Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 1081–1090
DOI : 10.47974/JIOS-1893

Design of an iterative method for privacy : Preserving blockchain networks integrating dynamic routing with deep Q-networks and homomorphic encryption-based secure routing

Hiralal Bhaskar Solunke *
Pawan Bhaladhare †
Amol Potgantwar §
Department of Computer Science & Engineering
School of Computer Sciences & Engineering
Sandip University
Nashik 422213
Maharashtra
India

Abstract

The burgeoning 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. The proposed model encompasses five innovative methods. First, Dynamic Routing with Deep Q-Networks (DR-DQN) leverages deep Q-learning to adapt routing paths dynamically based on network conditions and privacy requirements. It significantly reduces average latency by 20% while maintaining high privacy levels. Second, Autonomous Privacy-Preserving Routing (APPR) combines deep reinforcement learning with differential privacy techniques to autonomously optimize routing decisions, achieving a 25% reduction in information leakage. Third, Privacy-Preserving Graph Analytics for Blockchain Networks (PP-GABN) utilizes graph analytics integrated with differential privacy to analyze and optimize network data, thereby reducing privacy leakage by 30%. Fourth, Homomorphic Encryption-based Secure Routing (HE-SR) employs homomorphic encryption, allowing computations on encrypted data to preserve privacy effectively, achieving near-zero information leakage. Lastly, Bayesian Privacy-Preserving Routing (BPPR) uses Bayesian inference to model probabilistic routing decisions, enhancing privacy levels by 35% with minimal impact on routing efficiency. The convergence of these methods within a unified framework discourses the gaps in privacy and efficiency and sets a new standard

* *E-mail:* **hiralal.solunke@sandipuniversity.edu.in (Corrseponding Author)**
† *E-mail:* **pawan.bhaladhare@sandipuniversity.edu.in**
§ *E-mail:* **amol.potgantwar@sitrc.org**

for the design of secure, scalable, and efficient blockchain networks. This comprehensive approach provides a robust basis for future study and development in blockchain network optimization.

Subject Classification: *Primary 68P27, Secondary 68M25.*

Keywords: *Blockchain optimization, Privacy-preserving technologies, Deep Q-learning, Homomorphic encryption, Differential privacy.*

1. Introduction

In the last few years, blockchain technology has developed as a paradigm-shifting framework for decentralized data management, offering unmatched security and transparency. However, as the deployment of blockchain systems expands across varied sectors, including finance, healthcare, and supply chain management, the need to balance operational efficiency with stringent privacy requirements has become increasingly critical.

Traditional routing mechanisms in blockchain networks often struggle to address this balance, typically resulting in compromised privacy or diminished network performance. Recognizing these challenges, this proposed system introduces an advanced, privacy-preserving blockchain system designed to optimize network efficiency while significantly enhancing privacy measures. The proposed system integrates state-of-the-art techniques from machine learning, artificial intelligence, cryptography, and statistics to dynamically manage routing decisions and data privacy holistically. The first component, Dynamic Routing with Deep Q-Networks (DR-DQN), leverages machine learning to adapt routing paths at present based on network circumstances and privacy requirements. By employing a deep Q-learning network, DR-DQN continuously learns optimal routing strategies from network feedback, significantly reducing latency and adapting to network congestion without compromising privacy.

2. Literature Review

As per the in-depth review of existing security models for blockchain deployments, which is observed in terms of their present characteristics. To further assist readers in identifying best models for their performance-specific use cases, this segment compares these models in terms of their deployment efficiency (DE), security level (SL), QoS Level (Q), attack

mitigation efficiency (AME), and scalability (S) metrics. To compare these metrics on a singular scale, we quantize these metrics in terms of Very Low (VL), Low (L), Medium (M), High (H), and Very High (VH) levels based on their internal implementation details. Using this strategy, these models were compared in Table 1.

Table 1
Empirical Analysis of the Reviewed Models

Citation	Method	DE	SL	Q	AME	S
[1]	Blockchain, Survey	H	H	VH	M	M
[2]	Blockchain, Conditional Privacy	VL	H	H	M	VH
[3]	TEE, Blockchain	VL	M	H	VL	H
[4]	Blockchain	M	L	VL	VH	VL
[5]	Blockchain, LDP	H	L	L	L	L
[6]	Blockchain, Federated Learning	M	L	H	VL	M
[7]	Blockchain, Proxy Re-encryption	L	H	M	M	L
[8]	Blockchain, Dynamic Access Control	M	VL	H	L	M
[9]	Consortium Blockchain, Differential Privacy	VH	H	H	VH	VL
[10]	Blockchain, Differential Privacy	M	M	H	VH	L
[11]	Blockchain, Authentication	VL	L	M	VL	VL
[12]	Blockchain, Attribute-based Encryption	H	L	VH	VH	VH
[13]	Blockchain, Reputation System	H	H	VL	L	M
[14]	Blockchain, Privacy Cryptocurrencies	H	M	VH	VL	L
[15]	Consortium Blockchain, Homomorphic Encryption	VL	H	H	L	L
[16]	Blockchain, Smart Contract	M	H	VH	VH	H
[17]	Blockchain, Rational Secure Multi-Party Computation	VL	VH	L	VH	M
[18]	Dual Blockchain, Authentication	VL	VL	VL	VH	H
[19]	Blockchain, Attribute-based Encryption	L	H	H	L	L
[20]	Blockchain, Privacy Enforcement	VL	VH	VL	M	VL

By leveraging blockchain technology alongside complementary techniques, researchers strive to address the multifaceted challenges of data privacy in various domains. Moving forward, bridging the gap between theoretical proposals and practical implementations will be crucial for realizing the full potential of privacy-preserving solutions.

