Indonesian Journal of Electronics, Electromedical Engineering, and Medical Informatics e-ISSN: 2656-8624
Homepage: https://ijeeemi.org/; Vol. 7, No. 2, pp. 281-297, April 2025

RESEARCH PAPER

OPEN ACCES

Privacy-Preserving Healthcare Analytics in Indonesia Using Lightweight Blockchain and Federated Learning: Current Landscape and Open Challenges

Viddi Mardiansyah[1], Luhur Bayuaji[2], Iwa Ovyawan Herlistiono[1], Sriyani Violina[1], Adi Purnama[1], and Bagus Alit Prasetyo[1], Phuoc-Hai Huynh[3]

[1] Informatics Department, Engineering Faculty, Widyatama University, Bandung, Indonesia
[2] Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia
[3] An Giang University, Vietnam National University Ho Chi Minh City, Vietnam.

ABSTRACT

Healthcare data are invaluable assets in today's digital age; however, they are also highly vulnerable to misuse, breaches, and unauthorized access. The global healthcare sector faces a significant dilemma: To leverage exceptionally enormous and heterogeneous datasets, the protection of patient privacy must be ensured while simultaneously improving medical services and public health understanding. In recent years, blockchain technology has emerged as a promising solution to manage healthcare data in a decentralized, transparent, tamperproof, as well as secure way. However, several natural limitations often obstruct many conventional blockchain systems. These limitations include scalability issues, high energy consumption, in addition to increased latency, and they can greatly impede practical adoption in resource-limited settings, particularly in developing countries such as Indonesia. These many limitations considerably spurred developers to create lightweight blockchain frameworks. These frameworks aim to retain all of the core benefits of blockchain, such as its immutability in addition to traceability, and optimize both performance and efficiency. In the event that an individual integrates the proposed system by means of federated learning, which allows training of machine learning models across distributed data sources without data privacy being compromised, the system subsequently offers a compelling solution for healthcare analytics that preserves privacy in its entirety. This paper explores integrated technologies in Indonesian healthcare and highlights their potential and limitations. This study discusses how data can improve services while protecting patient confidentiality despite increasing cyber threats. It also considers regional policies like the Personal Data Protection Law and the BPJS health insurance. Identified are certain open challenges, in addition to particular future research directions, for the purpose of addressing the practical, technical, and regulatory hurdles that must be overcome to realize secure and privacy-aware healthcare analytics in Indonesia.

PAPER HISTORY

Received Jan. 02, 2025
Accepted March 25, 2025
Published April 24, 2025

KEYWORDS

Blockchain;
Lightweight Blockchain;
Federated Learning;
Healthcare

CONTACT:

viddi.mardiansyah@widyatama.ac.id
luhur.bayuaji@newinti.edu.my
ovyawan.herlistiono@widyatama.ac.id
sriyani.violina@widyatama.ac.id
adi.purnama@widyatama.ac.id
alit.prasetyo@widyatama.ac.id

1. INTRODUCTION

In today's digital age, healthcare data has become both an invaluable asset and has a significant vulnerability [1]. The global healthcare sector faces a profound dilemma: harnessing data's potential for improving healthcare services while safeguarding patient privacy. Shocking healthcare data breaches, from 2005 to 2019, the total number of individuals affected by healthcare data breaches was 249.09 million. Out of these, 157.40 million individuals were affected in the last five years alone [2], are stark reminders of these challenges.

Southeast Asia stands at the crossroads of this digital transformation. While Singapore and Malaysia have strengthened their healthcare data regulations [3], Indonesia has taken a bold step by implementing the PDP (Personal Data Protection) Law in 2024, classifying health data as "sensitive personal data" requiring special protection [4]. The PDP Law number 27 of 2022 has officially come into effect from October 17, 2024 .

BPJS (Social Security Organizing Agency) Kesehatan is a social security organizing agency in Indonesia established to administer the national social security

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

system, including health and employment insurance. Established under Law No. 40/2004, BPJS Kesehatan aims to provide social protection for all Indonesians. The challenge to securing the data becomes more intricate as BPJS Kesehatan manages health data for over 200 million Indonesians [5]. Imagine a system that has to store data centrally, as well as handle large amounts of sensitive data, ensure timely access to thousands of healthcare facilities, and comply with strict regulations..

The centralized storage of data in BPJS Kesehatan's service system poses a high security risk because data stored in a single location can be targeted by cyberattacks and potentially lose access in the event of a system failure. In addition, reliance on a single infrastructure can lead to issues related to scalability and flexibility, as well as challenges in system maintenance and updates that can disrupt operations. Another obstacle that is frequently encountered in centralized data storage is performance issues, where data access can be reduced if multiple users attempt to access information simultaneously.

Blockchain technology can solve the problem of centralized data storage. Blockchain technology enables decentralized and secure data storage, where each transaction is recorded in cryptographically linked blocks. The blockchain complements this solution by transparently and immutably recording every activity. However, like a sports car on a rocky road, traditional blockchain is too "heavy" for diverse healthcare infrastructure [6]. The lightweight blockchain offers an elegant solution, providing the same security with significantly reduced computational requirements [7, 8]. The lightweight blockchain, which is a more efficient variant, was designed to overcome the challenges of centralized data storage by reducing resource requirements and increasing transaction speed. With its smaller size and lower energy consumption, lightweight blockchain allows devices with limited capacity to participate in the network, thus expanding accessibility and inclusivity.

In addition to the need for secure data storage, the development of technology in the health sector has also raised the need for artificial intelligence (AI) technology. Artificial intelligence has great potential in data management, especially with regard to patient data, and it enables faster and more accurate analyses to support medical decisions. However, its application must always prioritize patient safety and privacy to maximize benefits. Artificial intelligence can process large amounts of patient data to identify patterns and anomalies that help diagnose and treat diseases. The patient data to be analyzed are generally collected centrally, resulting in an increased risk of data breaches.

The federated learning approach is emerging as a smart answer for maintaining patient data privacy. This technology allows healthcare facilities to collaborate on the development of AI models without sharing raw patient data. Imagine a learning system in which hospitals work together to improve disease diagnosis while patient data never leaves the original facility [9-12]. This approach not only enhances data privacy and security but also allows institutions to leverage diverse datasets, leading to more robust and accurate AI models. By maintaining data locality, federated learning addresses the challenges of data sharing while fostering innovation in healthcare analytics.

The integration of these two technologies creates a promising framework that enables secure and efficient analysis of healthcare data in compliance with applicable regulations. Like a bridge connecting the islands of health data in Indonesia, this system can modernize health data management while respecting patient privacy. Given the challenges faced by the healthcare system in Indonesia and the increasing amount of health data that must be managed, these two technologies are gaining increasing attention in academic and industry literature. Therefore, this study aims to gather and analyze existing evidence and provide better insights into their effectiveness and applicability while offering recommendations for better development and implementation in the healthcare sector.

While blockchain and federated learning show promise in healthcare data privacy, several crucial challenges remain unexplored. The traditional blockchain architecture often creates bottlenecks in day-to-day operations, with healthcare providers struggling under growing storage demands and processing delays [11, 13]. Privacy concerns in federated learning present another layer of complexity. Sophisticated attacks can piece together patient information from model updates, and healthcare providers need stronger guarantees that their patient's privacy remains intact [14-16].

The integration of these technologies is still largely theoretical. Much research has been conducted; however, there is a lack of a clear framework to combine blockchain and federated learning in real healthcare environments. The question of balancing privacy protection with system performance remains unanswered, especially in resource-constrained settings [13, 17, 18].

This research makes two key contributions: First, we conduct a comprehensive review of current architectures, examining them through the lens of real-world healthcare needs. Second, we provide a nuanced analysis of the opportunities and challenges that bridge the gap between academic research and practical implementation [19-21].

Through these contributions, we aim to guide future research and development toward solutions that are both technically sound and practically implementable across diverse healthcare settings [22, 23].

In this study, we collected more than 500 publications that were comprehensively reviewed to explore existing architectures and approaches for the use of blockchain, lightweight blockchain, and federated learning, especially implementation in the healthcare sector. All papers were published in the last 5 years. To further focus on the research, almost all the papers analyzed were published within the last 3 years, except highly relevant papers.

Selection of articles, journals, and publications from

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

journals or conferences with very good reputations and relevant from various academic databases, such as IEEE Access, Elsevier, MDPI, PubMed, and conference articles accessed from IEEE Xplore. The reference list we present in this study includes more than 100 relevant sources, covering recent research on security, privacy, and applications of blockchain and federated learning in the context of healthcare. The selection criteria ensure that only relevant and high-quality studies are processed. These criteria include a focus on blockchain applications, lightweight blockchain, and federated learning in the healthcare context, as well as relevance to data privacy issues. After collecting the literature, the next process is to analyze and synthesize the findings from the various studies to identify trends, challenges, and opportunities.

The remainder of this paper is organized into several sections. Section 2 contains literature reviews of blockchain technology, lightweight blockchain, and federated learning. In Section 3, the current landscape is presented. The opportunities of this research is discussed in Section 4, and the challenges and open issues are discussed in Section 5. Finally, we provide our summary conclusion in Section 6.

