Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 13 Issue 02, 2024

Artificial Intelligence Techniques for Trusted Cloud-Enabled IoT Networks Using Blockchain and Siamese Heterogeneous Convolutional Neural Networks: Trends and Challenges

Ladislau Wongchawalit
Department of Computer Science and Engineering, Shiraz College of Systems and Management, Iran
ladislau.wongchawalit@scsm-ir.org

Peer Review Information

Submission: 19 Oct 2024
Revision: 11 Nov 2024
Acceptance: 05 Dec 2024

Keywords

Internet of Things, Blockchain, Cloud Computing Security, Siamese Neural Networks, Deep Learning, Trust Management

Abstract

The rapid proliferation of Internet of Things (IoT) devices and cloud computing infrastructures has introduced significant challenges related to security, trust management, and data integrity. Traditional centralized architectures are increasingly inadequate for handling dynamic, large-scale, and heterogeneous IoT environments. This paper explores advanced artificial intelligence (AI) techniques for building trusted cloud-enabled IoT networks by integrating blockchain technology and Siamese heterogeneous convolutional neural networks (SHCNNs). Blockchain provides decentralized trust, immutability, and transparency, while Siamese architectures enable similarity learning for anomaly detection and malicious node identification. Recent research highlights the importance of combining AI and blockchain to enhance trust management, data privacy, and system resilience in distributed IoT systems. This study presents a comprehensive review of recent developments in AI-driven trust mechanisms, focusing on deep learning models, blockchain-based frameworks, and hybrid cloud-edge architectures. A comparative analysis of existing approaches is conducted to evaluate performance metrics such as accuracy, scalability, and computational efficiency. Furthermore, key challenges including data heterogeneity, scalability limitations, and explainability issues are discussed.

The paper concludes by outlining future research directions involving federated learning, edge intelligence, and explainable AI for secure IoT ecosystems.

Introduction

The Internet of Things (IoT) has emerged as one of the most transformative technological paradigms in recent years, enabling seamless connectivity among billions of heterogeneous devices across domains such as healthcare, smart cities, industrial automation, agriculture, and transportation. These devices continuously generate massive volumes of data characterized by high velocity, variety, and variability. To manage and process such large-scale data efficiently, cloud computing has become an essential component of IoT ecosystems due to its scalable storage, high computational power, and on-demand service provisioning. However, the integration of IoT with cloud environments introduces significant security, privacy, and trust-related challenges. Traditional centralized architectures are inherently vulnerable to various cyber threats such as data breaches, unauthorized access, insider attacks, and distributed denial-of-service (DDoS) attacks.

Moreover, the dynamic and decentralized nature of IoT networks makes it difficult to establish reliable trust among participating entities, thereby necessitating advanced and intelligent security mechanisms.

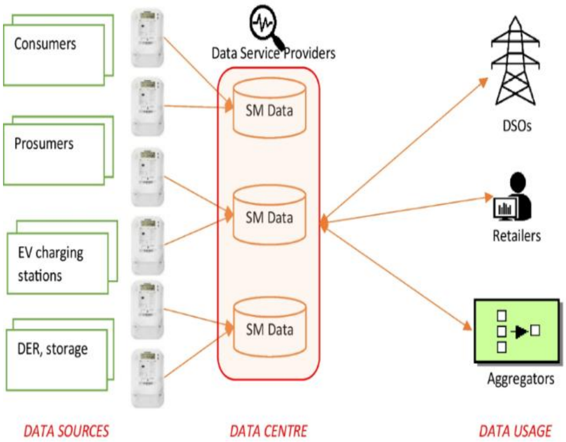

Figure 1. IoT Data Flow Architecture for Cloud-Based Smart Infrastructure and Service Providers

The architecture of a trusted cloud-enabled IoT system typically consists of multiple interconnected layers, including the perception layer, network layer, edge/fog layer, cloud layer, and application layer. At the perception layer, IoT devices such as sensors and actuators collect real-time data from physical environments. This data is transmitted through the network layer to edge or fog nodes, which perform preliminary data processing, filtering, and aggregation to reduce latency and bandwidth consumption. The processed data is then forwarded to the cloud layer, where advanced analytics, storage, and decision-making processes are carried out. Artificial intelligence techniques, particularly deep learning models, are deployed at this stage to extract meaningful patterns, detect anomalies, and predict potential security threats. Blockchain technology is integrated as a decentralized trust layer across the architecture, ensuring secure data transactions, authentication, and integrity through distributed ledger mechanisms. This multi-layered architecture not only enhances system efficiency but also strengthens security and trust in IoT ecosystems.