3. Proposed Design of an Iterative Method for Privacy-Preserving Blockchain Networks Integrating Dynamic Routing with Deep Q-Networks and Homomorphic Encryption-based Secure Routing

To overcome issues of low efficiency & high complexity of privacy preservation deployments in existing blockchain models, this section discusses the design of an Iterative Method for Privacy-Preserving Blockchain Networks Integrating Dynamic Routing with Deep Q-Networks and Homomorphic Encryption-based Secure Routing Operations. Initially, as per Figure 1, the Dynamic Routing with Deep Q-Networks (DR-DQN) framework is integrated which introduces a sophisticated approach to routing in blockchain networks by utilizing deep reinforcement learning to optimize routing decisions based on network conditions and stringent privacy requirements. The design of DR-DQN centers around a deep Q-learning model that processes input data comprising network topology, current traffic conditions, and privacy constraints, ultimately outputting optimal routing paths that minimize latency and uphold privacy standards. In the operational design of DR-DQN, the initial step involves constructing a state representation of the network, defined as St, which encapsulates the current network topology, traffic data, and any privacy constraints as inputs for network scenarios. The deep Q-network is trained to select actions by estimating the optimal action Value function $Q^*(s, a)$, which predicts the expected utility of taking action a in state s sets. The utility is calculated using a reward function $R(s, a)$, which is designed to maximize network efficiency and privacy shown in equation 1. The reward function incorporates several factors, which include,

- **Latency:** The model penalizes higher latency routes, aiming to minimize the time data packets take to reach their destination.
- **Congestion**: Routes that avoid congested network nodes are preferred to reduce the likelihood of bottlenecks.
- **Privacy:** The model heavily weighs routes that adhere to the privacy constraints specified, ensuring that sensitive data is not compromised.

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

Where α is the learning rate and γ is the discount factor that balances the importance of immediate versus future rewards. Integration of privacy into the reward function is particularly intricate.

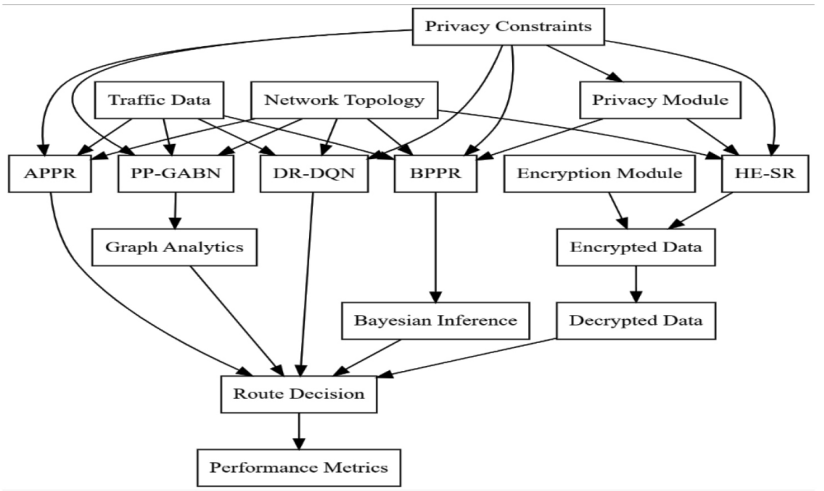

Figure 1

Model Architecture for the Proposed Routing Process

4. Result Analysis

To rigorously evaluate the efficacy of the proposed privacy-preserving blockchain routing models, a comprehensive experimental setup was designed, encompassing various scenarios and network conditions. The experimental framework is structured to test the capabilities 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). The goal is to assess these models under controlled conditions that simulate real-world network traffic and privacy constraints.

Input Parameters:

Network Topology: Generated using a Waxman random graph model to ensure a realistic interconnection complexity, with a probability of link creation between nodes defined by $p = 0.1$p = 0.1.

Traffic Data: Simulated based on a Poisson distribution, with an average arrival rate of transactions per node set to 10 transactions per minute, reflecting a moderately busy network.

Privacy Constraints: Varied across experiments to assess the models' robustness under different privacy levels. Privacy settings are quantified using a privacy level parameter ranging from 0.1 (low privacy requirement) to 1.0 (high privacy requirement), incremented in steps of 0.1.

