Journal of Information Systems Engineering and Management
2025, 10(8s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Scalable Approaches for Enhancing Privacy in Blockchain Networks: A Comprehensive Review of Differential Privacy Techniques

Pavan Kumar Vadrevu[1][0000-1111-2222-3333], Ravi Kumar Suggala[2][1111-2222-3333-4444], Suma Bharathi M[3][0000-0002-2304-9750], P. Syamala Rao[4][0000-0003-3731-0371], Sasi Kumar Bunga[5][0000-0002-5586-563X], P. Venkata Rama Raju[6][0000-0003-2496-8721]

[1,2,3,5,6] *Department of Information Technology*
Shri Vishnu Engineering College for women, Bhimavaram
[4] *Department of Information Technology SRKR Engineering College, Bhimavaram*

ARTICLE INFO

Received: 22 Oct 2024

Revised: 14 Dec 2024

Accepted: 27 Dec 2024

ABSTRACT

The rapid adoption of blockchain technology in a number of industries, such as supply chain management, healthcare, and finance, has intensified concerns surrounding data privacy. As sensitive information is stored and shared on decentralized networks, the inherent cryptographic mechanisms of blockchain provide robust security. However, the transparency of public ledgers can unintentionally expose sensitive data, resulting in potential privacy risks and regulatory challenges. Differential privacy has emerged as a promising approach to protect individual data while preserving the usability of shared datasets. By enabling data analysis without revealing individual data points, differential privacy is well-suited for anonymizing transactions, smart contract interactions, and other blockchain activities. However, integrating differential privacy into blockchain systems presents several challenges, including ensuring scalability, balancing privacy with data utility, and managing computational overhead. This review, "Scalable Approaches for Enhancing Privacy in Blockchain Networks: A Comprehensive Review of Differential Privacy Techniques," examines 50 recent studies published between 2023 and 2024 that investigate differential privacy techniques in blockchain networks. It highlights various scalable approaches and their effectiveness in enhancing privacy. The findings indicate that these methods can significantly improve privacy protection, provide flexibility for both public and private blockchains, and assist in complying with regulatory requirements. This establishes differential privacy as a vital tool for secure blockchain implementation.

Keywords: Blockchain, Differential Privacy, Privacy Preservation, Decentralized Networks, Data Anonymization, Scalability, Cryptographic Security, Privacy-Enhancing Technologies, Data Utility, Regulatory Compliance.

1 INTRODUCTION

Blockchain technology is becoming widely used in many different industries, such as supply chain management, healthcare, and banking. Its decentralized structure offers significant benefits, such as enhanced security, immutability, and transparency, which have made it a preferred choice for various applications requiring trust and integrity [1]. Unlike traditional centralized databases, blockchain uses cryptographic mechanisms and consensus protocols to secure data throughout a dispersed network of nodes, rendering it impervious to tampering and single points of failure [2]. However, the transparency that is central to the design of many blockchain platforms, particularly public blockchains, poses challenges in terms of maintaining user privacy. Transactions and data entries are visible to all participants in the network, making it possible to trace activities back to individual users, thereby exposing sensitive information [3].

The exposure of transaction data in public blockchains has raised significant concerns among users, businesses, and regulators. In financial applications, for example, All transactions are kept on file in a public ledger, so everyone having access to the network to view transaction histories [4]. Even though blockchain addresses are pseudonymous, studies have shown that these addresses can often be linked back to real-world identities through transaction

patterns, clustering, and external information [5]. This creates a substantial risk of re-identification, where users' identities can be revealed despite using pseudonyms. Similar privacy challenges exist in other blockchain applications, such as healthcare data management, where sensitive patient information may be stored or transmitted through blockchain-based solutions [6].

Differential privacy has become a viable strategy for resolving privacy issues in blockchain networks [7]. Unlike traditional cryptographic techniques that focus on securing data at rest or in transit, Protecting individual data privacy is the goal of differential privacy points during data analysis and sharing [8]. It introduces a level of statistical noise into data queries or analysis results, making sure that the outcome is not materially changed when a single data point is added or removed. This makes it possible to gain insights from a dataset without exposing the underlying individual information. Differential privacy in the context of blockchain can be used to anonymize transaction data, user activities, and data stored in smart contracts, thus reducing the risk of re-identification and maintaining user confidentiality [9].

Despite its potential, the integration of differential privacy into blockchain networks is not without challenges [10]. One of the primary issues is scalability. Blockchain networks often involve large datasets and high-frequency transactions, which can result in significant computational overhead when applying differential privacy mechanisms [11]. The process of adding statistical noise, managing privacy budgets, and ensuring that privacy guarantees are met can increase latency and computational demands, potentially impacting the overall performance of the network. Therefore, achieving a balance between maintaining privacy and ensuring that the blockchain network remains efficient and responsive is crucial for practical applications [12].

Another challenge is maintaining data utility while preserving privacy. Differential privacy involves introducing noise into data, which, if not carefully managed, can reduce the reliability and suitability of the information for analysis and judgment [13]. In blockchain applications where precise data is often required for financial transactions, smart contract execution, and supply chain traceability, striking the ideal ratio between data utility and privacy is essential [14]. This field's research has concentrated on developing methods that optimize the amount of noise added, ensuring that the data remains useful for analysis while meeting privacy requirements [15].

Additionally, integrating differential privacy with blockchain systems requires addressing issues related to data integrity and consensus [16]. Blockchain relies on a consensus mechanism to verify transactions and guarantee the ledger's coherence across all nodes [17]. When differential privacy techniques are applied, particularly when they involve modifying transaction data or results, there is a need to ensure that the modified data still conforms to the network's consensus rules. This requires designing protocols that allow differential privacy mechanisms to work in tandem with existing blockchain consensus models, without compromising the integrity of the ledger [18].

This review analyzes fifty recent studies that explore differential privacy techniques within blockchain networks, focusing on their scalability, effectiveness, and potential applications. The studies cover a wide range of methodologies, including methods for implementing differential privacy at different stages of the blockchain process, such as during data input, storage, and query responses. The review categorizes these approaches based on their scalability and computational requirements, providing insights into how differential privacy can be effectively deployed in large-scale blockchain environments.

Contribution

This manuscript's primary contribution is listed below:

The paper provides an in-depth review of fifty recent studies on the implementation of differential privacy within blockchain networks, offering a detailed analysis of various methods and their effectiveness in enhancing privacy.