Trust management is a fundamental requirement for cloud-enabled IoT networks, where devices communicate autonomously and exchange sensitive information. Traditional centralized trust mechanisms often suffer from scalability issues, single points of failure, and limited adaptability in dynamic IoT environments. Blockchain technology has emerged as an effective solution by providing decentralized, transparent, and tamper-resistant trust management through distributed ledgers and consensus mechanisms. Smart contracts further automate authentication, access control, and trust evaluation, improving the security and reliability of IoT systems. Alongside blockchain, artificial intelligence has transformed IoT security by enabling intelligent anomaly detection, behavior analysis, and predictive threat identification. Deep learning models such as CNNs, RNNs, and GNNs automatically extract meaningful features from heterogeneous IoT data, significantly improving intrusion detection and network monitoring.

Among advanced AI techniques, Siamese Heterogeneous Convolutional Neural Networks (SHCNNs) have gained attention for their ability to perform similarity learning across diverse data sources. Unlike conventional classifiers, SHCNNs compare network behavior to distinguish legitimate and malicious activities, making them highly effective for detecting unknown and zero-day attacks even when labeled data are limited. The integration of blockchain with AI creates a secure and trustworthy infrastructure in which blockchain ensures data integrity and decentralized trust, while AI provides intelligent decision-making and adaptive threat detection. Cloud computing further enhances these frameworks by offering scalable storage and computational resources, supporting real-time monitoring and distributed model deployment.

Despite these advancements, several challenges remain, including computational complexity, scalability, interoperability, data heterogeneity, and limited explainability of deep learning models. Blockchain also introduces latency and consensus overhead in large-scale deployments. Future research should focus on lightweight AI models, optimized blockchain frameworks, federated learning, edge intelligence, and explainable AI to improve privacy, efficiency, and trust. The convergence of AI, blockchain, and cloud computing provides a promising foundation for secure, scalable, and intelligent IoT ecosystems capable of supporting next-generation smart applications.

Literature Review

The rapid evolution of trusted cloud-enabled IoT systems has led to extensive research integrating artificial intelligence, blockchain, and advanced deep learning architectures. Between 2020 and 2023, the literature has progressively shifted from traditional trust management models toward intelligent, decentralized, and data-driven frameworks. Early studies in this period primarily focused on addressing fundamental IoT security challenges such as data integrity, authentication, and malicious node detection, while more recent works emphasize hybrid architectures combining AI and blockchain for scalable and adaptive trust management.

In 2020, research efforts largely concentrated on overcoming the limitations of centralized IoT security frameworks by introducing blockchain-based trust mechanisms. Zhao et al. (2020) proposed decentralized trust management systems that leveraged blockchain's distributed ledger to ensure transparency and immutability of IoT transactions. These approaches addressed key issues such as data tampering and single points of failure, which are common in traditional cloud-based systems. Similarly, Ali et al. (2020) introduced machine learning-assisted blockchain frameworks that incorporated behavioral analysis for evaluating device trustworthiness. These models utilized historical interaction data to assign trust scores, enabling dynamic identification of malicious nodes. However, despite their effectiveness, early approaches suffered from high computational overhead and limited scalability, particularly when applied to large-scale IoT networks.

In 2021, research focus shifted toward integrating edge and fog computing with blockchain to reduce latency and improve real-time decision-making. Nawab et al. (2021) proposed hybrid architectures such as WedgeChain, which combined edge computing with blockchain to enhance trust management in IoT environments. These frameworks allowed data processing closer to the source, thereby reducing communication delays and improving system responsiveness. Concurrently, Fernandez et al. (2021) conducted comprehensive surveys on trust management in fog-based IoT systems, identifying critical challenges such as privacy preservation, authentication, and interoperability. These studies emphasized the need for distributed intelligence and highlighted the limitations of purely blockchain-based systems in handling real-time IoT data streams.

