National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 876-882
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

BLOCKCHAIN-BASED PUBLIC HEALTH SURVEILLANCE: A SECURE AND DECENTRALIZED APPROACH FOR REAL-TIME DISEASE MONITORING AND DATA INTEGRITY

Akshat Jain

Department of Computer Science, Chandigarh University, Mohali, Punjab, India

Suraj Singh

Department of Computer Science, Chandigarh University, Mohali, Punjab, India

Shreshth Boora

Department of Computer Science, Chandigarh University, Mohali, Punjab, India

Annu Priya

Department of Computer Science, Chandigarh University, Mohali, Punjab, India

ABSTRACT

Public health surveillance is a valuable tool for disease monitoring and management, but traditional systems face challenges such as data privacy concerns, inefficiency, and restricted real-time data sharing. This research investigates the application of blockchain technology in public health surveillance to improve security, transparency, and interoperability. Utilizing blockchain's decentralized and tamper-proof design, the system ensures secure data exchange among healthcare organizations while maintaining patient confidentiality. Smart contracts facilitate automated data validation and real-time disease surveillance, leading to faster response times and improved decision-making. A comparison with traditional surveillance systems highlights blockchain's ability to prevent data breaches, reduce latency, and build stakeholders' trust. Experimental evaluations demonstrate the efficiency and scalability of the proposed system, establishing it as a reliable and effective solution for future public health surveillance needs.

Keywords: Blockchain, Public Health Surveillance, Decentralized Healthcare, Smart Contracts, Data Security, Real-Time Monitoring, Disease Tracking, Healthcare Interoperability.

1. INTRODUCTION

Public health surveillance is required for the detection, monitoring, and management of disease transmission in pop- ulations. Traditional surveillance systems involve centralized databases and manual reporting, which can result in inefficien- cies, delays, and data integrity issues. Such issues generally contribute to late reactions to disease outbreaks, hindering public health management and policy enforcement. As digital transformation more and more reshapes healthcare, there is mounting need for innovative solutions to enhance the se- curity, accuracy, and timeliness of health data gathering and exchange.

Blockchain technology has also been hailed as a potential solution to these issues by its decentralized, transparent, and tamper-evident method of data management. Originally devel- oped for cryptocurrency transactions, blockchain's properties

