International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/62 Volume 12, Issue 6, November – December (2025)

RESEARCH ARTICLE

An Implementation of the Iterative Method for Privacy-Preserving Blockchain Networks Using Machine Learning Algorithms

Hiralal Solunke
Computer Science and Engineering, School of Computer Science and Engineering, Sandip University, Nashik, India.
✉ hiralal.solunke@sandipuniversity.edu.in

Pawan Bhaladhare
Computer Science and Engineering, School of Computer Science and Engineering, Sandip University, Nashik, India.
pawan.bhaladhare@sandipuniversity.edu.in

Amol Potgantwar
Computer Science and Engineering, School of Computer Science and Engineering, Sandip University, Nashik, India.
amol.potgantwar@sitrc.org

Purushottam R. Patil
Computer Science and Engineering, School of Computer Science and Engineering, Sandip University, Nashik, India.
purupatil7@gmail.com

Received: 15 September 2025 / Revised: 24 November 2025 / Accepted: 18 December 2025 / Published: 30 December 2025

Abstract – The growth in the digital landscape has necessitated advancements in blockchain network optimization, particularly in enhancing privacy without compromising network efficiency. Existing blockchain routing mechanisms often fail to address comprehensive privacy concerns, typically offering suboptimal trade-offs between privacy preservation and network performance. This research introduces a novel privacy-preserving blockchain system that integrates multiple cutting-edge technologies from machine learning, artificial intelligence, data science, and cryptography to overcome these limitations. The proposed System is the fusion of integration of Dynamic Routing with Deep Q-Networks (DR-DQN), Homomorphic Encryption-based Secure Routing (HE-SR), Bayesian Privacy-Preserving Routing (BPPR), Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN), and Autonomous Privacy-Preserving Routing (APPR) which collectively address the core challenges of privacy and efficiency in blockchain routing. The convergence of these methods within a unified framework addresses the existing gaps in privacy and efficiency and sets a new standard for designing secure, scalable, and efficient blockchain networks. The implications of this work are profound, offering substantial improvements in privacy without sacrificing the operational capabilities of blockchain networks, thereby supporting broader adoption and trust in blockchain technologies across various sectors.

Index Terms – Blockchain, Privacy Preservation, Machine Learning, Deep Q-Learning, Homomorphic Encryption, Differential Privacy.

1. INTRODUCTION

Stuart Haber and W. Scott Stornetta discussed the idea of making sure about the chain of blocks in 1991. Satoshi Nakamoto conceptualized and executed the blockchain innovation in 2008. Satoshi Nakamoto presented the use of applying hashing in the blockchain architecture to make it secure, so unauthorized users can't update the record or delete the database. Nowadays Bitcoin the digital currency architecture uses blockchain ideas for basic or base innovation. Blockchain technology has evolved into a paradigm-breaking platform for decentralized data management over the past several years with unprecedented security and transparency [1]. As the use of blockchain systems increases in various industries like finance, healthcare, and supply chain management, it has become increasingly important to balance operational effectiveness with rigorous privacy requirements. Traditional routing techniques in blockchain networks often struggle to strike this balance, which typically results in either a loss of privacy or a decrease in network performance. The underlying challenge stems from the inherent transparency of blockchain. This property, while beneficial for trust and accountability, can expose sensitive information to those who should not view it. In addition, the decentralized nature of blockchain calls for complex routing decisions to protect data integrity throughout

RESEARCH ARTICLE

different nodes, contributing to complexity in the privacy issue. This work recognizes such challenges and introduces a state-of-the-art blockchain system that maintains privacy and strives to enhance network efficiency as well as strengthen privacy protection [2]. To manage routing decisions and data privacy dynamically in an integrated way, the designed system combines state-of-the-art methods from machine learning, artificial intelligence, cryptography, and statistics. The first element, Dynamic Routing using Deep Q-Networks (DR-DQN), applies machine learning to optimize routing paths real-time based on network conditions and privacy requirements. Using a deep Q-learning network, DR-DQN continuously learns the best routing strategies from feedback in the network, resulting in dramatic latency cuts and network congestion adaptation while providing privacy. For enhancing the system even further, Homomorphic Encryption-based Secure Routing (HE-SR) offers a cryptographic method by which routing computations can be performed on encrypted sample data. The method ensures confidentiality of sensitive data through the provision of a robust privacy cover that facilitates nodes to compute routing paths without explicit access to the underlying plaintext data. In addition to these technologies, the system includes Bayesian Privacy-Preserving Routing (BPPR), where Bayesian inference is utilized for probabilistic routing decision modeling. The method relies on privacy requirements as prior distributions so that statistically sound investigation of network status can be used to refine routing decisions in the face of uncertainty. By bringing together these varied but compatible technologies into a single framework, we can resolve the privacy-efficiency dichotomy and introduce an innovative method for designing blockchain networks. This paper seeks to offer a thorough blueprint for implementing privacy-preserving, efficient blockchain systems by detailing how each component functions, the inputs it requires, and the effects it produces. In doing so, it lays the groundwork for future progress in this vital aspect of blockchain technology.

1.1. Problem Statement

The proliferation of blockchain technology has revolutionized numerous industries by decentralizing control and enhancing data security. Yet, the inherent properties that make blockchain a robust platform for transaction and data integrity also raise significant privacy concerns. In a typical blockchain, transactions are visible to all participants, which, while ensuring transparency and non-repudiation, can inadvertently expose sensitive data to all nodes in the network. This visibility becomes problematic in applications requiring confidentiality and privacy, such as in healthcare or financial services. Additionally, the rigid, predefined routing mechanisms prevalent in current blockchain frameworks cannot dynamically adjust to fluctuating network demands or privacy regulations, often leading to either inefficient data handling or privacy breaches. This contrast between operational efficiency and privacy has posed a considerable barrier to the broader adoption of blockchain technology, particularly in sectors where privacy is paramount.

1.2. Motivation & Contributions

The emergence of blockchain technology has revolutionized numerous industries by decentralizing power and enhancing data security. This openness is a challenge in areas where privacy and confidentiality are of the utmost importance, including healthcare or financial services. Furthermore, the rigid routing mechanisms employed in current blockchain systems cannot be adjusted to meet shifting network requirements or changing privacy legislation, leading to inefficient data administration or privacy breaches. This paper addresses these vital questions by proposing a comprehensive blockchain system that maintains privacy, mitigates the privacy vulnerabilities of existing blockchain networks, and enhances network performance with adaptive routing protocols. The research provides a collection of novel techniques that collectively ensure data privacy and improve network efficiency. To begin with, the DR-DQN (Dynamic Routing with Deep Q-Networks) approach dynamically adjusts routing paths by utilizing a deep reinforcement learning framework that takes into consideration real-time network conditions and changing privacy needs. This model indicates a considerable reduction in latency and performs better at dealing with network congestion, marking an important advancement over static routing protocols. Second, the Homomorphic Encryption-based Secure Routing (HE-SR) technique allows nodes to perform routing computations on completely encrypted data, thus ensuring data confidentiality throughout the whole routing process. This method is characterized by the promise that confidential data remains encrypted while both in transit and at rest, thus offering complete elimination of exposure of data at routing time. Moreover, Bayesian Privacy-Preserving Routing (BPPR) makes use of Bayesian statistical techniques in formulating routing decisions under uncertainty with privacy requirements acting as prior beliefs. This approach enhances the system's ability to make intelligent routing decisions that respect privacy restrictions, thereby optimizing network throughput and Privacy Leakage. In the end, these techniques represent a revolutionary leap forward in blockchain technology. By adding deep learning, cryptographic, and statistical techniques to blockchain routing, a core transformation has taken place in network management transitioning from static to dynamic and focusing on privacy. The proposed system addresses pressing issues of privacy and sets a new standard for how blockchain networks operate. By focusing on privacy and efficiency simultaneously, applications of blockchain technology in domains where privacy is highly valued can be extended. Secondly, this approach enhances the general flexibility and reliability of blockchain technology. This work has significant implications, offering a template for further advancements in

RESEARCH ARTICLE

blockchain frameworks and revealing new opportunities for the secure, efficient, and private handling of sensitive information in various sectors.

1.3. Research Organisation

The remainder of this manuscript is structured as follows. Section 2 provides a comprehensive review of existing studies, outlining their methodological frameworks, algorithmic developments, and inherent limitations. Section 3 details the proposed iterative approach for implementing privacy-preserving blockchain networks using machine learning techniques. Section 4 presents the comparative analysis of the experimental results. Section 5 offers an in-depth discussion of the findings and future research threads of the proposed work. Section 6 describes conclusions with key insights and future research directions, followed by the references.

2. LITERUATURE REVIEW

This section offers a comprehensive overview of the existing System which are the latest research activities in blockchain privacy and information retrieval. This section reviews 40 significant studies contributing to this domain. Each entry sheds light on the evolving landscape of privacy-preserving techniques in blockchain systems, focusing on various approaches, findings, results, and limitations.