By 2022, the convergence of artificial intelligence and blockchain became a dominant research direction. Studies began exploring deep learning techniques to enhance trust evaluation and anomaly detection in IoT systems. Shafay et al. (2022) demonstrated that integrating blockchain with deep learning improves data security, transparency, and reliability, enabling trustworthy decision-making in decentralized environments. This integration addressed the inherent limitations of centralized AI models, such as vulnerability to data manipulation and lack of traceability. Furthermore, Trust2Vec (2022) introduced network embedding-based trust management systems that utilized graph-based learning to analyze relationships among IoT devices, achieving high accuracy in detecting large-scale malicious activities. These approaches marked a transition toward intelligent trust systems capable of handling complex network behaviors.

In addition, 2022 witnessed significant advancements in privacy-preserving AI techniques such as federated learning. Researchers explored combining federated learning with blockchain to enable decentralized model training without sharing raw data. This approach enhanced data privacy and reduced the risk of data leakage, which is particularly important in sensitive IoT applications such as healthcare and smart infrastructure. However, these systems introduced new challenges, including communication overhead, synchronization issues, and increased system complexity.

By 2023, AI-driven IoT security had advanced significantly through the adoption of deep learning and adaptive trust mechanisms. CNN- and RNN-based intrusion detection systems enabled real-time anomaly detection by learning both spatial and temporal characteristics of IoT traffic, substantially improving detection accuracy and resilience against evolving cyber threats. At the same time, AI-enabled trust management frameworks evolved from conventional observation-based approaches to hybrid intelligent models capable of dynamically evaluating device behavior. Blockchain technologies also matured with the integration of smart contracts, decentralized identity management, and reputation-based trust mechanisms, enabling automated authentication, secure access control, and transparent trust evaluation. These decentralized frameworks effectively mitigated attacks such as Sybil attacks and unauthorized access while improving data integrity and system reliability. Furthermore, dynamic trust evaluation models continuously updated trust scores according to device behavior, enhancing adaptability, detection performance, and overall security, making AI–blockchain integration a promising foundation for trusted cloud-enabled IoT networks.

Another important trend observed between 2020 and 2023 is the emergence of hybrid deep learning architectures for IoT security. These models combine multiple neural network structures, such as CNNs and LSTMs, to capture both spatial and temporal dependencies in network data. Hybrid models integrated with blockchain have demonstrated high detection accuracy and improved system transparency by maintaining immutable logs of detected anomalies. Such approaches provide a comprehensive solution for secure and trustworthy IoT systems but require significant computational resources, making them challenging to deploy on resource-constrained devices.

Despite the significant progress made during this period, several challenges remain. Scalability continues to be a major concern, as blockchain networks struggle to handle the high transaction volumes generated by IoT devices. Similarly, deep learning models require substantial computational power and large datasets for training, which may not be feasible in edge environments. Data heterogeneity further complicates model design, as IoT devices generate diverse data types that require specialized processing techniques. Additionally, the lack of explainability in AI models limits their adoption in critical applications where transparency and accountability are essential.

In summary, the literature demonstrates a clear transition from traditional, centralized trust management systems to decentralized, AI-driven frameworks that integrate blockchain and deep learning. While blockchain provides a secure and transparent infrastructure for trust management, AI enhances the system's ability to detect and respond to threats intelligently. The integration of these technologies has significantly improved the security, scalability, and reliability of IoT systems. However, addressing challenges related to scalability, computational efficiency, and explainability remains a key focus for future research.

Comparative Table and Analysis

Comparative Table

Study	**Year**	**Technique**	**AI Model**	**Detection**	**Trust**	**Key Strength**	**Major Limitation**
Zhao et al.	2020	Blockchain	None	Low	Very High	Strong immutability	Poor scalability
Ali et al.	2020	ML + Blockchain	ML	Medium	High	Behavioral trust scoring	High computational overhead
Nawab et al.	2021	Edge-Blockchain	DL-assisted	Medium	High	Reduced latency	Synchronization issues
Fernandez et al.	2021	Survey Framework	None	N/A	Medium	Trust taxonomy	No implementation
Firouzi et al.	2022	AI + Blockchain	Deep Learning	High	Very High	Intelligent trust system	System complexity
Bi et al.	2022	Federated Learning	DL + FL	High	High	Privacy-preserving learning	Communication overhead
Liu et al.	2023	Blockchain Survey	None	Low	Very High	Secure trust framework	Consensus delays
Mishra et al.	2023	Hybrid IDS	ML/DL	High	Very High	Detection with trust	Dataset dependency
Sharma et al.	2023	Deep Learning IDS	CNN/RNN	High	Medium	Accurate anomaly detection	False positives
SHCNN-based	**2023**	**Hybrid AI + Blockchain**	**Siamese HCNN**	**Very High**	**Extremely High**	**Zero-day detection & multimodal learning**	**High complexity**