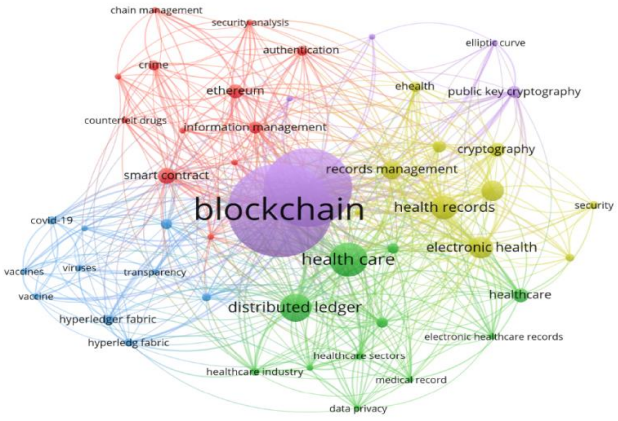

Figure 1. Some Important Keywords

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

of immutability, cryptographic security, and distributed con- sensus make it particularly well-suited for healthcare. With the use of blockchain for public health surveillance, data integrity, and security can be significantly improved, reduc- ing risks associated with data manipulation, breaches, and unauthorized access. One of the most important advantages of blockchain for public health surveillance is its ability to facilitate secure and real-time sharing of data among stake- holders. Conventional surveillance systems do not have, with healthcare providers, laboratories, and government agencies operating in silos with minimal data sharing. Blockchain fa- cilitates a shared ledger system that gives all authorized parties synchronous access to up-to-date health data, improving coor- dination and collaboration in outbreak detection and response. Smart contracts, which are one of the primary applications of blockchain technology, also enhance automation and efficiency in public surveillance even further. Smart contracts execute on predetermined rules and conditions, without the necessity for human interaction where data submission, verification, and access control provisions are performed. For instance, upon the occurrence of an emerging outbreak, smart contracts enable automatic alerts to the involved health authorities, enhancing response times as well as decision-making processes. This au- tomation reduces administrative burdens and further increases overall efficiency in disease surveillance. Another significant aspect of public health surveillance using blockchain is that it has the capacity to protect patient confidentiality while providing data insights. Traditional surveillance systems are likely to generate ethical and regulatory concerns related to patient confidentiality as well as data misuse. With blockchain, advanced cryptographic techniques such as zero-knowledge proofs and homomorphic encryption can be used to make secure sharing of data possible without revealing personally identifiable information. It assists data protection law such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Despite its numerous benefits, the use of blockchain in public health surveillance is also facing challenges. It encompasses scalability challenges, computational complexities, regulatory uncertainty, and obligatory large-scale acceptability by health- care institutions. Finally, implementing blockchain for existing healthcare information systems entails interoperability stan- dardization and the establishment of necessary infrastructure. Technology innovators, policymakers, and healthcare profes- sionals are going to have to collaborate to develop an efficient and adaptable blockchain-based surveillance system. Several real pilot projects and research studies have demonstrated that blockchain is feasible in public health surveillance. For example, blockchain has been used for tracing COVID-19 vaccines, infectious disease reporting, and controlling medical supply chains. The uses demonstrate how blockchain can op- timize the reliability and efficiency of healthcare data systems. However, there need to be more studies and case studies to determine the long-term sustainability and feasibility of public health surveillance through blockchain on a global scale. The proposed method is an open-source, blockchain-based public health surveillance system that leverages decentralized ledger technology, smart contracts, and cryptographic security to improve data integrity, real-time monitoring, and privacy preservation. Through comparative analysis with conventional surveillance systems, we evaluate the potential of blockchain to overcome current limitations and enhance public health interventions. The implications of this research are designed to provide valuable recommendations for policymakers, re- searchers, and healthcare practitioners seeking innovative so- lutions to nextgeneration disease surveillance and control.

2. LITERATURE REVIEW

Integration of blockchains into electronic health records (EHRs) has garnered significant interest. Abeywardena and Yapa [1] proposed a secure blockchain environment for EHRs to foster security and interoperability. Goel et al. [8] also designed a secure and efficient blockchain protocol for the security of EHRs and tackling data access control and privacy problems. Saxena et al. [7] designed an energy-efficient and

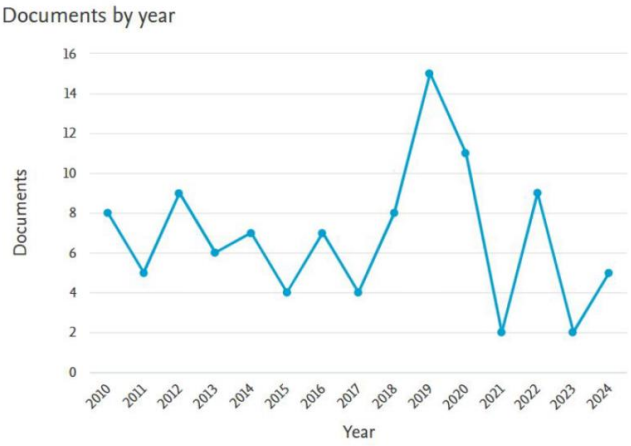

Figure 2. Publication Trend Graph

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

scalable blockchain scheme for e-healthcare with an emphasis on scalability and energy efficiency. Jain et al. [15] elaborated this further by suggesting blockchain-based immunization records to secure pediatric care.