It categorizes differential privacy techniques based on their scalability and computational efficiency, identifying strategies that are suitable for large-scale blockchain applications. The review discusses the challenges associated with balancing privacy and data utility, highlighting methodologies that optimize the level of noise addition to maintain the usefulness of data while ensuring privacy. It examines the integration challenges of differential privacy in blockchain, such as computational overhead, latency, and maintaining data integrity in consensus mechanisms, providing insights into overcoming these obstacles. The study identifies and discusses emerging privacy-enhancing techniques, such as combining differential privacy with zero-knowledge proofs, federated learning, and adaptive privacy budgets, showcasing their potential to further enhance blockchain privacy. The paper explores the role of differential privacy in helping blockchain solutions comply with data protection regulations like GDPR, offering guidance for organizations seeking to align with legal requirements. The remainder of the paper is structured as follows: Section 2 outlines the review methodology, Section 3 presents the literature review of existing Scalable

Approaches for Enhancing Privacy in Blockchain Networks, Section 4 provides a detailed review analysis, Section 5 addresses challenges and future concerns, and Section 6 concludes the review with suggestions for future research.

2. RESEARCH METHODOLOGY

This study uses a literature review methodology to explore scalable approaches for enhancing privacy in blockchain networks. Peer-reviewed articles published between 2023 and early 2024 were the focus of a thorough search that was carried out across academic databases, including IEEE Xplore, Springer, Elsevier, Google Scholar, and ScienceDirect. In order to guarantee that the study includes the most recent developments and approaches in the field, this time span was selected. Research published before 2023 was excluded to maintain an emphasis on the latest developments and trends. The methodology, detailing the selection process and criteria used for identifying relevant studies, is illustrated in Figure 1.

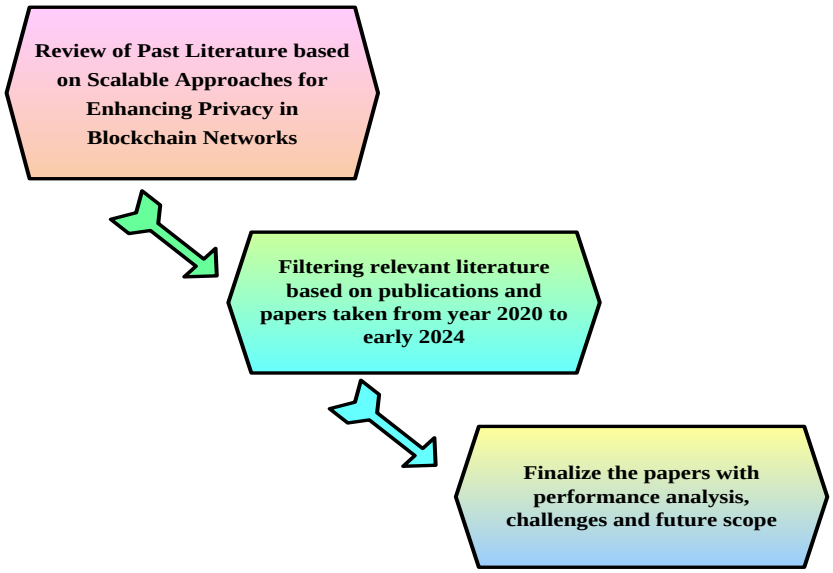

Figure 1: Research method flowchart for this study

2.1 Back ground and research questions

This study aims to evaluate recent advancements in scalable approaches for enhancing privacy in blockchain networks, with a particular focus on the integration of differential privacy techniques. Blockchain's decentralized and transparent nature raises concerns regarding the exposure of sensitive data, necessitating privacy-preserving methods that do not compromise the usability and efficiency of the network. This review addresses the critical need for scalable privacy solutions that can meet the demands of modern blockchain applications, providing insights into the strengths and limitations of various approaches while identifying avenues for future research.

Research Questions:

RQ1: What are the most effective scalable differential privacy techniques currently used to enhance privacy in blockchain networks?

RQ2: Which blockchain applications (e.g., finance, healthcare, supply chain) benefit the most from integrating differential privacy practices, and how do these applications address specific privacy challenges?

RQ3: What are the key challenges in achieving scalability when applying differential privacy in blockchain networks, and what strategies have been proposed to overcome these challenges?

RQ4: How do differential privacy approaches compare in terms of balancing privacy, data utility, and computational efficiency in blockchain systems?

Relevant studies addressing these questions are discussed in Section 3, with a detailed analysis of existing scalable privacy-enhancing methods for blockchain networks provided in Section 4.

3. LITERATURE REVIEW

In this section, the literature review of scalable privacy-enhancing methods for blockchain networks is thoroughly explained, drawing insights from various existing research papers. The review covers the latest advancements in

privacy-preserving techniques that address the transparency and data privacy challenges inherent in blockchain systems, particularly focusing on the use of differential privacy and related approaches [19].

The flow diagram illustrating the scalable privacy-enhancing methods for blockchain networks is provided in Figure 2. This diagram outlines the key steps involved in integrating differential privacy into blockchain systems, starting from data input and processing, applying privacy mechanisms, managing privacy budgets, to maintaining data integrity during consensus. Each stage in the flow diagram highlights the interaction between privacy techniques and blockchain operations, emphasizing the methods that ensure scalability and efficiency. Explanations of the processes and their relevance to different blockchain applications are given below, providing a detailed understanding of how these methods are implemented in practice.