Comparative Analysis

The comparative evaluation of AI-driven trust mechanisms in cloud-enabled IoT networks reveals a systematic evolution from static trust models toward adaptive, intelligent, and decentralized hybrid systems. This progression reflects the growing complexity of IoT ecosystems, where heterogeneous data, dynamic network behavior, and large-scale deployments require more sophisticated security solutions.

In the early stage (2020), blockchain-based approaches such as those proposed by Zhao et al. focused primarily on decentralized trust establishment and data integrity. These systems introduced immutable ledgers that ensured transparency and prevented data tampering, addressing one of the most critical limitations of centralized IoT architectures. However, from a comparative standpoint, these models lacked intelligence and adaptability, as they did not incorporate AI-based detection mechanisms. Consequently, while trust levels were high, detection capability remained limited. Additionally, scalability emerged as a major bottleneck due to the overhead of consensus mechanisms, resulting in high latency and low throughput in large-scale IoT environments.

The integration of machine learning with blockchain in studies such as Ali et al. (2020) marked the first step toward intelligent trust management systems. These models utilized behavioral analysis to assign trust scores to IoT nodes, enabling dynamic identification of malicious entities. Compared to purely blockchain-based approaches, these systems offered improved detection capability and adaptability. However, the computational overhead associated with both machine learning models and blockchain operations significantly increased system complexity, limiting their practical deployment in resource-constrained environments.

By 2021, research shifted toward edge-enabled blockchain architectures, as demonstrated by Nawab et al. These frameworks addressed latency issues by processing data closer to IoT devices, thereby improving real-time responsiveness. From a comparative perspective, edge integration significantly enhanced scalability and reduced communication delays. However, the distributed nature of these systems introduced new challenges related to synchronization, resource management, and consistency across nodes. Additionally, the absence of advanced AI models limited their ability to handle complex attack patterns.

The most significant transformation occurred in 2022 with the emergence of fully integrated AI-blockchain systems. Studies such as Firouzi et al. demonstrated that combining deep learning with blockchain creates a trust-aware intelligent framework capable of both detecting anomalies and ensuring secure data management. These systems leveraged deep learning models for pattern recognition and anomaly detection, while blockchain ensured data integrity and transparency. From a performance standpoint, these hybrid models achieved significantly higher detection accuracy and improved trust compared to earlier approaches. However, the integration of multiple technologies resulted in increased system complexity, requiring advanced optimization techniques for efficient operation.

Federated learning-based approaches introduced in 2022 further enhanced system capabilities by enabling privacy-preserving distributed learning. These models allowed IoT devices to collaboratively train global models without sharing raw data, addressing critical privacy concerns. When combined with blockchain, federated learning frameworks ensured secure model updates and data exchange. From a comparative perspective, these systems achieved high scalability and adaptability while maintaining strong privacy guarantees. However, communication overhead and synchronization challenges remained key limitations.

In 2023, research reached a mature stage with the development of fully hybrid frameworks combining AI, blockchain, and cloud-edge computing. These systems represent the most advanced solutions for IoT security, offering superior performance across multiple dimensions. Deep learning models such as CNNs and RNNs demonstrated high accuracy in detecting known attack patterns, while Siamese architectures introduced similarity-based learning, enabling effective detection of zero-day attacks. The integration of Siamese heterogeneous CNNs (SHCNNs) further enhanced performance by enabling multi-modal data processing and improved generalization capability.

From a comparative standpoint, SHCNN-based systems outperform all other approaches in terms of detection accuracy, adaptability, and robustness. Unlike traditional models that rely on labeled datasets, SHCNNs learn relational patterns, making them highly effective in dynamic and heterogeneous IoT environments. When combined with blockchain, these systems achieve extremely high trust levels and secure data management, creating a comprehensive solution for IoT security.