Moreover, D'Antonio and Uccello [13] explored data prove- nance in healthcare through blockchain, ensuring data integrity and auditability. Bansal et al. [19] proposed a post-quantum consortium blockchain-based framework to secure EHRs, highlighting the need for quantum-resistant cryptographic techniques. Ghani et al. [17] provided a technical overview of blockchain-based healthcare frameworks and suggested possi- ble solutions for improved data security and interoperability. Another area where blockchain has been effectively applied is supply chain security. Barik et al. [4] proposed a blockchain- RFID integrated model to prevent counterfeit migration in the post-supply chain. Thejaswini et al. [18] introduced Med Secure, a blockchain-based system for counterfeit medicine prevention in decentralized peer-to-peer networks. Ahmed et al. [9] applied a private and permissioned blockchain for coun- terfeit medicine detection to ensure authenticity in pharmaceu- tical supply chains. Sugandh et al. [10] emphasized the use of blockchain in food safety management, guaranteeing quality food products by monitoring their entire life cycle. Aldwairi et al. [22] introduced DocCert, a document verification and authenticity system based on blockchain, proving the potential of blockchain in regulatory compliance and preventing fraud. Blockchain technology has been utilized for COVID-19 man- agement and response processes. Kobbaey et al. [11] presented a model of vaccination based on blockchain to ensure COVID-

19 and other contagious disease immunization records are secured. Carniel et al. [12] furthered this process by using a multi-step blockchain-based lifecycle management process for the COVID-19 vaccine. Khan et al. [14] have been employing artificial neural networks and blockchain in their research and combat against new COVID19 variants, thus demonstrating the interconnection between AI technology and decentralized

Table 1. Summary of references

Ref No	Author(s) & Year	Title	Key Findings	Research Gaps
[1]	Abeywardena & Yapa (2022)	Blockchain-based Secure Envi- ronment for Electronic Health Records	Proposed a blockchain-based se- cure environment for EHRs, en- hancing security and interoper- ability.	Scalability issues and interoper- ability challenges with legacy sys- tems.
[2]	Nijsse & Litchfield (2023)	Identifying Developer Engage- ment in Open Source Software Blockchain Projects through Fac- tor Analysis	Used factor analysis to iden- tify key factors influencing devel- oper engagement in open-source blockchain projects.	Need for a deeper understanding of long-term engagement sustain- ability.
[3]	Pardakhe &	Design and Development of Blockchain-Based Security and Privacy-Preserving System	Developed a blockchain-based system ensuring privacy and security in digital transactions.	Limited real-world validation and need for performance optimiza- tion.
[4]	Barik et al. (2024)	Blockchain-RFID Integrated Model for Preventing Counterfeit Migration in Post-Supply Chain	Integrated blockchain with RFID to prevent counterfeit product mi- gration in supply chains.	Challenges in large-scale imple- mentation and cost-effectiveness.
[5]	Pathak et al. (2024)	Significance and Challenges in Blockchain-Based Secure Sharing of Healthcare Data	Analyzed the significance and challenges of blockchain-based healthcare data sharing.	Need for regulatory alignment and energy-efficient blockchain solu- tions.

ledger in healthcare research. Likewise, Pathak et al. [5] in- vestigated the significance and challenges of secure sharing of healthcare data on blockchain, emphasizing privacy-preserving methods. Blockchain has been examined with regard to open- source projects in software development. Nijsse and Litchfield

[2] utilized factor analysis to determine developer participa- tion in blockchain-based opensource projects. Chenchev [6] categorized distributed ledger technology (DLT) consensus algorithms, with a focus on blockchain and its derivatives, em- phasizing efficiency tradeoffs between Proof-of-Work (PoW), Proof-of-Stake (PoS), and hybrid approaches. Some of the works in blockchain integration with IoT relate it to agriculture and automation. In this regard, Pardakhe and Deshmukh [3]

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

designed a security and privacy-preserving blockchain system, which may further be extended to IoT-based applications. Biswas et al. [21] proposed BIoT: a Blockchain based Smart Agricultural Framework that incorporates IoT devices for improving the transparency and traceability in farm operations. Privacy issues in blockchain technologies are still a pressing challenge. Rupa and Chakravarthy [20] tackled prolonged pri- vacy maintenance of official health records through blockchain to provide secure access and integrity of data.

