Journal of Integrated
SCIENCE & TECHNOLOGY

Framework for dynamic block sizing in secured and efficient transaction systems

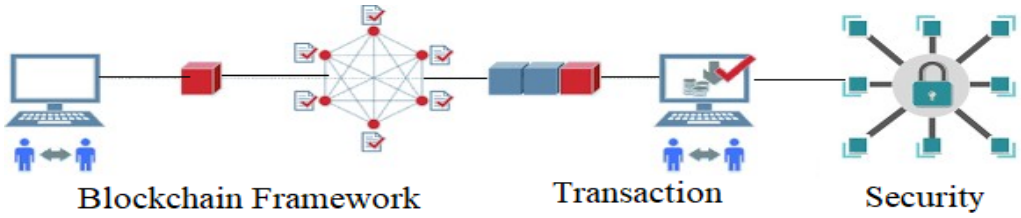
Priyanka Chorey,* Neeraj Sahu

Computer Science and Engineering, G. H. Raisoni University, Amravati, India.

Received on: 12-Dec-2023, Accepted and Published on: 26-Feb-2024

Article

ABSTRACT



In the age of the Internet of Things (IoT), secure online payment systems are crucial, especially in the banking sector. This study introduces an innovative hybrid access control-enabled consensus algorithm within a checkpoint-enabled blockchain model designed for secure banking transactions. Utilizing smart contracts and an advanced consensus algorithm, the model establishes a robust network security framework while expediting transaction processes. Incorporating checkpoints ensures secure block mining, boosting network security and scalability. Smart contracts automate transaction agreements, significantly reducing processing time. The algorithm offers tailored access control, exclusively authorizing legitimate users. To validate the model, metrics such as transaction recovery time, memory usage, and responsiveness were measured for varying block sizes. Results demonstrated notable efficiency with reduced transaction recovery time (10.88 ms), minimal memory usage (108.17 kb), and enhanced responsiveness (33.55 ms) compared to existing methods. Implementing this model can enhance user trust, safeguard data, and streamline transactions, contributing to a more secure and seamless banking experience for all stakeholders.

Keywords: IoT Security, Blockchain, Hybrid Access Control, Smart Contracts, Secure Banking Transactions

INTRODUCTION

In nearly every region of the nation, people carry mobile devices with advanced computing capabilities. This trend has contributed to the advancement of secure online transmissions..[1,2] Presently, banks worldwide offer mobile banking services to their entire clientele, enabling bill payments, balance checks, and numerous other conveniences directly accessible from users' hands.[3] A decentralized privacy-preserving mobile payment system using blockchain and threshold anonymous credentials, countering risks associated with centralized third-party payment platforms.[4] However, the proliferation of app services and online communication platforms poses risks to users' confidential data, exposing them to identity theft and misuse.[5] Enhancing security is essential to bridge the gap between online and mobile banking for more efficient transactions.[6] Traditional transaction methods relying on PIN codes are increasingly vulnerable to hacking by fraudulent entities. Consequently, ongoing technological advancements aim to enhance security and transaction efficiency.[7] Current cloud storage relies on large providers, functioning as untrusted third parties. A multi-user access control system using blockchain technology for stable, distributed data processing, enhancing security and privacy while addressing issues like high costs and software quality in traditional cloud storage systems.[8]

Near-field communication (NFC) is crucial in the Internet of Things (IoT), facilitating mobile payments. Despite its popularity, security issues persist, necessitating blockchain integration. This paper explores enhancing NFC security through blockchain technology, addressing concerns like double-spending and ensuring fair, direct transactions without intermediaries.[10] This technology operates as a distributed public ledger governed by predefined rules agreed upon by network participants.[11] It offers a trustless environment for transactions, securing data immutably through cryptographic linkage and validation across a decentralized network using a consensus protocol.[12] The integration of blockchain technology and the Internet of Things (IoT) to address security and privacy issues. It covers principles, challenges, survey methodology, findings, categorization of applications, and future considerations for integration.[13] This technology addresses conventional database synchronization challenges. Various consensus protocols exist for Blockchain, with Proof-of-Work (PoW) being the most widely used, notably by Bitcoin and Ethereum (although Ethereum is transitioning to Proof-of-Stake).