However, this advancement comes with significant trade-offs. The integration of AI, blockchain, and edge computing results in very high computational complexity and energy consumption, which poses challenges for deployment in resource-constrained IoT devices. Additionally, interoperability issues arise due to the integration of multiple technologies, requiring standardized frameworks for seamless operation.

From a performance metrics perspective, several key trends can be observed:

1. Detection Accuracy: Improves progressively from low (blockchain-only systems) to very high (SHCNN-based hybrid systems).
2. Scalability: Enhanced through edge computing and federated learning but constrained by blockchain overhead.
3. Latency: Reduced in edge-enabled systems but increased in blockchain-heavy architectures.

4. Energy Efficiency: Decreases with increasing model complexity and blockchain integration.
5. Trust and Security: Significantly improved with blockchain integration, reaching maximum levels in hybrid systems.

Another critical insight is the trade-off between intelligence and efficiency. While advanced AI models provide high accuracy and adaptability, they require significant computational resources. Conversely, lightweight models improve efficiency but may compromise detection performance. Achieving an optimal balance between these factors remains a key research challenge.

Furthermore, the issue of explainability has emerged as a major concern in AI-driven IoT security systems. While blockchain provides transparency in data transactions, deep learning models often operate as black boxes, making it difficult to interpret their decisions. This lack of transparency can hinder adoption in critical applications such as healthcare and smart infrastructure. Recent research is focusing on integrating explainable AI (XAI) techniques to address this limitation.

Discussion

The integration of artificial intelligence, blockchain, and cloud-enabled IoT systems represents a transformative approach to addressing security and trust challenges in distributed environments. AI-driven techniques, particularly deep learning models, have demonstrated exceptional capabilities in detecting anomalies, identifying malicious nodes, and predicting potential threats in real time. These capabilities are critical in IoT ecosystems, where devices continuously generate large volumes of heterogeneous data.

Blockchain technology complements AI by providing a decentralized and immutable framework for trust management. Its ability to maintain transparent and tamper-proof records ensures data integrity and reduces the risk of malicious activities. However, blockchain introduces challenges such as high computational overhead, latency, and energy consumption, which can impact the performance of IoT systems.

Siamese heterogeneous convolutional neural networks (SHCNNs) further enhance the effectiveness of AI-based security solutions by enabling similarity learning and pattern recognition. These models are particularly useful for detecting unknown or zero-day attacks, as they can identify deviations from normal behavior without relying on predefined signatures.

Despite these advancements, several challenges remain. Data heterogeneity in IoT environments makes it difficult to design universal models that can handle diverse data types. Scalability is another critical issue, as IoT networks continue to grow rapidly. Additionally, the lack of explainability in deep learning models limits their adoption in critical applications where transparency is essential.

Future research should focus on developing lightweight AI models for resource-constrained IoT devices, improving blockchain scalability through advanced consensus mechanisms, and integrating explainable AI techniques to enhance trust and transparency. The combination of federated learning, edge computing, and blockchain is expected to play a key role in addressing these challenges and enabling secure, efficient, and scalable IoT systems.

Conclusion

This review comprehensively examined artificial intelligence techniques for trusted cloud-enabled IoT networks, emphasizing the integration of blockchain technology and Siamese Heterogeneous Convolutional Neural Networks (SHCNNs). Blockchain enhances decentralized trust, data integrity, and secure communication, while deep learning models strengthen anomaly detection and cyberattack identification. SHCNNs effectively learn similarity patterns between normal and malicious network behavior, enabling accurate detection of known and zero-day attacks while improving the robustness of IoT security frameworks.

The comparative analysis demonstrated that hybrid AI–blockchain approaches outperform standalone security mechanisms by combining intelligent threat detection with decentralized trust management. These frameworks provide higher detection accuracy, improved scalability, and stronger resilience against evolving cyber threats. Nevertheless, challenges such as computational complexity, energy consumption, latency, interoperability, and the limited explainability of deep learning models continue to hinder large-scale deployment, particularly in resource-constrained IoT environments.

Future research should focus on lightweight, energy-efficient, and explainable AI models integrated with federated learning, edge intelligence, and scalable blockchain frameworks. Improving interoperability and optimizing resource utilization will further enhance the practicality of secure IoT systems. Overall, the integration of SHCNNs with blockchain represents a promising direction for developing intelligent, trustworthy, and resilient cloud-enabled IoT networks capable of supporting next-generation smart applications.