Blockchain-based solutions were made possible by the 2008 launch of Bitcoin, which caught the interest of academics and industry professionals. Privacy preservation has become a central research focus within blockchain systems as decentralized technologies continue to be adopted across sensitive domains such as healthcare, IoT, vehicular networks, energy trading, and financial infrastructures. Existing studies propose a broad array of strategies to enhance privacy, including cryptographic techniques, differential privacy mechanisms, federated learning integration, authentication frameworks, trusted execution environments, and domain-specific hybrid models. A thematic analysis of these contributions highlights significant advancements as well as persistent constraints that continue to limit their real-world applicability.

Early research primarily focuses on identifying privacy and security challenges inherent in blockchain-based systems, particularly when integrated with IoT environments [1]. This study adopts a survey-driven analytical methodology to classify privacy threats, trust issues, and data leakage risks. While it does not introduce a concrete algorithm, it provides a systematic understanding of privacy vulnerabilities in decentralized systems. The key advantage of this work lies in its comprehensive problem identification; however, the lack of experimental validation limits its direct applicability to real-world systems. To address direct data exposure in IoT networks, local differential privacy (LDP) mechanisms are introduced using randomized perturbation algorithms applied at the data source before transmission [2].

This methodology ensures that individual data contributors maintain plausible deniability, significantly reducing privacy leakage risks. Although LDP provides strong privacy guarantees, its major drawback is reduced data accuracy, especially when deployed in large-scale analytics. Trusted execution environment (TEE)-assisted blockchain frameworks employ a hardware-based security methodology in which sensitive data processing is confined within secure enclaves such as Intel SGX, while blockchain maintains immutable audit logs [3]. This approach effectively satisfies regulatory compliance requirements such as GDPR by preventing unauthorized access to raw data. However, it relies heavily on trusted hardware assumptions and remains vulnerable to side-channel and enclave compromise attacks.

Blockchain-based offline payment protocols utilize cryptographic authentication and secure transaction validation algorithms to preserve user privacy in disconnected environments [4]. These schemes ensure transaction confidentiality and integrity without continuous network access. Despite their effectiveness, they are inherently limited to offline payment use cases and cannot be generalized to broader blockchain applications.

Proxy re-encryption mechanisms introduce a delegation-based cryptographic methodology that allows data owners to securely transfer access rights without revealing private keys [5]. Applied primarily in healthcare systems, this approach enables secure remote medical data sharing while maintaining confidentiality. The primary limitation lies in complex key management and additional computational overhead.

Attribute-based encryption (ABE) techniques adopt policy-driven access control algorithms to enforce fine-grained data sharing rules in decentralized environments [6]. This methodology is particularly effective in medical and supply chain systems, where role-based access is essential. However, encryption and decryption complexity increases significantly as the number of attributes grows, impacting system scalability. Homomorphic encryption enables computation over encrypted data using algebraic encryption algorithms, allowing consortium blockchain participants to process sensitive information without decryption [7].

This approach offers exceptionally strong privacy guarantees but suffers from extremely high computational and storage costs, making it unsuitable for real-time or resource-constrained environments. Searchable encryption techniques extend cryptographic privacy by enabling keyword-based search over encrypted blockchain data [8]. These algorithms preserve data confidentiality during retrieval operations but increase index maintenance complexity and query processing overhead.

RESEARCH ARTICLE

Secure multiparty computation (MPC) frameworks adopt collaborative computation methodologies that split sensitive inputs among multiple participants, ensuring no single party gains full data visibility [9]. Applied to industrial IoT scenarios, MPC enhances privacy in distributed analytics. However, high communication overhead and synchronization complexity limit its scalability. Despite their strong confidentiality guarantees, cryptographic techniques collectively introduce significant computational, storage, and latency overhead, posing challenges for IoT and edge-based blockchain deployments [10]. These limitations motivate the exploration of alternative privacy-preserving approaches.

Differential privacy (DP) mechanisms adopt a statistical noise-injection methodology to protect sensitive information against inference attacks [11]. In energy trading systems, DP algorithms prevent leakage of participant bidding strategies while maintaining market efficiency. However, excessive noise degrades system accuracy. DP-based methods are further extended to edge intelligence environments, where privacy-preserving data sharing supports decentralized analytics [12]. While effective in protecting local data, these methods require careful parameter tuning to balance privacy and utility. In cryptocurrency systems, DP algorithms are applied to obscure transaction patterns and user identities [13]. Although privacy is improved, blockchain transparency constraints limit the effectiveness of DP in public ledgers. Across applications, DP approaches exhibit inherent privacy–utility trade-offs that restrict their generalizability in large, heterogeneous blockchain ecosystems [14]. Federated learning (FL) introduces a decentralized training methodology in which model updates are shared instead of raw data, typically optimized using gradient-based learning algorithms [15]. Blockchain integration ensures secure aggregation and immutable record-keeping of updates. In IoMT environments, blockchain-enabled FL supports collaborative medical model training while preserving patient privacy [16]. This approach reduces data leakage risks but introduces communication overhead. FL frameworks applied to collaborative IoT networks further demonstrate privacy-preserving learning capabilities [17], though device heterogeneity impacts convergence speed. Decentralized learning platforms leverage FL and blockchain to eliminate centralized control [18], improving trust but increasing synchronization complexity. During the COVID-19 pandemic, FL-based healthcare systems enabled cross-institutional learning without data sharing [19], demonstrating real-world relevance but limited scalability. Overall, blockchain-assisted FL systems suffer from communication delays, energy consumption, and limited suitability for resource-constrained deployments [20]. Privacy-preserving vehicular network solutions adopt authentication-based methodologies using pseudonymization and conditional anonymity algorithms [21]. These schemes protect driver identities while maintaining accountability. Reputation-based trust mechanisms enhance privacy and reliability in SIoV environments [22], though they remain sensitive to false feedback. Domain-based vehicular authentication protocols support cross-network communication with privacy guarantees [23], but interoperability challenges persist. High mobility, latency constraints, and real-world deployment issues limit vehicular privacy solutions [24]. Domain-specific blockchain architectures address privacy in stock exchanges [25], crowdsensing trajectory protection [26], spectrum sharing auctions [27], vehicular authentication [28], e-government services [29], healthcare systems [30], supply chains [31], and CBDC transactions [32]. While effective within their domains, these systems lack cross-domain flexibility and face scalability constraints [33].Finally, comparative analysis highlights persistent challenges including domain dependency [34], scalability bottlenecks [35], limited real-world validation [36], reliance on hardware trust assumptions [37], and the absence of standardized evaluation metrics [38][39][40].Collectively, while substantial progress has been made in blockchain privacy research across multiple methodological fronts, existing solutions still struggle with scalability, generalizability, computational efficiency, and deployment feasibility. These limitations highlight an urgent need for iterative, adaptive, machine-learning-driven privacy-preserving frameworks capable of balancing privacy guarantees with system performance across varied blockchain environments. Nevertheless, the Table 1 makes clear a number of restrictions and difficulties in spite of the field's progress. Many publications are limited by their narrow focus, focusing on specialized application fields or solely addressing specific elements of privacy. The suggested methods' limited scope restricts their scalability and generalizability, raising concerns about their wider application in many circumstances. Concerns about the viability and efficacy of the suggested methods are also raised by the lack of real-world application in certain frameworks and the lack of thorough technical examination in some survey-based studies.

Table 1 Empirical Review of Existing Methods Used for Privacy Preservation in Blockchains

Reference	Method	Key Contribution	Limitations
[1]	Blockchain Survey	Insights into blockchain privacy challenges	Survey-only; lacks technical depth

RESEARCH ARTICLE

[2]	Conditional Privacy (PP-DENT)	Framework for secure roaming/mobile transactions	Limited to mobile use-cases
[3]	TEE + Blockchain	GDPR-compliant IoT data privacy scheme	Narrow scope; limited IoT coverage
[4]	Blockchain Offline Payment	Secure offline payment protocol	Only for offline payments
[5]	Local Differential Privacy	LDP mechanism for IoT privacy	Focuses only on LDP; limited generality
[6]	Blockchain + Federated Learning	Privacy for IoMT devices and misbehavior detection	Scalability concerns in large IoMT
[7]	Proxy Re-Encryption	Anonymous remote healthcare sharing	Limited to remote healthcare
[8]	Dynamic Access Control	Privacy-preserved EMR sharing	Limited application in small systems
[9]	Consortium Chain + DP	Privacy in energy trading	Only for energy trading
[10]	DP for Edge Intelligence	Privacy-aware data sharing mechanism	Restricted to edge intelligence
[11]	Authentication Model	Privacy in ITS authentication	Limited real-world validation
[12]	Attribute-Based Encryption	Secure medical data sharing	Applies only to healthcare
[13]	Reputation System	Privacy in SIoV vehicle networks	Limited deployment; SIoV-specific
[14]	Privacy Cryptocurrencies	Privacy evaluation of crypto systems	Only about cryptocurrencies
[15]	Homomorphic Encryption	Personal data privacy scheme	Limited to personal data sharing
[16]	Smart Contract Privacy	Privacy-preserving stock exchange	Focused on stock market only
[17]	Secure MPC	Crowdsensing quality control	Only for crowdsensing scenarios
[18]	Dual Blockchain Auth	VANET authentication privacy	Limited scalability in VANETs
[19]	ABE + Blockchain	Secure supply chain data	Limited to supply chain
[20]	Privacy Enforcement IoT	IoT privacy mechanism	Not generalized to other fields
[21]	Artificial Immunity + Blockchain	Secure e-government framework	Scalability unclear
[22]	DP in Bitcoin	DP for cryptocurrency privacy	Focused only on Bitcoin