*Corresponding to: Priyanka Chorey, Department of Computer Science and Engineering, G. H. Raisoni University, Amravati, Maharashtra, INDIA
Email: priyankachorey07@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(5), 816.*
URN: NBN:sciencein.jist.2024.v12.816

PoW requires participants to solve complex cryptographic puzzles to add data to the ledger, deterring malicious activities due to the significant resources required for block mining.[14]

The main aim of the research is to perform secure online transactions in banking sector with high privacy and security using the checkpoint enabled blockchain network.[15] A blockchain-based trusted suite (TS) for multi-agent systems (MAS) in energy trading. It addresses dynamic behavior challenges, enhances cooperation, and ensures confidentiality in a smart grid. Simulation results demonstrate its superiority over existing models.[26,29] Ethereum and Hyperledger stand out as blockchain platforms that facilitate the implementation of smart contracts, allowing for self-executing contractual agreements without the need for centralized authority.[16] Cloud computing, though advantageous, faces security issues. Blockchain offers a decentralized trust infrastructure, solving challenges like high costs and network congestion in the typical centralized cloud trust model.[17] The enabling of the smart contract helps in improving the transparency, speed and reduces the cost and the consensus algorithm used in hybrid access control validates and evaluate the transaction without third parties. The main contribution of the research is as follows:

Checkpoint enabled blockchain: The scalability and security of the network is enhanced using the checkpoint and the checkpoint allows only the users who have the information about the preceding blocks. This avoided the illegal users, who try to embed blocks in the network. The checkpoints enabled in the blockchain also helps in dealing with storage issues by permanently storing the data in the blockchain.

Hybrid access control based consensus algorithm: The access control mechanism using consensus algorithm achieved reliability, and verified the users and provided authentication. An agreement is maintained for each outcome, which helps in avoiding legal obligations. A new block initiated for transactions helps in obtaining better efficiency in transactions and provides high security with low complexity.

Checkpoint functionality within the blockchain serves to enhance the scalability and security of the network. It influences the mining process, which involves integrating blocks into the distributed public ledger containing existing transactions. Currently, the miner mines the block by deriving the desired hash function through hashing the nonce, and in checkpoint, the hashing is performed with all the previous blocks in the network, which is predefined by the checkpoint parameter [27]

Inclusion of blocks in the Checkpoint based blockchain architecture: Initially, the blockchain network consists of the genesis block and therefore, the checkpoint parameter is zero and when subsequent blocks are added then, the checkpoint parameter is varied, which is denoted by and this attribute is represented as checkpoint blocks. During the mining process, the miner is required to hash all blocks as dictated by the checkpoint parameter. Upon the addition of a new block to the blockchain, the miner must hash not only the new block but also include and hash the specified number of blocks according to the checkpoint size to derive the target hash string for the current block at any given time.[28]

Smart contract: Blockchain are trustless network due to the fact that the networks allow third parties to perform transactions. This initiates a path for the intermediaries to perform illegal actions more easily. To avoid these smart contracts are enabled for maintaining transparency, immutability and security. The smart contract is a computer code that comprised of set of rules embedded in the blockchain that enables proper, distributed, highly automated workflows.[2]

Challenges

- The Blockchain encompasses an extensive volume of transactional data, with each block requiring substantial storage space. The interconnection of numerous blocks to form the blockchain contributes significantly to storage challenges.
- Scalability poses another concern as the increasing number of blocks within the blockchain strains system capacity, hampering the system's ability to enhance speed. Consequently, this escalation negatively impacts the overall performance level of the system.
- Data immutability has always been one of the biggest disadvantages of the blockchain based transaction models
- There is no way to back up the files or folders in P2P secure transaction.

The current study is meant to explore and evaluate the various secure transaction in banking using the blockchain technology to obtain deep insight into blockchain techniques along with designing and development of an online transaction model-based on blockchain-enabled check point approach.

LITERATURE REVIEW

Many researchers are currently engaged in leveraging blockchain technology to create secure systems. However, there is a limited body of literature on the exploration of the blockchain-based checkpoint approach. Consequently, efforts are being made to identify relevant literature and delve into developing a more secure system.