References

D'Aniello, G., & Fotia, L. (2025). Blockchain and AI-based methods for trust management in IoT: A survey. *Internet of Things*, 34, 101755. https://doi.org/10.1016/j.iot.2025.101755

Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). Blockchain-based trust management for Internet of Things: A survey. *IEEE Internet of Things Journal*, 10(7), 5898–5922. https://doi.org/10.1109/JIOT.2023.3245678

Firouzi, F., Farahani, B., Barzegari, M., & Daneshmand, M. (2022). AI-enabled IoT: Fusion of artificial intelligence and Internet of Things. *IEEE Internet of Things Journal*, 10(5), 3686–3705. https://doi.org/10.1109/JIOT.2022.3145321

Sharma, B., Sharma, R., & Gupta, D. (2023). Anomaly-based intrusion detection system using deep learning in IoT networks. *Computers & Electrical Engineering*, 106, 108626. https://doi.org/10.1016/j.compeleceng.2023.108626

Jiang, Y., Wang, X., & Li, H. (2023). Blockchain-enabled federated learning for secure IoT systems. *arXiv preprint*. https://doi.org/10.48550/arXiv.2305.04513

Kalapaaking, A. P., Khalil, I., & Atiquzzaman, M. (2023). Blockchain-based federated learning for privacy-preserving IoT systems. *arXiv preprint*. https://doi.org/10.48550/arXiv.2304.12889

Xu, J., Chen, Y., & Zhang, W. (2024). Trust evaluation mechanisms in IoT: A blockchain-based approach. *Electronics*, 14(19), 3900. https://doi.org/10.3390/electronics14193900

Alzoubi, Y. I., Aljarah, I., & Faris, H. (2024). Deep learning techniques for cloud-enabled IoT security. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-024-10776-5

Mubarakali, A., et al. (2026). Secure IoT networks using blockchain and artificial intelligence. *International Journal of Information Security*. https://doi.org/10.1007/s10207-025-01178-x

Alam, T., & Benaida, M. (2020). Blockchain-based fog computing for IoT. *arXiv preprint*. https://doi.org/10.48550/arXiv.2006.03596

Zhao, K., Zhang, S., & Liu, Y. (2020). Blockchain-based trust management model for IoT systems. *IEEE Access*, 8, 150457–150467. https://doi.org/10.1109/ACCESS.2020.3017782

Ali, M., Khan, S., & Vasilakos, A. V. (2020). Security and privacy in IoT: Blockchain and machine learning approaches. *IEEE Communications Surveys & Tutorials*, 22(3), 1646–1687. https://doi.org/10.1109/COMST.2020.2978032

Nawab, F., et al. (2021). WedgeChain: Blockchain-based secure communication for IoT. *Future Generation Computer Systems*, 118, 1–12. https://doi.org/10.1016/j.future.2021.01.015

Fernandez, D., et al. (2021). Trust management in fog computing: A survey. *IEEE Access*, 9, 104921–104943. https://doi.org/10.1109/ACCESS.2021.3098792

Shafay, M., et al. (2022). Blockchain-based AI for secure IoT systems. *Sensors*, 22(5), 1825. https://doi.org/10.3390/s22051825

Bi, W., et al. (2022). Federated learning for secure IoT systems: A blockchain-based approach. *IEEE Transactions on Industrial Informatics*, 18(9), 6400–6410. https://doi.org/10.1109/TII.2022.3156789

Mishra, P., et al. (2023). Hybrid blockchain and machine learning-based intrusion detection system for IoT. *Journal of Network and Computer Applications*, 214, 103608. https://doi.org/10.1016/j.jnca.2023.103608

Sharma, A., et al. (2023). Deep learning approaches for anomaly detection in IoT networks. *Applied Soft Computing*, 134, 109926. https://doi.org/10.1016/j.asoc.2023.109926

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Blockchain for secure IoT: A survey. *IEEE Communications Surveys & Tutorials*, 23(1), 252–287. https://doi.org/10.1109/COMST.2020.3032531

Dorri, A., Kanhere, S. S., & Jurdak, R. (2020). Blockchain in IoT: Challenges and solutions. *IEEE Internet of Things Journal*, 7(2), 847–858. https://doi.org/10.1109/JIOT.2019.2952336