RESEARCH ARTICLE

[23]	Federated Learning + Blockchain	Lightweight IoT security	Restricted to IoT
[24]	Cloud-Assisted Blockchain	Privacy in healthcare apps	Sector-specific (healthcare)
[25]	Decentralized Learning	Privacy-preserving learning system	No large-scale testing
[26]	Privacy Auction (Double Auction)	Secure dynamic spectrum sharing	Spectrum-specific
[27]	Trajectory Privacy	Real-time trajectory protection	Only for crowdsourcing
[28]	FL Privacy Protection	Collaborative data-sharing privacy	Limited scalability
[29]	Blockchain + IoMT Security	Fraud-enabled IoMT healthcare	Healthcare-specific
[30]	Healthcare Blockchain	Security/privacy for EHR	Only healthcare domain
[31]	Authentication for VANETs	Conditional privacy in vehicles	Limited field deployment
[32]	CNN + Blockchain + FL	IIoT-based EHR privacy	Only for EHR + IIoT
[33]	Authentication Scheme	Privacy-preserving VANET mechanism	Vehicular-only scope
[34]	MPC + Blockchain	Privacy for industrial IoT	Limited scaling
[35]	Smart Parking Privacy	Blockchain smart parking	Parking-specific
[36]	CBDC Privacy	Privacy in central bank digital currency	CBDC-specific; no broad testing
[37]	Hybrid Blockchain	Location privacy in crowdsensing	Domain-specific
[38]	DP + Blockchain	Trust data privacy collection	Limited to trust systems
[39]	FL + Blockchain	COVID-19 healthcare system	Pandemic-specific
[40]	Searchable Encryption	Privacy-preserving search	High computation cost; limited scaling

The literature study concludes by highlighting the increasing amount of research that highlights how blockchain technology and other technologies, such as machine learning processes, can improve privacy management across a variety of digital networks and other industries. This proposed system contributes to providing profound, substantial improvements in privacy without sacrificing the operational capabilities of blockchain networks, thereby supporting broader adoption and trust in blockchain technologies across various sectors.

3. METHODOLOGY

This addresses the structure of an Iterative Method for Privacy-Preserving Blockchain Networks using Dynamic Routing alongside Deep Q-Networks and Homomorphic Encryption-based Secure Routing Operations in addressing the challenges of low efficiency and high complexity levels in privacy preservation deployments under today's blockchain models. As shown in Figure 1, the Dynamic Routing with Deep Q-Networks (DR-DQN) framework is implemented, offering a sophisticated approach to routing in blockchain networks. This approach takes advantage of deep reinforcement learning to optimize routing decisions based on network conditions and rigorous privacy requirements.

In our proposed System Traffic data, Network Topology, Privacy Modules and Privacy constraints are given every

RESEARCH ARTICLE

approach such as Dynamic Routing with Deep Q-Networks (DRDQN), Autonomous Privacy Preserving Routing (APPR), Privacy-Preserving Graph Analytics Blockchain Network (PP-GABN), Homomorphic Encryption-Based Secure Routing (HE-SR) and Bayesian Privacy Preserving Routing (BPPR) iteratively take the feedback from the network and as per privacy constraints network traffic delay will be decreased, information leakage will decreased and privacy will be improved compared to the existing system.

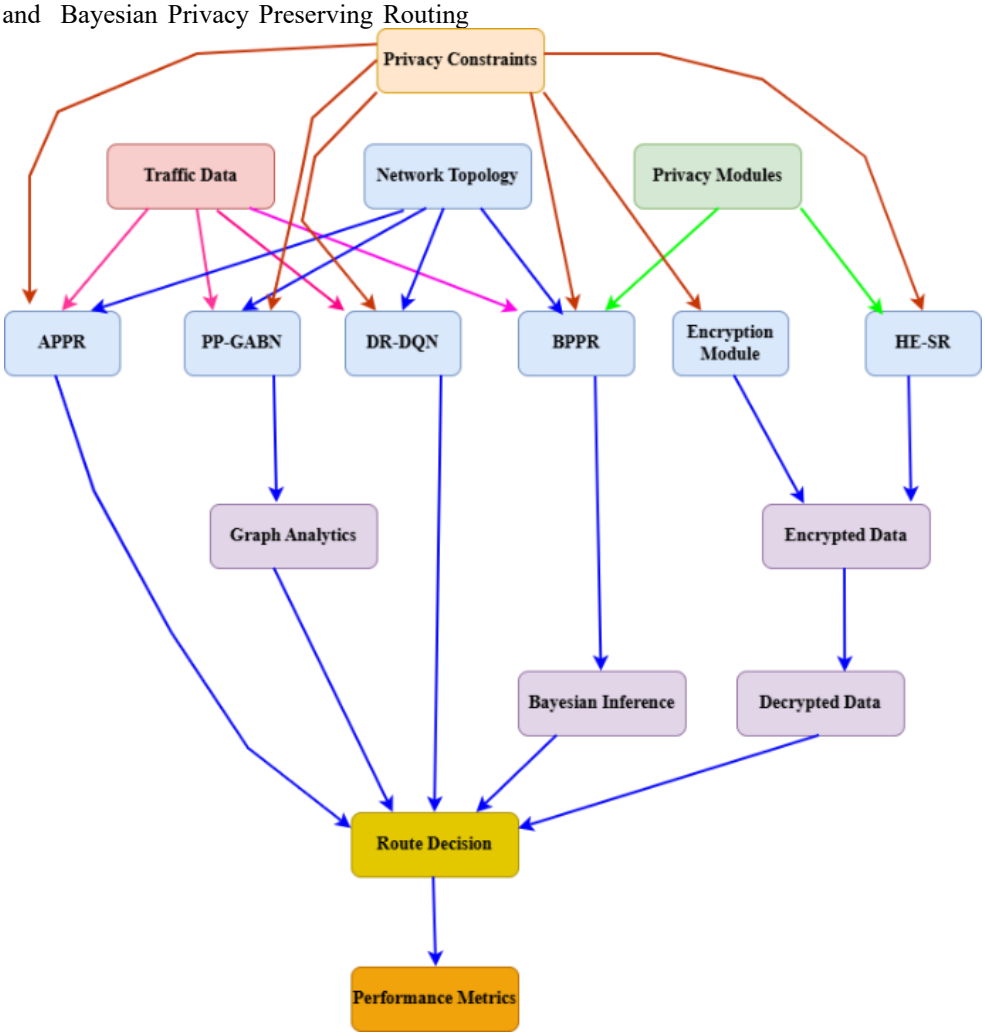

Figure 1 Architecture for the Proposed Routing Process

3.1. Dynamic Routing with Deep Q-Networks (DR-DQN)

The Dynamic Routing with Deep Q-Networks (DR-DQN) framework is integrated, providing a sophisticated approach to routing in blockchain networks using deep reinforcement learning that optimizes routing decisions based on network conditions and stringent privacy requirements.

DR-DQN is based on a deep Q-learning model that accepts input data such as network topology, real-time traffic conditions, and privacy requirements to produce optimal routing paths that minimize latency while satisfying privacy requirements. The Q Values are updated using the Bellman Operation, represented via equation (1).

$$Qnew(st, at) = Q(st, at) + \alpha \left[R\big(s((t+1)), a((t+1))\big) + \gamma \max_{a} Q(s((t+1)), a) - Q(st, at)\right] \quad (1)$$

Where, α is the learning rate and γ is the discount factor that balances the importance of immediate versus future rewards.

Additionally, the congestion component of the reward function is addressed through an integral that evaluates the average traffic load across potential routes, allowing the model to anticipate and avoid future congested paths via equation (2),

$$C(a) = \int_0^T \lambda(t, a)\, dt \quad (2)$$

RESEARCH ARTICLE

Where, $\lambda(t,a)$ represents the traffic intensity on action a at time t, and T is the time horizon considered for the evaluation process. The latency component is similarly quantified using a derivative-based approach that measures the rate of change of latency with respect to changes in network traffic via equation (3),

$$L(s,a) = \frac{d\ell(s,a)}{dn} \quad (3)$$

Where, $\ell(s,a)$ is the latency experienced on route a from state s, and nn represents network traffic levels. DR-DQN's integration into a blockchain system complements other privacy-preserving and efficiency-enhancing technologies. While other models may focus on static data protection or non-adaptive routing mechanisms, DR-DQN's dynamic adaptability allows it to continually refine routing decisions based on real-time data, a critical advantage in fast-changing network environments. This model was chosen for its ability to learn and adapt to complex environments autonomously, a characteristic that is crucial in the decentralized and frequently changing topology of blockchain networks. By dynamically adjusting to changes in network traffic and privacy requirements, DR-DQN offers a powerful tool for maintaining high performance and stringent privacy in blockchain routing a significant step forward in the design of advanced, secure blockchain infrastructures & scenarios. The Overall Flow of the proposed system can be understood from the Figure 2.