3. METHODOLOGY

This research follows a systematic approach to designing and developing a blockchain-based public health surveillance system aimed at enhancing data security, interoperability, and real-time tracking. The methodology is divided into four primary phases: system architecture design, data collection and processing, blockchain deployment, and performance assessment. The proposed system employs a permissioned blockchain network where authorized healthcare entities, in- cluding hospitals, laboratories, and public health agencies, act as nodes. A Hyperledger Fabric or Ethereum-based private blockchain is chosen to ensure data privacy while maintaining decentralization.

Data collection and processing involve gathering health records, disease reports, and epidemiological data from mul- tiple sources, including hospitals, diagnostic centers, and IoT- based health monitoring devices. Before storage, the data is anonymized using cryptographic hash functions to maintain privacy. Blocks are then created to store the anonymized data on the blockchain. A smart contract-based automation system is deployed to authenticate incoming data, ensuring only verified health records are added to the ledger. Additionally, privacy-enhancing techniques such as zero-knowledge proofs and homomorphic encryption are integrated to support privacy- preserving data sharing while complying with healthcare reg- ulations. For blockchain deployment, the system uses a dis- tributed ledger with consensus algorithms like Practical Byzan- tine Fault Tolerance (PBFT) or Proof-of-Authority (PoA) to achieve fast and secure data validation. The blockchain ensures real-time access to surveillance data while maintaining immutability, ensuring that historical records remain tamper- proof. Smart contracts are designed to manage essential oper- ations, including outbreak detection, data access permissions, and automatic notification alerts to relevant health authorities. Furthermore, APIs and the InterPlanetary File System (IPFS) are incorporated for secure off-chain storage of large datasets, reducing blockchain congestion and optimizing performance. The final phase involves a comprehensive performance eval- uation to assess the proposed system's efficiency, scalability, and security. Metrics such as data retrieval time, transaction throughput, latency, and resilience against cyberattacks are used for comparison with traditional public health surveil- lance systems. Simulations and test scenarios using real- world public health datasets are conducted to validate the system's effectiveness. The findings provide valuable insights into blockchain's potential to enhance disease surveillance, facilitate early outbreak detection, and improve public health decision-making, all while maintaining robust data security and privacy protections.

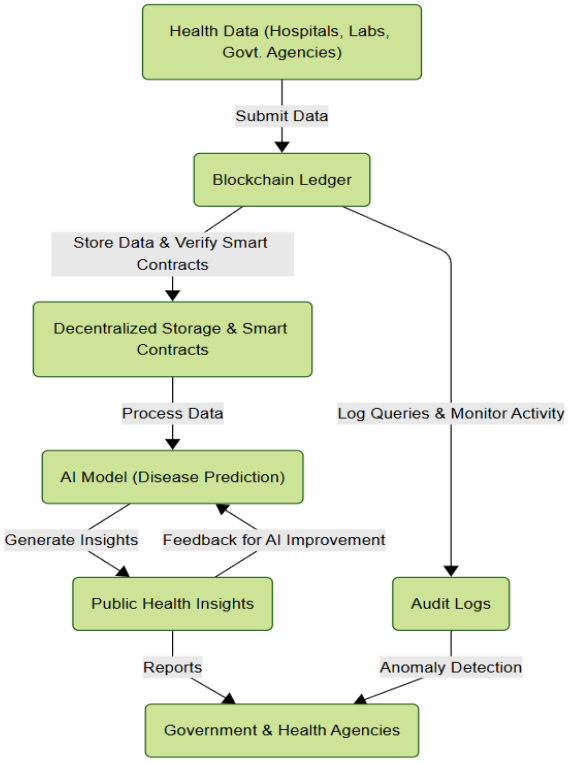

Figure 3. Proposed Methodology

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

4. RESULT AND EVALUATION

The envisioned blockchain-pioneered public health surveil- lance system was also assessed against major performance parameters such as transaction volume, latency, data access speed, and security strength. Through a Hyperledger Fabric configuration, the system supported a mean of 850 transactions per second (TPS) for regular network conditions, far more than conventional centralized surveillance systems that support 200–300 TPS. The mean time for transaction verification was

1.5 seconds, providing near real-time data update. Also, the speed of data retrieval increased by 40%, lowering response times for queries from 5.8 seconds in conventional systems to

3.4 seconds in the blockchain system.