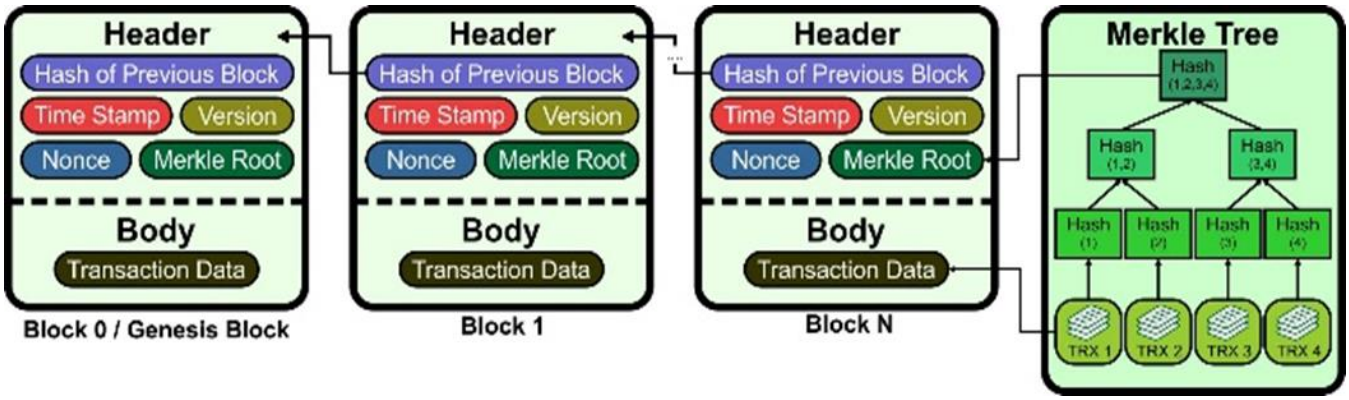

Fig. 1. Blockchain structure with Merkle Tree.

2. LITERATURE REVIEW

A. Blockchain Technology

Blockchain technology was introduced by Satoshi Nakamoto in 2008 with the issuance of Bitcoin, the first digital currency to use blockchain technology [24]. Bitcoin was created to address the problem of double-spending in digital transactions without the need for a third-party authority. The proposed technology uses a proof-of-work (PoW) consensus algorithm, which requires users to solve complex math problems to add new transactions to the blockchain.

Currently, blockchain is considered the most secure data storage medium because it uses an advanced database mechanism that ensures data security and transparency. Data security is achieved because once a transaction is recorded or entered into the blockchain, no one can change it, and the transactions stored in a block are visible to everyone (data transparency). Each block in the blockchain has a cryptographic seal (a hashing mechanism) that makes it difficult to open or change the information contained therein. All transactions are stored through a Merkle tree mechanism, where all stored transactions generate a Merkle tree root value, which is then stored in the block [25]. Fig. 1 shows the general blockchain structure with the Merkle tree mechanism for storing transactions that occur. Thus, if an incorrect transaction is detected, a new block is created to correct it, and both transactions can be observed and validated by all nodes in the blockchain network.

Blockchain technology use is highly dependent on the specific purpose of the user and control and access rights. There are four types of blockchain networks that depend on the characteristics of the user [26]. Generally, there are four types of blockchain networks, each designed to suit different user characteristics and application contexts. A public blockchains is the most open and widely used type, especially in distributed ledger systems. Anyone can see the transactions taking place, and joining is as simple as downloading the required software. Public blockchains are more censorship-resistant than private (or semi-private) blockchains. Since anyone can join the network, the protocol must incorporate certain mechanisms to prevent malicious parties from gaining access to the network anonymously [26, 27].

On the other hand, private blockchain is more suitable for enterprise environments where only authorized participants are allowed to access and interact with the network. This model is a permissioned network in which only authorized members can access the network. This means that the data stored in the network cannot be tampered with and is securely accessed by network member [26].

A consortium or federated blockchains are blockchain technologies that combine the features of private and public blockchains. It is primarily used by companies or groups of organizations that share a common database. Consortium blockchains combine the features of both private and public blockchain networks; however, what qualities define this type of blockchain network? As consortium blockchains are permissioned networks, only members with permission can access the network. This

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

means that the data stored in the network cannot be tampered with and is securely accessed by network members [26, 28].

Lastly, a hybrid blockchain merges the strengths of both public and private blockchains. Organizations will be allowed to set up private and permission-based systems alongside public permissionless systems. With private blockchains, data are stored openly for the public; however, with hybrid blockchains, organizations can decide which data are accessible to the public and control who can access such data. Transactions are typically performed privately on hybrid blockchains; however, they can be verified if required by allowing external smart contracts to verify the information [26, 29].

The types of blockchains that depend on control and access rights can be divided into two types: permissioned and permissionless. A permissioned blockchain operates in a controlled environment where access is restricted to users who receive explicit permission or invitations to join the network. This type of blockchain is commonly used within organizations or business entities, where data security, internal governance, and customization are prioritized. Its advantages include greater control over network participation and the ability to tailor the system to specific operational needs. However, this model also carries potential downsides, such as vulnerability to internal attacks and the possibility of censorship due to centralized authority over access rights [30-33].

In contrast, a permissionless blockchain is open to anyone who meets the basic requirements for participation. It emphasizes transparency and openness, allowing any user to contribute to the network without needing approval. However, a permissionless blockchain also involves risks related to control and customization [30, 34].

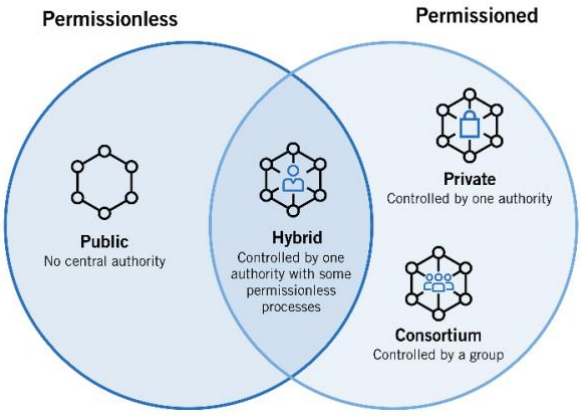

Fig. 2. Blockchain types and access rights.

The specification of user requirements and the selection to exercise control and access rights when using the blockchain are illustrated in Fig. 2.

B. Lightweight Blockchain

Lightweight blockchain is a concept designed to address some of the issues with conventional blockchains that require large data storage and high processing power, and it can be problematic for resource-constrained

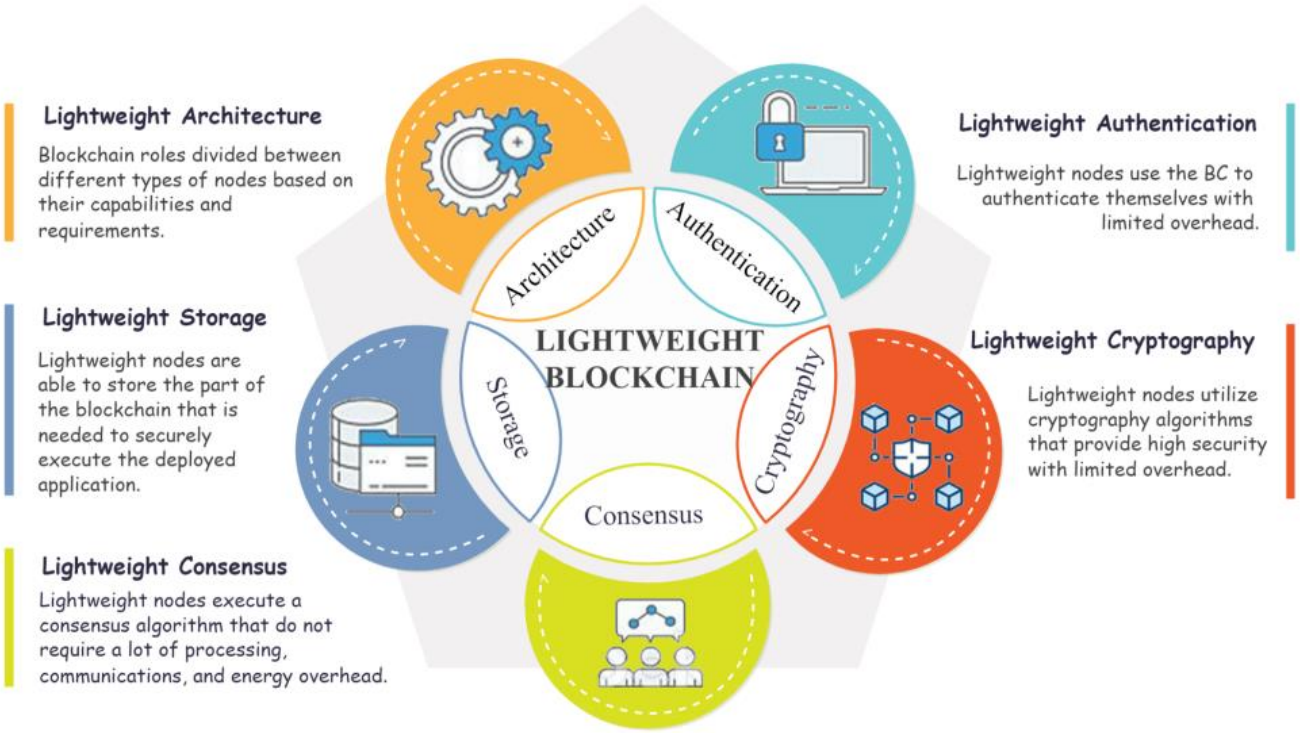

Fig. 3. Lightweight blockchain category.

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

devices, such as Internet of Things (IoT) devices [35-39]. The lightweight blockchain employs a different approach. Instead of storing the entire blockchain, the lightweight blockchain stores blocks of headers or summarized information. This allows devices with limited resources to interact with the blockchain without the need to store the entire blockchain data. Fig. 3 shows the implementation of lightweight blockchain catagories.

The key differences between a lightweight blockchain and a conventional blockchain lie in how they manage storage, computation, and network interaction. In terms of storage, a conventional full node stores all blockchain data, whereas a light client only stores a small portion of the blockchain data, such as headers or summary information [40, 41]. This significantly reduces the storage burden, making it ideal for devices with limited capacity. When it comes to processing power, lightweight clients are designed to operate with minimal computational requirements. Unlike full nodes, which process and validate all transactions and blocks independently, light clients offload these tasks to full nodes. As a result, light nodes are more efficient and can run on resource-constrained devices without compromising too much on performance [41, 42].

