International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Enhanced Cybersecurity Via Decentralized AI and Blockchain

Assistant Professor Kirandeep Kaur[1], Assistant Professor Manmeet Kaur[2], Ms. Arwinderjit Kaur[3]

Abstract

As artificial intelligence (AI) becomes ever more prevalent in cyber security, the call for AI systems that are both secure and decentralized grows stronger. In this context, block chain technology stands out as a powerful tool for enhancing both the security and the privacy of AI systems — thanks to its decentralized architecture and immutable record-keeping. This literature review explores how block chain technology and decentralized AI interlock within the cyber-security space. It begins by presenting a detailed taxonomy of block chain technologies and decentralized AI approaches in the context of cyber security, thereby providing the conceptual foundation for the study. Starting with an overview of block chain technology, the paper outlines its potential applications in cyber security — and also honestly discusses the challenges and opportunities involved. Next, it turns to decentralized AI, examining its possible advantages in cyber security settings (such as resilience, distributed intelligence, and improved privacy) along with the obstacles it faces.

On that basis, the review presents compelling findings that illustrate how block chain technology and decentralized AI can work together in beneficial ways — enhancing security, boosting privacy, and increasing trust in AI systems. The paper also highlights real-world use cases of block chain-enabled decentralized AI to show how these ideas can be applied to actual cyber security problems. Finally, the study sketches future research directions: what remains to be done, which applications hold real promise, and what implications this emerging convergence of technologies may have — emphasizing the potential of block chain-enabled decentralized AI to strengthen security, preserve privacy, and build trust in AI systems.

Keywords: Blockchain, Artificial intelligence, Decentralized ,Cybersecurity

INTRODUCTION:

The research questions regarding the convergence of blockchain (or Distributed Ledger Technology, DLT) and Artificial Intelligence (AI), especially in its decentralized form, for cybersecurity (or digital defense/security measures) can be addressed by examining their synergistic capabilities, the practical realities of their implementation, and existing academic efforts.

1) How does the integration of blockchain and AI enhance the robustness of cybersecurity measures?

The integration of AI and blockchain significantly enhances cybersecurity robustness by combining AI's predictive and analytical capabilities with blockchain's decentralized, immutable, and transparent architecture.

Proactive Threat Detection and Response: AI's Machine Learning (ML) and Deep Learning (DL) algorithms excel at anomaly detection and predictive analysis in real-time network traffic and behavior,

identifying subtle threats faster and more accurately than traditional systems. When integrated, blockchain secures the logging of these alerts and security events, ensuring the tamper-proof integrity of the evidence.

Example: AI detects an unusual pattern; this event is immediately recorded as an immutable block, preventing attackers from erasing their tracks.

Secure and Trustworthy AI Systems: Blockchain provides a decentralized, verifiable ledger for AI model parameters, training data, and updates. This ensures the integrity and trustworthiness of the AI's decision-making process, guarding against Adversarial AI attacks where malicious input could subtly corrupt the model.

Decentralized Identity and Access Management (DIAM): Blockchain enables self-sovereign identity (SSI), where users control their digital credentials. AI can enhance this by analyzing behavioral biometrics for continuous authentication, making access control more resilient and less reliant on single-point-of-failure password systems.

Automated and Secure Incident Response: Smart contracts on the blockchain can be programmed to execute automated incident response actions (e.g., isolating a compromised device or revoking access) the moment an AI model confirms a threat, reducing response latency and human error.

2) What are the primary obstacles and opportunities associated with implementing decentralized AI in the field of cybersecurity?

🚧 **Primary Obstacles**

Computational and Energy Overhead: Blockchain operations, particularly those using resource-intensive consensus mechanisms (like Proof-of-Work), introduce significant computational overhead and high energy consumption, which can be challenging for real-time security applications.

Scalability and Latency: The inherent design of many blockchain networks limits their transaction throughput and can introduce latency, potentially hindering the real-time responsiveness required for modern cyber defense, especially in high-volume environments like IoT.

Interoperability and Legacy Systems: Integrating decentralized AI and blockchain systems with existing legacy security infrastructure can be complex due to incompatible protocols, data formats, and governance models.

Governance and Skill Gaps: Decentralized security models can lead to governance complexities (lack of uniformity in policy enforcement) and require specialized expertise in cryptography, distributed systems, and decentralized AI/ML, which are often missing in organizational teams (skill gaps).

Adversarial AI: Malicious actors can also leverage AI to launch more sophisticated, automated cyberattacks (e.g., generating convincing phishing emails or discovering zero-day vulnerabilities), escalating the "cybersecurity arms race."

Primary Opportunities

Decentralized Threat Intelligence (DTI): A DLT-based platform allows organizations to securely and transparently share threat intelligence (e.g., newly detected malware signatures) without compromising data privacy. AI algorithms can analyze this globally distributed dataset for faster, more comprehensive threat analysis.

Enhanced Auditability and Accountability: The immutable ledger of the blockchain provides a transparent, unchangeable audit trail for all security events and AI decisions, greatly improving accountability and compliance, especially in regulated sectors like finance and healthcare.

Resilience and Single Point of Failure Mitigation: The distributed nature of the combined system eliminates single points of failure, making it inherently more resilient to Distributed Denial of Service (DDoS) and centralized compromise attacks.

Ethical and Transparent AI: Blockchain can enforce transparency in AI decision-making by logging model executions, moving toward Explainable AI (XAI), which is critical for ethical accountability in autonomous defense systems.

3) How have other researchers combined blockchain technology and decentralized AI within the realm of cybersecurity?

Researchers have explored several dominant models for combining DLT and decentralized AI:

Blockchain-Secured Federated Learning (FL): This is a key focus of decentralized AI. Researchers use FL to train a global AI/ML model collaboratively across many devices (nodes) without sharing the raw, sensitive data. The blockchain is then used to secure and verify the updates submitted by local models, ensuring the global model's integrity and preventing malicious nodes from poisoning the training process.

AI-Driven Smart Contracts for Incident Response: Work has been done on creating adaptive smart contracts. Here, an AI threat-detection engine (e.g., a machine learning classifier) serves as an "oracle" that triggers pre-defined security policies encoded in a smart contract. The contract automatically and immutably executes a remediation step (e.g., network segmentation) upon a high-confidence threat alert.

Decentralized Secure Logging and Auditing Systems: Many studies propose frameworks where security logs (from intrusion detection systems, firewalls, etc.) are hashed and recorded on a blockchain after being analyzed by an AI system. This creates a secure, verifiable record of events, which is essential for forensic analysis and compliance.

Biometric and Behavioral Authentication using DLT and AI: Research proposes combining AI's behavioral analysis (e.g., typing patterns, mouse movements) with blockchain-based decentralized identity systems. The AI verifies the user's continuous behavior, and the DLT secures the identity credentials and access permissions.

4) How do real-world use cases demonstrate the practical application of blockchain-enabled, decentralized AI solutions in effectively addressing cybersecurity challenges?

While large-scale commercial implementations are still emerging, the practical applications of blockchain-enabled, decentralized AI solutions are demonstrated in several critical areas:

Securing IoT Ecosystems: Challenge: IoT devices are numerous, heterogeneous, and often underpowered, creating vast attack surfaces.

Implementation: Ethereum-based frameworks use local AI models to detect anomalies while blockchain manages device identity, data sharing, and immutable event logging—enhancing detection accuracy and operational efficiency.

Decentralized Identity and Access Management:

Challenge: Centralized identity databases are prime targets for breaches.

Implementation: Blockchain-based identity systems, augmented by AI-driven behavioral authentication, are being piloted in financial and governmental sectors to secure identity data and mitigate unauthorized access.

