chains: A comprehensive study of Industry 4.0 technologies (IoT, Big Data, AI, etc.). *International Journal of Scientific Research in Engineering and Management*, 8(4), 4191. <https://doi.org/10.55041/ijrsrem30037>
- Hammoudeh, M. (2021). Blockchain, internet of things and digital twins in trustless security of critical national infrastructure. In ICFNDS'20: *Proceedings of the 4th International Conference on Future Networks and Distributed Systems* (Article No. 43, p. 1). <https://doi.org/10.1145/3440749.3442650>

- IBM. (2025). IBM Food Trust – Documentation. IBM Documentation. Retrieved January 10, 2025, from <https://www.ibm.com/docs/en/food-trust>
- Ige, A. B., Adepoju, P. A., Akinade, A. O., & Afolabi, A. I. (2025). Machine learning in industrial applications: An in-depth review and future directions. *International Journal of Multidisciplinary Research and Growth Evaluation*, 6(1), 36–44. <https://doi.org/10.54660/ijmrge.2025.6.1.36-44>
- Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B., & Raza, U. (2020). Blockchain enabled supply chain: Analysis, challenges, and future directions. *Multimedia Systems*, 27(4), 787–806. <https://doi.org/10.1007/s00530-020-00687-0>
- Jasim, L. H. (2023). Analysing blockchain-based cryptography: Enhancing security, transparency, and practical implementations. In 2023 *International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD)* (pp. 39–44). Al-Najaf, Iraq. <https://doi.org/10.1109/ICTEASD57136.2023.10585016>
- Justinia, T. (2019). Blockchain technologies: Opportunities for solving real-world problems in healthcare and biomedical sciences. *ACTA INFORM MED.*, 27(4), 284–291. <https://doi.org/10.5455/aim.2019.27.284-291>
- Kumar, P., Choubey, D., Amosu, O. R., & Ogunsuji, Y. M. (2024). Blockchain and smart contracts for supply chain transparency and vendor management. *World Journal of Advanced Research and Reviews*, 23(2), 39–56. <https://doi.org/10.30574/wjarr.2024.23.2.2262>
- Latif, S., Idrees, Z., Huma, Z., & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies*, 32. <https://doi.org/10.1002/ett.4337>
- Michael, X. G., Kogias, D. G., Leligou, H.-C., Chatzigeorgiou, C., Feidakis, M., & Patrikakis, C. Z. (2020). A survey on the available blockchain platforms and protocols for supply chain management. In IOT4SAFE@ESWC. Retrieved from <https://api.semanticscholar.org/CorpusID:222008035>
- Oliveir, M., & Afonso, D. (2019). Industry focused in data collection: How Industry 4.0 is handled by big data. In DSIT 2019: *Proceedings of the 2019 2nd International Conference on Data Science and Information Technology* (pp. 12–18). Seoul, Republic of Korea. <https://doi.org/10.1145/3352411.3352414>
- Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in computing* (4th ed.). Prentice Hall.
- Pieroni, A., Scarpato, N., & Felli, L. (2020). Blockchain and IoT convergence—A systematic survey on technologies, protocols and security. *Applied Sciences*, 10(19), Article 6749. <https://doi.org/10.3390/app10196749>
- Rahman, A., Kundu, D., Debnath, T., Rahman, M., Aishi, A. A., & Islam, J. (2024). Blockchain-based AI methods for managing industrial IoT: Recent developments, integration challenges and opportunities. *arXiv preprint arXiv:2405.12550*. <https://api.semanticscholar.org/CorpusID:269930324>
- Shankaran, S. (2024). Maximizing operational efficiency: Utilizing blockchain for comprehensive tracking and visibility throughout the supply chain. *International Journal of Supply Chain and Logistics*, 8(4), 46–59. <https://doi.org/10.47941/ijscsl.2403>
- Tariq, U., Ibrahim, A., Ahmad, T., Bouteraa, Y., & Elmogy, A. (2019). Blockchain in Internet-of-Things: A necessity framework for security, reliability, transparency, immutability and liability. *IET Communications*, 13(19), 3187–3192. doi: 10.1049/iet-com.2019.0194

Tidrea, A., Korodi, A., & Silea, I. (2019). Cryptographic considerations for automation and SCADA systems using trusted platform modules. *Sensors*, 19(19), 4191. <https://doi.org/10.3390/s19194191>

Wagh, S. D. (2024). Implementation of manufacturing execution system (MES) to increase productivity and competitiveness in the manufacturing sector. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 12(IV). <https://doi.org/10.22214/ijraset.2024.60682>

Ana Đokić

Faculty of Engineering,
University of Kragujevac
Serbia

ana.djokic@its.edu.rs

ORCID 0009-0002-3469-586X

Milan Erić

Faculty of Engineering,
University of Kragujevac,
Serbia

ericm@kg.ac.rs

ORCID 0000-0001-8691-4863

Milan Čabarkapa

Faculty of Engineering,
University of Kragujevac,
Serbia

mcabarkapa@kg.ac.rs

ORCID 0000-0002-2094-9649

Hana Stefanović

School of Electrical and
Computer Engineering,
Belgrade,
Serbia

hanas@viser.edu.rs

ORCID 0000-0003-0890-4410