In term of authentication, full nodes have the capability to validate transactions and blocks directly, ensuring complete trust and accuracy in the blockchain's operation. Light clients, on the other hand, cannot perform validation on their own. Instead, they depend on full nodes to verify and relay transaction information, creating a trust-based interaction model [40, 41]. From an architectural perspective, light clients are structurally simpler and communicate with the blockchain network through trusted full nodes. This allows them to maintain connectivity with the blockchain without the overhead of storing and processing large datasets [40].

In term of security, light clients can be considered secure as long as they are connected to reputable and trustworthy full nodes. Their reliance on cryptographic protocols and the integrity of full nodes helps maintain a reasonable level of trust in the network [40, 43]. Finally, in the context of consensus mechanisms, lightweight blockchains often adopt simplified consensus algorithms tailored for scalability, low computational overhead, and faster transaction processing. These adaptations make them better suited for applications in environments with limited infrastructure or where speed and efficiency are critical [41, 44].

C. Federated Learning

Federated learning is a model of machine learning that enables model training across decentralized devices. Machine earning is a branch of artificial intelligence that focuses on developing algorithms that allow computers to learn from data and make predictions. In traditional approaches, ML models are trained using data that is collected and stored in centralized data centers, where the training process requires sending data to a server for analysis. While this method has proven effective, a major challenge faced is the issue of data privacy and security, especially when the data being used is sensitive or personal. Federated Learning represents an evolution in data distribution within machine learning, allowing datasets to be trained in a decentralized manner without sending raw data from devices to data centers. The purpose of this decentralized approach is to maintain the privacy of the data owner. In contrast to traditional machine learning, which is centralized, the confidentiality of the owner's data is not well protected according to user privacy laws [45-47]. Fig. 4 shows the structure of federated learning, which is an extension of machine learning.

Research using Federated Learning was first proposed by Konecný et al. [48] in 2017. This research proposes that federated learning can be used to maintain data privacy and work effectively despite limited resources and data heterogeneity. Federated Learning can be used to train ML models in a distributed manner across multiple devices, allowing models to be learned from data residing on those devices without transmitting data between them. It allows models to be learned in a distributed manner across multiple devices without transmitting data between them, thus allowing models to be learned from data residing on those devices without the need to transmit data between them.

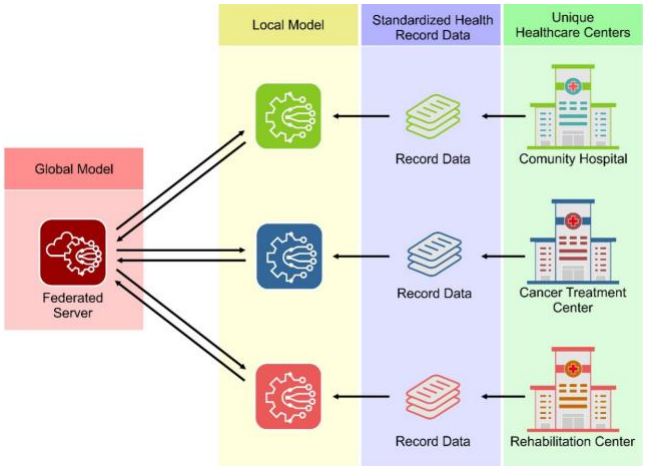

Fig. 4. Federated learning and machine learning structure.

Federated Learning is increasingly recognized for its potential in healthcare, particularly in enhancing data privacy and enabling collaborative model training across decentralized institutions. This approach is particularly relevant in regions like Asia especially Indonesia, where regulatory, data heterogeneity, scalability concerns and diverse healthcare systems can benefit from shared insights without compromising patient confidentiality [11, 49-51].

D. Blockchain, Lightweight and Federated Learning Implementation in Healthcare

The integration of blockchain, lightweight blockchain and

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

federated learning has emerged as a promising solution for privacy-preserving healthcare analytics, especially in regions like Indonesia, where data privacy and security are paramount. Blockchain technology offers a decentralized and tamper-proof ledger for data sharing, lightweight blockchain offers a lighter or simpler blockchain technology without compromising the data security factor, and FL enables collaborative training of artificial intelligence models without having to expose raw data; thus, data security and privatization can be well maintained.

Collaborations between tech companies and healthcare providers foster innovation, leading to the development of tailored solutions that address local challenges in data management and privacy. As awareness grows, more stakeholders will explore the benefits of this integration, paving the way for broader implementation in the healthcare sector.

Several researchers have tried to explore and conduct research related to this technology. Some of the research conducted by previous researchers is summarized in Table 1.

Table. 1. Comparison of Blockchain, Lightweight Blockchain and Federated Learning Approaches.

Approach	Key Features	Author
Blockchain-Based Federated Learning	Decentralized model aggregation, smart contracts, incentive mechanisms, Internet of Things	[8], [13], [17], [18], [19], [26], [30], [32], [52], [53], [54], [55], [56]
Lightweight Blockchain	Simplified consensus, off-chain transactions, pruned blockchains	[9], [35], [39], [43], [57], [58], [59], [60], [61]
Hybrid Approaches	Homomorphic encryption, SMPC, federated metric learning, cloud environment	[14], [15], [26], [62], [63], [64], [65], [66], [67]
Incentive Mechanisms	Tokenized rewards, reputation systems, image classification	[57], [60], [67], [68], [69], [70],

3. CURRENT LANDSCAPE

Healthcare in Indonesia has undergone a significant transformation with the implementation of the Health and Social Security Organizing Agency (BPJS Kesehatan). BPJS Kesehatan was implemented under Law No. 24/2011, replacing Indonesia's Askes system [71]. BPJS Kesehatan aims to provide better and more equitable access to healthcare for all Indonesians, but challenges in its implementation, such as service quality and public awareness, still need to be addressed.

Studies show that while BPJS Kesehatan has improved access, the healthcare system still needs to be evaluated and improved to achieve the goal of optimal national health insurance [72-75].

An architecture combining lightweight blockchain technology and federated learning has emerged as an innovative solution in the current landscape to enhance privacy-preserving health analytics. The solution is designed to address the challenges faced in managing sensitive health data, while enabling effective and collaborative analysis. The proposed solution looks at several aspects, such as existing architecture and privacy-preserving mechanisms.

A. Existing Solution

Several architectural approaches have been proposed for implementing blockchain and federated learning in healthcare systems, each with distinct advantages and limitations. One of the fundamental design choices involves selecting between centralized and decentralized architectures. In centralized systems, a central server aggregates model parameters from participating clients. While this approach is relatively simple and efficient, it remains susceptible to single points of failure and raises concerns about privacy due to data centralization [13, 52]. In contrast, decentralized architectures leverage blockchain technology to distribute the task of model aggregation across multiple nodes. This design minimizes reliance on a central authority, thereby enhancing both security and privacy in federated learning environments [53, 60].

In response to the trade-offs of both models, hybrid architectures have been proposed to combine their respective strengths. These hybrid solutions often use blockchain to ensure data integrity and transparency, while federated learning enables distributed model training without the need to share raw data among participants. This balance helps address privacy concerns while maintaining operational efficiency [76].

The integration patterns between blockchain and federated learning also play a critical role in healthcare system design. One common pattern involves storing model parameters on the blockchain to ensure transparency and integrity [13, 53]. Another approach places the aggregation process directly on the blockchain, thereby eliminating the need for a central server and enhancing trust across the network [52, 60]. In some cases, even the gradients uploaded by clients are stored on the blockchain to strengthen data security and protect against tampering [77, 78].

These systems typically consist of several key components. Healthcare institutions or IoT devices serve as data owners, contributing sensitive information while retaining local control [13, 52]. A federated learning server coordinates the training process and aggregates model parameters [53, 60], whereas the blockchain network acts as a secure and immutable platform for storing and verifying transactions [77, 78]. Smart contracts are often integrated into the system to automate processes such as data validation and parameter aggregation, further enhancing reliability and scalability [76, 79].

Beyond architectural design, practical implementations are increasingly being explored through case studies, deployment scenarios, and real-world applications. For example, Abbas et al. [50] introduces a framework that uses blockchain and federated learning to detect lung diseases using CT scan data. The proposed system achieves 90% accuracy in lung disease classification [60]. Similarly, Alkhalifa et al. [18] developed

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

a system for diabetes detection, reaching an accuracy rate of 97.11%. [53].

In term of deployment scenarios, a number of promising directions have emerged. In IoT-enabled healthcare, smart devices collect health data, which is then processed through federated learning and securely stored using blockchain [13, 52]. Another scenario is multi-institutional collaboration, where several healthcare providers train a global model collaboratively while ensuring data privacy and integrity via blockchain [53, 60]. Real-time health monitoring systems, such as those used for COVID-19 patients, also exemplify how blockchain and federated learning can work together to deliver secure, on-the-fly insights [77, 78].

As for real-world applications, the integration of blockchain and federated learning has been used in systems for disease diagnosis, such as lung cancer, Alzheimer's, and other respiratory diseases using securely processed medical data [53, 57, 60]. Personalized treatment planning has also benefited from this integration, allowing systems to generate tailored recommendations while maintaining patient confidentiality [52, 76]. the realm of epidemiological research, federated learning makes it possible to analyze aggregated data across institutions without exposing sensitive individual-level information [77, 78].

Evaluating the performance of such integrated systems typically involves several metrics. Computational efficiency is a major concern, especially as blockchain's involvement may impact latency and throughput. For instance, Basak et al. [80] reported an average latency of 43.518625 ms and a throughput of over 10034017 bytes/s or 10MB/s in their proposed system [81]. Privacy assurance is often assessed based on the system's ability to secure sensitive data and prevent unauthorized access, with some studies adopting advanced techniques such as homomorphic encryption and differential privacy to reinforce security [82, 83]. Finally, model accuracy remains a core measure of success, with several implementations demonstrating impressive performance, such as 90% accuracy in lung disease detection [60] and 97.11% in diabetes prediction [53].

