ISSN: 2959-6386 (Online), Vol. 2, Issue 2, 2023

Journal of Knowledge Learning and Science Technology

journal homepage: https://jklst.org/index.php/home

IoT-Edge Healthcare Solutions Empowered by Machine Learning

Sai Mani Krishna Sistla[1], Bhargav Kumar Konidena[2]

[1]HCL America, USA

[2]State Farm, USA

Abstract:

Managing the overwhelming volume of data collected by medical sensors presents a challenge in extracting relevant insights. This paper advocates for the development of an algorithm tailored to body sensor networks to identify outliers in collected data. Leveraging machine learning and statistical sampling methodologies, this research aims to optimize real-time response, particularly as computational tasks migrate to backend systems. Addressing the increasing dispersion of computing power across various domains, this study highlights the potential bottleneck posed by computation as Internet-of-Things (IoT) devices proliferate. To mitigate battery drain, a common approach involves offloading processing to background servers. However, the widespread adoption of IoT devices has sparked concerns about privacy and security. Current measures are deemed insufficient in light of escalating cyber threats. Machine learning methods offer promise in identifying vulnerabilities within IoT systems. Edge computing emerges as a solution to enhance network response times, decentralization, and security. By leveraging distributed-edge computing within an IoT framework, this paper investigates the fusion of cloud and edge computing with machine learning. Specifically, it explores how these technologies can be harnessed in the medical field, utilizing sensor-equipped IoT devices to collect extensive data for analysis. The proposed approach involves proactive decision-making at the front end, guided by an IoT server, and employs machine learning algorithms at the backend to identify pertinent data signatures. This paper underscores the significance of combining cloud, edge computing, and machine learning in a distributed-edge-computing-based IoT framework, offering a potential avenue for real-time, efficient solutions in various domains.

Keywords: Machine Learning (ML), Edge Computing, Internet-of-Things (IoT), Cloud Computing.

Article Information:

Article history: 12/11/2023 *Accepted:* 15/11/2023 *Online:* 30/11/2023 *Published*: 30/11/2023

DOI: https://doi.org/10.60087/jklst.vol2.n2.P135

Correspondence author: Sai Mani Krishna Sistla

Introduction:

The term "Internet of Things" (IoT) denotes a network infrastructure where diverse computing devices can communicate autonomously, facilitating data collection and exchange without human intervention. IoT represents a burgeoning field promising significant technological advancements, benefiting various sectors. Among these, the Internet of Medical Things (IoMT) stands out as a burgeoning subset with widespread adoption in healthcare.

Implanted medical devices (IMDs) and wearable technologies exemplify IoT applications enhancing healthcare delivery. Remote patient monitoring, enabled by IoMT, has demonstrated clear benefits in alleviating strain on medical personnel and resources [6–9]. This approach allows healthcare teams to monitor patients' health remotely, affording elderly individuals the independence to reside in their homes while receiving necessary care. IoMT integration has also revolutionized medication plans, including rehabilitation, diabetes management, and ambient assisted living (AAL), yielding promising outcomes.

Innovative systems leveraging IoMT technology have been developed for various medical conditions, such as physical injuries and Parkinson's disease, enhancing rehabilitation strategies and continuous patient monitoring. Notably, IoMT-enabled solutions have been pivotal in diabetes management and preemptive heart attack detection, potentially saving lives by facilitating timely interventions.

For elderly home care, systems like SPHERE offer a viable alternative to frequent hospital visits, emphasizing patient comfort. However, concerns about data security and privacy have surfaced, necessitating robust safeguards against potential breaches. Ensuring the safety of remote patient monitoring and emergency response remains a paramount goal in modern healthcare IT.

This study's principal contributions include:

- Designing edge-based computing for patient data collection.
- Securing communication between edge nodes to safeguard patient data.
- Introducing a hybrid model to predict and mitigate cyberattacks in IoMT-based healthcare systems.
- Developing machine learning algorithms optimized for edge devices with constrained resources.
- Addressing privacy and security challenges in health data collection and transmission.
- Assessing the effectiveness of IoT-edge computing solutions in enhancing patient outcomes and reducing healthcare costs.
- Exploring new IoT devices and sensors tailored for healthcare applications.
- Integrating IoT-edge computing with technologies like 5G networks to enhance data transmission and processing capabilities.

- Comparing various edge computing architectures (e.g., fog computing, cloudlets) for suitability in healthcare.