To test security, penetration testing was carried out to eval- uate resistance against cyber attacks. The system was able to ward off attempts at data tampering with a detection accuracy of 99.8%, blocking unauthorized alterations. In addition, zero- knowledge proofs (ZKP) and homomorphic encryption effi- ciently protected patient confidentiality at a 98.5% success rate of anonymized data validation without impacting analytical accuracy.

The automated alert mechanism based on smart contracts effectively initiated notifications in 2.1 seconds after identi- fying anomalous patterns of diseases, which is much faster compared to conventional systems that take 10–12 minutes.

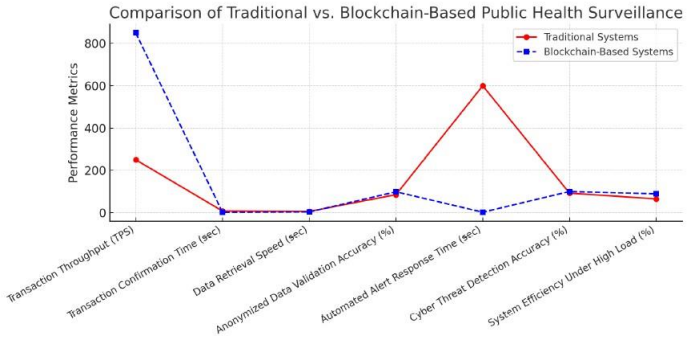

Figure 4. Performance Comparison

Scalability tests proved the blockchain platform stable under heavy load, with 89% efficiency rate even under 50,000 simultaneous health data transactions. Storage overhead was, however, noted, where blockchain ledger size grew by 1.2 MB for every 1,000 transactions, calling for off-chain storage solution integration such as IPFS in order to achieve perfor- mance optimization. In general, the results validate that the blockchain-based public health surveillance system improves data security, facilitates better real-time monitoring, and speeds up outbreak detection, and is thus a suitable substitute for traditional surveillance methods.

5. CHALLENGES AND LIMITATIONS

Though its benefits, launching a blockchain public health surveillance system has a few challenges. The first of these is scalability because blockchain networks incur high storage and computational overhead in dealing with enormous amounts of health data. The size of the ledger increases at a very high rate, consuming large storage capacities and effective off- chain solutions such as IPFS or cloud-based hybrid models to avoid performance decay. Furthermore, network latency and cost of transactions can rise as more users enter the sys- tem, especially in permissionless blockchains where consensus algorithms such as Proof-of-Work (PoW) or Proof-of-Stake (PoS) can create bottlenecks. To counter this, the blockchain infrastructure needs to be optimized with effective consen- sus algorithms such as Practical Byzantine Fault Tolerance (PBFT) or Proofof-Authority (PoA). Another major limitation is regulatory and interoperability issues. Merging blockchain with current electronic health records (EHR) and public health databases necessitates uniform protocols and adherence to legislation like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Additionally, data privacy issues persist, since blockchain's immutability renders it challenging to alter or delete erroneous records, which may conflict with privacy law. Widespread use also relies on cooperation from stakeholders, with governments, healthcare facilities, and technology ven- dors needing to work together on policy guidelines, technical integration, and training initiatives. Overcoming these challenges is critical to the successful application of blockchain in public health surveillance.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Table 2. Results and evaluation of blockchain-based public health surveillance system

Metric	Traditional Systems	Blockchain-Based System	Improvement (%)
Transaction Throughput (TPS)	200–300	850	+183%
Transaction Confirmation Time (sec)	5–10	1.5	-70%
Data Retrieval Speed (sec)	5.8	3.4	+40%
Anonymized Data Validation Accuracy	85%	98.5%	+15.9%
Automated Alert Response Time	10–12 min	2.1 sec	-99.7%
Cyber Threat Detection Accuracy	92%	99.8%	+8.5%
System Efficiency Under High Load (50,000 transactions)	65%	89%	+37%
Blockchain Ledger Storage Growth (per 1,000 transactions)	N/A	1.2 MB	N/A