B. Privacy-Preserving Mechanisms

In healthcare systems that integrate blockchain and federated learning, maintaining data privacy is a critical priority. To address this, several privacy-preserving mechanisms have been widely adopted, including encryption methods, differential privacy, and secure aggregation protocols. Encryption, particularly homomorphic encryption, is one of the most commonly used techniques in this domain. It allows computations to be performed directly on encrypted data without requiring decryption, which helps ensure that sensitive health data remain private throughout the processing lifecycle [82, 83]. Another well-established method is secure multi-party computation (SMPC), where multiple parties can collaboratively compute a function over their inputs while keeping those inputs private. This approach enables collaborative learning without exposing raw data [62, 68].

Zero-knowledge proofs (ZKPs) also play a significant role in enhancing privacy. They allow one party to prove the validity of a piece of information without revealing the information itself. In the healthcare context, ZKPs can verify data integrity or authenticity while keeping sensitive details confidential [76, 84]. Additionally, key management is essential for protecting encryption schemes. Several studies have emphasized the importance of designing secure and efficient key management protocols to prevent unauthorized access to encryption keys and ensure data remains protected [57, 79].

Another widely used privacy mechanism is differential privacy, which can be implemented in two main ways: locally or globally. In the local model, each client adds noise to their data before sending it to the server, ensuring privacy at the source. In the global approach, noise is introduced after the aggregation process, which protects the final result [68, 83]. A key parameter in differential privacy is the privacy budget, which determines how much noise is added. A smaller privacy budget offers stronger privacy protection but may reduce the utility of the data [68, 83]. Striking the right balance between utility and privacy is a major focus in current research, and many studies have shown that with proper tuning, systems can achieve both high utility and adequate privacy [68, 83].

Beyond encryption and differential privacy, secure aggregation protocols are crucial in ensuring that individual data contributions remain private during model training. These protocols are designed to securely combine data or model updates from multiple clients without revealing individual inputs. Blockchain technology is often integrated into these protocols to provide verifiability, transparency, and integrity of the aggregation process. Designing secure aggregation systems also involves addressing practical concerns. One of the main challenges is the communication burden introduced by blockchain, as it may increase network overhead. Nonetheless, this trade-off is often justified by the enhanced security it offers [77, 78]. Security guarantees are typically measured by how effectively the system can prevent malicious attacks and maintain data integrity during aggregation [53, 60]. Moreover, failure management mechanisms are necessary to ensure system resilience. Some implementations use blockchain to track aggregation steps, helping the system recover from faults or dropped communications without compromising data security [77, 78]. Together, these privacy-preserving techniques form a robust framework for building secure, decentralized, and privacy-aware healthcare analytics systems that can operate in real-world environments, especially those with constrained resources or heightened regulatory requirements

C. Limitations of Blockchain and Federated Learning

While blockchain and federated learning hold great promise for enhancing healthcare analytics, especially in safeguarding patient privacy, there are still several

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

limitations and challenges that must be addressed to ensure effective implementation.

One of the primary concerns is scalability. Even though lightweight blockchain architectures have been introduced to mitigate this issue, real-world deployments, particularly in dynamic and high-volume environments like hospitals, still face significant hurdles. Healthcare data is generated rapidly and in large quantities from sources such as IoT medical devices, electronic health records, and diagnostic systems. As the volume of transactions increases, blockchain networks may struggle to process them efficiently, leading to delays and reduced system performance.

Another major limitation lies in the complexity of implementation. Successfully integrating blockchain and federated learning requires a solid technical foundation, including knowledge of cryptographic algorithms, distributed systems, and machine learning frameworks. Unfortunately, not all healthcare institutions have the technical resources or specialized personnel required to support such implementations. This complexity can become a barrier to adoption, especially in smaller or resource-constrained facilities..

Data quality and availability also play a crucial role in the effectiveness of federated learning models. For these systems to provide reliable and accurate insights, they must be trained on high-quality, representative datasets. However, in many cases, data may be fragmented, incomplete, or biased, especially when distributed across various healthcare institutions. This can lead to underperforming models that fail to generalize well across different patient populations or clinical scenarios.

Lastly, regulatory compliance presents its own set of challenges. While blockchain and federated learning are inherently privacy-aware, their deployment must still align with national regulations, such as Indonesia's Personal Data Protection (PDP) Law. Ensuring full compliance involves not only technological safeguards but also a thorough understanding of legal requirements and the implementation of proper administrative procedures. For many organizations, especially those with limited legal or compliance teams, this can add another layer of complexity and slow down the adoption process.

4. OPPORTUNITIES

The integration of lightweight blockchain and federated learning models into healthcare analytics presents many opportunities and challenges. This approach improves privacy and security while maintaining the efficiency and scalability of healthcare systems. The current landscape reveals significant potential for technological advancements and healthcare applications, which can be leveraged to address existing challenges in data privacy and system efficiency.

A. Technical Oportunities

From a technical standpoint, there remains a wealth of opportunities to further develop and refine the integration of lightweight blockchain and federated learning in the healthcare sector—particularly in areas like scalability, resource optimization, and IoT/edge computing integration.

In terms of scalability, several techniques show great promise. One such method is sharding, where the blockchain network is divided into smaller, more manageable partitions. This allows for parallel processing of transactions, significantly enhancing the network's ability to handle large volumes of healthcare data more efficiently [52]. Similarly, layer-2 solutions, such as state channels, can ease the burden on the main blockchain by offloading certain operations, resulting in faster transaction times and lower costs [54]. Another promising direction is the development of optimized consensus mechanisms. These are particularly important for healthcare environments where devices might have limited computing power, like in many IoT applications [52]. Additionally, cross-chain integration, the ability for different blockchain networks to interoperate, can foster improved data sharing and collaboration across various healthcare platforms, breaking down the silos that often hinder progress [54].

On the topic of resource optimization, there's a growing interest in techniques that make systems more efficient without sacrificing performance. Data compression methods, for example, can help reduce the storage and bandwidth requirements when dealing with large healthcare datasets [85]. At the same time, efficient validation protocols can lighten the computational load on individual devices, making secure data processing faster and more manageable [86]. Healthcare applications can also benefit from smart caching, where frequently accessed data is temporarily stored for quick retrieval, leading to better system responsiveness [63]. Moreover, adaptive protocols that automatically adjust to changing network conditions can enhance both reliability and efficiency, particularly in environments with inconsistent connectivity [87].

One of the most exciting frontiers is the integration of IoT and edge computing. By moving computation closer to where data is generated, edge computing can drastically reduce latency and bandwidth consumption, making real-time analysis feasible even in remote healthcare settings [18]. Efforts to optimize IoT devices, making them more energy-efficient and capable of handling federated learning tasks, can further boost their utility in healthcare monitoring [52]. In addition, advances in network efficiency can ensure smoother, safer transmission of sensitive medical data, reducing the likelihood of breaches [54]. And with real-time processing capabilities, healthcare providers can make faster decisions, especially crucial in time-sensitive scenarios like remote patient monitoring or emergency response [18].

B. Healthcare Applications

Integrating lightweight blockchain and federated learning into healthcare applications offers substantial potential to

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

enhance clinical analytics, improve operational efficiency, and ultimately boost patient health outcomes. This combination ensures the protection of patient data while also fostering increased collaboration among healthcare providers, helping to create a more dynamic and innovative healthcare ecosystem. Clinical analytics, which involves collecting, processing, and analyzing health data to improve clinical decision-making and patient outcomes, can significantly benefit from these technologies. They help improve the effectiveness of clinical analytics while maintaining the security of sensitive patient information.

In this context, several key areas of clinical analytics are being explored. For instance, predictive modeling is made possible through federated learning, allowing the development of models for patient outcomes without compromising data privacy [88]. Furthermore, the ability to analyze patient data across multiple institutions enhances risk assessment and early detection of health problems, enabling healthcare professionals to take proactive steps [89, 90]. Data-driven insights can also optimize care, improving treatment plans and resource allocation, ensuring patients receive the most effective care possible [91, 92]. Efficient data analysis in this domain also aids in the optimal distribution of healthcare resources, ultimately enhancing the delivery of services [90, 92].

In addition to clinical analytics, the integration of innovative healthcare approaches, such as remote patient monitoring, presents new opportunities for improvement. The use of wearable sensors and IoT (Internet of Things) devices allows for continuous, real-time monitoring of patient health. This data can then be analyzed to offer valuable insights that support timely and informed healthcare decisions [18]. Real-time analytics significantly improve the effectiveness of remote monitoring systems, allowing for quick interventions and alerts when needed [54]. Moreover, by developing robust warning systems, patient engagement can be enhanced, leading to better adherence to treatment plans and improved health outcomes [63]. Enhanced data analytics also drives greater patient engagement, as personalized health insights empower individuals to take a more active role in managing their health [87].

Moreover, privacy-preserving healthcare innovations enabled by blockchain and federated learning have spurred collaboration and increased understanding of diseases and effective treatments. These advancements involve multiple institutions, researchers, and healthcare providers working together. Collaborative research has expanded the ability to collect and analyze data on a larger scale, leading to more impactful findings. Federated learning allows institutions to collaborate on research without needing to share sensitive data, protecting privacy while enabling scientific discovery [89]. Blockchain can facilitate secure data-sharing frameworks, further enhancing collaboration and fostering innovation [52]. Instead of sharing raw data, healthcare providers can share trained models, ensuring privacy protection while still enabling collaborative research [85]. Additionally, the use of advanced analytics allows for knowledge discovery, uncovering new insights from diverse data sets, which can drive significant advancements in healthcare and medical treatments [91].

5. CHALLENGES AND OPEN ISSUES

The existence of BPJS (Social Security Organizing Agency) Kesehatan in Indonesia has become a significant effort to achieve Universal Health Coverage (UHC) through the National Health Insurance (JKN) program. The existence of this program raises a number of challenges, opportunities, and strategic adjustments in improving the effectiveness and sustainability of the health insurance system.