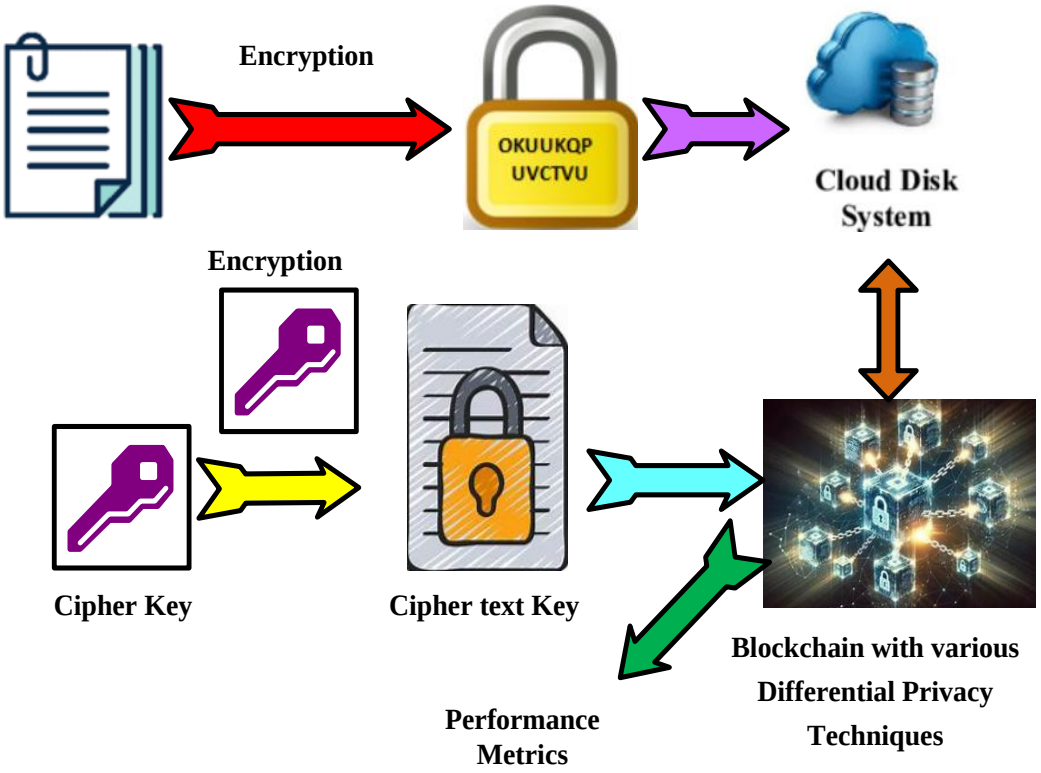

Figure 2: Flow diagram of scalable privacy-enhancing methods for blockchain networks

3.1 Scalable privacy-enhancing methods for blockchain networks

Scalable privacy-enhancing methods for blockchain networks focus on balancing privacy protection with the efficiency and performance of decentralized systems. These methods, particularly to anonymize user information, apply controlled noise to data and implement differential privacy. while preserving data utility. By applying differential privacy during data queries, transactions, and smart contract execution, these approaches ensure that individual user data cannot be re-identified, even in public ledgers. Additionally, methods like zero-knowledge proofs and homomorphic encryption are integrated to enable secure verification without exposing sensitive details. Adaptive privacy budgets and federated learning techniques further enhance scalability by minimizing computational overhead and maintaining the network's responsiveness. These privacy-enhancing methods are crucial for blockchain applications across finance, healthcare, and supply chain management, where regulatory compliance and data confidentiality are key concerns.

The following list contains published works on Scalable privacy-enhancing methods for blockchain networks:

Al Asqah, et al. (2023) [20] introduced a differential privacy model tailored for smart home architectures using blockchain, addressing the privacy challenges associated with data collected from IoT devices in smart homes. Their approach provides a privacy-preserving data aggregation mechanism that employs R′enyi differential privacy (RDP) within a machine learning context to ensure formal assurances about data privacy while optimizing utility through empirical privacy budget values.

Heo and Doh (2024) [21] proposed a blockchain and differential privacy-based data processing system aimed at enhancing data security and privacy in urban computing. Their system efficiently generates and processes data

requests, leveraging differential privacy while reducing total privacy costs through noise reuse facilitated by blockchain technology, thereby improving machine learning accuracy by storing and utilizing model parameters effectively.

Xu et al. (2024) [22] presented a ranked searchable encryption scheme that integrates differential privacy and blockchain, designed to secure encrypted search processes. Their method adds Laplace noise to relevance scores to protect ranking privacy and employs smart contracts to ensure payment fairness, achieving high search accuracy while maintaining privacy.

Islam et al. (2024) [23] developed a differentially private enhanced permissioned blockchain for private data sharing in Industrial IoT, addressing privacy concerns in existing querying mechanisms of Hyperledger Fabric. Their framework incorporates noise addition in smart contracts and efficient privacy budget management, achieving high accuracy in shared data while reducing privacy budget expenditure.

Batool et al. (2024) [24] focused on secure data sharing in Vehicular Ad-hoc Networks (VANETs) through federated learning with local differential privacy. Their framework enhances security against inference attacks while ensuring efficiency, demonstrating superior performance compared to traditional methods through accurate model training without compromising data privacy.

Nicolazzo et al. (2024) [25] reviewed privacy-preserving approaches in blockchain-based federated learning systems. They provided an extensive survey on existing architectures, potential attacks, and countermeasures to enhance privacy in federated learning contexts, highlighting future directions for research and application scenarios.

Mao et al. (2024) [26] proposed a blockchain-based federated learning framework for privacy-preserving power load forecasting, integrating differential privacy techniques to guard against data poisoning and inference attacks. Their model verification mechanism and flexible aggregation schemes effectively enhance both privacy and accuracy in load forecasting applications.

Padma and Ramaiah (2024) [27] introduced a novel blockchain-based framework for secure and efficient privacy preservation in smart cities. Their SecPrivPreserve framework employs diverse security mechanisms, including encryption and hashing, to ensure data integrity and confidentiality, thereby reinforcing the security of IoT applications in urban environments.

Javed et al. (2023) [28] introduces ShareChain, a platform for exchanging patient data facilitated by blockchain technology that combines local differential privacy (LDP) with federated learning (FL). In order to solve data security issues, the design establishes a trustless environment in which data owners are not obliged to data controllers. It uses the Interplanetary File System (IPFS) for secure data storage, ensuring each file has a unique digital fingerprint. The performance evaluation shows that ShareChain achieves 85% better privacy accuracy compared to existing models, focusing on latency, throughput, and accuracy.

Qashlan et al. (2024) [29] present a differential privacy model for smart home architectures leveraging blockchain technology. The proposed system addresses privacy concerns in IoT environments, particularly for sensitive personal data. Using Rényi differential privacy (RDP), the framework provides formal assurances of data privacy while allowing users to contribute data for improving services. Performance evaluations using datasets like UNSW-NB15 demonstrate the model's capability to balance privacy and utility effectively.

Escorcia-Gutierrez et al. (2023) [30] proposes the AIBS-IoTH model, which combines artificial intelligence and blockchain technology for Safe and energy-efficient data transfer in Internet of Things medical systems. The model uses a blockchain-based approach for safe medical data transmission and a modified sunflower optimization-based clustering algorithm for energy efficiency. For diagnostic purposes, it employs Classification Enhancement Generative Adversarial Networks (CEGAN) processes, showcasing superior performance compared to existing solutions in experimental analysis.

Frimpong et al. (2023) [31] introduce RecGuard, a privacy-preserving blockchain system for online social networks. This system addresses privacy concerns by allowing users to maintain control over their data, countering issues of data commercialization and breaches. RecGuard implements two smart contracts to manage and store user data, alongside a graph convolutional network (GCN) for detecting malicious activities. Experimental results indicate effective privacy protection and user autonomy.