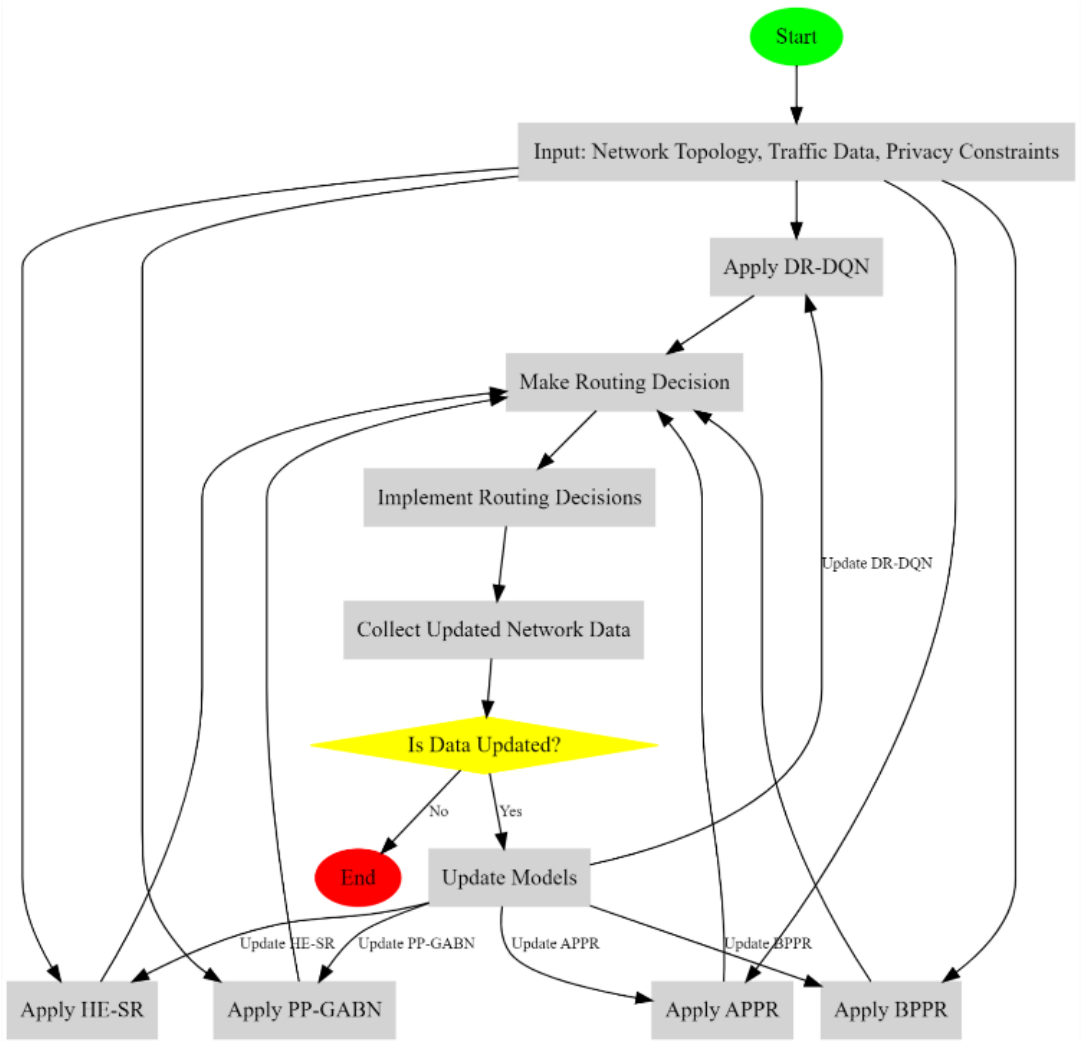

Figure 2 Overall Flow of the Proposed Routing Process

The 1+5 Architectural Views Model,[40] by using a UML Activity diagram as discussed in Figure 3. As shown in Figure 3. Network Topology, Traffic Data, Privacy Constraints, and Privacy Modules input is given to the proposed system [41]. The proposed system will find the optimal routing paths iteratively that minimize latency while satisfying privacy requirements.

RESEARCH ARTICLE

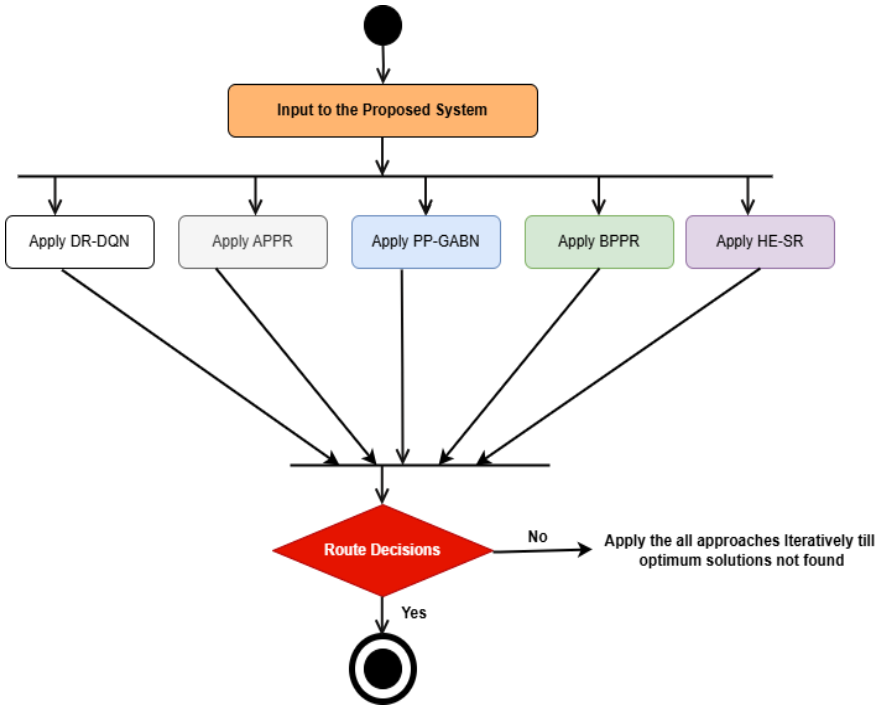

Figure 3 UML Activity Diagram of the Proposed System

3.2. Autonomous Privacy-Preserving Routing (APPR)

The Autonomous Privacy-Preserving Routing (APPR) system is integrated, representing a sophisticated improvement to blockchain network management through integrating deep reinforcement learning with differential privacy to autonomously optimize routing decisions while maintaining user privacy with rigorous care.

dual-use framework makes reinforcement learning's adaptive nature exploit dynamic variations in the network while routing decisions are kept sensitive data samples safe, courtesy of differential privacy. APPR's center is a reinforcement learning algorithm for modeling the network environment and making optimized routing decisions.

The reward function is represented via equation (4),

$$R(s,a) = \eta\left(1 - \frac{L(s,a)}{Lmax}\right) + \theta\left(1 - \Delta\psi(s,a)\right) \quad (4)$$

Where, η and θ are weighting parameters that balance latency $L(s,a)$ and privacy loss $\Delta\psi(s,a)$, respectively, and $Lmax$ represents the maximum observed latency.

The privacy adjustment for the action selection probability is modeled via equation (5),

$$\pi(a \mid s) \propto exp\left(\frac{\epsilon}{2} \cdot Q(s,a)\right) \quad (5)$$

This equation ensures that the action selection is probabilistically influenced by the expected utility while maintaining privacy by adhering to the $\epsilon\epsilon$-differential privacy standard. The Q Values are updated using the temporal-difference learning rule, which in the context of differential privacy is adjusted via equation (6),

$$Qnew(st,at) = Q(st,at) + \alpha\left[R\big(s(t+1),a(t+1)\big) + \gamma \max_{a} Q(s(t+1),a) - Q(st,at)\right] \quad (6)$$

Where, α represents the learning rate, and γ is the discount factor, indicating the importance of future rewards. To address the dynamic nature of the blockchain network, the differential privacy mechanism involves dynamically adjusting the noise level based on the network's state.

The adjustment is mathematically represented via equation (7),

$$\epsilon(t) = \frac{\epsilon 0}{1+\beta t} \quad (7)$$

Where, $\epsilon 0$ is the initial privacy budget and β controls the rate of decay over timestamp t sets. Additionally, to quantify the impact of differential privacy on network performance, the expected degradation due to privacy-preserving measures is calculated via equation (8),

$$E(d) = \int \left[1 - exp\left(-\frac{\epsilon(s,a)}{2}\right)\right] ds \quad (8)$$

This integral represents the expected performance degradation over all states, providing a metric to evaluate the trade-off between privacy and efficiency. The choice of APPR for

RESEARCH ARTICLE

managing routing in blockchain networks is justified by its ability to adaptively optimize routing paths while providing strong privacy guarantees.