Fraud Detection in Financial Systems:
Challenge: Modern financial fraud requires instantaneous analysis of complex transaction behaviors.
Implementation: AI algorithms analyze DLT-recorded transaction data to identify anomalies or suspicious transfers. Blockchain's transparency and immutability ensure integrity in fraud detection and investigation.
Supply Chain Integrity and Data Provenance:
Challenge: Ensuring product authenticity and data integrity across multi-stakeholder ecosystems.
Implementation: AI models monitor quality and logistics data, while blockchain records each stage immutably, offering verifiable proof of authenticity and reducing tampering risks throughout the supply chain
A nuanced viewpoint is offered through this research, which seeks to expand upon and bridge the gaps identified within the current body of literature. Furthermore, as illustrated in Figure 1, the taxonomy of blockchain technology and decentralized artificial intelligence in the context of cybersecurity is introduced, serving as an initial conceptual framework for further exploration.
Fig. 1. A taxonomy of blockchain and decentralized AI for cybersecurity.
The principal contributions of this research can be articulated as follows:
To begin with, this study delivers a holistic overview of the rapidly evolving field that integrates blockchain technology with decentralized artificial intelligence (AI) in the realm of cybersecurity.
Furthermore, it undertakes a thorough investigation of the potential advantages and limitations associated with the fusion of blockchain and decentralized AI to strengthen digital security frameworks.
In addition, the study introduces a well-structured taxonomy that systematically categorizes and organizes the essential elements and conceptual foundations of blockchain, decentralized AI, and their combined relevance to cybersecurity.
Moreover, it examines and presents empirical case studies that highlight the practical deployment of blockchain-based decentralized AI applications in mitigating cybersecurity risks.
Finally, the study outlines prospective research pathways intended to enhance the implementation of blockchain-driven decentralized AI in cybersecurity, thereby overcoming existing challenges and stimulating further innovation in this domain.
In the subsequent sections, this study provides an in-depth exploration of the convergence between blockchain technology and decentralized artificial intelligence (AI), along with their broader implications for cybersecurity. Section 2 investigates the application of blockchain technology within cybersecurity, detailing its core attributes, advantages, and limitations, and reviewing current solutions and frameworks. Section 3 turns attention to decentralized AI, analyzing its contributions, benefits, and challenges, as well as surveying existing implementations in the cybersecurity domain. Section 4, representing the central focus of this research, examines the integration of blockchain with decentralized AI for cybersecurity, illustrating this relationship through real-world case studies and evaluating their overall effectiveness. Section 5 discusses future research prospects, identifying potential directions for advancement and innovation in this emerging field. Finally, Section 6 presents a comprehensive conclusion, summarizing the key findings, insights, and contributions derived from the study.

2. Blockchain technology for cybersecurity

2.1. Blockchain technology and its features

Blockchain technology can be described as a distributed ledger system that enables the creation and mai-

ntenance of secure, transparent, and verifiable digital records [19]. It functions through a decentralized network of interconnected nodes, each responsible for verifying, validating, and recording transactions within a shared ledger. These transactions are grouped into blocks, which are cryptographically linked to one another, forming an immutable chain that ensures data integrity and chronological consistency [20]. The system employs consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to achieve agreement among nodes on the validity of transactions without relying on a central authority. Figure 2 provides a schematic representation of this operational process, illustrating how blockchain ensures trust, transparency, and immutability within a distributed environment [21].

Fig. 2. An overview of blockchain technologies [21].

The following are the Pros. of blockchain technology.

1) Decentralization:

Blockchain technology functions through a distributed network of nodes, eliminating dependence on any centralized authority or controlling body [22]. This decentralized structure enhances the security, transparency, and reliability of the network by minimizing single points of failure and making it more resistant to attacks or system breakdowns. By distributing decision-making and control across multiple nodes, organizations can develop systems that are more resilient, trustworthy, and less vulnerable to disruptions or malicious activities.

According to Chen and Bellavitis [23], Decentralized Finance (DeFi) represents a transformative financial framework built on blockchain technology, enabling financial transactions without intermediaries such as banks. The advantages of DeFi include greater accessibility, reduced transaction costs, and improved transparency. However, the authors emphasize that for DeFi to achieve its full potential, challenges concerning regulatory frameworks, scalability, and security must be effectively addressed. Additionally, the study highlights emerging trends within the DeFi ecosystem, including the proliferation of decentralized exchanges and the increasing use of stablecoins, reflecting its growing significance in reshaping the global financial landscape.

Aderibole et al. [24] suggested a decentralized conceptual model based on blockchain technology for smart grids to overcome the difficulties in controlling complicated energy infrastructure and facilitating safe and reliable energy transactions.

Balcerzak et al. [25] investigated how blockchain technology and smart contracts can be used in decentralized government techniques. The authors undertook a thorough literature review and highlighted the benefits of blockchain-based smart government systems, such as enhanced public engagement, trust in computationally networked urbanism, and democratized governing structures.

2) Security:

Blockchain technology guarantees tamper-resistant transaction security through the application of advanced cryptographic techniques [26,27]. Each transaction recorded on the blockchain becomes a permanent and immutable entry, ensuring that once data is added, it cannot be altered, deleted, or manipulated. This immutable ledger provides a transparent and verifiable record of all transactions, thereby enhancing trust and data integrity within the system.

Biswas and Muthukkumarasamy [28] proposed a security framework that integrates smart devices with blockchain technology to create a secure communication infrastructure for smart cities, as illustrated in Figure 3.

2.2. Challenges of blockchain in cybersecurity

1) Scalability:

Scalability represents a major limitation of blockchain technology [47]. The distributed framework of blockchain often poses challenges for large-scale cybersecurity applications, as it can lead to slower transaction throughput, increased latency, and network congestion, thereby affecting overall system performance and responsiveness.

2) Regulatory Compliance:

Compliance with regulatory standards remains a significant challenge in the adoption of blockchain for cybersecurity purposes [48]. Owing to its decentralized and autonomous nature, aligning blockchain operations with existing regulatory policies, legal requirements, and data governance frameworks can be complex and difficult to enforce.

3) Security Risks:

While blockchain is inherently designed to offer robust security, it is not entirely immune to cyber threats and vulnerabilities [49,50]. Attacks targeting consensus protocols or compromising specific nodes may jeopardize the security and reliability of the entire network, undermining the trust it seeks to establish.

4) Lack of Interoperability:

A lack of interoperability among different blockchain platforms and protocols continues to hinder the integration and scalability of blockchain-based cybersecurity systems [51]. This fragmentation restricts cross-platform communication, reduces operational efficiency, and limits the effectiveness of blockchain in addressing diverse cybersecurity challenges.

3. Decentralized AI for Cybersecurity

3.1 Overview of Decentralized AI and Its Benefits for Cybersecurity

Decentralized Artificial Intelligence (AI) refers to the deployment of AI algorithms and models across multiple distributed network nodes, rather than relying on a centralized computing system. Unlike conventional centralized AI architectures, where all data and computational processes occur within a single infrastructure, decentralized AI leverages distributed computing resources to enhance efficiency, scalability, and resilience.

Rawat et al. [77] presented a broad overview of AI applications in cybersecurity, examining the latest advancements in the field—particularly in security analysis and performance evaluation. Their research underscores the significance of employing AI-based solutions to mitigate cybersecurity challenges and proposes an AI-driven framework to strengthen system security. Furthermore, the authors emphasize the necessity for continued research to optimize AI integration in cybersecurity defense mechanisms.

Similarly, Trifonov et al. [78] explored cybersecurity challenges in Industrial Control Systems (ICSs) within the context of Industry 4.0. They advocated for the adoption of AI-driven techniques to improve resilience against cyber threats. The authors contrasted ICSs with traditional information systems and proposed a decentralized, flock-behavior-based architecture, suggesting it outperforms centralized management models for large-scale industrial operations. Their findings highlight the importance of identifying key performance indicators to assess and compare the efficiency of decentralized security frameworks.

In the healthcare sector, Ameen et al. [79] examined cybersecurity vulnerabilities in the Internet of Medical Things (IoMT) and stressed the associated privacy and security concerns. To address these

risks, they proposed integrating blockchain technology with AI within IoMT frameworks. Their study emphasizes the potential of combining decentralized AI and blockchain to enhance data security, privacy, and operational efficiency in healthcare ecosystems.