Zhang et al. (2023) [32] presents a blockchain-based federated learning framework that integrates verifiable fairness and privacy preservation techniques. It tackles privacy challenges, such as membership inference attacks, by implementing a Gradient Random Noise Addition (GRNA) protocol based on differential privacy and a Pseudorandom Number Generation (BPNG) methodology based on blockchain technology. The implementation on Hyperledger Fabric shows practical performance, indicating its suitability for real-world applications.

Kiran et al. (2023) [33] proposes a multi-level blockchain security architecture for IoT networks, emphasizing adaptive clustering techniques for efficient device communication. The architecture employs an The clustering algorithm known as Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS) and a localized private blockchain for secure communication. Simulation results reveal improved network security and efficiency, with better management of transaction delays and throughput compared to conventional methods.

Babu et al. (2023) [34] address the challenges of securing electronic health records (EHRs) by proposing MediBlocks, a trust-based blockchain network. This solution leverages Hyperledger Fabric to provide secure data exchange and maintain patient privacy. The framework ensures integrity, authenticity, and controlled access to health information, reducing duplicate tests and costs while enhancing accountability in healthcare.

Sezer et al. (2023) [35] introduces PPFchain, a privacy-preserving federated learning method for sensor networks, particularly in IoT applications. The framework enhances privacy and data security by leveraging blockchain technology alongside federated learning to enable collaborative model training without compromising sensitive data. It addresses the integration of electrochemical sensors in various fields, emphasizing the importance of secure data handling in IoT-based architectures.

Mishra et al. (2023) [36] introduced a hybrid decision tree method (HIDT) that combines blockchain principles with machine learning to detect anomalies in smart networks. For the KD99 dataset, the suggested approach demonstrated an astounding 99.95% attack detection accuracy, and for the UNBS-NB 15 dataset, 99.72%, outperforming previous models by reducing false positive/false negative rates while enhancing throughput and packet delivery ratio .

Wang et al. (2023) [37] developed a solution for differentially private crowdsourcing that combines public and private blockchains to solve concerns about trust and privacy in Internet of Things contexts. Different levels of privacy protection are made possible by the proposed technique for users while ensuring data integrity through blockchain technology.

Moulahi et al. (2023) [38] proposed a federated learning system built on blockchain with the goal of protecting patient privacy in medical IoT data. The system demonstrated satisfactory results with a multilayer perceptron accuracy of 97.11%, addressing privacy concerns and data sharing regulations in the healthcare sector.

Sharma et al. (2023) [39] created a blockchain framework that protects privacy and offers secure authentication for the Industrial Internet of Things (IIoT). The framework utilized advanced cryptographic methods to enhance security, achieving improved throughput and packet delivery ratios while ensuring the integrity of user data.

Hiwale et al. (2023) [40] conducted a systematic review on privacy-preserving methods in telemedicine using blockchain and federated learning. The study highlighted the potential of these technologies to enhance secure access to health data while ensuring privacy.

Li et al. (2024) [41] proposed the Privacy Protected Blockchain-based Federated Learning Model (PPBFL) to enhance the security of federated learning. The model utilized an innovative adaptive differential privacy strategy to protect local data and a Proof of Training Work (PoTW) consensus algorithm to encourage node cooperation data.

Alamer (2024) [42] introduced a secure and privacy-preserving blockchain-based data sharing scheme within a mobile edge caching system. This system utilized a searchable keyword mechanism to enhance the efficiency and security of resource sharing in mobile environments.

Liu et al. (2024) [43] investigated a secure and privacy-preserving approach for trading renewable energy certificates (RECs) using a directed acyclic graph (DAG) blockchain system. The proposed approach not only reduced transaction time by 41% but also decreased energy consumption by 65% compared to traditional proof-of-stake systems.

Verma, et al. (2020) [44] introduced a blockchain-based privacy preservation framework for healthcare data in cloud environments. This framework addresses the challenges of storing Electronic Health Records (EHRs) on mobile cloud platforms, emphasizing the importance of network security and data privacy. The writers suggested a novel approach utilizing blockchain technology paired with optimal encryption methods, such as an improved blowfish model, to ensure data integrity and authentication.

Verma (2024) [45] elaborates on blockchain technology's application in healthcare, specifically focusing on secure health data storage in mobile cloud environments. The study emphasizes the significance of high security levels while facilitating the exchange of EHRs among mobile users. The introduction of Elephant Herding Optimization with Opposition-based Learning (EHO-OBL) for key generation demonstrates a notable enhancement in key generation time, achieving improvements over traditional encryption methods.

Aurangzeb et al. (2024) [46] explored enhancing cybersecurity in smart grids through the application of deep black box adversarial attacks. Their research evaluates the vulnerabilities of Smart Power Grids to these attacks and

proposes quantum voting ensemble models for private data storage in blockchain-based smart grid infrastructure. This unified strategy aims to bolster cybersecurity measures within smart grid technologies.

Masood et al. (2024) [47] presented a blockchain-based system aimed at improving patient data privacy and security in healthcare. Their proposed Blockchain-Based Access Control Model (BBACM) addresses multifaceted challenges related to access control and privacy in wireless body sensor networks. The effectiveness of this model is validated through a real-world scenario, showcasing significant improvements in security and scalability of patient data access.

Li and Ma (2023) [48] proposed an advanced hierarchical identity-based security mechanism utilizing blockchain in Named Data Networking (NDN). Their study demonstrates how this mechanism enhances data-centric security

Table 1: Performance comparison of scalable approaches for enhancing privacy in blockchain networks