Uzair J. et al.[18] conducted a study on the significance of the Industrial Internet of Things (IIoT) in realizing Industry 4.0. They highlighted the limitations posed by network scalability and robust security in this context. The traditional structure of blockchain, along with the Proof-of-Work (PoW) consensus, was deemed inadequate to address these constraints. The scholars suggested an alternative blockchain structure that combines the delayed Proof of Work (dPoW) consensus with a checkpoint mechanism.Unlike conventional PoW-based mining, the dPoW operates with fluctuating mining difficulty levels, enabling efficient scaling in IIoT environments with increased communication traffic. Additionally, the checkpoint system enhances architecture security by intensifying attack complexity. These features allow the proposed model to accommodate escalating transaction traffic in industrial networks while bolstering security with minimal block mining time.

Vuppala A. et al. [19] explains due to technological advancements, the data transfer rate via cryptographic devices like smart cards is surging, rendering them susceptible to attacks. Cryptography, with its diverse algorithms, safeguards data, with Triple Data Encryption Standard (Triple-DES) employing the Data Encryption Standard

(DES) block thrice, enhancing key size to 192 bits. However, Triple-DES faces vulnerabilities in key generation, facilitating cryptanalysis. Addressing this, the FORTIS algorithm enhances sub-key generation, reducing leakage power glitches by approximately 53.3%. Power traces from the key schedule algorithm exhibit uniform operations, making it challenging for attackers, leading to an 86.6% reduction in guessing entropy probability.

Silenskyte A et. al.[20] proposed disruptive technologies fuel digital globalization, prompting a crucial interdisciplinary exploration of digital connectivity in international business (IB). Focused on blockchain-based digital connectivity, our research delves into its role in shaping value within international digital platforms and ecosystems (DPEs). Through empirical analysis across diverse international DPEs utilizing various blockchain technologies, we establish a typology illustrating how distinct blockchain types foster different connectivity, leading to varied value creation approaches. This nuanced understanding refines explanations for blockchain adoption in DPEs, unveiling three new DPE types. Our interdisciplinary approach also sheds light on why certain blockchain features, theoretically beneficial, may not consistently support value creation in the IB-DPE model.

Alcaraz C. et al.[21] In their work, represented a checkpoint model focused on a collaborative cyber-physical network incorporating reliable elements. This model oversees the distribution of warning replicas to guarantee sufficient data redundancy for detecting faults and intrusions within checkpoints. The study incorporated the utilization of graph theory and control theory to define the application context, highlighting the effectiveness of power-law distributions in accommodating checkpoint-based methodologies. Future work entails incorporating anomaly-based detection techniques and analyzing large datasets using fog-computing systems for local processing support.

Wu C. et al.[22] explicate digital signatures, crucial in cryptography, find broad applications in e-commerce, authentication, and cloud computing. Certificateless Public Key Cryptography (PKC) addresses certificate management issues in traditional PKI and eliminates key-escrow problems in identity-based PKC. However, a recent Certificateless Signature (CLS) scheme by Kyung-Ah Shim claimed provable security but falls prey to a concrete Type I adversary attack. We propose an enhanced CLS scheme, more efficient and with shorter signatures, offering improved resistance against such attacks, surpassing both the original and recent CLS schemes in precomputation scenarios.

Toorajipour R. et al.[23] developed Third-party involvement in business transactions introduces challenges like heterogeneity, complex processes, information leakage risks, and increased costs. Addressing these issues, our study introduces a novel mechanism for international trade. Utilizing Business Process Model and Notation (BPMN) 2.0 standards, we propose a blockchain technology-based letter of credit (BTLC) system. This system leverages blockchain and smart contracts to enhance the efficiency and security of letters of credit in business transactions.

Qian Y. et. al. [24] addresses the growing Internet of Things (IoT) offers convenience in diverse fields, yet poses security risks. The challenge by examining the three IoT layers – perception, network, and application. Qian Y. et. al.[24] identify security concerns within each layer and propose a comprehensive blockchain-based security management scheme for the entire lifecycle of IoT devices. Open research problems and future directions are also outlined to guide further exploration in this evolving landscape.

Ali A et al.[25] explored the evolution of smartphones, with their customizable configurations and diverse capabilities, has transformed technology use. This paper introduces NFC-Stego, a data hiding technique leveraging Near Field Communication in Android smartphones. Addressing a crucial challenge of recovering deleted cover-files, the proposed method enhances security. Experimental results affirm NFC-Stego as a robust, user-friendly system, capable of securely concealing substantial data with high imperceptibility.