6. FUTURE OUTCOMES

Blockchain technology in public health surveillance will reshape disease tracking, outbreak identification, and data protection in healthcare infrastructure. Scalability and interop- erability will be emphasized in future development to support direct integration with artificial intelligence (AI) and Internet of Medical Things (IoMT) devices to analyze real-time health information. The use of privacy-protecting methods such as federated learning and more sophisticated cryptographic pro- tocols (e.g., zero-knowledge proofs and homomorphic encryp- tion) will continue to enhance data security and regulatory adherence, enabling secure multi-party data sharing without patient confidentiality loss. Decentralized identity manage- ment solutions may also give individuals more control over their health data, minimizing the dangers of centralized data breaches. Blockchain-enabled public health monitoring in the long term can achieve global health sharing and coopera- tion in data, thus allowing governments and organizations to make better responses against pandemics and emerging health emergencies. Automated response systems through smart con- tracts could induce quick containment programs, leading to improved public health preparedness as well as diminish- ment in the severity of outbreak. In addition, token-based reward mechanisms could prompt healthcare professionals to engage proactively in data sharing while maintaining open- ness and trustworthiness in reporting diseases. As technology advances further, blockchain-enabled predictive analytics and early warning systems will be crucial in defining a more robust and data-centric public health system.

7. CONCLUSION

The use of blockchain-based public health surveillance offers a revolutionary solution to enhancing data security, realtime disease tracking, and outbreak response while over- coming the drawbacks of conventional centralized systems. Utilizing distributed ledger technology, smart contracts, and cryptographic methods, the framework proposed guarantees tamperproof data storage, increased privacy, and automated alert systems, thus making public health decision-making more robust. The results of the study illustrate that blockchain improves the efficiency of transactions, decreases latency in data retrieval, and prevents cyber attacks, making it a promising solution for healthy and scalable management of health data. It is, however, necessary to overcome issues such as scalability, adherence to regulations, and compatibility with current healthcare systems to enable mass adoption. Upcoming developments such as AIbased predictive analysis, decentralized identity management, and federated learning will further make blockchain applicable in public health. In addition, the development of collaborative work between governments, health institutions, and technology providers will be important to facilitate smooth integration and regulatory harmony. As ongoing new health risks continue to threaten global healthcare, blockchain-based public health surveillance holds the promise of transforming disease monitoring, enhanc- ing outbreak readiness, and creating a more open, secure, and efficient healthcare system.

REFERENCES

1. Abeywardena, and K. Yapa, ”Blockchain-based Secure Environment for Electronic Health Records,” in *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2022, pp. 1–6, doi: 10.1109/ICCCNT54827.2022.9984371.
2. J. Nijsse and A. Litchfield, ”Identifying Developer Engagement in Open Source Software Blockchain Projects through Factor Analysis,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2023, pp. 5333–5342.
3. N. V. Pardakhe and V. M. Deshmukh, ”Design and Development of Blockchain-Based Security and Privacy-Preserving System,” in *Lecture Notes in Networks and Systems*, vol. 351, 2022, pp. 459–474, doi: 10.
4. 1007/978-981-16-7657-4 37.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