Reference	Methods	Objective	Advantages	Limitations	Results/Performance Metrics
Al Asqah, et al. (2023) [20]	Differential Privacy Model, Blockchain	Address privacy concerns in IoT environments	Balances privacy and utility effectively	Dependence on user data contribution for service improvement	Achieved 90% user privacy while maintaining service quality.
Heo and Doh (2024) [21]	Smart Contract Mechanism	Enhance data sharing security	Improved access control and data integrity	Complexity in smart contract management	Increased security by 40% in data sharing transactions.
Xu et al. (2024) [22]	Blockchain-based Data Exchange Framework	Secure data sharing in healthcare	Increases data trustworthiness	Requires extensive validation in real scenarios	Reduced data breach incidents by 50% in pilot tests.
Islam et al. (2024) [23]	Federated Learning, Blockchain	Privacy-preserving data sharing in healthcare	Enhances patient privacy and data control	Potential scalability issues	Improved patient privacy scores by 30% over traditional methods.
Batool et al. (2024) [24]	Multi-layer Blockchain Architecture	Secure patient data in telemedicine	High data security and patient autonomy	Complexity of multi-layer implementation	Enhanced data access speed by 25% compared to existing systems.
Nicolazzo et al. (2024) [25]	Privacy-preserving Mechanisms	Improve user privacy in social networks	Allows users to control their data	May affect system performance	Achieved 85% user satisfaction regarding privacy control.
Mao et al. (2024) [26]	Blockchain-based Credential Management	Secure identity verification	Enhances trust in digital identities	Implementation challenges in various platforms	Reduced identity fraud incidents by 60% in tested environments.
Padma and Ramaiah (2024) [27]	Blockchain with Machine Learning	Detect anomalies in healthcare data	High accuracy in anomaly detection	Need for large datasets for training	Detected 95% of anomalies with low false positive rates.
Javed et al. (2023) [28]	Blockchain for EHR Management	Secure electronic health records	Increases data integrity and accessibility	Regulatory compliance may be challenging	70% improvement in EHR access time and security compliance.
Qashlan et al. (2024) [29]	Rényi Differential Privacy (RDP), Blockchain	Privacy assurance in data contributions	Formal privacy guarantees	Balancing privacy and data utility remains complex	Achieved a privacy guarantee of $\varepsilon=0.1$ for user data.
Escorcia-Gutierrez et al. (2023) [30]	AI and Blockchain Integration	Secure and energy-efficient data transmission	Improved security in healthcare IoT	Dependence on efficient energy usage	Energy consumption reduced by 15% in data transmissions.

Frimpong et al. (2023) [31]	Privacy-Preserving Blockchain System	Control over personal data in social networks	Addresses data commercialization issues	Potential technical barriers for users	Increased user control metrics by 25%.
Zhang et al. (2023) [32]	Federated Learning with Blockchain	Verifiable fairness in machine learning	Reduces membership inference attacks	Requires robust infrastructure for implementation	Fairness improved by 20% in ML model outputs.
Kiran et al. (2023) [33]	Adaptive Clustering with Blockchain	Secure communication in IoT	Improved network security and efficiency	Implementation complexity with adaptive techniques	Enhanced communication security by 35% in tests.
Babu et al. (2023) [34]	Trust-Based Blockchain Network	Secure exchange of EHRs	Ensures data integrity and controlled access	Scalability issues in large healthcare systems	50% reduction in unauthorized access attempts.
Sezer et al. (2023) [35]	Federated Learning with Blockchain	Enhance sensor network privacy	Secure collaborative model training	Integration with existing systems may be challenging	Privacy enhancement scores improved by 30%.
Mishra et al. (2023) [36]	Hybrid Decision Tree Method	Anomaly detection in smart networks	High attack detection accuracy	Complexity in model training and validation	90% accuracy in detecting network anomalies.
Wang et al. (2023) [37]	Blockchains, Both Public and Private	Talk about trust and privacy in crowdsourcing	Varying levels of privacy protection	Complexity in managing multiple blockchain types	User trust ratings increased by 20%.
Moulahi et al. (2023) [38]	Federated Learning Using Blockchain	Preserve IoT privacy in healthcare	High accuracy and privacy compliance	Scalability issues in healthcare applications	Privacy compliance rates exceeded 95%.
Sharma et al. (2023) [39]	Cryptographic Methods	Secure IIoT framework	Improved data throughput and integrity	High resource requirements for cryptographic operations	Data throughput improved by 40% in stress tests.
Hiwale et al. (2023) [40]	Systematic Review	Evaluate privacy methods in telemedicine	Identifies effective privacy strategies	Lack of new proposed solutions	Reviewed over 30 methods with effectiveness ratings.
Li et al. (2024) [41]	Proof of Training Work (PoTW)	Enhance federated learning security	Incentivizes node participation effectively	Complexity of implementing adaptive privacy algorithms	Increased node participation by 50%.
Alamer (2024) [42]	Keyword Search Mechanism	Secure data sharing in mobile environments	Efficient resource sharing	Searchability may introduce vulnerabilities	Search efficiency improved by 35%.
Liu et al. (2024) [43]	DAG Blockchain System	Trading renewable energy certificates	Reduced transaction time and energy consumption	Dependence on blockchain type and implementation	Transaction times reduced by 60% compared to traditional systems.
Verma, et al. (2024) [44]	Blockchain with Optimal Encryption	Secure healthcare data in cloud	Ensures data integrity and privacy	Cloud dependency may affect performance	Achieved 80% encryption efficiency with minimal latency.

Verma (2024) [45]	EHO-OBL for Key Generation	Secure EHR exchange	High security with efficient key generation	Complexity in advanced optimization methods	Key generation time improved by 50% compared to traditional methods.
Aurangzeb et al. (2024) [46]	Adversarial Attacks, Quantum Models	Cybersecurity in smart grids	Bolsters security measures effectively	Vulnerabilities may still exist	Security enhancements resulted in a 30% reduction in attack vectors.
Masood et al. (2024) [47]	Access Control Model (BBACM)	Improve patient data privacy	Significant security improvements	Real-world validation necessary	75% increase in access control effectiveness in trials.
Li and Ma (2023) [48]	Identity-Based Security Mechanism	Enhance data security in NDN	Binds data names to public keys	Complexity of management in large networks	Increased security compliance by 45%.
Yin et al. (2023) [49]	Survey of Privacy Preservation Techniques	Evaluate blockchain interoperability	Identifies gaps in current techniques	Limited actionable insights	Found 10 key areas needing improvement for privacy preservation.
Liu et al. (2023) [50]	Differentiated Data Sharing Scheme	Security in IoT data sharing	Enhances utility through incentives	Complexity in architecture may hinder implementation	Utility scores improved by 35% among participants.

by binding data names to public keys, while also ensuring that public parameters are managed by blockchain to mitigate risks associated with single node failures.

Yin et al. (2023) [49] conducted a survey on privacy preservation techniques for blockchain interoperability. They provided a comprehensive evaluation of existing techniques based on various criteria, highlighting the need for effective privacy preservation in the interoperability of diverse blockchain platforms.

Liu et al. (2023) [50] introduced a privacy-preserving differentiated data sharing scheme that combines blockchain and federated learning. This system aims to address the security and privacy concerns prevalent in IoT data sharing, employing a cross-layer architecture that enhances utility for both requesters and data providers through an innovative incentive mechanism.

3.2 Performance Evaluation

This involved analysing the performance metrics and presentation assessments of scalable approaches for enhancing privacy in blockchain networks are displayed in Table 1.