The implementation of BPJS Kesehatan also faces various challenges related to its effectiveness and efficiency. These challenges include several areas, such as administrative and operational areas, financial challenges, Service Quality and Equity, Data Privacy and Compliance.

A. Administrative and Operational Challenges

In Indonesia, the implementation of BPJS Kesehatan, which aims to improve access to and quality of healthcare services, faces several significant administrative and operational challenges. One of the key issues is the problem of pending claims and verification delays. Hospitals and healthcare providers often experience delays in claim processing due to incomplete medical records, coding errors, and insufficient documentation. For example, a study conducted at a Type D General Hospital revealed that 29% of pending claims were due to incomplete medical records, and 21% were attributed to coding errors .

Another challenge is the post-claim audits carried out by BPJS Kesehatan, which frequently result in claim adjustments or reversals. This has created financial uncertainties for healthcare providers, especially hospitals, which need to adapt to these verification processes . Additionally, the increased patient load under BPJS Kesehatan has not been matched with proportional increases in medical staff incentives. This disparity has led to dissatisfaction among healthcare workers, further complicating the operational aspects of the program .

B. Financial Challenges

Financial factors are also critical when implementing BPJS Kesehatan. One of the major concerns is the program's consistent financial deficits, which are partly due to rising healthcare costs and inadequate funding sources. These deficits raise questions about the long-term sustainability of the program and its ability to provide continuous healthcare services to the population [72, 93]. Another financial issue faced by healthcare providers is the delay in receiving reimbursements for services rendered under BPJS. These delayed payments place additional financial pressure on hospitals, making it difficult for them to maintain their operations and provide

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

quality care to patients .

C. Service Quality and Equity

There are also operational challenges related to the quality and equity of services provided under BPJS Kesehatan. Despite efforts to expand coverage, significant disparities remain in access to healthcare services, particularly between urban and rural areas. For example, the use of skilled birth attendants is still much lower in eastern Indonesia compared to western regions, highlighting the unequal distribution of healthcare resources [94]. Furthermore, the benefits provided under BPJS Kesehatan tend to favor wealthier groups, with urban and Java-based populations benefiting more than those in rural or eastern regions. This inequity in the distribution of benefits further exacerbates the gap in healthcare access and outcomes across different socio-economic and geographic groups [95].

D. Data Privacy and Compliance

The integration of lightweight blockchain and federated learning into Indonesia's PDP 2024 presents several regulatory challenges, particularly around data privacy, security, and system efficiency. One of the strengths of blockchain technology is its ability to provide immutable data transactions [69]. This ensures compliance with user data deletion requests through verifiable mechanisms, enhancing trust among participants, as all actions are transparently recorded and cannot be altered retroactively [96]. Blockchain's decentralized nature also addresses security concerns associated with traditional federated learning, which often relies on a central server that presents a single point of failure. By decentralizing the structure, blockchain mitigates these risks and enhances system security [97]. Lightweight blockchain solutions, such as SLABFL, help protect against malicious clients, ensuring the integrity of the learning process [98]. Moreover, hierarchical blockchain frameworks optimize throughput while maintaining model accuracy, which is crucial for decentralized applications [69]. Solutions like LFL-COBC reduce latency and storage overhead, making them ideal for resource-constrained environments [98].

However, despite the benefits, challenges remain in developing efficient consensus mechanisms and managing the increased complexity of these systems. Overcoming these hurdles is essential for the widespread adoption of blockchain and federated learning technologies in the healthcare sector.

6. CONCLUSION

The aim of this paper is to explore the potential of using lightweight blockchain and federated learning technologies to improve privacy-preserving healthcare analytics in Indonesia. Given the critical importance of healthcare data privacy, especially in a country like Indonesia, where the healthcare system is undergoing rapid modernization, this paper discusses the integration of these technologies to enhance security, privacy, and interoperability in the healthcare sector.

The findings indicate that blockchain offers a secure, decentralized infrastructure that enhances data integrity and transparency. Its immutable nature ensures that once data is recorded, it cannot be tampered with, fostering trust among healthcare providers and patients. The decentralized architecture significantly reduces the risk of data breaches compared to traditional centralized systems. Furthermore, blockchain facilitates interoperability between different healthcare systems, enabling smoother data sharing while ensuring that sensitive information remains secure. However, challenges remain in terms of scalability, especially when applied to large-scale healthcare applications.

Lightweight blockchain solutions, such as permissioned blockchains and hybrid database systems, have been proposed to address these challenges, offering a balance between security and performance. Federated learning, which allows for decentralized model training, complements blockchain by enabling healthcare organizations to train models on local data without sharing it, thus preserving patient privacy. Despite its advantages, federated learning faces issues such as expensive communication costs, system heterogeneity, and security challenges, particularly with malicious actors potentially interfering with the learning process.

The study also identifies the ethical considerations and regulatory compliance requirements, specifically in relation to Indonesia's Personal Data Protection (PDP) Law. Ethical measures, such as data anonymization, encryption, and obtaining patient consent, are essential in ensuring that these technologies are deployed in a manner that protects individual privacy.

Looking forward, the integration of blockchain, lightweight blockchain, and federated learning presents a promising solution to healthcare privacy challenges in Indonesia. However, to fully realize its potential, future work should focus on addressing the scalability issues, particularly in smaller healthcare settings and rural areas, where infrastructure may be limited. Further research is needed to explore the effectiveness of these technologies in different healthcare contexts and to ensure that the proposed frameworks can handle larger and more complex data sets. Additionally, incorporating IoT devices and big data analytics could further improve the quality of healthcare analytics. Lastly, it is crucial to develop a clear and comprehensive regulatory framework to support the adoption of these technologies, ensuring that they comply with local laws and ethical standards. Future research should continue to focus on refining these technologies, improving their interoperability, and developing more advanced privacy-preserving techniques, ultimately contributing to the betterment of Indonesia's healthcare system.

ACKNOWLEDGMENT

This journal article was written by (Viddi Mardiansyah, Luhur Bayuaji, Phuoc-Hai Hyunh, Iwa Ovyawan Herlistiono, Sriyani Violina, Adi Purnama, and Bagus Alit

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

Prasetyo) from the Informatics Department, Engineering Faculty, Widyatama University, based on the report "Securing Data using Federated Learning Based on Lightweight Blockchain Approach". Bureau of Research, Community Service and Intellectual Capital provided funding for this research in the year 2024. The authors' opinions are expressed here, and they may not represent the funders's viewpoints.

REFERENCES

[1] R. Zhang, R. Xue, and L. Liu, "Security and Privacy for Healthcare Blockchains," IEEE Transactions on Services Computing, vol. 15, no. 6, pp. 3668-3686, 2022, doi: 10.1109/TSC.2021.3085913.

[2] P. R. Clearinghouse. "Data Breach Chronology Archive - PRC Historical Data 2005 - 2019." https://public.tableau.com/views/DataBreachChronologyArchive-PRCHistoricalData2005-2019/KeyInsights-BreachbyType (accessed August 7, 2024).

[3] A. Organization. "ASEAN REVS UP - Digital Transformation." https://asean.org/wp-content/uploads/2022/11/Issue-23-Digital-Transformation-digital-version.pdf (accessed August 7, 2024).

[4] C. C. o. t. R. o. Indonesia. "Govt: Law on Personal Data Protection Provides Legal Protection." https://en.mkri.id/news/details/2023-02-13/Govt:_Law_on_Personal_Data_Protection_Provides_Legal_Protection (accessed Dec 3, 2024).

[5] B. Ketenagakerjaan. "Law of The Republic of Indonesia Number 24 of 2011 on Social Security Agency." https://www.bpjsketenagakerjaan.go.id/assets/uploads/peraturan/Terjemahan_Batang_Tubuh_UU_Nomor_24_Tahun_2011_(1).pdf (accessed Dec 10, 2024).

[6] A. S. C. Edward Torres Cruz, D. Rajani, Damian Dziembek, K. Suresh Kumar, Sorabh Lakhanpal, Lucero D. Mamani-Chipana, "Studying the Application of Blockchain in Healthcare for Security and Transparent Record-Keeping," in Recent Trends In Engineering and Science for Resource Optimization and Sustainable Development, S. t. A. o. B. i. H. f. S. a. T. Record-Keeping Ed. London: CRC Press, 2024.

[7] V. Mardiansyah and R. F. Sari, "Implementation of Proof-of-Work Concept Algorithm using SimBlock Simulator," in 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 19-21 April 2021 2021, pp. 1-6, doi: 10.1109/NTMS49979.2021.9432645.

[8] A. Gautama, A. F. Rochim, and L. Bayuaji, "Privacy Preserving Electronic Health Record with Consortium Blockchain," in 2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 13-14 Dec. 2022 2022, pp. 303-308, doi: https://doi.org/10.1109/ICITISEE57756.2022.10057649.

[9] V. Mardiansyah and R. F. Sari, "Lightweight Blockchain Framework For Medical Record Data Integrity," Journal of Applied Science and Engineering, vol. 26, no. 1, pp. 91-103, 2022/04/05 2022, doi: https://doi.org/10.6180/jase.202301_26(1).0010.

[10] K. Lazaros, D. E. Koumadorakis, A. G. Vrahatis, and S. Kotsiantis, "Federated Learning: Navigating the Landscape of Collaborative Intelligence," Electronics, vol. 13, no. 23, p. 4744, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/23/4744.

[11] C. Bandla, "Distributed Database Architectures for Federated Medical Training," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 4, no. 2, pp. 633-640, Dec 2024 2024, doi: https://doi.org/10.48175/ijarsct-22774.

[12] M. H. Jung, I. Song, and K. Lee, "Federated Learning Lifecycle Management for Distributed Medical Artificial Intelligence Applications: A Case Study on Post-Transcatheter Aortic Valve Replacement Complication Prediction Solution," Applied Sciences, vol. 15, no. 1, p. 378, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/1/378.