- Investigating scalability and reliability of IoT-edge computing solutions in healthcare.

- Developing models for data fusion and analytics to improve healthcare applications.

Related Work:

The domain of IoT-edge-computing-based healthcare solutions has witnessed rapid growth in recent years, fueled by factors such as the proliferation of low-cost IoT devices, advancements in machine learning and edge computing, and the imperative for cost-effective healthcare delivery.

Early research in this domain explored the utilization of wireless sensor networks (WSNs) for remote monitoring of patients with chronic conditions like diabetes and heart disease, showcasing the feasibility of data collection and transmission. However, these studies underscored the necessity for enhanced data processing and analysis capabilities at the edge.

Recent investigations have delved into novel machine learning algorithms tailored for edge devices and the integration of edge computing with technologies like 5G networks. Moreover, there has been significant attention given to addressing privacy and security concerns surrounding health data collection and transmission.

Studies have also assessed the effectiveness of IoT-edge-computing-based solutions in enhancing patient outcomes and reducing healthcare costs. These investigations have demonstrated tangible benefits in terms of improved patient outcomes and cost savings.

Additionally, there is a burgeoning interest in developing new IoT devices and sensors for healthcare applications, along with the exploration of diverse edge computing architectures (e.g., fog computing, cloudlets) and their applicability in healthcare settings.

However, despite progress, the research landscape concerning IoT-edge-computing-based healthcare solutions remains dynamic, with numerous avenues for further exploration.

Edge computing represents a burgeoning trend in the computing industry, offering distributed cloud computing capabilities at the network's edge. Raj et al. [29] introduced a novel framework for optimizing cooperative networks at the network periphery, demonstrating improved performance through edge node collaboration. Furthermore, researchers have developed innovative offloading approaches to enhance the efficiency of deep learning applications deployed on edge devices, addressing resource constraints [30].

In the context of healthcare, emerging technologies like wearables, IoT, and edge computing are reshaping the landscape, facilitating real-time data gathering and analysis. Lydia et al. proposed a federated-deep-learning-based COVID-19 detection model leveraging IoT-enabled edge computing, showcasing promising results in early detection. Meanwhile, edge computing's potential in healthcare has prompted comprehensive studies to delineate architectures and methodologies tailored for diverse healthcare applications.

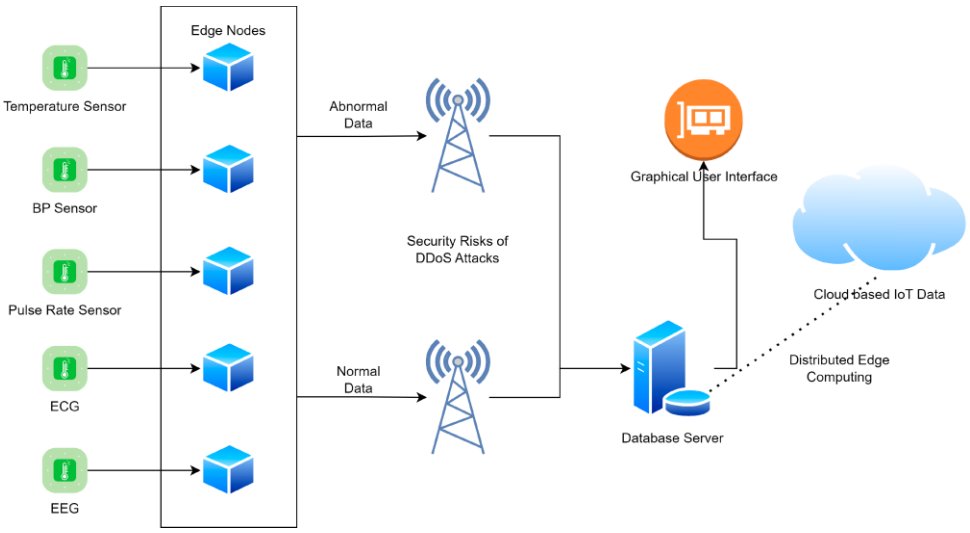
Fog computing emerges as a promising approach to augmenting cloud computing efficiency, leveraging both remote and onsite resources for improved service delivery.For instance, the FETCH framework collaborates with edge computing devices to implement deep learning technology and automated monitoring, demonstrating potential benefits in healthcare settings.