By facilitating faster threat detection, proactive response, and effective prevention, decentralized AI has the potential to transform the cybersecurity landscape. Its key benefits include:

Improved Threat Detection:

Decentralized AI enables organizations to identify and analyze potential cyber threats more accurately by utilizing diverse data sources and distributed computational capabilities [80].

Enhanced Privacy and Security:

By dispersing data processing across multiple nodes, decentralized AI ensures data confidentiality and reduces single points of failure, thereby minimizing the risk of cyberattacks [81].

Faster Response Time:

Distributing AI models across numerous nodes allows for rapid response and adaptation to emerging threats, improving both efficiency and resilience [82].

Increased Resilience:

Decentralized AI enhances the fault tolerance of cybersecurity systems by distributing data storage and processing tasks, thus mitigating risks associated with node failures or targeted attacks [83].

Better Collaboration:

It facilitates collaborative intelligence sharing among organizations and stakeholders, promoting a collective defense approach to cybersecurity [84].

Despite these significant advantages, implementing decentralized AI in cybersecurity poses several challenges—particularly concerning data integrity, interoperability, and regulatory compliance. Nevertheless, as decentralized technologies continue to evolve, they hold substantial promise for strengthening the robustness and adaptability of cybersecurity infrastructures.

3.2 Analysis of Challenges and Limitations of Decentralized AI in Cybersecurity

While decentralized AI offers transformative potential, its adoption in cybersecurity is hindered by multiple technical and regulatory challenges, including the following:

Data Quality and Integrity:

Effective training and deployment of decentralized AI models rely on high-quality, trustworthy data [85]. Ensuring consistency and reliability across diverse data sources remains difficult, especially when inputs vary in accuracy or credibility.

Interoperability:

The coexistence of different programming languages, architectures, and frameworks can impede model sharing and integration across heterogeneous networks or organizations [86].

Scalability:

Decentralized AI systems often demand substantial computational and storage resources, which can create scalability constraints in large or complex networks [86].

Security Risks:

Although designed for resilience, decentralized AI networks remain vulnerable to attacks on nodes or data pipelines. Ensuring the confidentiality, integrity, and authenticity of distributed models is an ongoing challenge [87].

Regulatory and Compliance Issues:

Adhering to legal and regulatory standards becomes complex when decentralized AI processes sensitive

or regulated data across multiple jurisdictions [48].

Lack of Standardization:

The absence of standardized protocols and evaluation metrics makes it difficult to compare and ensure compatibility among decentralized AI models and systems [88].

Addressing these constraints is crucial for unlocking the full potential of decentralized AI in cybersecurity, enabling more effective threat prediction, detection, and mitigation.

3.3 Review of Existing Decentralized AI Solutions for Cybersecurity

Decentralized AI holds the potential to redefine cybersecurity practices by supporting autonomous threat detection, faster response mechanisms, and proactive defense systems. Despite existing implementation barriers, several promising solutions illustrate its effectiveness in enhancing security, resilience, and trust within digital ecosystems.

Federated Learning (FL):

Federated Learning is a distributed machine learning paradigm that allows multiple devices or nodes to collaboratively train a shared model without exchanging raw data [89]. This approach preserves data privacy while maintaining model performance and adaptability. Figure 24 depicts the mechanism through which FL safeguards privacy by keeping sensitive data localized [90].

Blockchain-Enabled AI:

AI models can be decentralized and managed through blockchain-integrated frameworks, where the models are distributed across multiple network nodes [95]. This approach enhances the security, reliability, and robustness of AI systems while supporting efficient training, deployment, and scalability for various cybersecurity applications.

Lakhan et al. [96] proposed an innovative solution to address security and efficiency challenges in Industrial Internet of Things (IIoT)–based healthcare systems by introducing the Deep Reinforcement Learning-Aware Blockchain-Based Task Scheduling (DRLBTS) algorithm. This model facilitates secure and optimized task allocation within healthcare environments, effectively tackling issues related to privacy protection, data security, and processing efficiency such as makespan optimization.

3)

Decentralized Intrusion Detection: By utilizing distributed computing resources and AI algorithms, decentralized intrusion detection systems can be employed to identify and respond to cyber threats [97]. By allowing faster detection of and response to emerging threats, this strategy can help increase the resilience and responsiveness of cybersecurity systems. A cooperative intrusion detection framework serves as a case study to assess the effectiveness and practicality of the proposed system for unmanned aerial vehicles (UAVs) and similar applications. The findings demonstrate superior detection accuracy and reduced performance overhead in comparison with centralized methodologies. Moreover, the framework enhances data privacy and security by minimizing inter-node data exchange requirements. Future investigations will focus on evaluating the scalability and resilience of the proposed architecture under real-world UAV scenarios exposed to a variety of known cyber threats.

Fig. 26. A blockchain-based decentralized machine learning system [98].

4. Blockchain-enabled decentralized AI for cybersecurity

4.1. Introduction of the concept of blockchain-enabled decentralized AI for cybersecurity

In recent years, both Artificial Intelligence (AI) and blockchain technology have witnessed substantial progress and widespread adoption [103]. While AI continues to enhance its efficiency and effectiveness

across various domains, including cybersecurity, blockchain stands out for its ability to ensure secure, transparent, and decentralized record management. A promising intersection of these technologies lies in the development of decentralized AI models for cybersecurity, which leverage blockchain's distributed infrastructure alongside AI's analytical intelligence [95]. By utilizing the computational decentralization of blockchain networks, AI models can be deployed across multiple nodes, thereby strengthening their security, resilience, and fault tolerance.

Moreover, decentralized AI addresses several limitations of conventional centralized AI frameworks, particularly those concerning data confidentiality, privacy protection, and system reliability. Through approaches such as Federated Learning (FL) and other distributed AI training mechanisms, sensitive data can remain localized and protected while still enabling collaborative and efficient model training.

Within the scope of the Industrial Internet of Things (IIoT), Singh et al. [104] proposed a blockchain-enabled intelligent IoT framework that integrates AI to support real-time big data analytics, as depicted in Figure 30. The framework aims to overcome the shortcomings of centralized architectures—such as security risks, privacy breaches, resource limitations, and the shortage of training data for AI systems. Both qualitative and quantitative assessments revealed that the proposed model outperformed existing IoT frameworks in several aspects, including accuracy, latency, security, privacy, computational complexity, and energy efficiency. The integration of blockchain and AI thus facilitates scalable, transparent, and adaptive data analysis for IoT-based applications.

Nonetheless, certain challenges remain—most notably scalability, interoperability, and energy efficiency constraints. To mitigate these issues, the authors recommend incorporating machine intelligence principles and adaptive learning strategies into the architectural design, thereby enhancing system scalability, performance, and resilience in future implementations.

4.2. Analysis of the challenges and difficulties of blockchain-enabled decentralized AI for cybersecurity

The challenges of blockchain-enabled decentralized AI for cybersecurity are listed below.

Scalability: Deploying and maintaining decentralized AI models enabled by blockchain can be computationally intensive and require significant computing resources. As a result, scalability may be a considerable difficulty [12].

Network Connectivity: For decentralized AI models to be effective, they need very high levels of network connectivity and stability. In certain environments, especially in distant and/or less developed areas, this can be difficult [120].

Lack of Standards: For blockchain-enabled decentralized AI, there is presently a lack of standards and best practices. As a consequence, maintaining interoperability and security across many systems and networks may be difficult [121].

Regulatory and Legal Issues: A number of regulatory and legal challenges, specifically those related to data privacy and security, are brought up by the use of blockchain and AI in cybersecurity. Therefore, for enterprises seeking to adopt this strategy, overcoming regulatory and legal frameworks can be a major problem [121].

4.3. Review of existing blockchain-enabled decentralized AI solutions for cybersecurity

This section shows some of the existing solutions that offer insight into the future of cybersecurity and the role that blockchain and AI will play in tackling growing threats.