[13] Z. Ngoupayou Limbepe, K. Gai, and J. Yu, "Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey," Blockchains, vol. 3, no. 1, p. 1, 2025. [Online]. Available: https://www.mdpi.com/2813-5288/3/1/1.

[14] J. Kaur, R. Rani, and N. Kalra, "Healthcare Data Security and Privacy Protection Framework Based on Dual Channel Blockchain," Transactions on Emerging Telecommunications Technologies, vol. 36, no. 1, p. e70049, 2025, doi: https://doi.org/10.1002/ett.70049.

[15] M. Mehraeen and L. Mahmoudi, "Tracing the Blockchain Challenges in Healthcare: A Topic Modeling and Bibliometric Analysis," Blockchain in Healthcare Today, vol. 7, no. 3, 12/16 2024, doi: 10.30953/bhty.v7.335.

[16] K. Li, "A Blockchain-Integrated Federated Learning Approach for Secure Data Sharing and Privacy Protection in Multi-Device Communication," Applied Artificial Intelligence, vol. 39, no. 1, p. 2442770, 2025/12/31 2025, doi: 10.1080/08839514.2024.2442770.

[17] D. Gana and F. Jamil, "DAG-Based Swarm Learning Approach in Healthcare: A Survey," IEEE Access, vol. 13, pp. 13796-13815, 2025, doi: 10.1109/ACCESS.2025.3531216.

[18] A. K. ALKHALIFA et al., "HARNESSING PRIVACY-PRESERVING FEDERATED LEARNING WITH BLOCKCHAIN FOR SECURE IOMT APPLICATIONS IN SMART HEALTHCARE

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

SYSTEMS," Fractals, vol. 32, no. 09n10, p. 2540020, 2024, doi: 10.1142/s0218348x25400201.

[19] M. E. O. Ursan, C. D. Căleanu, and M. Bucos, "An Architecture of a Web Application for Deploying Machine Learning Models in Healthcare Domain," in 2024 International Symposium on Electronics and Telecommunications (ISETC), 7-8 Nov. 2024 2024, pp. 1-6, doi: 10.1109/ISETC63109.2024.10797433.

[20] A. Freek, "Enhancing Healthcare Analytics and Accelerating Personalized Treatment through Comparative Studies of High-Throughput Database Architectures," Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023, vol. 7, no. 01, pp. 120-139, 12/30 2024, doi: 10.60087/jaigs.v7i01.303.

[21] K. David-mukoro, A. Atulegwu, and S. E. Audu, "Perception of Medical Doctors on the Effectiveness of Therapeutic Architecture," African Journal of Environmental Sciences and Renewable Energy, vol. 17, no. 1, pp. 11-24, 11/07 2024, doi: 10.62154/ajesre.2024.017.010424.

[22] M. Alruwaili, A. Alsayat, M. Idris, S. Alanazi, and K. Aurangzeb, "Integration and analysis of diverse healthcare data sources: A novel solution," Computers in Human Behavior, vol. 157, p. 108221, 2024/08/01/ 2024, doi: https://doi.org/10.1016/j.chb.2024.108221.

[23] L. R. Soenksen et al., "Integrated multimodal artificial intelligence framework for healthcare applications," npj Digital Medicine, vol. 5, no. 1, p. 149, 2022/09/20 2022, doi: 10.1038/s41746-022-00689-4.

[24] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[25] V. Mardiansyah, A. Muis, and R. F. Sari, "Multi-State Merkle Patricia Trie (MSMPT): High-Performance Data Structures for Multi-Query Processing Based on Lightweight Blockchain," IEEE Access, vol. 11, pp. 117282-117296, 2023, doi: 10.1109/ACCESS.2023.3325748.

[26] S. N. Sangjukta Das, and Victor Hugo C. de Albuquerque, "Blockchain technology: fundamentals, applications, and challenges," in Blockchain Technology in e-Healthcare Management, 2024, pp. 1-30.

[27] N. Kaur and N. Kshetri, "Blockchain Technology," in Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures: CRC Press, 2025.

[28] B. Huang, H. Zheng, X. Qu, and T. Xiong, "Consortium Blockchain Efficient Storage Access Control Solution," in 2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT), 28-30 April 2023 2023, pp. 570-575, doi: 10.1109/ICCECT57938.2023.10140311.

[29] S. S. Luke Jebaraj, Irisappane Soubache, "Blockchain Technologies and Applications for Business and Finance Systems," in Data-Driven Modelling and Predictive Analytics in Business and Finance: Auerbach Publications, 2024.

[30] D. Hossain, Q. Mamun, and R. Islam, "Unleashing the Potential of Permissioned Blockchain: Addressing Privacy, Security, and Interoperability Concerns in Healthcare Data Management," Electronics, vol. 13, no. 24, p. 5050, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/24/5050.

[31] A. Bulzan, R. Botez, and V. Dobrota, "Permissioned Blockchain-as-a-Service: Architecting Secure and Efficient Private Blockchain Networks," in 2024 International Symposium on Electronics and Telecommunications (ISETC), 7-8 Nov. 2024 2024, pp. 1-4, doi: 10.1109/ISETC63109.2024.10797365.

[32] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas, "Permissioned blockchain network for proactive access control to electronic health records," BMC Medical Informatics and Decision Making, vol. 24, no. 1, p. 303, 2024/10/15 2024, doi: 10.1186/s12911-024-02708-8.

[33] P. H. B. Correia, M. A. Marques, M. A. Simplicio, L. Ermlivitch, C. C. Miers, and M. A. Pillon, "Comparative Analysis of Permissioned Blockchains: Cosmos, Hyperledger Fabric, Quorum, and XRPL," in 2024 IEEE International Conference on Blockchain (Blockchain), 19-22 Aug. 2024 2024, pp. 464-469, doi: 10.1109/Blockchain62396.2024.00068.

[34] A. Rosli, S. Hassan, M. H. Omar, M. S. Sajat, Z. S. Attarbashi, and K. M. Zaini, "Blockchain Applications and Management: A Multidisciplinary Analysis," in 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS), 6-7 Nov. 2024 2024, pp. 1-8, doi: 10.1109/NETAPPS63333.2024.10823600.

[35] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing," Journal of Systems and Software, vol. 154, pp. 22-36, 2019, doi: https://doi.org/10.1016/j.jss.2019.04.050.

[36] V. Mardiansyah and R. F. Sari, "SimBlock Simulator Enhancement with Difficulty Level Algorithm Based on Proof-of-Work Consensus for Lightweight Blockchain," Sensors, vol. 22, no. 23, p. 9057, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/23/9057.

[37] M. Alaslani, S. Suri, B. Shihada, and F. Nawab, "Synopsis: a Scalable Byzantine Distributed Ledger for IoT Networks," in 2024 6th International Conference on Blockchain Computing and Applications (BCCA), 26-29 Nov. 2024 2024, pp.

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

30-38, doi: 10.1109/BCCA62388.2024.10844486.

[38] S. R. Al-Hafidh and E. H. Al-Hemiary, "Simplified Distributed Ledger for Task Offloading In Edge Networks," Iraqi Journal of Information and Communication Technology, vol. 7, no. 3, pp. 18-28, 12/31 2024, doi: 10.31987/ijict.7.3.247.

[39] K. Selvakumarasamy, T. R. Kumar, A. Meenambika, R. B, and R. M, "Decentralized Security in IoT: Lightweight Blockchain with Optimized CA-LSTM for Improved Performance and Privacy," in 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), 18-20 Nov. 2024 2024, pp. 244-251, doi: 10.1109/ICDICI62993.2024.10810781.

[40] Y. Elgountery, M. Lasaad, M. Oualla, A. Jakimi, and H. Sadki, "A Lightweight Blockchain Architecture for IoT Based on Delegated Nodes," in 2024 Mediterranean Smart Cities Conference (MSCC), 2-4 May 2024 2024, pp. 1-6, doi: 10.1109/MSCC62288.2024.10697081.

[41] K. Mershad, "COSIER: A comprehensive lightweight blockchain system for IoT networks," Computer Communications, vol. 224, pp. 125-144, 2024/08/01/ 2024, doi: https://doi.org/10.1016/j.comcom.2024.06.007.

[42] W. Lv, Y. Chen, and J. Liu, A survey of lightweight block cipher (International Conference on Algorithms, High Performance Computing, and Artificial Intelligence). SPIE, 2024.

[43] P. Sharma, K. S. Saini, and P. K. Sidhu, "Lightweight, Secure and Authenticated Blockchain-Optimized Network Routing Protocol for Wireless Body Area Networks," in 2024 2nd World Conference on Communication & Computing (WCONF), 12-14 July 2024 2024, pp. 1-6, doi: 10.1109/WCONF61366.2024.10692195.

[44] T. Sylla, L. Alouache, and A. Chorti, "A Lightweight Blockchain Strategy for Managing Smart Grids and Distributing Energy," in 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 21-23 Oct. 2024 2024, pp. 1-6, doi: 10.1109/WiMob61911.2024.10770445.

[45] L. Xu, D. Xu, X. Yi, C. Deng, T. Chai, and T. Yang, "Decentralized Federated Learning Algorithm Under Adversary Eavesdropping," IEEE/CAA Journal of Automatica Sinica, vol. 12, no. 2, pp. 448-456, 2025, doi: 10.1109/JAS.2024.125079.

[46] K. Wang, Q. Wu, and Y. Qin, A distributed machine learning dynamic remote proof scheme that resists collusion attacks (International Conference on Network Communication and Information Security (ICNCIS 2024)). SPIE, 2025.

[47] J. Reeti, P. Surya Narayan, and K. Vikas, "Federated Learning: An Approach for Managing Data Privacy and Security in Collaborative Learning," Recent Advances in Electrical & Electronic Engineering, vol. 18, pp. 1-16, 2025, doi: http://dx.doi.org/10.2174/0123520965328724241218110637.