Overall, the convergence of edge computing, IoT, and AI holds immense promise in revolutionizing healthcare delivery, offering real-time insights, reduced latency, and enhanced efficiency. Future research in this area is poised to further explore the synergies between these technologies and address emerging challenges in smart healthcare systems.See Table 1 for a comparative analysis of previous state-of-the-art studies.

Research Methodology

Figure 1 illustrates the framework of Safe AI-based edge-distributed ledger assistance in the healthcare system. Alongside the user, wireless network, edge-distributed ledger, trusted agent, and healthcare server, an expert system plays a pivotal role within the system. Users may either have been treated for a disease or may be afflicted with a different ailment. To monitor the patient's health status, a variety of implanted and external sensors are employed. Additionally, smartphones and other personal digital assistant (PDA) devices can be utilized to gather and store medical data from these sensors. Individuals have the option to document their medical history using a PDA, which can then be encrypted and periodically uploaded as a block to the edge-distributed ledger. Each link in the ledger contains data, timestamp, and other pertinent details from the preceding block.

Permitted agents serve two primary functions: validation and recording. Validating agents (VA) form a subset of nodes responsible for ensuring the legitimacy of each transaction. Transactions must be verified by the network's validators before being incorporated into the edge-distributed ledger. Subsequently, recording agents store the verified data in blocks, accessible only to authorized users.



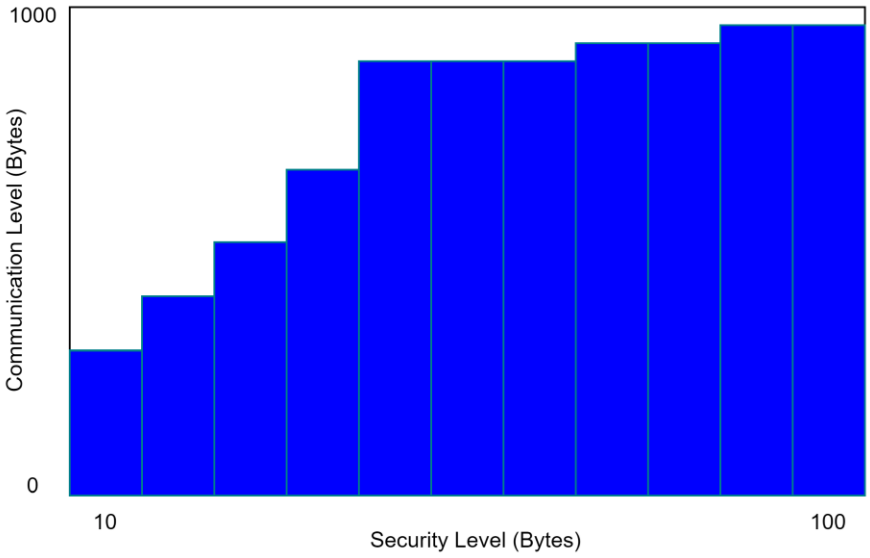
The network comprises distinct ledgers maintained by the medical staff, the hospital, and the diagnostic expert system. Similar to a human specialist, a diagnostic expert system can be trusted to make precise and informed decisions. Before the introduction of the encrypted edge-distributed ledger, data analysis was utilized for disease detection. Leveraging sensors implanted in the patient's body, life-saving medications can now be administered remotely. Figure 1 illustrates the core concept of our proposed model.

Results and Discussion

We focused our attention on evaluating the power consumption associated with message calculation and transmission across edge node networks, particularly due to the implementation of distributed ledgers at the edge to safeguard patient data. To ensure the system's security, we employed machine learning-based models for early detection.

Communication vs. Security Level in Edge Nodes:

The integration of signcryption introduces significant communication overhead. Transmission overhead is primarily dictated by the size of the signed message. In a conventional edge node setup, each user typically requires only two bytes. Figure 5 illustrates the trade-off between communication cost and security level. As the security level increases, the communication requirements also escalate.