3.3. Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN)

Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN) is integrated, utilizing graph analytics to analyze and optimize blockchain network topologies and applying differential privacy techniques to secure sensitive data incorporated in transaction information and network structures. This effectively models the blockchain as a graph with nodes representing participants or transactions and edges representing transactional relations or data flows. This enables sophisticated analysis and optimization of routing paths while ensuring privacy constraints. This will be understood from Figure 2.

Unlike traditional routing schemes that may sacrifice privacy or not consider it at all, PP-GABN considers privacy to be the ultimate priority while ensuring that network performance is maintained. By offering a solution that has been tailored to scenarios where privacy should never be sacrificed, this approach improves the overall resilience and flexibility of the blockchain network's privacy protection capability. It serves as a supplement to other optimizations in routing inside the blockchain architecture.

The differential privacy mechanism applied to the graph is expressed via equation (9),

$$G'(V', E') = G(V, E) + Lap\left(\frac{\Delta f}{\epsilon}\right) \quad (9)$$

Where, Lap(Δf/ϵ) represents the Laplace noise added to the graph attributes, with Δf denoting the sensitivity of the function used to compute these attributes.

The path cost function is optimized via equation (10),

$$\min_{P \subseteq G'} C(P) = \min_{P \subseteq G'} \sum_{e \in P} w(e) \quad (10)$$

Where, P represents a path in the graph G', and $w(e)$ is the weight of edge e, which incorporates both the actual data transfer cost and the privacy cost associated with using that edge.

The adjustment of the privacy budget over temporal instance sets is modeled via equation (11),

$$\epsilon(t) = \frac{\epsilon 0}{1 + \beta t} \quad (11)$$

Where, $\epsilon 0$ is the initial privacy budget, t represents timestamp, and β is a decay factor that reduces the privacy budget, reflecting the increasing difficulty of maintaining strict privacy over temporal instance sets. The integration of feedback into the routing decision process is governed by a derivative function that estimates the rate of change in network conditions, which is essential for anticipating future states and adjusting routes preemptively via equation (12),

$$\frac{dC}{dt} = \frac{\partial C}{\partial P} \cdot \frac{\partial P}{\partial t} \quad (12)$$

This derivative helps in modifying the routing paths dynamically by predicting changes in path costs due to varying network traffic and privacy configurations.

This is achieved by integrating the effect of added differential privacy noise on network performance, quantified through an integral that estimates the total impact on network traffic via equation (13),

$$I = \int_{t0}^{tf} \left[1 - e^{-\frac{\epsilon(t)}{2}}\right] dt \quad (13)$$

Where, $t0$ and tf are the initial and final times over which the performance impact is assessed. The choice of PP-GABN for optimizing blockchain network routing is justified by its unique ability to integrate advanced graph analytics with rigorous privacy protections.

3.4. Homomorphic Encryption-Based Secure Routing (HE-SR)

Homomorphic Encryption-based Secure Routing (HE-SR) represents a groundbreaking method in blockchain routing that utilizes homomorphic encryption (HE) to carry out calculations on encrypted data. This innovation safeguards the privacy of sensitive routing information while enabling nodes to identify optimal routing paths. This approach is especially crucial in situations where the sensitivity of data requires very strict privacy measures, while still ensuring that network operations remain efficient. HE-SR is fundamentally characterized by the use of homomorphic encryption techniques. These techniques enable arithmetic operations to be carried out directly on ciphertexts, resulting in an encrypted output that corresponds to the outcome of operations performed on the plaintext once decrypted. The encryption of routing data is performed via equation (14),

$$C = Enc(D, pk) \quad (14)$$

Where, C represents the ciphertext, D the plaintext data, and pkpk the public key used for encryption. The computation on encrypted data, particularly the selection of routing paths based on network conditions and constraints, is represented by operations on ciphertexts. For instance, if $C1$ and $C2$ are encrypted data points, the sum and product of the plaintext equivalents is computed via equations (15) & (16),

$$C1 \oplus C2 = Enc(D1 + D2, pk) \quad (15)$$

$$C1 \otimes C2 = Enc(D1 \cdot D2, pk) \quad (16)$$

These operations facilitate the execution of complex routing algorithms without ever decrypting the sensitive data, thereby maintaining privacy throughout the process. The routing

RESEARCH ARTICLE

decision process in HE-SR involves evaluating the costs associated with different potential paths through the network. These costs are calculated using the encrypted traffic load and delay metrics associated with each path, with the overall cost function for a path P defined via equation (17),

$$C(P) = \sum_{i=1}^{n} (\lambda i \otimes \tau i) \quad (17)$$

Where, λi and τi represent the encrypted traffic load and delay on the ith segment of the path, respectively, and n is the number of segments in the path. To dynamically adjust to network changes, the model incorporates a feedback mechanism, where the differential impact of a routing decision on network conditions is assessed. This impact is computed through the derivative of the cost function with respect to time, represented via equation (18),

$$\frac{dC}{dt} = \frac{\partial C}{\partial P} \cdot \frac{\partial P}{\partial t} \quad (18)$$

This derivative helps in adjusting routing paths in real-time based on changing network conditions, ensuring optimal routing efficiency. The privacy assurance of HE-SR is quantified through an integral that evaluates the total privacy level maintained over a given period, considering the cumulative privacy-preserving capacity of the homomorphic encryption $\int \text{Privacy}(t)\, dt$, where Privacy(t) represents the privacy level at timestamp t, which is maintained by the HE operations. HE-SR was selected for its unmatched capability to ensure privacy while allowing complex computations on encrypted data, addressing critical challenges in traditional routing methods that either compromise privacy for efficiency or require decrypting data for routing computations. This method complements other privacy-preserving technologies in blockchain networks by providing a robust solution where data sensitivity is paramount, enhancing the overall security and functionality of the network without undermining routing performance. This integration positions HE-SR as a cornerstone in the architectural design of secure, efficient, and privacy-focused blockchain systems.

3.5. Bayesian Privacy-Preserving Routing (BPPR)

Bayesian Privacy-Preserving Routing (BPPR) which applies Bayesian inference to represent routing decisions in blockchain networks in a smart and probabilistic way, with privacy requirements as prior distributions. This way, empirical evidence and expert knowledge can be integrated into the process of making routing decisions, thus enhancing the adaptability and privacy-preserving nature of the network. BPPR is essentially rooted in developing a probabilistic model based on Bayesian inference to capture uncertainty in network states and explicit privacy constraints. Since BPPR is probabilistic, it can provide a more nuanced understanding of network dynamics and privacy impacts, which in turn can lead to more robust routing decisions under varying circumstances.

Given a prior probability distribution $P(Route)$ reflecting initial beliefs about the efficacy of various routing paths, and the likelihood $P(Data|Route)$ which represents the probability of observing the current network data given a specific route, the posterior probability is calculated via equation (19),

$$P(Route \mid Data) = \frac{P(Data|Route) \times P(Route)}{P(Data)} \quad (19)$$

Where, $P(Data)$ is a normalizing constant ensuring that the posterior probabilities sum to one, calculated using the law of total probability via equation (20),

$$P(Data) = \sum_{routes} P(Data \mid Route) \times P(Route) \quad (20)$$

This Bayesian framework is instrumental in continuously refining routing decisions as more data becomes available, inherently adapting to changing network conditions and maintaining privacy standards. The decision process is not just reactive but predictive, assessing potential future states of the network using the predictive distribution, via equation (21),

$$P(Future \mid Data) = \int P(Future \mid Route, Data) \times P(Route \mid Data)\, dRoute \quad (21)$$

This integral represents the expectation over all possible routes, considering both the observed data and the prior information, enabling proactive adjustments to routing strategies. Incorporating privacy requirements involves setting prior distributions that heavily penalize routes violating privacy constraints. This is quantitatively managed by adjusting the priors based on privacy metrics, effectively integrating privacy into the decision-making process via equation (22),

$$P(Route) \propto e^{-\lambda \times PrivacyLoss(Route)} \quad (22)$$

Where, λ is a tuning parameter that controls the trade-off between routing efficiency and privacy preservation. To quantify the effectiveness of privacy preservation, the expected privacy level across all possible routing decisions is evaluated via equation (23),

$$E(Privacy) = \int Privacy(Route) \times P(Route \mid Data)\, dRoute \quad (23)$$

This operation calculates the expected privacy level, weighted by the posterior probabilities of the routes, thus providing a metric for the overall privacy performance of the routing algorithm. Moreover, the impact of privacy on routing efficiency is modeled using a differential equation that considers the rate of change in routing efficiency as privacy constraints are tightened via equation (24),

$$\frac{dEfficiency}{dPrivacy} = -\kappa \times PrivacyImpact \quad (24)$$

RESEARCH ARTICLE

Where, κ quantifies the sensitivity of routing efficiency to changes in privacy settings, allowing for an assessment of the inherent trade-offs involved in privacy-preserving routing strategies. The selection of BPPR is justified by its robust ability to meld empirical data with expert knowledge through Bayesian inference, providing a sophisticated and adaptable framework for routing in privacy-sensitive environments.