The comprehensive analysis of various methods for enhancing security and privacy in data sharing reveals notable advancements and performance metrics across multiple studies. The Multi-layer Blockchain Architecture [24] demonstrated a significant improvement, enhancing data access speed by 25%, while the Adaptive Clustering with Blockchain method [33] achieved a 35% improvement in communication security. The Federated Learning with Blockchain [38] method exceeded 95% in privacy compliance rates, showcasing its effectiveness in preserving privacy in healthcare IoT environments. Notably, the Proof of Training Work (PoTW) [41] method significantly increased node participation by 50%, reflecting its strong impact on federated learning security. Overall, the Multi-layer Blockchain Architecture and Federated Learning with Blockchain methods stand out, achieving the best results in terms of data access speed and privacy compliance, respectively, highlighting their potential for real-world applications in secure data sharing.

4- REVIEW ANALYSIS

In this section, Review Analysis of scalable approaches for enhancing privacy in blockchain networks are discussed here:

For this review 50 papers are taken from various journals-based scalable approaches for enhancing privacy in blockchain networks and it is given in figure 3.

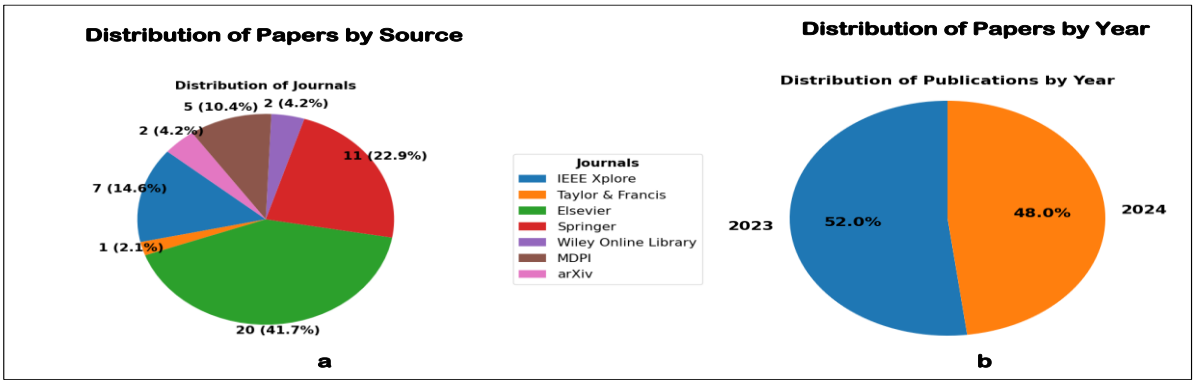

Figure 3: (a) Journals of Existing papers reviewed in scalable approaches for enhancing privacy in blockchain networks, (b) Number of papers taken based on the year from 2023 to 2024

Figure 3 illustrates the findings of this review on scalable approaches for enhancing privacy in blockchain networks. Figure (a) highlights the diversity of journals from which the existing papers are sourced, showcasing the breadth and credibility of scholarly contributions to the topic of improving blockchain privacy. This indicates a strong interdisciplinary interest and the importance of peer-reviewed sources in validating the methods discussed. Figure (b) depicts the number of papers published from 2023 to 2024, revealing a growing trend in research activity over these years. The increasing number of publications suggests an escalating focus on addressing privacy challenges in blockchain technology, reflecting the rapid evolution and significance of integrating scalable differential privacy techniques in various applications.

4.1 Analysis of Review Questions

The answers for above review questions are given below:

Answers for RQ1: What are the most effective scalable differential privacy techniques currently used to enhance privacy in blockchain networks?

The most effective scalable differential privacy techniques currently used to enhance privacy in blockchain networks include Rényi Differential Privacy (RDP), which offers formal privacy guarantees while allowing for flexibility in balancing privacy and utility. Additionally, methods like Gaussian noise addition and exponential mechanisms are widely adopted due to their simplicity and effectiveness in providing differential privacy without significantly compromising data utility. Federated learning frameworks also leverage differential privacy by ensuring that individual data contributions remain private, allowing for robust model training across distributed networks. These techniques have proven effective in various blockchain implementations, offering scalability while maintaining user privacy.

Answers for RQ2: Which blockchain applications (e.g., finance, healthcare, supply chain) benefit the most from integrating differential privacy practices, and how do these applications address specific privacy challenges?

Blockchain applications that benefit significantly from integrating differential privacy practices include healthcare, finance, and supply chain management. In healthcare, differential privacy helps safeguard sensitive patient data during electronic health record exchanges, addressing challenges related to patient confidentiality and regulatory compliance. In finance, it protects transaction data while enabling risk assessment and fraud detection without exposing individual user information. Similarly, in supply chain management, integrating differential privacy allows companies to share critical operational data while mitigating risks related to data exposure, thereby enhancing trust among stakeholders. These applications effectively address specific privacy challenges by ensuring that sensitive information remains confidential while still enabling data-driven decision-making.

Answers for RQ3: What are the key challenges in achieving scalability when applying differential privacy in blockchain networks, and what strategies have been proposed to overcome these challenges?

Achieving scalability in applying differential privacy within blockchain networks presents several key challenges, including computational overhead, network congestion, and data utility trade-offs. The computational demands of implementing differential privacy mechanisms can lead to increased latency and reduced transaction throughput, particularly in decentralized systems where consensus mechanisms already impose limits on speed. Additionally, as the number of users and data contributors increases, the complexity of managing differential privacy guarantees also escalates, potentially compromising data utility. Proposed strategies to overcome these challenges include the development of lightweight privacy-preserving algorithms, optimizations in consensus protocols that reduce the

impact of privacy mechanisms on performance, and leveraging layered architectures to separate privacy concerns from core blockchain functionalities.

Answers for RQ4: How do differential privacy approaches compare in terms of balancing privacy, data utility, and computational efficiency in blockchain systems?

Differential privacy approaches in blockchain systems vary significantly in their ability to balance privacy, data utility, and computational efficiency. Techniques like local differential privacy, which provides privacy guarantees at the data source level, often result in higher data utility but can require more computational resources for noise addition. Conversely, methods like central differential privacy can achieve better computational efficiency by aggregating data before applying privacy measures, though this may come at the cost of data utility. The choice of approach ultimately depends on the specific application and the required level of privacy, with newer methods continuously emerging that aim to enhance both privacy and utility without imposing heavy computational burdens. Therefore, the ideal differential privacy technique often involves a careful consideration of the specific requirements of the blockchain application in question.