[48] J. Konecný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated Learning: Strategies for Improving Communication Efficiency," ArXiv, vol. abs/1610.05492, 2016.

[49] Q. W. Xiaoming Xu, and Jing Wen, "Real-World Application of Federated Learning for Collaborative Medical Image Classification: A Case Study in Shenzhen's Hospitals and Research Institutions," 2024.

[50] S. R. Abbas, Z. Abbas, A. Zahir, and S. W. Lee, "Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration," Healthcare, vol. 12, no. 24, p. 2587, 2024. [Online]. Available: https://www.mdpi.com/2227-9032/12/24/2587.

[51] S. Mishra, R. Tondon, and N. P. S. Rathore, "Revolutionizing Healthcare with Federated Learning: A Comprehensive Review," in 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), 27-28 Sept. 2024 2024, pp. 1-5, doi: 10.1109/ACROSET62108.2024.10743932.

[52] Nazar Waheed et al., "FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare through Federated Learning and Blockchain," arXiv, 2023, doi: https://doi.org/10.48550/arXiv.2304.07668.

[53] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. Alabdulatif, "A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data," Computers in Biology and Medicine, vol. 167, p. 107630, 2023/12/01/ 2023, doi: https://doi.org/10.1016/j.compbiomed.2023.107630.

[54] S. El Haddouti and M. D. Ech-Cherif El Kettani, "A Secure and Privacy-Preserving Paradism Based on Blockchain and Federated Learning for CIoMT in Smart Healthcare Systems," in Innovations in Smart Cities Applications Volume 7, Cham, M. Ben Ahmed, A. A. Boudhir, R. El Meouche, and İ. R. Karaş, Eds., 2024// 2024: Springer Nature Switzerland, pp. 447-456.

[55] T. K. Vashishth, V. Sharma, B. Kumar, K. K. Sharma, S. Chaudhary, and R. Panwar, "Blockchain for Securing Federated Learning Systems: Enhancing Privacy and Trust," in Model Optimization Methods for Efficient and Edge AI, 2025, pp. 299-320.

[56] Z. Cheng et al., "Decentralized IoT data sharing: A blockchain-based federated learning approach with joint optimizations for efficiency and privacy," Future Generation Computer Systems, vol. 160, pp. 547-563, 2024/11/01/ 2024, doi: https://doi.org/10.1016/j.future.2024.06.035.

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

[57] A. A. Noman, M. Rahaman, T. H. Pranto, and R. M. Rahman, "Blockchain for medical collaboration: A federated learning-based approach for multi-class respiratory disease classification," Healthcare Analytics, vol. 3, p. 100135, 2023/11/01/ 2023, doi: https://doi.org/10.1016/j.health.2023.100135.

[58] C. Dhasaratha et al., "Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things," CAAI Transactions on Intelligence Technology, vol. n/a, no. n/a, doi: https://doi.org/10.1049/cit2.12287.

[59] A. Emamhosseini, S. Sobuti, S. Khorsandi, and A. Hashemi-Golpayeghani, "Improving Privacy Protection in a Collaborative Blockchain-based E-Health Records System," in 2023 14th International Conference on Information and Knowledge Technology (IKT), 26-28 Dec. 2023 2023, pp. 141-147, doi: 10.1109/IKT62039.2023.10433059.

[60] M. Gupta, M. Kumar, and Y. Gupta, "A blockchain-empowered federated learning-based framework for data privacy in lung disease detection system," Computers in Human Behavior, vol. 158, p. 108302, 2024/09/01/ 2024, doi: https://doi.org/10.1016/j.chb.2024.108302.

[61] A. Singh and K. K. Singh, "Blockchain with Federated Learning for Secure Healthcare Applications," in Blockchain and Deep Learning for Smart Healthcare, 2023, pp. 35-44.

[62] A. P. Kalapaaking, I. Khalil, and X. Yi, "Blockchain-Based Federated Learning With SMPC Model Verification Against Poisoning Attack for Healthcare Systems," IEEE Transactions on Emerging Topics in Computing, vol. 12, no. 1, pp. 269-280, 2024, doi: 10.1109/TETC.2023.3268186.

[63] S. B. Babu and K. R. Jothi, "A Secure Framework for Privacy-Preserving Analytics in Healthcare Records Using Zero-Knowledge Proofs and Blockchain in Multi-Tenant Cloud Environments," IEEE Access, vol. 13, pp. 8439-8455, 2025, doi: 10.1109/ACCESS.2024.3509457.

[64] B. T. H. Dang, P. H. Luan, V. D. T. Ngan, N. T. Trong, P. T. Duy, and V. H. Pham, "TrustFedHealth: Federated Learning with Homomorphic Encryption and Blockchain for Heart Disease Prediction in the Smart Healthcare," in 2023 International Conference on Advanced Technologies for Communications (ATC), 19-21 Oct. 2023 2023, pp. 178-183, doi: 10.1109/ATC58710.2023.10318944.

[65] H. Zhang, Z. Liu, L. Wu, and H. Li, "A Healthcare Data Sharing Scheme Based on Homomorphic Encryption and Federated Metric Learning," in 2024 5th International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI), 27-29 Sept. 2024 2024, pp. 131-138, doi: 10.1109/ICHCI63580.2024.10807931.

[66] P. S. S. V. D. Sarada, N. Sindhu, and U. M, "Blockchain-based federated learning with smpc model verification against poisoning attack for healthcare systems," International Journal of Engineering, Science and Advanced Technology, vol. 24, no. 10, pp. 60-71, 2024, doi: http://doi.org/10.36893/IJESAT.2024.V24I10.08.

[67] M. Firdaus and K. H. Rhee, "Towards Trustworthy Collaborative Healthcare Data Sharing," in 2023 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 5-8 Dec. 2023 2023, pp. 4059-4064, doi: 10.1109/BIBM58861.2023.10385319.

[68] F. Imboccioli, G. Cialone, and S. Ferretti, "Decentralization of Learning and Trust in the Healthcare: Blockchain-driven Federated Learning for Alzheimer's MRI Image Classification," in 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 11-15 March 2024 2024, pp. 739-744, doi: 10.1109/PerComWorkshops59983.2024.10502820.

[69] H. Wang, H. Gao, T. Ma, C. Li, and T. Jing, "A hierarchical blockchain-enabled distributed federated learning system with model-contribution based rewarding," Digital Communications and Networks, 2024/07/06/ 2024, doi: https://doi.org/10.1016/j.dcan.2024.07.002.

[70] J. Passerat-Palmbach et al., "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data," in 2020 IEEE International Conference on Blockchain (Blockchain), 2-6 Nov. 2020 2020, pp. 550-555, doi: 10.1109/Blockchain50366.2020.00080.

[71] M. Y. Alkayyis, "Implementation of the National Health Insurance Programme in Achieving Universal Health Coverage in Indonesia," Jurnal Jaminan Kesehatan Nasional, vol. 4, no. 2, pp. 85 - 95, 12/30 2024, doi: 10.53756/jjkn.v4i2.197.

[72] D. A. Arimbi, "Legal Opportunities Solutions to Tackle the Deficit in Indonesia's National Health Insurance Program," Padjadjaran Jurnal Ilmu Hukum, vol. 11, no. 3, 2024, doi: https://doi.org/10.22304/pjih.v11n3.a1.

[73] F. F. Rahman, "Indonesia's healthcare landscape: embracing innovation in the new health regime," Current Medical Research and Opinion, vol. 40, no. 6, pp. 929-933, 2024/06/02 2024, doi: 10.1080/03007995.2024.2349732.

[74] R. Agustin and T. Syahuri, "Implementasi Undang-Undang Kesehatan: Implikasi Terhadap Kesejahteraan Masyarakat Dan Perspektif Tenaga Kesehatan Di Indonesia," Bacarita Journal, vol. 4, no. 2, 2024, doi: https://doi.org/10.30598/bacarita.v4i2.12362.

[75] R. Siti Rofiatun, "Analysis of Access, Quality and Health Services on the Effectiveness of Health Insurance System," Miracle Get Journal, vol. 1, no. 3, pp. 17-26, 09/12 2024, doi:

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

10.69855/mgj.v1i3.62.

[76] R. Malik, A. ur-Rehaman, H. Razzaq, C. Bhatt, K. Kaushik, and I. U. Khan, "Advancing Healthcare IoT: Blockchain and Federated Learning Integration for Enhanced Security and Insights," in 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), 9-11 May 2024 2024, pp. 308-314, doi: 10.1109/IC3SE62002.2024.10593078.

[77] Z. Lian, W. Wang, Z. Han, and C. Su, "Blockchain-Based Personalized Federated Learning for Internet of Medical Things," IEEE Transactions on Sustainable Computing, vol. 8, no. 4, pp. 694-702, 2023, doi: 10.1109/TSUSC.2023.3279111.

[78] P. M. K. D, J. A. B, C. B. S. Lakshmi, T. Fatima, and N. R, "Blockchain-Based Federated Learning-Convolutional Neural Network for Preserving Data Privacy and Security," in 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT), 20-21 Oct. 2023 2023, pp. 1-5, doi: 10.1109/EASCT59475.2023.10393069.

[79] S. Kumar and J. S. Kumar, "Federated Blockchain Based Highly-Available Healthcare System to Protect the Privacy and Security of Users," in 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), 24-28 June 2024 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10725386.

[80] S. Basak, A. Kumar, and K. Chatterjee, "Blockchain Enabled Federated Learning-Based Medical Cyber-Physical System," in 2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP), 8-10 Aug. 2024 2024, pp. 1-6, doi: 10.1109/ICECSP61809.2024.10698609.

[81] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani, and X. Wei, "Blockchain Meets Federated Learning in Healthcare: A Systematic Review With Challenges and Opportunities," IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14418-14437, 2023, doi: 10.1109/JIOT.2023.3263598.