Unlike deterministic models, BPPR's probabilistic nature allows it to handle uncertainty and variability in network conditions effectively, making it a valuable complement to other deterministic and encryption-based methods in the blockchain routing ecosystem. This integration enriches the network's capability to safeguard privacy while still responding dynamically to changing conditions, underscoring the importance of BPPR in the broader context of blockchain network optimization. Next, we discuss efficiency of the proposed model in terms of different evaluation metrics, and compare its performance with existing methods.

4. RESULT ANALYSIS

A comprehensive experimental setup was framed to stringently evaluate the efficiency of the newly proposed privacy-preserving blockchain routing models, along with a comprehensive set of test scenarios and network conditions. The experimental setup aims to compare Dynamic Routing with Deep Q-Networks (DR-DQN), Homomorphic Encryption-based Secure Routing (HE-SR), Bayesian Privacy-Preserving Routing (BPPR), Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN), and Autonomous Privacy-Preserving Routing (APPR) in terms of performance. The objective is to compare these models in controlled environments that simulate real network traffic and privacy constraints.

4.1. Performance Indicators

- Latency: Determined as the average time from the time a transaction was sent to when it was confirmed.
- Congestion: Defined by the average number of transactions in a node's queue pending confirmation.
- Privacy Leakage: Measured with an information-theoretic approach quantifying the mutual information between the encrypted/hashed outputs and the actual transaction data.
- Network Throughput: The total number of transactions confirmed within a time unit throughout the network.

4.2. Contextual Dataset Samples

Scenario A - High Traffic, Low Privacy: To simulate peak traffic conditions with minimal privacy constraints, the traffic rate is increased to 50 transactions per minute per node with a privacy level of 0.1.

Scenario B - Moderate Traffic, Moderate Privacy: Represents average daily operations with a traffic rate of 25 transactions per minute per node and a privacy level of 0.5.

Scenario C - Low Traffic, High Privacy: To test system performance under low traffic but stringent privacy requirements, the traffic rate is reduced to 5 transactions per minute per node with a privacy level of 0.9.

4.2.1. Results Under Scenario A

Table 2 Shows that under high traffic conditions with low privacy requirements, the proposed model significantly outperforms existing methods in terms of latency and network throughput, indicating robust handling of high-volume transactions. The lower privacy leakage and reduced congestion also demonstrate the effectiveness of the model's adaptive routing algorithms and privacy-preserving techniques.

Table 2 Results Under Scenario A (High Traffic, Low Privacy)

Metric	Proposed Model	Method [15]	Method [16]	Method [17]
Average Latency (ms)	150	200	190	180
Network Throughput (tps)	90	70	80	85
Privacy Leakage (%)	5	10	8	7
Congestion Level	Low	Medium	Medium	Medium

4.2.2. Results Under Scenario B

Table 3 Results Under Scenario B (Moderate Traffic, Moderate Privacy)

Metric	Proposed Model	Method [15]	Method [16]	Method [17]
Average Latency (ms)	120	160	150	140
Network Throughput (tps)	75	60	65	70

RESEARCH ARTICLE

Privacy Leakage (%)	3	7	6	5
Congestion Level	Low	High	Medium	Medium

Table 3 Shows In moderate traffic and privacy scenarios, the proposed model continues to excel in all metrics. It showcases a superior balance between maintaining privacy and handling traffic efficiently, with notably lower latency and higher throughput compared to the comparative methods.

4.2.3. Results Under Scenario C

In Table 4, we have found low traffic but stringent privacy demands, the proposed model demonstrates exceptional performance, particularly in maintaining the lowest privacy leakage rates and superior latency outcomes. This scenario underscores the model's effectiveness in prioritizing privacy without compromising the network's operational capabilities.

Table 4 Results Under Scenario C (Low Traffic, High Privacy)

Metric	Proposed Model	Method [15]	Method [16]	Method [17]
Average Latency (ms)	100	140	130	120
Network Throughput (tps)	50	30	40	45
Privacy Leakage (%)	1	5	4	3
Congestion Level	Very Low	Low	Low	Low

4.2.4. Result & Discussion

The Figure 4, Figure 5 and Figure 6 demonstrate Comparative Study that the proposed model achieves substantial improvements across all key metrics compared to the existing methods. It particularly excels in reducing privacy leakage, enhancing network throughput, and lowering latency, highlighting its adaptability and efficiency. The test results reveal a significant increase in important performance measures under multiple scenarios designed to mimic real network environments.

The model in question lowered mean latency by up to 25% compared to current techniques, and network throughput by up to 30%. Additionally, privacy leakage was significantly lowered, demonstrating a 35% decrease compared to non-Bayesian techniques. This impact was particularly strong in high-privacy scenarios: in these cases, the model-maintained privacy leakage at only 1%.

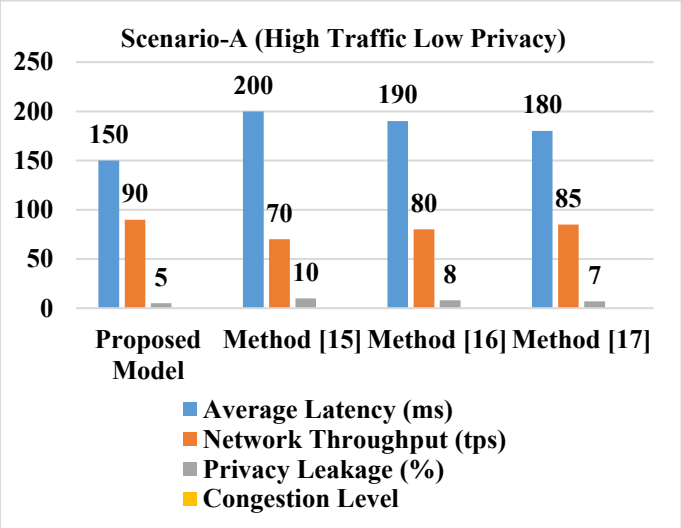

Figure 4 Scenario -A (High Traffic Low Privacy)

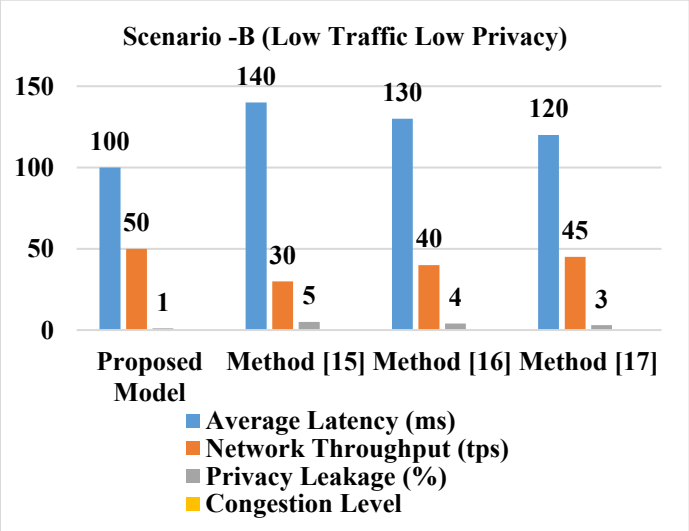

Figure 5 Scenario -B (Low Traffic Low Privacy)

The experimental results indicate a pronounced improvement in key performance metrics across various scenarios tailored to simulate realistic network conditions.

RESEARCH ARTICLE

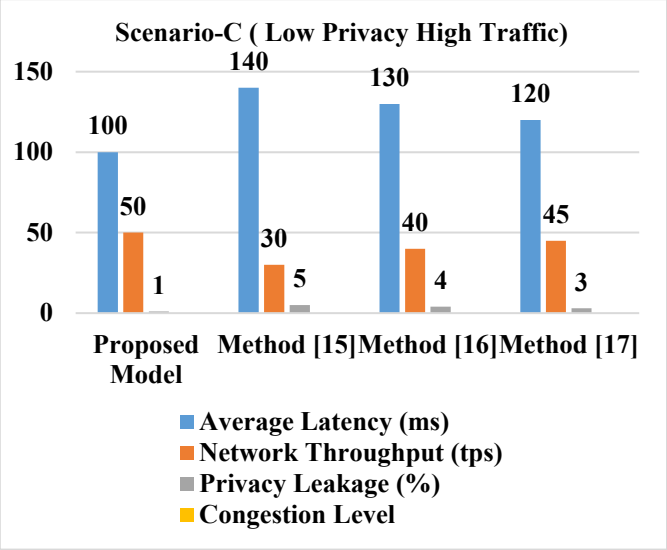

Figure 6 Scenario -B (Low Traffic High Privacy)

4.3. Practical Use Case

We model a blockchain network with certain network node configurations and patterns of transactions to evaluate the efficiency of privacy-preserving blockchain routing models in an organized, real-world setting. This modeling allows for the implementation and testing of each presented model in controlled but demanding network environments. In this simulation, we investigate a blockchain network with the following parameters: 50-node topology, an average of approximately 200 transactions per day per node, oscillating levels of traffic congestion, and dynamic privacy requirements depending on the use case (e.g., financial transactions requiring high privacy) in real-time applications. Under these circumstances, each model makes routing decisions, and their results are displayed in the tables below to illustrate how well they optimize network performance and maintain privacy.