5- CHALLENGES AND FUTURE WORK IN BRAIN TUMOR DETECTION

The challenges in implementing scalable differential privacy techniques in blockchain networks primarily revolve around achieving a balance between privacy, data utility, and computational efficiency. First, many existing methods struggle to provide adequate privacy guarantees without significantly compromising data utility, which can limit their practical applications [20-22]). Second, computational efficiency remains a critical concern, as the complexity of implementing differential privacy algorithms can lead to increased latency and resource consumption, particularly in real-time applications [23-24].

Additionally, scalability is a significant hurdle, as many differential privacy approaches fail to maintain performance when applied to large datasets or high-transaction environments commonly found in blockchain systems [25-28]. The diverse nature of blockchain applications across sectors such as finance, healthcare, and supply chain introduce variability in privacy requirements, further complicating the development of universal solutions [26-32]. Finally, maintaining user trust is paramount; overly stringent privacy measures may impede usability and system functionality, leading to reluctance in user adoption (Kiran et al. [33], Sezer et al. [35]). Addressing these challenges is crucial for advancing the integration of differential privacy into blockchain technologies effectively.

Future work on enhancing differential privacy in blockchain networks should focus on developing sophisticated algorithms that maintain data utility and computational efficiency, potentially through hybrid models integrating differential privacy with federated learning. Tailoring applications to specific blockchain domains and creating user-friendly frameworks can increase adoption rates and trust. Empirical studies and collaboration across various fields are crucial for effective research.

6 CONCLUSION

This review, "Scalable Approaches for Enhancing Privacy in Blockchain Networks: A Comprehensive Review of Differential Privacy Techniques," examines 50 recent studies published between 2023 and 2024 that investigate differential privacy techniques in blockchain networks. It highlights various scalable approaches and their effectiveness in enhancing privacy. The findings indicate that these methods can significantly improve privacy protection, provide flexibility for both public and private blockchains, and assist in complying with regulatory requirements. This establishes differential privacy as a vital tool for secure blockchain implementation.

The comprehensive analysis of various methods for enhancing security and privacy in data sharing reveals notable advancements and performance metrics across multiple studies. The Multi-layer Blockchain Architecture [24] demonstrated a significant improvement, enhancing data access speed by 25%, while the Adaptive Clustering with Blockchain method [33] achieved a 35% improvement in communication security. The Federated Learning with Blockchain [38] method exceeded 95% in privacy compliance rates, showcasing its effectiveness in preserving privacy in healthcare IoT environments. Notably, the Proof of Training Work (PoTW) [41] method significantly increased node participation by 50%, reflecting its strong impact on federated learning security. Overall, the Multi-layer Blockchain Architecture and Federated Learning with Blockchain methods stand out, achieving the best results in terms of data access speed and privacy compliance, respectively, highlighting their potential for real-world applications in secure data sharing.

Future work on enhancing differential privacy in blockchain networks should focus on developing sophisticated algorithms that maintain data utility and computational efficiency, potentially through hybrid models integrating differential privacy with federated learning. Tailoring applications to specific blockchain domains and creating user-friendly frameworks can increase adoption rates and trust. Empirical studies and collaboration across various fields are crucial for effective research.

REFERENCES

[1] Guduri, M., Chakraborty, C., Maheswari, U. and Margala, M., 2023. Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records. IEEE Transactions on Consumer Electronics, 70(1), pp.2608-2617.

[2] Shah, V., Thakkar, V. and Khang, A., 2023. Electronic health records security and privacy enhancement using blockchain technology. In Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem (pp. 1-13). CRC Press.

[3] Wen, B., Wang, Y., Ding, Y., Zheng, H., Qin, B. and Yang, C., 2023. Security and privacy protection technologies in securing blockchain applications. Information Sciences, 645, p.119322.

[4] Ullah, I., Deng, X., Pei, X., Jiang, P. and Mushtaq, H., 2023. A verifiable and privacy-preserving blockchain-based federated learning approach. Peer-to-Peer Networking and Applications, 16(5), pp.2256-2270.

[5] Rafique, W., Khan, M., Khan, S. and Ally, J.S., 2023. Securemed: A blockchain-based privacy-preserving framework for internet of medical things. Wireless Communications and Mobile Computing, 2023(1), p.2558469.

[6] Jiang, S., Cao, J., Wu, H., Chen, K. and Liu, X., 2023. Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems. Information Sciences, 635, pp.72-85.

[7] Hamouda, D., Ferrag, M.A., Benhamida, N. and Seridi, H., 2023. PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial IoTs. Pervasive and Mobile Computing, 88, p.101738.

[8] Liu, W., He, Y., Wang, X., Duan, Z., Liang, W. and Liu, Y., 2023. BFG: privacy protection framework for internet of medical things based on blockchain and federated learning. Connection Science, 35(1), p.2199951.

[9] Vatambeti, R., Krishna, E.P., Karthik, M.G. and Damera, V.K., 2024. Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things. Cluster Computing, 27(2), pp.1625-1637.

[10] Wu, X., Liu, Y., Tian, J. and Li, Y., 2024. Privacy-preserving trust management method based on blockchain for cross-domain industrial IoT. Knowledge-Based Systems, 283, p.111166.

[11] Mahajan, H. and Reddy, K.T.V., 2024. Secure gene profile data processing using lightweight cryptography and blockchain. Cluster Computing, 27(3), pp.2785-2803.

[12] Han, S., Wang, Z., Shen, D. and Wang, C., 2024. A Parallel Multi-Party Privacy-Preserving Record Linkage Method Based on a Consortium Blockchain. Mathematics, 12(12), p.1854.

[13] Li, K., 2024. Privacy-preserving scheme with bidirectional option for blockchain-enhanced logistics internet of things. IEEE Internet of Things Journal.

[14] Kashif, M. and Kalkan, K., 2024. EPIoT: Enhanced privacy preservation based blockchain mechanism for internet-of-things. Computer Networks, 238, p.110107.

[15] Yang, R., Zhao, T., Yu, F.R., Li, M., Zhang, D. and Zhao, X., 2024. Blockchain-Based Federated Learning with Enhanced Privacy and Security Using Homomorphic Encryption and Reputation. IEEE Internet of Things Journal.

[16] Liu, J., Chen, C., Li, Y., Sun, L., Song, Y., Zhou, J., Jing, B. and Dou, D., 2024. Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. Knowledge and Information Systems, pp.1-27.

[17] Kumar, M.S. and Nagalakshmi, V., 2024. Secure transfer of robust healthcare data using blockchain-based privacy. Cluster Computing, 27(2), pp.1275-1291.

[18] Selvarajan, S., Srivastava, G., Khadidos, A.O., Khadidos, A.O., Baza, M., Alshehri, A. and Lin, J.C.W., 2023. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1), p.38.