1)

PolySwarm: PolySwarm is a blockchain-based marketplace for threat intelligence that detects and responds to threats using a decentralized network of security experts and AI models [122]. The platform uses blockchain technology to facilitate secure and transparent interaction among various security experts and organizations.

DeepBrain Chain: DeepBrain Chain is a decentralized AI computing platform that employs blockchain technology to provide effective and affordable AI training and inference. Due to the platform's ability to share computational resources over a network of nodes, large-scale AI models can be trained more rapidly and cost-effectively than conventional centralized methods [123].

SingularityNET: Blockchain technology is used by SingularityNET, a decentralized AI marketplace, to facilitate the cooperation and sharing of AI models and services [124]. The platform makes it possible for developers and entrepreneurs to acquire and utilize AI models from many suppliers, fostering a more productive and cooperative AI ecosystem.

Enigma: Enigma is a blockchain-based, decentralized privacy protocol that permits secure and private data sharing and analysis [125]. Without disclosing sensitive information to a single party, the platform uses secure multi-party computational techniques to facilitate data analysis and AI model training.

IOTA: Using blockchain technology, the IOTA Foundation has created a decentralized method for intrusion detection. The system employs a distributed network of sensors and AI models to enhance the precision and effectiveness of intrusion detection while also detecting cyber threats in real time [126].

Sovrin: A blockchain-based IDMS called Sovrin leverages decentralized AI to offer secure and accurate identity authentication [127]. By allowing individuals and entities to securely communicate and verify identity information, a mechanism reduces the probability of fraud and identity theft [128].

5. Future research directions

Future Research Directions

This section outlines potential future research avenues for blockchain-enabled decentralized AI in cybersecurity, aimed at further advancing and strengthening this emerging technological paradigm. The following areas warrant deeper investigation from researchers and practitioners:

1) Integration of Blockchain and Decentralized AI:

Future research should focus on exploring more sophisticated integrations of blockchain and decentralized AI technologies to enhance cybersecurity capabilities. For example, blockchain could serve as a secure, transparent, and immutable framework for training, validating, and sharing AI models. Such integration may facilitate secure information exchange, collaborative threat detection, and rapid incident response, thereby transforming the cybersecurity landscape. Advancements in this domain could pave the way for more resilient and intelligent defense systems, enabling organizations to counter increasingly complex and evolving cyber threats.

2) Enhanced Interoperability:

Developing standardized and interoperable frameworks for blockchain and decentralized AI can substantially improve the efficiency and coordination of cybersecurity mechanisms. Future studies should explore methods to achieve cross-platform interoperability among different blockchain networks and decentralized AI architectures. Addressing this challenge would mitigate the current fragmentation of technologies, fostering seamless collaboration and data exchange between systems. Consequently,

improved interoperability could lead to faster, more accurate, and resource-efficient cybersecurity operations across diverse digital ecosystems.

3) Decentralized Identity Management:

Identity management remains a core pillar of cybersecurity, and future research should examine how blockchain and decentralized AI can be leveraged to design secure, scalable, and autonomous identity management systems. Investigating decentralized identity (DID) protocols and their integration with AI-driven authentication mechanisms can yield more robust, privacy-preserving, and user-centric solutions. Such innovations would significantly enhance the protection of user data and mitigate risks associated with unauthorized access to sensitive information. This research direction holds promise for developing trustworthy and scalable digital identity ecosystems critical for cybersecurity resilience.

4) Privacy-Preserving Blockchain and AI:

Given the growing importance of data confidentiality, future studies should investigate privacy-preserving techniques that combine blockchain and AI to safeguard sensitive information. Researchers could explore the incorporation of advanced cryptographic approaches, such as homomorphic encryption, zero-knowledge proofs, and differential privacy, to ensure secure computation and storage. This line of inquiry could lead to the development of trustworthy, privacy-enhancing blockchain-AI frameworks capable of protecting critical data assets while preventing unauthorized access and data leakage.

Conclusions

The escalating need for secure and distributed artificial intelligence (AI) within the realm of cybersecurity has motivated this investigation into the potential of blockchain technology. This study has explored the advantages and limitations of integrating blockchain and decentralized AI for cybersecurity applications, analyzing existing frameworks, real-world implementations, and emerging research trends. The findings indicate that the convergence of blockchain and decentralized AI systems holds immense potential to redefine cybersecurity by enabling trustworthy, transparent, and efficient data exchange, as well as intelligent threat identification and mitigation. Nonetheless, the realization of these benefits depends on addressing persistent challenges such as scalability, interoperability, and regulatory compliance. While existing solutions—including blockchain-based defense architectures and decentralized AI platforms—have demonstrated encouraging outcomes, there remains significant room for continued advancement toward more reliable, adaptive, and efficient systems.

The integration of blockchain with decentralized AI offers transformative benefits for cybersecurity. Through blockchain's immutable and transparent ledger, data authenticity and auditability are ensured, safeguarding AI-generated insights from manipulation or unauthorized alteration. Furthermore, the distributed and cooperative nature of these technologies facilitates autonomous threat detection, reduces response latency, and enhances accuracy in identifying and countering cyber threats, thereby reinforcing the resilience of digital defense mechanisms.

Looking forward, future research efforts should emphasize the seamless fusion of blockchain and decentralized AI, the development of interoperable standards, and the design of decentralized identity management systems that can strengthen user authentication and privacy protection. In addition, advancing privacy-preserving mechanisms and aligning with regulatory and ethical frameworks will be essential to ensure the trustworthy adoption of these technologies. Collectively, these directions can

accelerate the evolution of blockchain-empowered decentralized AI ecosystems that are more secure, transparent, and adaptable to the dynamic nature of cyber threats.

Ultimately, the synergy between blockchain and decentralized AI marks a pivotal step toward the next generation of cybersecurity infrastructure. Continued collaboration among academia, industry, and policymakers will be vital to developing innovative, resilient, and future-ready cybersecurity solutions capable of addressing the complex challenges of the modern digital landscape.

References

1. Z. Zhang, H. Ning, F. Shi, et al. Artificial intelligence in cyber security: research advances, challenges, and opportunities Artif. Intell. Rev., 55 (2) (2022), pp. 1029-1053, 10.1007/s10462-021-09976-0 View at publisherView in ScopusGoogle Scholar
2. J. Li Cyber security meets artificial intelligence: a survey Front. Inf. Technol. Electron. Eng., 19 (12) (2018), pp. 1462-1474, 10.1631/FITEE.1800573 View at publisherView in ScopusGoogle Scholar
3. I.H. Sarker, M.H. Furhad, R. Nowrozy AI-driven cybersecurity: an overview, security intelligence modeling and research directions SN Comput. Sci., 2 (3) (2021), p. 173, 10.1007/s42979-021-00557-0 View at publisherView in ScopusGoogle Scholar
4. B. Guembe, A. Azeta, S. Misra, et al. The emerging threat of AI-driven cyber attacks: a review Appl. Artif. Intell., 36 (1) (2022), Article 2037254, 10.1080/08839514.2022.2037254 View at publisher View in ScopusGoogle Scholar
5. M. Abdullahi, Y. Baashar, H. Alhussian, et al. Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: a systematic literature review Electron, 11 (2) (2022), p. 198, 10.3390/electronics11020198 View at publisherView in ScopusGoogle Scholar
6. P. Domingos A few useful things to know about machine learning Commun. ACM, 55 (10) (2012), pp. 78-87, 10.1145/2347736.2347755 View at publisherView in ScopusGoogle Scholar
7. L. Zhao, D. Zhu, W. Shafik, et al. Artificial intelligence analysis in cyber domain: a review Int. J. Distributed Sens. Netw., 18 (4) (2022), 10.1177/15501329221084882 View at publisher Google Scholar
8. R. Kaur, D. Gabrijelčič, T. Klobučar Artificial intelligence for cybersecurity: literature review and future research directions Inf. Fusion, 97 (2023), Article 101804, 10.1016/j.inffus.2023.101804 View PDFView articleView in ScopusGoogle Scholar
9. B.S. Sagar, S. Niranjan, K. Nithin, et al. Providing cyber security using artificial intelligence–a survey Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), IEEE (2019), pp. 717-720, 10.1109/iccmc.2019.8819719 View in ScopusGoogle Scholar
10. Y. Badr On the integration of artificial intelligence and blockchains 3.0: prospects and challenges Proceedings of the 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C), IEEE (2021), 10.1109/ICSA-C52384.2021.00031 120–120 Google Scholar
11. M. Liu, W. Yeoh, F. Jiang, et al. Blockchain for cybersecurity: systematic literature review and classification J. Comput. Inf. Syst., 62 (6) (2022), pp. 1182-1198, 10.1080/08874417.2021.1995914 View in ScopusGoogle Scholar