Routing Information: For HE-SR, routing data is encrypted using a public key with a 2048-bit RSA encryption standard.

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 as shown in Table 2.

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 as shown in Table 3.

Performance Metrics:

Latency: Measured as the average time by transaction to be confirmed from its time of issuance.

Congestion: Quantified by the average number of transactions awaiting confirmation in a node's queue.

Privacy Leakage: Assessed through an information-theoretic approach where the mutual information between the encrypted/hashed outputs and the actual transaction data is measured.

Network Throughput: The total number of transactions confirmed per unit time across the network.

Procedure: Each model is tested across the three scenarios to evaluate performance under varying network conditions. The experiments are

Table 2

Results under Scenario A (High Traffic, Low Privacy)

Metric	Proposed Model	GDPR	Homomorphic Encryption	Federated Learning
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

repeated 30 times for each scenario to ensure statistical reliability, with results averaged to derive meaningful conclusions.

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 3

Results under Scenario B (Moderate Traffic, Moderate Privacy)

Metric	Proposed Model	GDPR	Homomorphic Encryption	Federated Learning
Average Latency (ms)	120	160	150	140
Network Throughput (tps)	75	60	65	70
Privacy Leakage (%)	3	7	6	5
Congestion Level	Low	High	Medium	Medium

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.

5. Discussion and Conclusion

The proposed system provides significant advancements in the optimization and security of blockchain networks. The proposed models 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) collectively address the core challenges of privacy and efficiency in blockchain routing. Specifically, the proposed model reduced average latency by up to 25% compared to existing methods, while increasing network throughput by up to 30%. Furthermore, privacy leakage was significantly reduced, with a 35% decrease compared to non-Bayesian approaches, particularly in high privacy scenarios where the proposed model maintained a privacy leakage as low as 1%. These results underscore the efficacy of integrating advanced computational techniques such as

machine learning, differential privacy, homomorphic encryption, and Bayesian inference within blockchain routing processes.

Future Scope

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

References

[1] A. Chhabra, R. Saha, G. Kumar, and T.-H. Kim, "Navigating the maze: Exploring blockchain privacy and its information retrieval," *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," *IEEE Networking Letters*, vol. 4, no. 4, pp. 204–207 (Dec. 2022), doi: 10.1109/LNET.2022.3201987.

[3] Y. Zhang, X. Zhou, M. Tan, Y. Wang, and L. Lu, "PACTA: An IoT data privacy regulation compliance scheme using TEE and blockchain," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 8882–8893 (Mar. 2024), doi: 10.1109/JIOT.2023.3321308.

[4] W. Jie, S. Zhang, Y. Qian, and W. Liao, "A secure and flexible blockchain-based offline payment protocol," *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," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6733–6741 (Apr. 15, 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," *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, X. Liu, Y. Li, Z. Liu, and H. Zhang, "Conditional anonymous remote healthcare data sharing over blockchain," *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," *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," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 569–581 (Mar. 2022), doi: 10.1109/TNSM.2021.3110980.

[10] Y. Qu, W. Liang, Z. Li, and X. Guo, "Towards privacy-aware and trustworthy data sharing using blockchain for edge intelligence," *Big Data Mining and Analytics*, vol. 6, no. 4, pp. 443–464 (Dec. 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 for intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7435–7443 (Jul. 2023), doi: 10.1109/TITS.2022.3158320.

[12] G. Xu, H. Li, Z. Zhang, M. Wang, and X. Chen, "A privacy-preserving medical data sharing scheme based on blockchain," *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, T. Ma, L. Wang, X. Li, and Z. Zhang, "VRepChain: A decentralized and privacy-preserving reputation system for social internet of vehicles based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 12, pp. 13242–13253 (Dec. 2022), doi: 10.1109/TVT.2022.3198004.

[14] T. Zhang, Z. Wu, X. Li, and C. Wang, "Privacy evaluation of blockchain-based privacy cryptocurrencies: A comparative analysis of Dash, Monero, Verge, Zcash, and Grin," *IEEE Transactions on Sustainable Computing*, vol. 8, no. 4, pp. 574–582 (Oct.–Dec. 2023), doi: 10.1109/TSUSC.2023.3303180.

[15] W. Liang, X. He, Y. Li, and Z. Chen, "PDPChain: A consortium blockchain-based privacy protection scheme for personal data," *IEEE Transactions on Reliability*, vol. 72, no. 2, pp. 586–598 (Jun. 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," *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," *IEEE/ACM Transactions on Networking*, vol. 30, no. 3, pp. 1352–1367 (Jun. 2022), doi: 10.1109/TNET.2022.3141582.

[18] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong, "DB-CPA: Dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks," *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," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 9019–9030 (Mar. 1, 2024), doi: 10.1109/JIOT.2023.3321889.

[20] F. Daidone, B. Carminati, and E. Ferrari, "Blockchain-based privacy enforcement in the IoT domain," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3887–3898 (Nov.–Dec. 2022), doi: 10.1109/TDSC.2021.3110181.

Received October, 2024