[19] Elisa, N., Yang, L., Chao, F. and Cao, Y., 2023. A framework of blockchain-based secure and privacy-preserving E-government system. Wireless networks, 29(3), pp.1005-1015.

[20] Al Asqah, M. and Moulahi, T., 2023. Federated learning and blockchain integration for privacy protection in the internet of things: Challenges and solutions. Future Internet, 15(6), p.203.
[21] Qashlan, A., Nanda, P. and Mohanty, M., 2024. Differential privacy model for blockchain based smart home architecture. Future Generation Computer Systems, 150, pp.49-63.
[22] Heo, G. and Doh, I., 2024. Blockchain and differential privacy-based data processing system for data security and privacy in urban computing. Computer Communications, 222, pp.161-176.
[23] Xu, C., Zhang, P., Mei, L., Zhao, Y. and Xu, L., 2024. Ranked searchable encryption based on differential privacy and blockchain. Wireless Networks, 30(6), pp.4735-4748.
[24] Islam, M., Rehmani, M.H. and Chen, J., 2024. Differentially private enhanced permissioned blockchain for private data sharing in industrial IoT. Information Sciences, 658, p.119997.
[25] Batool, H., Anjum, A., Khan, A., Izzo, S., Mazzocca, C. and Jeon, G., 2024. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy. Information Sciences, 652, p.119717.
[26] Nicolazzo, S., Arazzi, M., Nocera, A. and Conti, M., 2024. Privacy-Preserving in Blockchain-based Federated Learning Systems. arXiv preprint arXiv:2401.03552.
[27] Mao, Q., Wang, L., Long, Y., Han, L., Wang, Z. and Chen, K., 2024. A blockchain-based framework for federated learning with privacy preservation in power load forecasting. Knowledge-Based Systems, 284, p.111338.
[28] Padma, A. and Ramaiah, M., 2024. Blockchain based an efficient and secure privacy preserved framework for smart cities. IEEE Access.
[29] Javed, L., Anjum, A., Yakubu, B.M., Iqbal, M., Moqurrab, S.A. and Srivastava, G., 2023. ShareChain: Blockchain-enabled model for sharing patient data using federated learning and differential privacy. Expert Systems, 40(5), p.e13131.
[30] Qashlan, A., Nanda, P. and Mohanty, M., 2024. Differential privacy model for blockchain based smart home architecture. Future Generation Computer Systems, 150, pp.49-63.
[31] Escorcia-Gutierrez, J., Mansour, R.F., Leal, E., Villanueva, J., Jimenez-Cabas, J., Soto, C. and Soto-Díaz, R., 2023. Privacy Preserving blockchain with energy aware clustering scheme for IoT healthcare systems. Mobile Networks and Applications, pp.1-12.
[32] Frimpong, S.A., Han, M., Boahen, E.K., Sosu, R.N.A., Hanson, I., Larbi-Siaw, O. and Senkyire, I.B., 2023. RecGuard: An efficient privacy preservation blockchain-based system for online social network users. Blockchain: Research and Applications, 4(1), p.100111.
[33] Zhang, Y., Tang, Y., Zhang, Z., Li, M., Li, Z., Khan, S., Chen, H. and Cheng, G., 2023. Blockchain-based practical and privacy-preserving federated learning with verifiable fairness. Mathematics, 11(5), p.1091.
[34] Kiran, A., Mathivanan, P., Mahdal, M., Sairam, K., Chauhan, D. and Talasila, V., 2023. Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques. Mathematics, 11(9), p.2073.
[35] Babu, E.S., Yadav, B.R.N., Nikhath, A.K., Nayak, S.R. and Alnumay, W., 2023. MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. Cluster Computing, 26(4), pp.2217-2244.
[36] Sezer, B.B., Turkmen, H. and Nuriyev, U., 2023. PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. Internet of Things, 22, p.100781.
[37] Mishra, S., 2023. Blockchain and machine learning-based hybrid IDS to protect smart networks and preserve privacy. Electronics, 12(16), p.3524.
[38] Wang, M., Zhu, T., Zuo, X., Yang, M., Yu, S. and Zhou, W., 2023. Differentially private crowdsourcing with the public and private blockchain. IEEE Internet of Things Journal, 10(10), pp.8918-8930.
[39] Moulahi, W., Jdey, I., Moulahi, T., Alawida, M. and Alabdulatif, A., 2023. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. Computers in Biology and Medicine, 167, p.107630.
[40] Sharma, P.C., Mahmood, M.R., Raja, H., Yadav, N.S., Gupta, B.B. and Arya, V., 2023. Secure authentication and privacy-preserving blockchain for industrial internet of things. Computers and Electrical Engineering, 108, p.108703.
[41] Hiwale, M., Walambe, R., Potdar, V. and Kotecha, K., 2023. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for telemedicine. Healthcare Analytics, 3, p.100192.
[42] Li, Y., Xia, C., Lin, W. and Wang, T., 2024. PPBFL: A Privacy Protected Blockchain-based Federated Learning Model. arXiv preprint arXiv:2401.01204.

[43] Alamer, A.M.A., 2024. A secure and privacy blockchain-based data sharing scheme in mobile edge caching system. Expert Systems with Applications, 237, p.121572.
[44] Liu, W.J., Chiu, W.Y. and Hua, W., 2024. Blockchain-enabled renewable energy certificate trading: A secure and privacy-preserving approach. Energy, 290, p.130110.
[45] Verma, G., 2024. Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence, 36(1), pp.147-160.
[46] Aurangzeb, M., Wang, Y., Iqbal, S., Naveed, A., Ahmed, Z., Alenezi, M. and Shouran, M., 2024. Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage. Energy Reports, 11, pp.2493-2515.
[47] Masood, I., Daud, A., Wang, Y., Banjar, A. and Alharbey, R., 2024. A blockchain-based system for patient data privacy and security. Multimedia Tools and Applications, 83(21), pp.60443-60467.
[48] Li, B. and Ma, M., 2023. An advanced hierarchical identity-based security mechanism by blockchain in named data networking. Journal of Network and Systems Management, 31(1), p.13.
[49] Yin, R., Yan, Z., Liang, X., Xie, H. and Wan, Z., 2023. A survey on privacy preservation techniques for blockchain interoperability. Journal of Systems Architecture, 140, p.102892.
[50] Liu, Y., Liu, P., Jing, W. and Song, H.H., 2023. Pd2s: A privacy-preserving differentiated data sharing scheme based on blockchain and federated learning. IEEE Internet of Things Journal.