A. Deshmukh, N. Sreenath, A.K. Tyagi, et al. Blockchain enabled cyber security: a comprehensive survey Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI), IEEE (2022), pp. 1-6, 10.1109/ICCCI54379.2022.9740843 Google Scholar
12. J. Angelis, E. Ribeiro da Silva Blockchain adoption: a value driver perspective Bus. Horiz., 62 (3) (2019), pp. 307-314, 10.1016/j.bushor.2018.12.001 View PDFView articleView in ScopusGoogle Scholar
13. M. Swan Blockchain: Blueprint for a New Economy (first ed.), O'Reilly Media (2015) Google Scholar
14. K.Y. Yap, H.H. Chin, J.J. Klemeš Blockchain technology for distributed generation: a review of current development, challenges and future prospect Renew. Sustain. Energy Rev., 175 (2023), Article 113170, 10.1016/j.rser.2023.113170 View PDFView articleView in ScopusGoogle Scholar
15. Y. Maleh, S. Lakkineni, L. Tawalbeh, et al. Blockchain for cyber-physical systems: challenges and applications Y. Maleh, L. Tawalbeh, S. Motahhir, et al. (Eds.), Advances in Blockchain Technology for Cyber Physical Systems. Internet of Things, Springer, Cham (2022), pp. 11-59, 10.1007/978-3-030-93646-4_2 View in ScopusGoogle Scholar
A. Ekramifard, H. Amintoosi, A.H. Seno, et al. A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence. Advances in Information Security Springer International Publishing, Cham (2020), pp. 147-160, 10.1007/978-3-030-38181-3_8 Google Scholar
16. V. Buterin, J. Illum, M. Nadler, et al. Blockchain privacy and regulatory compliance: towards a practical equilibrium Blockchain Res. Appl, 5 (1) (2024), Article 100176, 10.1016/j.bcra.2023.100176 View PDFView articleView in ScopusGoogle Scholar
17. S. Nakamoto Bitcoin: a peer-to-peer electronic cash system http://www.bitcoin.org/bitcoin.pdf (2009), Accessed 1st Apr 2023 Google Scholar
18. W. Li, M. He, H. Sang An overview of blockchain technology: applications, challenges and future trends
19. Proceedings of the 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC), IEEE (2021), pp. 31-39, 10.1109/ICEIEC51955.2021.9463842 View in ScopusGoogle Scholar
20. D. Puthal, N. Malik, S.P. Mohanty, et al. Everything you wanted to know about the blockchain: its promise, components, processes, and problems IEEE Consum. Electron. Mag., 7 (4) (2018), pp. 6-14, 10.1109/MCE.2018.2816299 View in ScopusGoogle Scholar
21. W. Cai, Z. Wang, J.B. Ernst, et al. Decentralized applications: the blockchain-empowered software system IEEE Access, 6 (2018), pp. 53019-53033, 10.1109/ACCESS.2018.2870644 View in ScopusGoogle Scholar
22. Y. Chen, C. Bellavitis Decentralized finance: blockchain technology and the quest for an open financial system SSRN (2019), 10.2139/ssrn.3418557 Preprint Google Scholar
A. Aderibole, A. Aljarwan, M.H. Ur Rehman, et al. Blockchain technology for smart grids: decentralized NIST conceptual model IEEE Access, 8 (2020), pp. 43177-43190, 10.1109/ACCESS.2020.2977149 View in ScopusGoogle Scholar
23. A.P. Balcerzak, E. Nica, E. Rogalska, et al. Blockchain technology and smart contracts in decentralized governance systems, Adm Science, 12 (3) (2022), p. 96, 10.3390/admsci12030096 View in ScopusGoogle Scholar

24. H. Guo, X. Yu A survey on blockchain technology and its security Blockchain Res. Appl., 3 (2) (2022), Article 100067, 10.1016/j.bcra.2022.100067 View PDFView articleView in ScopusGoogle Scholar
25. O. Popoola, M. Rodrigues, J. Marchang, et al. A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions Blockchain Res. Appl., 5 (2) (2024), Article 100178, 10.1016/j.bcra.2023.100178 View PDFView articleView in ScopusGoogle Scholar
26. K. Biswas, V. Muthukkumarasamy Securing smart cities using blockchain technology Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE (2016), pp. 1392-1393, 10.1109/HPCC-SmartCity-DSS.2016.0198 Google Scholar
27. S.M. Idrees, M. Nowostawski, R. Jameel, et al. Security aspects of blockchain technology intended for industrial applications Electron, 10 (8) (2021), p. 951, 10.3390/electronics10080951 View in ScopusGoogle Scholar
A. Ghosh, S. Gupta, A. Dua, et al. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects J. Netw. Comput. Appl., 163 (2020), Article 102635, 10.1016/j.jnca.2020.102635 View PDFView articleView in ScopusGoogle Scholar
28. M. AlShamsi, S.A. Salloum, M. Alshurideh, S. Abdallah Artificial intelligence and blockchain for transparency in governance Stud. Comput. Intell., 912 (2021), pp. 219-230, 10.1007/978-3-030-51920-9_11 View in ScopusGoogle Scholar
29. M.M. Ibrahimy, A. Norta, P. Normak Blockchain-based governance models supporting corruption-transparency: a systematic literature review Blockchain Res. Appl., 5 (2) (2024), Article 100186, 10.1016/j.bcra.2023.100186 View PDFView articleView in ScopusGoogle Scholar
30. J. Sedlmeir, J. Lautenschlager, G. Fridgen, et al. The transparency challenge of blockchain in organizations, Electron Market, 32 (3) (2022), pp. 1779-1794, 10.1007/s12525-022-00536-0 View in ScopusGoogle Scholar
31. C. Bai, J. Sarkis A supply chain transparency and sustainability technology appraisal model for blockchain technology Int. J. Prod. Res., 58 (7) (2020), pp. 2142-2162, 10.1080/00207543.2019.1708989 View in ScopusGoogle Scholar
32. V. Singh, S.K. Sharma Application of blockchain technology in shaping the future of food industry based on transparency and consumer trust J. Food Sci. Technol., 60 (4) (2023), pp. 1237-1254, 10.1007/s13197-022-05360-0 View in ScopusGoogle Scholar
33. S.F. Papa Use of blockchain technology in agribusiness: transparency and monitoring in agricultural trade Proceedings of the Proceedings of the 2017 International Conference on Management Science and Management Innovation (MSMI 2017), Atlantis Press, Paris, France (2017), pp. 38-40, 10.2991/msmi-17.2017.9 Google Scholar
34. D. Ahmad, N. Lutfiani, A.D.A.R. Ahmad, et al. Blockchain technology immutability framework design in E-government J. Adm. Publik Public Adm. J., 11 (1) (2021), pp. 32-41, 10.31289/jap.v11i1.4310 Google Scholar
35. S. Rashidibajgan, T. Hupperich Utilizing blockchains in opportunistic networks for integrity and confidentiality Blockchain Res. Appl., 5 (1) (2024), Article 100167, 10.1016/j.bcra.2023.100167 View PDFView articleView in ScopusGoogle Scholar