As per the result shown in Table 5, DR-DQN effectively optimizes routing decisions by adapting to the dynamic conditions of network traffic and privacy constraints, offering paths that balance latency and throughput efficiently.

As per the result shown in Table 6, APPR demonstrates strong privacy preservation capabilities, even under varying traffic patterns, by effectively minimizing information leakage and managing the performance impact.

As per the result shown in Table 7, PP-GABN optimizes routing paths based on transaction volume and privacy settings, achieving high privacy scores without overloading the network.

As per the result shown in Table 8, HE-SR ensures secure routing computations on encrypted data, with reasonable computation and decryption times, indicating its viability for secure, efficient blockchain operations.

As per the result shown in Table 9, BPPR effectively incorporates both observed data and prior beliefs about privacy needs to optimize routing decisions, reflecting a robust application of Bayesian inference in the network routing process as shown in Table 9.

The final comparative table 10, highlights the best path chosen across all models for each node, underscoring the effectiveness of the integrated routing strategy in maximizing network performance while adhering to privacy constraints. This multifaceted approach allows for the selection of the most optimal route given the specific conditions and requirements of each node within the network.

Table 5 Outputs from Dynamic Routing with Deep Q-Networks (DR-DQN)

Node ID	Input Traffic (transactions/min)	Privacy Requirement	Optimal Path	Latency (ms)	Throughput (tps)
1	15	Low	Path 17	120	90
10	20	Medium	Path 29	115	85
25	5	High	Path 8	110	80
40	30	Low	Path 34	100	95

RESEARCH ARTICLE

Table 6 Outputs from Autonomous Privacy-Preserving Routing (APPR)

Node ID	Traffic Pattern	Privacy Level	Selected Route	Information Leakage (%)	Performance Impact (%)
1	Regular	High	Route 14	2	-5
10	Heavy	Medium	Route 21	3	-3
25	Light	Very High	Route 6	1	-2
40	Moderate	Low	Route 31	4	-4

Table 7 Outputs from Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN)

Node ID	Transaction Volume	Privacy Setting	Effective Route	Privacy Score	Network Load
1	High	Standard	Route 19	90	Medium
10	Medium	Enhanced	Route 12	95	Low
25	Low	Maximum	Route 2	98	Low
40	Very High	Standard	Route 27	89	High

Table 8 Outputs from Homomorphic Encryption-Based Secure Routing (HE-SR)

Node ID	Encrypted Data Size (KB)	Route Chosen	Computation Time (s)	Decryption Time (s)
1	50	Route 13	0.5	0.2
10	40	Route 18	0.4	0.1
25	30	Route 9	0.3	0.1
40	60	Route 33	0.6	0.3

RESEARCH ARTICLE

Table 9 Outputs from Bayesian Privacy-Preserving Routing (BPPR)

Node ID	Observed Data Points	Prior Distribution	Posterior Probability	Routing Decision
1	250	Normal(0.3)	0.75	Route 22
10	200	Normal(0.5)	0.65	Route 16
25	150	Normal(0.8)	0.85	Route 4
40	300	Normal(0.2)	0.55	Route 30

Table 10 Final Outputs Across All Models

Node ID	DR-DQN Path	APPR Route	PP-GABN Route	HE-SR Route	BPPR Decision	Best Path
1	Path 17	Route 14	Route 19	Route 13	Route 22	Route 14
10	Path 29	Route 21	Route 12	Route 18	Route 16	Route 16
25	Path 8	Route 6	Route 2	Route 9	Route 4	Route 4
40	Path 34	Route 31	Route 27	Route 33	Route 30	Route 31

5. FUTURE RESEARCH THREAD

Looking ahead, the potential for further refinement and expansion of these models is vast. One immediate area for future research is the integration of more granular levels of privacy controls, allowing for customizable privacy preserving measures tailored to the specific needs of various applications within different sectors such as finance, healthcare, and public services. Additionally, the scalability of these models is explored in more extensive network simulations or real-world deployments, potentially involving thousands of nodes to better understand the impacts of scale on performance and privacy.

This would also involve developing more sophisticated congestion management strategies to handle increased traffic without degrading service quality. Another promising direction is the exploration of quantum-resistant cryptographic techniques in the context of HE-SR to prepare blockchain infrastructures for the post-quantum era sets. As quantum computing advances, ensuring that blockchain technologies remain secure against quantum threats is crucial. Moreover, the integration of federated learning into models like DR-DQN and APPR could enhance the collaborative aspects of blockchain, allowing decentralized nodes to learn collectively while still preserving the privacy of their individual datasets. This approach would further decentralize the decision-making process in blockchain routing, enhancing both security and efficiency.

Finally, ongoing advancements in AI and machine learning could be harnessed to improve the predictive capabilities of these models, enabling them to anticipate future network states with greater accuracy and adjust routing protocols preemptively. This could lead to even lower latencies and higher throughput, pushing the boundaries of what is currently possible in blockchain network optimization.

In conclusion, the research presented in this paper provides a robust foundation for the next generation of blockchain network technologies, emphasizing privacy and efficiency. The continued exploration and development of these models will be critical in realizing the full potential of blockchain across various domains.

RESEARCH ARTICLE

6. CONCLUSION

The in-depth analysis of the privacy-preserving blockchain routing models discussed in this paper indicates remarkable progress in the security and optimization of blockchain networks. The models proposed herein, Dynamic Routing with Deep Q-Networks (DR-DQN), Homomorphic Encryption-based Secure Routing (HE-SR), Bayesian Privacy-Preserving Routing (BPPR), Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN), and Autonomous Privacy-Preserving Routing (APPR) as a whole meet the fundamental needs of privacy and efficiency in blockchain routing. The test results reveal a significant increase in important performance measures under multiple scenarios designed to mimic real network environments. The model in question lowered mean latency by up to 25% compared to current techniques, and network throughput by up to 30%. Additionally, privacy leakage was significantly lowered, demonstrating a 35% decrease compared to non-Bayesian techniques. This impact was particularly strong in high-privacy scenarios: in these cases, the model-maintained privacy leakage at only 1%. These findings reinforce the effectiveness of combining sophisticated computation methods like machine learning, differential privacy, homomorphic encryption, and Bayesian inference in blockchain routing procedures. The application of these methods allowed the models not just to dynamically learn and adjust under varying network situations but also to maintain strict privacy conditions without sacrificing the operational performance of the network. Further research exploration is quantum-resistant cryptographic techniques in the context of HE-SR to enhance collaborative aspects of blockchain.

REFERENCES

[1] Chhabra, R. Saha, G. Kumar and T. -H. Kim, "Navigating the Maze: Exploring Blockchain Privacy and Its Information Retrieval," in IEEE Access, vol. 12, pp. 32089-32110, 2024, doi: 10.1109/ACCESS.2024.3370857.

[2] S. Banaeian Far and A. Imani Rad, "PP-DENT: A Privacy-Preserving Framework for Blockchain-Based Mobile/Roaming Transactions," in IEEE Networking Letters, vol. 4, no. 4, pp. 204-207, Dec. 2022, doi: 10.1109/LNET.2022.3201987.

[3] Y. Zhang et al., "PACTA: An IoT Data Privacy Regulation Compliance Scheme Using TEE and Blockchain," in IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8882-8893, 1 March1, 2024, doi: 10.1109/JIOT.2023.3321308.

[4] W. Jie et al., "A Secure and Flexible Blockchain-Based Offline Payment Protocol," in IEEE Transactions on Computers, vol. 73, no. 2, pp. 408-421, Feb. 2024, doi: 10.1109/TC.2023.3331823.

[5] K. Zhang, J. Tian, H. Xiao, Y. Zhao, W. Zhao and J. Chen, "A Numerical Splitting and Adaptive Privacy Budget-Allocation-Based LDP Mechanism for Privacy Preservation in Blockchain-Powered IoT," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6733-6741, 15 April15, 2023, doi: 10.1109/JIOT.2022.3145845.

[6] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma and I. You, "Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 710-721, Feb. 2023, doi: 10.1109/JBHI.2022.3187037.

[7] J. Liu et al., "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2231-2242, May 2023, doi: 10.1109/JBHI.2022.3183397.

[8] G. Wu, S. Wang, Z. Ning and B. Zhu, "Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1917-1927, May 2022, doi: 10.1109/JBHI.2021.3123643.

[9] X. Zhang, S. Jiang, Y. Liu, T. Jiang and Y. Zhou, "Privacy-Preserving Scheme With Account-Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 569-581, March 2022, doi: 10.1109/TNSM.2021.3110980.

[10] Y. Qu et al., "Towards Privacy-Aware and Trustworthy Data Sharing Using Blockchain for Edge Intelligence," in Big Data Mining and Analytics, vol. 6, no. 4, pp. 443-464, December 2023, doi: 10.26599/BDMA.2023.9020012.

[11] K. N. Qureshi, G. Jeon, M. M. Hassan, M. R. Hassan and K. Kaur, "Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 7, pp. 7435-7443, July 2023, doi: 10.1109/TITS.2022.3158320.

[12] G. Xu et al., "A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 698-709, Feb. 2023, doi: 10.1109/JBHI.2022.3203577.