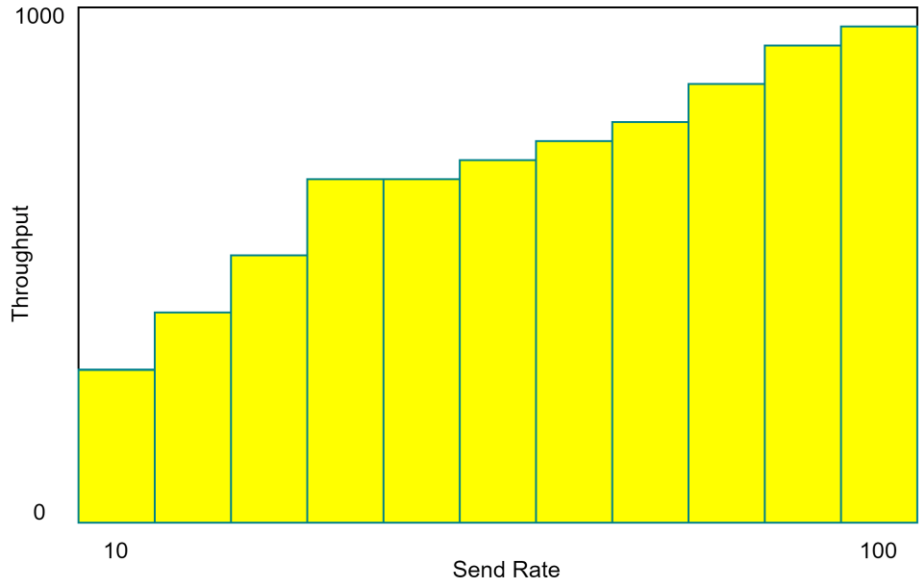


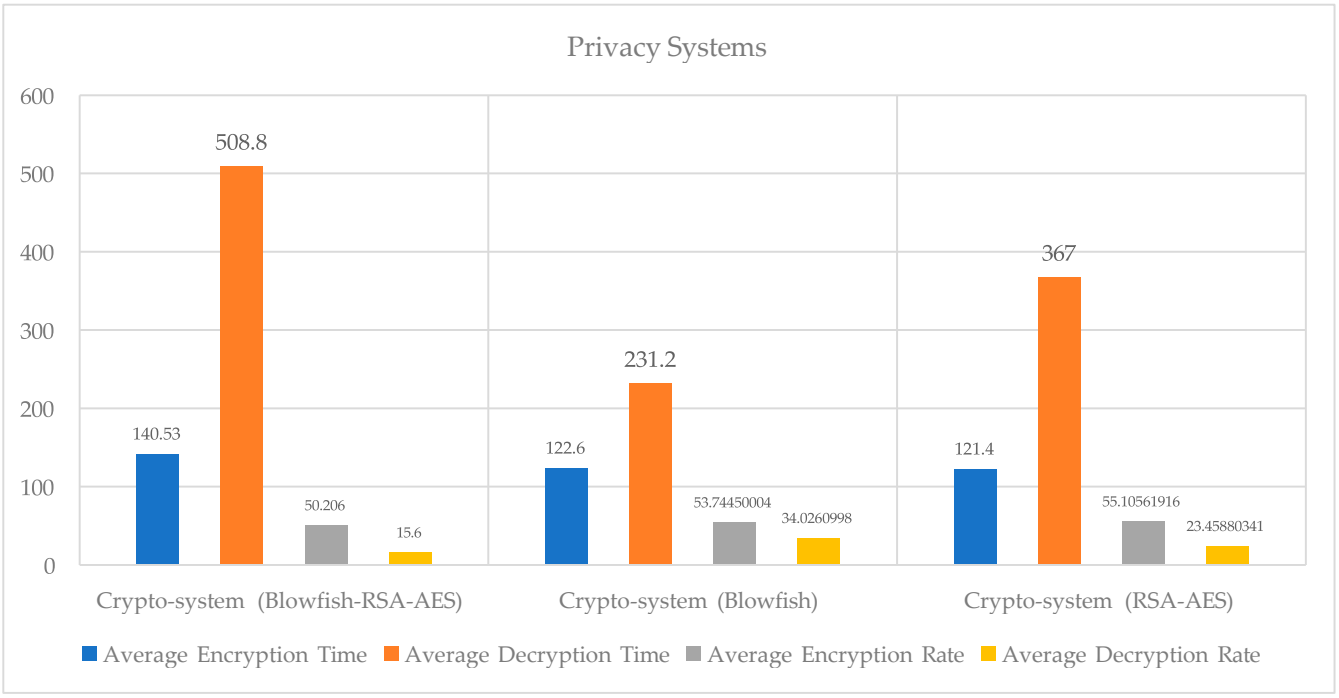
Performance Evaluation of Edge-Distributed Ledger:

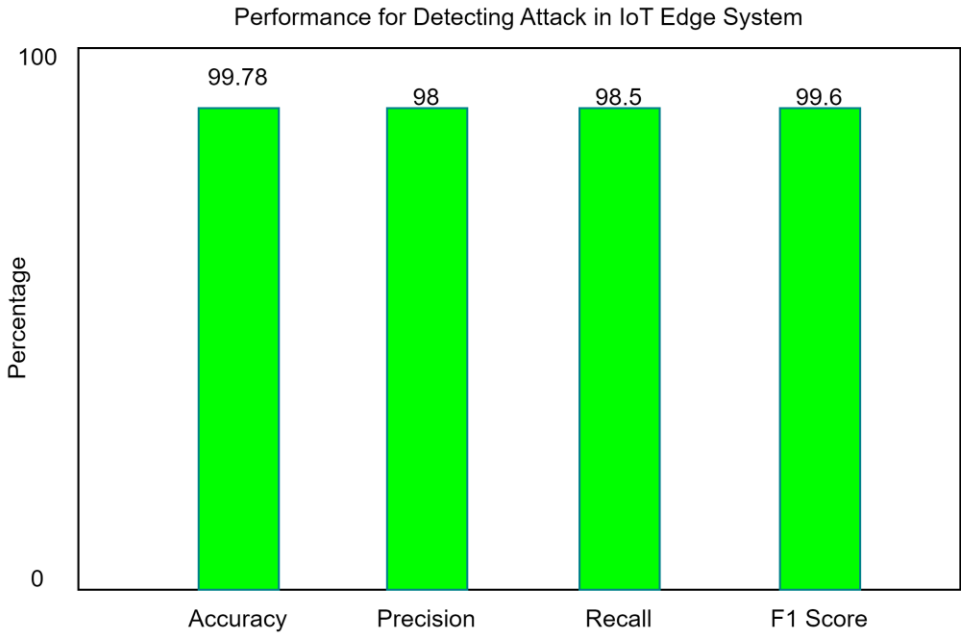
In this subsection, we conducted tests on the proposed EDGE NODE platform with its distributed ledger functionality activated to assess its performance. We employed one ordered node and four peer nodes to evaluate the efficiency of the edge-distributed ledger network. Our objective was to determine the throughput, measured in transactions per second (TPS), achievable using the proposed EDGE NODE technology across various send rates.

Transaction throughput was defined as the total number of edge-distributed ledger transactions processed within a specified time interval. We measured the amount of reading performed by nodes at the periphery of the distributed ledger networks using readthrough during the designated time frame. Variations in transaction-read throughput were analyzed under different TPS transmission rates and random machine utilization settings.

Figure 5 illustrates the complete transaction reading process, while Figure 6 presents a similar depiction. Additionally, Figure 7 showcases the total number of committed blocks from concurrent transactions, and Figure 8 illustrates the average throughput of the proposed edge-distributed ledger per parallel transaction.


1000
Throughput
0
10
100
Send Rate


Privacy Systems
600
500
400
300
200
100
0
508.8
140.53
50.206
15.6
231.2
122.6
53.74450004
34.0260998
367
121.4
55.10561916
23.45880341
Crypto-system (Blowfish-RSA-AES)
Crypto-system (Blowfish)
Crypto-system (RSA-AES)
Average Encryption Time
Average Decryption Time
Average Encryption Rate
Average Decryption Rate



Privacy Preservation:

In this study, we propose a hybrid algorithm for privacy preservation, integrating three primary cryptography algorithms: the Advanced Encryption Standard, Blowfish, and RSA. While various encryption algorithms are currently utilized in edge node networks (EDGE NODEs) to secure data, the rapid advancement of sophisticated technologies renders these existing systems increasingly outdated. Hardware advancements have notably reduced the time required to breach cryptographic systems, and various types of attacks have exposed vulnerabilities in these systems. Figure 7 presents the results and performance analysis of our privacy preservation strategy.

Prediction of DDoS Attacks:

We gathered transaction data and trained a machine learning model to detect attacks on the privacy preservation solution for healthcare based on edge-node-based edge-distributed ledger.