36. N. Emmadi, H. Narumanchi Reinforcing immutability of permissioned blockchains with keyless signatures' infrastructure Proceedings of the Proceedings of the 18th International Conference on Distributed Computing and Networking, ACM (2017), pp. 1-6, 10.1145/3007748.3018280
37. Google Scholar
38. H. Stančić, V. Bralić Digital archives relying on blockchain: overcoming the limitations of data immutability Computers, 10 (8) (2021), p. 91, 10.3390/computers10080091 View in ScopusGoogle Scholar
39. F. Hofmann, S. Wurster, E. Ron, et al.
40. The immutability concept of blockchains and benefits of early standardization Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), IEEE (2017), pp. 1-8, 10.23919/ITU-WT.2017.8247004 View in ScopusGoogle Scholar
41. C. Zhang, C. Wu, X. Wang Overview of blockchain consensus mechanism Proceedings of the Proceedings of the 2020 2nd International Conference on Big Data Engineering, ACM (2020), pp. 7-12, 10.1145/3404512.3404522 Google Scholar
42. M. Hu, T. Shen, J. Men, et al. CRSM: an effective blockchain consensus resource slicing model for real-time distributed energy trading IEEE Access, 8 (2020), pp. 206876-206887, 10.1109/ACCESS.2020.3037694 View in ScopusGoogle Scholar
43. S. Zhang, J.H. Lee Analysis of the main consensus protocols of blockchain ICT Express, 6 (2) (2020), pp. 93-97, 10.1016/j.icte.2019.08.001 View PDFView articleGoogle Scholar
44. S. Maitra, V.P. Yanambaka, A. Abdelgawad, et al. Proof-of-authentication consensus algorithm: blockchain-based IoT implementation Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), IEEE (2020), pp. 1-2, 10.1109/WF-IoT48130.2020.9221187 Google Scholar
45. S. Mahmood, M. Chadhar, S. Firmin Cybersecurity challenges in blockchain technology: a scoping review Hum. Behav. Emerg. Technol., 2022 (2022), Article 7384000, 10.1155/2022/7384000 Google Scholar
46. D. Yang, C. Long, H. Xu, et al. A review on scalability of blockchain Proceedings of the Proceedings of the 2020 2nd International Conference on Blockchain Technology, ACM (2020), pp. 1-6, 10.1145/3390566.3391665 View in ScopusGoogle Scholar
47. P. Yeoh Regulatory issues in blockchain technology J. Financ. Regul. Compl., 25 (2) (2017), pp. 196-208, 10.1108/jfrc-08-2016-0068 View articleView in ScopusGoogle Scholar
48. E. Zamani, Y. He, M. Phillips, On the security risks of the blockchain J. Comput. Inf. Syst., 60 (6) (2020), pp. 495-506, 10.1080/08874417.2018.1538709 View in ScopusGoogle Scholar
49. H. Chen, X. Luo, L. Shi, et al. Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective, Blockchain Res Appl, 4 (3) (2023), Article 100135, 10.1016/j.bcra.2023.100135 View PDFView articleView in ScopusGoogle Scholar
50. R. Belchior, A. Vasconcelos, S. Guerreiro, et al. A survey on blockchain interoperability: past, present, and future trends ACM Comput. Surv., 54 (8) (2021), pp. 1-41, 10.1145/3471140 Google Scholar
A. Lakhan, M. Abed Mohammed, J. Nedoma, et al. Blockchain-enabled cybersecurity efficient IIOHT cyber-physical system for medical applications IEEE Trans. Netw. Sci. Eng., 10 (5) (2023), pp. 2466-2479, 10.1109/TNSE.2022.3213651 View in ScopusGoogle Scholar

51. O. Pal, B. Alam, V. Thakur, et al. Key management for blockchain technology ICT Express, 7 (1) (2021), pp. 76-80, 10.1016/j.icte.2019.08.002 View PDFView articleView in ScopusGoogle Scholar
52. S.S. Panda, D. Jena, B.K. Mohanta, et al. Authentication and key management in distributed IoT using blockchain technology IEEE Internet Things J., 8 (16) (2021), pp. 12947-12954, 10.1109/JIOT.2021.3063806 View in ScopusGoogle Scholar
53. H. Zhao, P. Bai, Y. Peng, et al. Efficient key management scheme for health blockchain CAAI Trans. Intell. Technol., 3 (2) (2018), pp. 114-118, 10.1049/trit.2018.0014 View in ScopusGoogle Scholar
54. Z. Ma, J. Zhang, Y. Guo, et al. An efficient decentralized key management mechanism for VANET with blockchain IEEE Trans. Veh. Technol., 69 (6) (2020), pp. 5836-5849, 10.1109/TVT.2020.2972923 View in ScopusGoogle Scholar
55. Y. Liu, D. He, M.S. Obaidat, et al. Blockchain-based identity management systems: a review J. Netw. Comput. Appl., 166 (2020), Article 102731, 10.1016/j.jnca.2020.102731 View PDFView articleView in ScopusGoogle Scholar
56. L. Stockburger, G. Kokosioulis, A. Mukkamala, et al. Blockchain-enabled decentralized identity management: the case of self-sovereign identity in public transportation Blockchain Res. Appl., 2 (2) (2021), Article 100014, 10.1016/j.bcra.2021.100014 View PDFView articleView in ScopusGoogle Scholar
57. I.T. Javed, F. Alharbi, B. Bellaj, et al. Health-ID: a blockchain-based decentralized identity management for remote healthcare Healthcare (Basel), 9 (6) (2021), p. 712, 10.3390/healthcare9060712 View in ScopusGoogle Scholar
58. S. El Haddouti, M.D. Ech-Cherif El Kettani Analysis of identity management systems using blockchain technology Proceedings of the 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE (2019), pp. 1-7, 10.1109/COMMNET.2019.8742375 Google Scholar
59. S.A. George, A. Jaekel, I. Saini Secure identity management framework for vehicular ad-hoc network using blockchain Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), IEEE (2020), pp. 1-6, 10.1109/ISCC50000.2020.9219736 Google Scholar
60. M. Naz, F.A. Al-zahrani, R. Khalid, et al. A secure data sharing platform using blockchain and interplanetary file system Sustain. Times, 11 (24) (2019), p. 7054, 10.3390/su11247054 View in ScopusGoogle Scholar
61. C. Singh, D. Chauhan, S.A. Deshmukh, et al. Medi-Block record: secure data sharing using block chain technology Inform. Med. Unlocked, 24 (2021), Article 100624, 10.1016/j.imu.2021.100624 View PDFView articleView in ScopusGoogle Scholar
62. M. Cash, M. Bassiouni Two-tier permission-ed and permission-less blockchain for secure data sharing Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), IEEE (2018), pp. 138-144, 10.1109/SmartCloud.2018.00031 View in ScopusGoogle Scholar
63. M.M. Queiroz, R. Telles, S.H. Bonilla Blockchain and supply chain management integration: a systematic review of the literature Supply Chain Manag., 25 (2) (2020), pp. 241-254, 10.1108/scm-03-2018-0143 View in ScopusGoogle Scholar