[82] X. Yang and C. Xing, "Federated Medical Learning Framework Based on Blockchain and Homomorphic Encryption," Wireless Communications and Mobile Computing, vol. 2024, no. 1, p. 8138644, 2024, doi: https://doi.org/10.1155/2024/8138644.

[83] Daniel Commey, Sena Hounsinou, and G. V. Crosby, "Securing Health Data on the Blockchain: A Differential Privacy and Federated Learning Framework," ArXiv, 2024, doi: https://doi.org/10.48550/arXiv.2405.11580.

[84] V. Stephanie, I. Khalil, M. Atiquzzaman, and X. Yi, "Trustworthy Privacy-Preserving Hierarchical Ensemble and Federated Learning in Healthcare 4.0 With Blockchain," IEEE Transactions on Industrial Informatics, vol. 19, no. 7, pp. 7936-7945, 2023, doi: 10.1109/TII.2022.3214998.

[85] V. Stephanie, I. Khalil, and M. Atiquzzaman, "Weight-Based Privacy-Preserving Asynchronous SplitFed for Multimedia Healthcare Data," ACM Trans. Multimedia Comput. Commun. Appl., vol. 20, no. 12, p. Article 377, 2024, doi: 10.1145/3695876.

[86] V. Ramesh, H. S, S. G. Sundaram, P. N. B, and H. G. R, "A Federated Learning-Based Light-Weight Privacy-Preserving Framework for Smart Healthcare Systems," in Handbook of Research on Design, Deployment, Automation, and Testing Strategies for 6G Mobile Core Network, D. Satishkumar, G. Prabhakar, and R. Anand Eds. Hershey, PA, USA: IGI Global, 2022, pp. 382-411.

[87] Moirangthem Biken Singh and A. Pratap, "BPFISH: Blockchain and Privacy-preserving FL Inspired Smart Healthcare," ArXiv, 2022, doi: https://doi.org/10.48550/arXiv.2207.11654.

[88] Kehinde Josephine Olowe, Ngozi Linda Edoh, Stephane Jean Christophe Zouo, and J. Olamijuwon, "Comprehensive review of advanced data analytics techniques for enhancing clinical research outcomes," International Journal of Scholarly Research in Biology and Pharmacy, vol. 5, no. 1, pp. 008–017, 2024, doi: https://doi.org/10.56781/ijsrbp.2024.5.1.0229.

[89] Guodong Long, Tao Shen, Yue Tan, Leah Gerrard, Allison Clarke, and J. Jiang, "Federated Learning for Privacy-Preserving Open Innovation Future on Digital Health," ArXiv, 2021, doi: https://doi.org/10.48550/arXiv.2108.10761.

[90] W. Alamgir and A. Mohyuddin, "Healthcare Analytics: Applications and Challenges," Life Science, vol. 3, no. 3, p. 2, 2022, doi: 10.37185/lns.1.1.263.

[91] K. Narmadha and P. Varalakshmi, "Federated Learning in Healthcare: A Privacy Preserving Approach," (in eng), Stud Health Technol Inform, vol. 294, pp. 194-198, May 25 2022, doi: 10.3233/shti220436.

[92] D. Womack, R. Kennedy, and B. Bria, "Current Practices in Clinical Analytics: A Hospital Survey Report," 2012. [Online]. Available: http://knowledge.amia.org/amia-55142-cni2012a-1.641359/t-004-1.643470/f-001-1.643471/a-113-1.643478/a-114-1.643475.

[93] E. Erniaty and H. Harun, "Understanding the impacts of NPM and proposed solutions to the healthcare system reforms in Indonesia: the case of BPJS," Health Policy and Planning, vol. 35, no. 3, pp. 346-353, 2020, doi: 10.1093/heapol/czz165.

[94] S. K. Nasution, Y. Mahendradhata, and L. Trisnantoro, "Can a National Health Insurance Policy Increase Equity in the Utilization of Skilled Birth Attendants in Indonesia? A Secondary Analysis of the 2012 to 2016 National Socio-

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

Economic Survey of Indonesia," Asia Pacific Journal of Public Health, vol. 32, no. 1, pp. 19-26, 2020, doi: 10.1177/1010539519892394.

[95] N. P. Sambodo, E. Van Doorslaer, M. Pradhan, and R. Sparrow, "Does geographic spending variation exacerbate healthcare benefit inequality? A benefit incidence analysis for Indonesia," Health Policy and Planning, vol. 36, no. 7, pp. 1129-1139, 2021, doi: 10.1093/heapol/czab015.

[96] M. M. Islam and D. P. Z. Msekelwa, "The Role of Blockchain in Secure and Scalable Distributed Learning Systems," Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023, vol. 6, no. 1, pp. 492-502, 12/08 2024, doi: 10.60087/jaigs.v6i1.274.

[97] H. Huang, L. Duan, C. Li, and W. Ni, "A Secure and Lightweight Aggregation Method for Blockchain-based Distributed Federated Learning," in 2024 IEEE International Conference on Web Services (ICWS), 7-13 July 2024 2024, pp. 447-456, doi: 10.1109/ICWS62655.2024.00066.

[98] Q. Li et al., "LFL-COBC: Lightweight Federated Learning on Blockchain-Based Device Contribution Allocation," Electronics, vol. 13, no. 22, p. 4395, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/22/4395.

AUTHOR BIOGRAPHY

Viddi Mardiansyah (M' 2012, SM' 2024, IEEE) received the B.Sc. degree in Mathematics and Natural Science, majoring in Computer Science from Universitas Padjajaran, Bandung, in 1998, and received the M. Eng. degree in Computer Science/Informatics, majoring in Software Engineering from Institut Teknologi Bandung, Indonesia, in 2007. He finished and received the Dr. Eng. in Electrical Engineering, majoring in Computer Engineering from the Universitas Indonesia in July 2023. Since 2015, he has been a permanent Computer Science/Informatics lecturer for undergraduate students at the Engineering Faculty, Universitas Widyatama, Bandung, Indonesia. He is an IEEE senior member. His research interests include blockchains, software engineering, programming languages, networking, and the Internet of Things (IoT).

Luhur Bayuaji (Member, IEEE, since 2014) received the Ph.D. degree in Remote Sensing and Earth Observation from Chiba University, Japan, in 2010, where he also obtained the M.Eng. degree in Multimedia over Computer Networks in 2006. He holds a B.Eng. degree in Computer Engineering from Universitas Indonesia, Indonesia, awarded in 2001. From 2013 to 2023, he served as an Assistant Professor at the Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), Malaysia. Since 2024, he has been serving as an Associate Professor at the Faculty of Data Science and Information Technology, INTI International University, Malaysia. His research interests include remote sensing, satellite image processing, Geographic Information Systems (GIS), computer networks, and cybersecurity.

Iwa Ovyawan Herlistiono holds a Master's degree in Engineering (M.T) from Institut Teknologi Bandung and a Bachelor's degree in Engineering (S.T). His master thesis subject was formal method for optimization.

He held teaching and research positions at the Informatics department, the Faculty of Engineering of Widyatama University, Bandung, Indonesia since 2016.

His research interests include image processing, artificial intelligence, machine learning and computer vision. Through his diverse research endeavors, He continues to make significant contributions to the fields of informatics and technology-enhanced learning.

Sriyani Violina holds a Master's degree in Engineering (M.T) from Institut Teknologi Bandung and a Bachelor's degree in Engineering (S.T), her master thesis topic was genetic algorithm for optimization.

She held teaching and research positions at the Informatics department, the Faculty of Engineering of Widyatama University, Bandung Indonesia since 2003.

Her research interests include image processing, artificial intelligence, machine learning and computer vision. She has contributed to various research studies and scientific publications, particularly focusing on algorithms and optimization.

Adi Purnama received a Bachelor's degree in Informatics with a specialization in Interfacing Systems from Widyatama University in 2014. He then earned his Master's degree in Informatics with a specialization in Media Technology and Mobile Devices from Bandung Institute of Technology in 2018.

Since 2022, he has been a permanent lecturer in the Informatics undergraduate program at the Faculty of Engineering, Universitas Widyatama, Bandung, Indonesia. He is also currently the head of the Interfacing Systems Laboratory. His research interests include the Internet of Things (IoT), Wireless Sensor Networks (WSN), Image Processing, and Software Engineering.

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63

Bagus Alit Prasetyo received a B.Sc. degree in Interfacing systems, majoring in informatics engineering from Universitas Widyatama, Bandung, in 2017, and received a master of science degree in control and system, majoring in electrical engineering from National Chin-Yi University of Technology, Taiwan, in 2021. He is an Electrical Engineering lecturer for undergraduate students at the Faculty of Engineering, Universitas Widyatama, Bandung, Indonesia. His research interests include embedded engineering, edge computing, mobile programming, smart control, artificial intelligence, and the Internet of Things (IoT).

Phuoc-Hai Huynh, Ph.D is a lecturer at the Software Engineering Department of An Giang University, Vietnam, since 2008. His teaching portfolio includes courses such as Data Mining, Machine Learning, Web Programming (PHP-MySQL), Python Programming, Project Management Software, Software Testing and Quality Assurance, Professional Skills in IT, and Artificial Intelligence. His research interests focus on data mining using support vector machines, ensemble methods, and deep learning; mining complex data such as very-high-dimensional and small sample datasets, large-scale data, and gene expression data; as well as applications of machine learning in Bioinformatics and Medical Informatics. He also has a strong interest in Information Systems. In addition to his academic role, he served as a Technical Manager at Leopard Solutions JSC from 2015 to 2016 and has been an Information Technology Advisory Expert at VNSP SOFTWARE JSC since 2016.

Corresponding author: Viddi Mardiansyah, viddi.mardiansyah@widyatama.ac.id, Informatics Department, Engineering Faculty, Widyatama University, Jl. Cikutra No. 204A, 40125, Bandung, Indonesia.
DOI: https://doi.org/10.35882/ijeeemi.v7i2.63