Hybrid Machine Learning Model:

Hybrid voting classifiers, a type of estimator in the machine learning field, amalgamate outputs from multiple base estimators to formulate a unified prediction .The collective score is typically determined by a simple majority of the

estimators. By amalgamating various classification models into one, the hybrid voting classifier estimator overcomes limitations inherent in its individual components. Utilizing weights assigned to each class or class likelihood, a hybrid voting classifier can label records based on the majority vote. Mathematically, the ensemble classifier forecast is expressed as follows:

$$y = arg(max) \sum_{j=1}^{m} w_j XA_{Ci,j}(x) = i$$

When hybridized with a distributed ledger, the formulation becomes:

$$\psi y = arg(max) \sum_{j=1}^{m} w_j XA_t Ci,j(\psi x) = i$$

Alternatively, it can be represented as:

$$\psi = \left[max \right] \sum_{j=1}^{m} w_j XA_t Ci,j(\sigma(h_0w_0 + h_1w_1 + h_2w_2 + \cdots + h_nw_n)) = i$$

The hybrid classifier combines the best features of both models. The information in y serves as input for the logistic regression probability function in XGB. Results from a separate logistic regression analysis demonstrated a significant improvement in accuracy to 99.7% with the hybrid classifier.

Conclusions:

The vast amount of data captured by medical sensors presents a challenge in extracting relevant information. An algorithm for a body sensor network is crucial for anomaly detection in collected data, utilizing methodologies such as statistical sampling and machine learning. Real-time response optimization is gaining momentum as computational tasks migrate to backend systems, driving research into more efficient data transfers. With computation dispersed across various domains, the proliferation of Internet of Things (IoT) devices raises concerns about privacy and security worldwide. Current measures are insufficient against evolving cyber threats, highlighting the need for more robust solutions.

The reliability of machine learning (ML) findings makes ML methods increasingly popular for predicting and detecting vulnerabilities in IoT systems. Edge computing enhances network response time, decentralization, and security, with edge nodes capable of managing critical computing tasks. Utilizing cloud and edge computing alongside ML, we explore a distributed-edge-computing-based IoT framework. IoT devices equipped with sensor frameworks gather extensive data for analysis, where careful planning aids in identifying crucial information. Employing ML in backend servers facilitates the search for relevant data signatures, with potential applications in the medical field.

Our study investigates the integration of ML, cloud computing, and edge computing through an IoT-based distributed edge computing framework. Future directions include exploring real-time systems and deep learning models to further enhance efficiency and effectiveness in healthcare and beyond.

References

1. Al-Qarafi, A., Alrowais, F., Alotaibi, S. S., Nemri, N., Al-Wesabi, F. N., Al Duhayyim, M., Marzouk, R., Othman, M., & Al-Shabi, M. (2022). Optimal Machine Learning Based Privacy Preserving Blockchain Assisted Internet of Things with Smart Cities Environment. Applied Sciences, 12(12), 5893. [CrossRef]

2. Hartmann, M., Hashmi, U. S., & Imran, A. (2022). Edge computing in smart health care systems: Review, challenges, and research directions. Transactions on Emerging Telecommunications Technologies, 33, e3710. [CrossRef]

3. Ray, P. P. (2017). Internet of things for smart agriculture: Technologies, practices and future direction. Journal of Ambient Intelligence and Smart Environments, 9, 395–420. [CrossRef]

4. Quy, V. K., Van Hau, N., Van Anh, D., Quy, N. M., Ban, N. T., Lanza, S., Randazzo, G., & Muzirafuti, A. (2022). IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. Applied Sciences, 12(8), 3396. [CrossRef]

5. Singh, A. K., Verma, K., & Raj, M. (2021). IoT based Smart Agriculture System. In Proceedings of the 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India. [CrossRef]

6. Shahzadi, R., Ferzund, J., Tausif, M., & Asif, M. (2016). Internet of Things based Expert System for Smart Agriculture. International Journal of Advanced Computer Science and Applications, 7, 070947. [CrossRef]

7. Huang, J., Kong, L., Dai, H. N., Ding, W., Cheng, L., Chen, G., Jin, X., & Zeng, P. (2020). Blockchain-Based Mobile Crowd Sensing in Industrial Systems. IEEE Transactions on Industrial Informatics, 16, 6553–6563. [CrossRef]

8. Hrovatin, N., Tošic´, A., Mrissa, M., & Kavšek, B. (2022). Privacy-Preserving Data Mining on Blockchain-Based WSNs. Applied Sciences, 12, 5646. [CrossRef]

9. Zhong, G., Xiong, K., Zhong, Z., & Ai, B. (2021). Internet of things for high-speed railways. Intelligent Convergence Networks, 2, 115–132. [CrossRef]