64. C. Allenbrand Smart contract-enabled consortium blockchains for the control of supply chain information distortion Blockchain Res. Appl., 4 (3) (2023), Article 100134, 10.1016/j.bcra.2023.100134
65. View PDFView articleView in ScopusGoogle Scholar
A. Di Vaio, L. Varriale Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry Int. J. Inf. Manag., 52 (2020), Article 102014, 10.1016/j.ijinfomgt.2019.09.010 View PDFView articleView in ScopusGoogle Scholar
A. Rejeb, J.G. Keogh, H. Treiblmaier Leveraging the Internet of Things and blockchain technology in supply chain management Future Internet, 11 (7) (2019), p. 161, 10.3390/fi11070161 View in ScopusGoogle Scholar
66. K. Almutairi, S.J. Hosseini Dehshiri, S.S. Hosseini Dehshiri, et al. Blockchain technology application challenges in renewable energy supply chain management Environ. Sci. Pollut. Res. Int., 30 (28) (2023), pp. 72041-72058, 10.1007/s11356-021-18311-7 View in ScopusGoogle Scholar
67. R. Saxena, E. Gayathri Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution Mater. Today Proc., 51 (2022), pp. 682-689, 10.1016/j.matpr.2021.06.204View PDFView articleView in ScopusGoogle Scholar
68. R. Graf, R. King Neural network and blockchain based technique for cyber threat intelligence and situational awareness Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon), IEEE (2018), pp. 409-426, 10.23919/CYCON.2018.8405028 Google Scholar
69. Y. Wu, Y. Qiao, Y. Ye, et al. Towards improved trust in threat intelligence sharing using blockchain and trusted computing Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE (2019), pp. 474-481, 10.1109/IOTSMS48152.2019.8939192 View in ScopusGoogle Scholar
70. D. Homan, I. Shiel, C. Thorpe A new network model for cyber threat intelligence sharing using blockchain technology Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE (2019), pp. 1-6, 10.1109/NTMS.2019.8763853 Google Scholar
71. H. Min Blockchain technology for enhancing supply chain resilience Bus. Horiz., 62 (1) (2019), pp. 35-45, 10.1016/j.bushor.2018.08.012 View PDFView articleView in ScopusGoogle Scholar Y. Kazancoglu, M. Ozbiltekin-Pala, M.D. Sezer, et al. Resilient reverse logistics with blockchain technology in sustainable food supply chain management during COVID-19 Bus. Strat. Environ., 32 (4) (2022), pp. 2327-2340, 10.1002/bse.3251 Google Scholar
72. R. Dubey, A. Gunasekaran, D.J. Bryde, et al. Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting Int. J. Prod. Res., 58 (11) (2020), pp. 3381-3398, 10.1080/00207543.2020.1722860 View in ScopusGoogle Scholar
73. B.S. Rawat, D. Gangodkar, V. Talukdar, et al. The empirical analysis of artificial intelligence approaches for enhancing the cyber security for better quality Proceedings of the 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), IEEE (2022), pp. 247-250, 10.1109/IC3I56241.2022.10072877 View in ScopusGoogle Scholar
74. R. Trifonov, S. Manolov, G. Tsochev, et al. Analytical choice of an effective cyber security structure with artificial intelligence in industrial control systems Proceedings of the 2022 10th International

Scientific Conference on Computer Science (COMSCI), IEEE (2022), pp. 1-6, 10.1109/COMSCI55378.2022.9912608 Google Scholar

75. A.H. Ameen, M. Abed Mohammed, A.N. Rashid Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: opportunities, challenges, and future directions J. Intell. Syst., 32 (1) (2023), Article 20220267, 10.1515/jisys-2022-0267 View in ScopusGoogle Scholar
76. H. Karimipour, F. Derakhshan Artificial intelligence for threat detection and analysis in industrial IoT: applications and challenges H. Karimipour, F. Derakhshan (Eds.), AI-enabled Threat Detection and Security Analysis for Industrial IoT, Springer, Cham (2021), pp. 1-6, 10.1007/978-3-030-76613-9_1 View in ScopusGoogle Scholar
77. V. Wylde, N. Rawindaran, J. Lawrence, et al. Cybersecurity, data privacy and blockchain: a review SN Comput. Sci., 3 (2) (2022), p. 127, 10.1007/s42979-022-01020-4 View in ScopusGoogle Scholar

B. Cicconetti, M. Conti, A. Passarella, A decentralized framework for serverless edge computing in the Internet of Things IEEE Trans. Netw. Serv. Manag., 18 (2) (2021), pp. 2166-2180, 10.1109/TNSM.2020.3023305 View in ScopusGoogle Scholar

78. X. Liang, C. Konstantinou, S. Shetty, et al. Decentralizing cyber physical systems for resilience: an innovative case study from A cybersecurity perspective Comput. Secur., 124 (2023), Article 102953, 10.1016/j.cose.2022.102953 View PDFView articleView in ScopusGoogle Scholar
79. P. Trakadas, P. Simoens, P. Gkonis, et al. An artificial intelligence-based collaboration approach in industrial IoT manufacturing: key concepts, architectural extensions and potential applications Sensors, 20 (19) (2020), p. 5480, 10.3390/s20195480 Google Scholar

A. Sundararajan, T. Khan, A. Moghadasi, et al. Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies J. Mod. Power Syst. Clean Energy, 7 (3) (2019), pp. 449-467, 10.1007/s40565-018-0473-6 View in ScopusGoogle Scholar

80. K. Salah, M.H.U. Rehman, N. Nizamuddin, et al. Blockchain for AI: review and open research challenges IEEE Access, 7 (2019), pp. 10127-10149, 10.1109/ACCESS.2018.2890507 View in ScopusGoogle Scholar
81. H. Yuan, S. Li Cyber security risks of net zero technologies Proceedings of the 2022 IEEE Conference on Dependable and Secure Computing (DSC), IEEE (2022), pp. 1-11, 10.1109/DSC54232.2022.9888883 View in ScopusGoogle Scholar
82. P. Asuquo, C. Ogah, W. Hathal, et al., Blockchain meets cybersecurity: security, privacy, challenges, and opportunity. in: S. Kim, G. Deka, (Eds.) Advanced Applications of Blockchain Technology. Springer, Singapore, pp. 115–127. https://doi.org/10.1007/978-981-13-8775-3_5. Google Scholar
83. L. Bhatia, S. Samet A decentralized data evaluation framework in federated learning Blockchain Res. Appl., 4 (4) (2023), Article 100152, 10.1016/j.bcra.2023.100152 View PDFView articleView in ScopusGoogle Scholar
84. M. Alazab, S.P. Rm, M. Parimala, et al. Federated learning for cybersecurity: concepts, challenges, and future directions IEEE Trans. Ind. Inf., 18 (5) (2022), pp. 3501-3509, 10.1109/TII.2021.3119038 View in ScopusGoogle Scholar
85. K. Li, H. Zhou, Z. Tu, et al. Blockchain empowered federated learning for distributed network security behaviour knowledge base in 6G Secur. Commun. Network., 2022 (2022), Article 4233238, 10.1155/2022/4233238 View in ScopusGoogle Scholar

C. Ghimire, D.B. Rawat Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things IEEE Internet Things J., 9 (11) (2022), pp. 8229-8249, 10.1109/JIOT.2022.3150363 View in ScopusGoogle Scholar
86. V. Mothukuri, R.M. Parizi, S. Pouriyeh, et al. FabricFL: blockchain-in-the-loop federated learning for trusted decentralized systems IEEE Syst. J., 16 (3) (2022), pp. 3711-3722, 10.1109/JSYST.2021.3124513 View in ScopusGoogle Scholar
87. M. Abed Mohammed, A. Lakhan, K.H. Abdulkareem, et al. Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks Internet Things, 22 (2023), Article 100815, 10.1016/j.iot.2023.100815 Google Scholar
88. F. Muheidat, L. Tawalbeh Artificial intelligence and blockchain for cybersecurity applications Y. Maleh, Y. Baddi, M. Alazab, et al. (Eds.), Studies in Big Data, Springer, Cham (2021), pp. 3-29, 10.1007/978-3-030-74575-2_1 Google Scholar
A. Lakhan, M.A. Mohammed, J. Nedoma, et al. DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system Sci. Rep., 13 (1) (2023), p. 4124, 10.1038/s41598-023-29170-2 View in ScopusGoogle Scholar
89. S.D. Roy, S. Debbarma, A. Iqbal A decentralized intrusion detection system for security of generation control IEEE Internet Things J., 9 (19) (2022), pp. 18924-18933, 10.1109/JIOT.2022.3163502 View in ScopusGoogle Scholar
90. A.A. Khan, M.M. Khan, K.M. Khan, et al. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs Comput. Network., 196 (2021), Article 108217, 10.1016/j.comnet.2021.108217 View PDFView articleView in ScopusGoogle Scholar
91. M. Abdel-Basset, N. Moustafa, H. Hawash, et al. Federated intrusion detection in blockchain-based smart transportation systems IEEE Trans. Intell. Transport. Syst., 23 (3) (2022), pp. 2523-2537, 10.1109/TITS.2021.3119968 View in ScopusGoogle Scholar
92. R. Amirta, M.S. Deepika, R.G. Franklin Decentralized access control with anonymous authentication of data stored using blockchain Rese. Jour. Engin. And Technol., 11 (1) (2020), p. 10, 10.5958/2321-581x.2020.00002.1 Google Scholar
93. H. Mrabet, A. Alhomoud, A. Jemai, et al. A secured industrial Internet-of-Things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing
94. Appl. Sci., 12 (9) (2022), p. 4641, 10.3390/app12094641- View in ScopusGoogle Scholar
95. Y. Ding, H. Sato Derepo: a distributed privacy-preserving data repository with decentralized access control for smart health Proceedings of the 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), IEEE (2020), pp. 29-35, 10.1109/CSCloud-EdgeCom49738.2020.00015 View in ScopusGoogle Scholar
96. M. Javaid, A. Haleem, R.P. Singh, et al. Blockchain technology applications for Industry 4.0: a literature-based review Blockchain Res. Appl., 2 (4) (2021), Article 100027, 10.1016/j.bcra.2021.100027
97. View PDFView articleView in ScopusGoogle Scholar\