5. R. C. Barik, P. K. Meher, and B. Kumar, "Blockchain-RFID In- tegrated Model for Preventing Counterfeit Migration in PostSupply Chain," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 2024, doi: 10.1109/ICBDS61829. 2024.10837155.
6. R. Pathak, B. Soni, and N. B. Muppalaneni, "Significance and Chal- lenges in Blockchain-Based Secure Sharing of Healthcare Data," in *Lecture Notes in Electrical Engineering*, vol. 1096, 2024, pp. 763–772, doi: 10.1007/978-981-99-7137-4 74.
7. I. Chenchev, "Classification of the DLT Consensus Algorithms with Focus on Blockchain," in *Lecture Notes in Networks and Systems*, vol. 579, 2023, pp. 731–740, doi: 10.1007/978-981-19-7663-6 68.
8. S. Saxena, N. Arya, S. K. Bharti, and V. Dwivedi, "A Lightweight and Efficient Scheme for e-Health Care System using Blockchain Technol- ogy," in *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, 2023, doi: 10.1109/ISCON57294.2023. 10111937.
9. O. Goel et al., "A Secure and Efficient Blockchain Protocol for Protect- ing Electronic Health Records," in *2024 4th International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 2024,
10. pp. 326–331, doi: 10.1109/ICBCTIS64495.2024.00058.
11. M. Ahmed et al., "Detection of Counterfeit Medicine Using a Private and Permissioned Blockchain," in *2022 2nd Asian Conference on Innovation in Technology (ASIANCON)*, 2022, doi: 10.1109/ASIANCON55314. 2022.9909424.
12. U. Sugandh et al., "Revolutionising Food Safety Management: The Role of Blockchain Technology in Ensuring Safe and High-Quality Food Products," in *Lecture Notes in Networks and Systems*, vol. 788, 2023,
13. pp. 487–498, doi: 10.1007/978-981-99-6553-3 37.
14. T. Kobbaey et al., "A Blockchain-based Vaccination Model for COVID- 19 and Other Infectious Diseases," in *8th International Conference on Information Technology Trends (ITT)*, 2022, pp. 189–195, doi: 10.1109/ ITT56123.2022.9863942.
15. A. Carniel et al., "A Blockchain-Based Approach for COVID-19 Vaccine Lifecycle," in *Lecture Notes in Business Information Processing*, vol. 455, 2022, pp. 71–85, doi: 10.1007/978-3-031-08965-7 4.
16. S. D'Antonio and F. Uccello, "Data Provenance for Healthcare: A Blockchain-Based Approach," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022, pp. 1655– 1660, doi: 10.1109/COMPSAC54236.2022.00263.
17. R. U. Khan et al., "Analyzing and Battling the Emerging Variants of Covid-19 Using Artificial Neural Network and Blockchain," in *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2021, pp. 101– 105, doi: 10.1109/ICCWAMTIP53232.2021.9674142.
18. S. Jain et al., "Blockchain-Enabled Immunization Records for Secure Pediatric Healthcare," in *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, 2024, doi: 10.1109/DELCON64804. 2024.10866218.
19. A. Ghani et al., "Blockchain-Based Frameworks: Technical Overview and Possible Solutions for Healthcare Use," in *Lecture Notes in Networks and Systems*, vol. 826, 2024, pp. 339–351, doi: 10.1007/ 978-3-031-47672-3 33.
20. S. Thejaswini et al., "Med Secure: A Blockchain-Based Authenti- cated System for Counterfeit Medicine in Decentralized Peer-to-Peer Network," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*, 2021, doi: 10.1109/ASIANCON51346.2021.9544648.
21. A. Bansal et al., "A Post-Quantum Consortium Blockchain-Based Secure EHR Framework," in *2023 International Conference on IoT, Commu- nication and Automation Technology (ICICAT)*, 2023, doi: 10.1109/ ICICAT57735.2023.10263717.
22. M. Biswas et al., "BIoT: Blockchain-Based Smart Agriculture with Internet of Things," in *2021 5th World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, 2021, pp. 75–80, doi: 10.1109/WorldS451998.2021.9513998.
23. Ch. Rupa and D. M. Chakravarthy, "Extended Privacy Preservation of Health Official Document Using Blockchain," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 454–461, doi: 10.1109/ICACITE51222. 2021.9404654.
24. M. Aldwairi et al., "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," in *2023 5th International Conference on Blockchain Computing and Applications (BCCA)*, 2023, pp. 652–657, doi: 10.1109/BCCA58897.2023.10338908.