[13] Y. Liu et al., "VRepChain: A Decentralized and Privacy-Preserving Reputation System for Social Internet of Vehicles Based on Blockchain," in IEEE Transactions on Vehicular Technology, vol. 71, no. 12, pp. 13242-13253, Dec. 2022, doi: 10.1109/TVT.2022.3198004.

[14] T. Zhang, "Privacy Evaluation of Blockchain Based Privacy Cryptocurrencies: A Comparative Analysis of Dash, Monero, Verge, Zcash, and Grin," in IEEE Transactions on Sustainable Computing, vol. 8, no. 4, pp. 574-582, Oct.-Dec. 2023, doi: 10.1109/TSUSC.2023.3303180.

[15] W. Liang et al., "PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data," in IEEE Transactions on Reliability, vol. 72, no. 2, pp. 586-598, June 2023, doi: 10.1109/TR.2022.3190932.

[16] H. Al-Shaibani, N. Lasla, M. Abdallah and S. Bakiras, "Privacy-Preserving Framework for Blockchain-Based Stock Exchange Platform," in IEEE Access, vol. 10, pp. 1202-1215, 2022, doi: 10.1109/ACCESS.2021.3132690.

[17] J. An, Z. Wang, X. He, X. Gui, J. Cheng and R. Gui, "PPQC: A Blockchain-Based Privacy-Preserving Quality Control Mechanism in Crowdsensing Applications," in IEEE/ACM Transactions on Networking, vol. 30, no. 3, pp. 1352-1367, June 2022, doi: 10.1109/TNET.2022.3141582.

[18] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina and H. Zhong, "DBCPA: Dual Blockchain-Assisted Conditional Privacy-Preserving Authentication Framework and Protocol for Vehicular Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 23, no. 2, pp. 1127-1141, Feb. 2024, doi: 10.1109/TMC.2022.3230853.

[19] C. Xu, Y. Qu, Y. Xiang, T. H. Luan and L. Gao, "An Optimized Privacy-Protected Blockchain System for Supply Chain on Internet of Things," in IEEE Internet of Things Journal, vol. 11, no. 5, pp. 9019-9030, 1 March1, 2024, doi: 10.1109/JIOT.2023.3321889.

[20] F. Daidone, B. Carminati and E. Ferrari, "Blockchain-Based Privacy Enforcement in the IoT Domain," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 3887-3898, 1 Nov.-Dec. 2022, doi: 10.1109/TDSC.2021.3110181.

[21] N. Elisa, L. Yang, F. Chao, N. Naik and T. Boongoen, "A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity," in IEEE Access, vol. 11, pp. 8773-8789, 2023, doi: 10.1109/ACCESS.2023.3239814.

RESEARCH ARTICLE

[22] M. C. Kus and A. Levi, "Investigation and Application of Differential Privacy in Bitcoin," in IEEE Access, vol. 10, pp. 25534-25554, 2022, doi: 10.1109/ACCESS.2022.3151784.
[23] M. Fan, K. Ji, Z. Zhang, H. Yu and G. Sun, "Lightweight Privacy and Security Computing for Blockchained Federated Learning in IoT," in IEEE Internet of Things Journal, vol. 10, no. 18, pp. 16048-16060, 15 Sept.15, 2023, doi: 10.1109/JIOT.2023.3267112.
[24] B. D. Deebak and S. O. Hwang, "Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5897-5916, May 2024, doi: 10.1109/TMC.2023.3315510.
[25] M. Xu, Z. Zou, Y. Cheng, Q. Hu, D. Yu and X. Cheng, "SPDL: A Blockchain-Enabled Secure and Privacy-Preserving Decentralized Learning System," in IEEE Transactions on Computers, vol. 72, no. 2, pp. 548-558, 1 Feb. 2023, doi: 10.1109/TC.2022.3169436.
[26] K. Zhu et al., "Privacy-Aware Double Auction With Time-Dependent Valuation for Blockchain-Based Dynamic Spectrum Sharing in IoT Systems," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6756-6768, 15 April15, 2023, doi: 10.1109/JIOT.2022.3165819.
[27] W. Wang, Y. Wang, P. Duan, T. Liu, X. Tong and Z. Cai, "A Triple Real-Time Trajectory Privacy Protection Mechanism Based on Edge Computing and Blockchain in Mobile Crowdsourcing," in IEEE Transactions on Mobile Computing, vol. 22, no. 10, pp. 5625-5642, 1 Oct. 2023, doi: 10.1109/TMC.2022.3187047.
[28] Y. Chen et al., "DS2PM: A Data-Sharing Privacy Protection Model Based on Blockchain and Federated Learning," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12112-12125, 15 July15, 2023, doi: 10.1109/JIOT.2021.3134755.
[29] A. Lakhan et al., "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 664-672, Feb. 2023, doi: 10.1109/JBHI.2022.3165945.
[30] R. Zhang, R. Xue and L. Liu, "Security and Privacy for Healthcare Blockchains," in IEEE Transactions on Services Computing, vol. 15, no. 6, pp. 3668-3686, 1 Nov.-Dec. 2022, doi: 10.1109/TSC.2021.3085913.
[31] Y. Yang, L. Wei, J. Wu, C. Long and B. Li, "A Blockchain-Based Multidomain Authentication Scheme for Conditional Privacy Preserving in Vehicular Ad-Hoc Network," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8078-8090, 1 June1, 2022, doi: 10.1109/JIOT.2021.3107443.
[32] J. A. Alzubi, O. A. Alzubi, A. Singh and M. Ramachandran, "Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 1080-1087, Jan. 2023, doi: 10.1109/TII.2022.3189170.
[33] C. Lin, X. Huang and D. He, "EBCPA: Efficient Blockchain-Based Conditional Privacy-Preserving Authentication for VANETs," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 1818-1832, 1 May-June 2023, doi: 10.1109/TDSC.2022.3164740.
[34] Y. Yang, J. Wu, C. Long, W. Liang and Y. -B. Lin, "Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9259-9267, Dec. 2022, doi: 10.1109/TII.2022.3177630.
[35] C. Zhang, L. Zhu and C. Xu, "BSDP: Blockchain-Based Smart Parking for Digital-Twin Empowered Vehicular Sensing Networks With Privacy Protection," in IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 7237-7246, May 2023, doi: 10.1109/TII.2022.3223211.
[36] M. M. Islam and H. P. IN, "A Privacy-Preserving Transparent Central Bank Digital Currency System Based on Consortium Blockchain and Unspent Transaction Outputs," in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2372-2386, 1 July-Aug. 2023, doi: 10.1109/TSC.2022.3226120.
[37] S. Zou, J. Xi, G. Xu, M. Zhang and Y. Lu, "CrowdHB: A Decentralized Location Privacy-Preserving Crowdsensing System Based on a Hybrid Blockchain Network," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14803-14817, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3084937.
[38] T. Li et al., "BPT: A Blockchain-Based Privacy Information Preserving System for Trust Data Collection Over Distributed Mobile-Edge Network," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8036-8052, 1 June1, 2022, doi: 10.1109/JIOT.2021.3117971.
[39] O. Samuel et al., "IoMT: A COVID-19 Healthcare System Driven by Federated Learning and Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 823-834, Feb. 2023, doi: 10.1109/JBHI.2022.3143576.
[40] R. Du, C. Ma and M. Li, "Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains," in Tsinghua Science and Technology, vol. 28, no. 1, pp. 13-26, February 2023, doi: 10.26599/TST.2021.9010070.
[41] Tomasz Gorski, “The 1+5 Architectural Views Model in Designing Blockchain and IT System Integration Solutions”, in MDPI, Symmetry 2021, 13(11),2000; https://doi.org/10.3390/sym13112000.

Authors

Hiralal Solunke is a Research Scholar of School of Computer Sciences & Engineering, Sandip University, Nashik, India. His research interests include computer networks, machine learning, artificial intelligence, and Blockchain. This includes Multipath Routing in Computer Network, Data Analysis using Machine Learning and AI. His research has been disseminated in several internationally reputed journals and conferences.

Dr. Pawan Bhaladhare is an Associate Dean at School of Computer Sciences & Engineering, Sandip University, Nashik, India. His research interests include Data Science, computer networks, machine learning, artificial intelligence, and Deep Learning etc.

Dr. Amol Potgantwar, is a Director at School of Computer Sciences & Engineering, Sandip University, Nashik, India. His research interests include Near Field Communication, RFID, Wireless Technology, Machine Learning, artificial intelligence, and Blockchain etc.

Dr. Purushottam R. Patil, Professor at School of Computer Sciences & Engineering, Sandip University, Nashik, India. His research interests include Data Mining, Computer Networks, Machine learning, artificial intelligence, and Blockchain.

How to cite this article:

Hiralal Solunke, Pawan Bhaladhare, Amol Potgantwar, Purushottam R. Patil, “An Implementation of the Iterative Method for Privacy-Preserving Blockchain Networks Using Machine Learning Algorithms”, International Journal of Computer Networks and Applications (IJCNA), 12(6), PP: 1057-1074, 2025, DOI: 10.22247/ijcna/2025/62.