98. S.K. Singh, S. Rathore, J.H. Park, BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence Future Generat. Comput. Syst., 110 (2020), pp. 721-743, 10.1016/j.future.2019.09.002 View PDFView articleView in ScopusGoogle Scholar
99. H. ElHusseini, C. Assi, B. Moussa, et al. Blockchain, AI and smart grids: the three musketeers to a decentralized EV charging infrastructure IEEE Internet Things Mag, 3 (2) (2020), pp. 24-29, 10.1109/IOTM.0001.1900081 View in ScopusGoogle Scholar
100. S.A. Wright, Blockchain-enabled decentralized network management in 6G. in: M.D. Borah, P. Singh, G.C. Deka, (Eds.) AI and Blockchain Technology in 6G Wireless Network. Blockchain Technologies. Springer, Singapore. pp. 45–69. https://doi.org/10.1007/978-981-19-2868-0_3. Google Scholar
101. X. Lin, R. Xu, Y. Chen, et al. A blockchain-enabled decentralized time banking for a new social value system Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), IEEE (2019), pp. 1-5, 10.1109/CNS.2019.8802734 View in ScopusGoogle Scholar
102. S. Ismail, M. Nouman, D.W. Dawoud, et al. Towards a lightweight security framework using blockchain and machine learning Blockchain Res. Appl., 5 (1) (2024), Article 100174, 10.1016/j.bcra.2023.100174
103. View PDFView articleView in ScopusGoogle Scholar
104. K. Kaushik, Blockchain enabled artificial intelligence for cybersecurity systems. in: M. Ouaissa, Z. Boulouard, M. Ouaissa, et al, (Eds.) Big Data Analytics and Computational Intelligence for Cybersecurity. Springer, Cham. pp. 165–179. https://doi.org/10.1007/978-3-031-05752-6_11. Google Scholar
D. Rabieinejad, A. Yazdinejad, A. Dehghantanha, et al.Secure AI and blockchain-enabled framework in smart vehicular networks Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), IEEE (2021), pp. 1-6, 10.1109/GCWkshps52748.2021.9682140 Google Scholar
105. A.K. Das, B. Bera, S. Saha, et al. AI-envisioned blockchain-enabled signature-based key management scheme for industrial cyber–physical systems IEEE Internet Things J., 9 (9) (2022), pp. 6374-6388, 10.1109/JIOT.2021.3109314 View in ScopusGoogle Scholar
106. F.S.A. Pour, P.N.-M. Gheorghe A blockchain-enabled model to enhance disaster aids network resilience, Rom Cyber Secur. J., 3 (2) (2021) https://digitalcommons.odu.edu/emse_fac_pubs/87, Accessed 30th Mar 2023 Google Scholar
107. F.S.A. Pour Application of a Blockchain Enabled Model in Disaster Aids Supply Network Resilience – ProQuest Old Dominion University (2021) Google Scholar
108. M. Mylrea, S.N.G. Gourisetti Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security Proceedings of the 2017 Resilience Week (RWS), IEEE (2017), pp. 18-23, 10.1109/RWEEK.2017.8088642 View in ScopusGoogle Scholar
A. Hajian, H.C. Chang A blockchain-based smart grid to build resilience through zero-trust cybersecurity M. Fathi, E. Zio, P.M. Pardalos (Eds.), Handbook of Smart Energy Systems, Springer, Cham (2022), pp. 1-19, 10.1007/978-3-030-72322-4_161-1 Google Scholar
109. Z. Mahmood, V. Jusas Blockchain-enabled: multi-layered security federated learning platform for preserving data privacy Electronics, 11 (10) (2022), p. 1624, 10.3390/electronics11101624
110. View in ScopusGoogle Schola

111. Y. Qu, L. Gao, T.H. Luan, et al., Decentralized privacy using blockchain-enabled federated learning in fog computing IEEE Internet Things J., 7 (6) (2020), pp. 5171-5183, 10.1109/JIOT.2020.2977383, View in ScopusGoogle Scholar
A. Kanak, N. Ugur, S. Ergun, A visionary model on blockchain-based accountability for secure and collaborative digital twin environments Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), IEEE (2019), pp. 3512-3517, 10.1109/SMC.2019.8914304 View in ScopusGoogle Scholar
112. Y. Song, Y. Fu, F.R. Yu, et al. Blockchain-enabled Internet of vehicles with cooperative positioning: a deep neural network approach IEEE Internet Things J., 7 (4) (2020), pp. 3485-3498, 10.1109/JIOT.2020.2972337 View in ScopusGoogle Scholar
A. Kumari, R. Gupta, S. Tanwar, et al. A taxonomy of blockchain-enabled softwarization for secure UAV network Comput. Commun., 161 (2020), pp. 304-323, 10.1016/j.comcom.2020.07.042 View PDFView articleView in ScopusGoogle Scholar
113. R. Shinde, S. Patil, K. Kotecha, et al. Blockchain for securing AI applications and open innovations J. Open Innov. Technol. Mark. Complex., 7 (3) (2021), p. 189, 10.3390/joitmc7030189 View PDFView articleView in ScopusGoogle Scholar
114. PolySwarm - Crowdsourced threat detection. https://polyswarm.io. Accessed: 18 March 2023. Google Scholar
115. Reshi, M. Khan, S. Shafi, et al. AI-Powered Smart Contracts: the Dawn of Web 4 TechRxiv (2023), 10.36227/TECHRXIV.22189438.V1 Google Scholar
116. C.B. Goertzel, S. Giacomelli, D. Hanson, et al. SingularityNET: a decentralized, open market and inter-network for AIs, Thoughts Theor. Stud. Artif. Intell. Res (2017) Google Scholar
117. S.K. Rana, S.K. Rana, K. Nisar, et al. Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare Sustainability, 14 (15) (2022), p. 9471, 10.3390/su14159471 View in ScopusGoogle Scholar
118. IOTA, https://www.iota.org/. Accessed: 1 April 2023. Google Scholar
119. Sovrin, https://sovrin.org/. Accessed: 1 April 2023. Google Scholar
120. N. Naik, P. Jenkins Sovrin network for decentralized digital identity: analysing a self-sovereign identity system based on distributed ledger technology Proceedings of the 2021 IEEE International Symposium on Systems Engineering (ISSE), IEEE (2021), pp. 1-7, 10.1109/ISSE51541.2021.9582551
121. View at publisherGoogle Scholar