The table 1 presents an summery of various methods discuss earlier for enhancing security and efficiency in transactional systems, particularly within the context of blockchain technology. Each method offers unique advantages while also presenting certain drawbacks that need consideration. These methods demonstrate the ongoing efforts to enhance transactional security, privacy, and efficiency. While they offer notable advantages such as improved security features and decentralized frameworks, they also exhibit limitations, including potential delays in transactions, reduced data transfer rates, and issues related to storage and viewing account balances.

Table 1 Summery of related works

Author	Method	Advantage	Disadvantage
Uzair Javaid et. al. [18]	Decentralized, Secure, and Flexible Lightweight Payment System (BPS)	The blockchain based payment system prevent the transaction from an unauthorized access and can store the whole transaction securely	Users and administrators on this system will not be able to see the balance from users accounts.
Vuppala A. et al. [19]	TripleDES encryption	Enhances system efficiency by broadening its utility and bolstering security measures.	There is the chance for alteration in the transaction as it fails to include blockchain technology.
Silenskyte A et. al [20]	Blockchain based using a new connectivity technology	This model achieves accessible, transparent and secure	There is a possibility of mobile transaction delay.
Alcaraz C. et.al [21]	QoS-aware Secure Transaction Framework using Blockchain Mechanism	In Quality of Service (QoS)-conscious transactions, users.	Slow data transfer rate
Wu C et. al.[22]	Improved certificate less signature CLS scheme.	This model ensures the secure processing of mobile device payments in vulnerable public communication networks.	The bilinear pairing operation is still used for signature verification

Toorajipour R et. al. [23]	A Blockchain-Based peer to peer (P2P) Transaction Method	This model effectively solves the information leakage issue	The is a chance for transaction delay if more people or nodes joins the network
Qian Y. et. al. [24]	Enhancing IOT Security via Decentralized Data Privacy	Protected from cyber attackers or intruders, data can be segregated into distinct blocks, making it challenging to pinpoint specific information.	The third party centered, and achieve the high efficiency of processing. are the main drawback
Ali A. et al. [25]	NFC into smartphones	A key data hiding challenge by securely connecting and restoring deleted files.	This offers low data transfer rate

Research Gap Identified

The banking sector holds immense significance in our daily lives. However, during transactions and interactions involving bank policies, both customers and banks encounter numerous challenges due to fraudsters and criminals, leading to heightened risks of deception. Hence, the detection of such fraudulent activities becomes crucial.

- A fundamental issue in banking services revolves around inadequate data protection and security measures, particularly in the verification and transmission of data.
- Due to the existence of vast databases in most systems, ensuring data ownership and privacy is a crucial priority. This involves implementing measures to protect datasets from unauthorized alterations. Restrictions are in place for remote access, and stringent controls are applied to personnel conducting reviews.
- Occasionally, information may be incorrect, or users may face difficulties accessing any information due to the absence of an online connection.
- Securing transaction-related data online poses a significant challenge in the absence of adequate security measures.

RESEARCH METHODOLOGY

Parameter metrics

Transaction Recovery Time: This metric measures the time taken by each algorithm to recover transactions in a system. Lower transaction recovery times generally indicate better efficiency and faster processing of transactions. By comparing transaction recovery times across different algorithms, it can assess the speed and efficiency of each algorithm in handling transactions.

Memory Usage: Memory consumption is a critical factor in evaluating the practicality and resource efficiency of algorithms. By measuring memory usage, researchers can determine how much memory each algorithm consumes to perform its operations. Lower memory usage indicates better efficiency in resource utilization.

Responsiveness: Responsiveness refers to the speed at which an algorithm can process or respond to requests or transactions. It measures the time taken by an algorithm to complete its tasks. A more responsive algorithm tends to provide quicker processing of transactions or operations. The effectiveness of the research is established by evaluating these metrics concerning the number of blocks.

Number of Blocks: The number of blocks in a blockchain affects its size and complexity. Testing algorithms with varying block counts allows to observe how they perform in different blockchain structures and sizes.

By conducting comparisons across these metrics and parameters (blocks), it can provide a comprehensive evaluation of the proposed HACBCA against other established cryptographic algorithms. This helps in understanding its strengths, weaknesses, scalability, and efficiency in real-world scenarios, thereby establishing the effectiveness of the proposed algorithm in handling varying workloads and maintaining performance across different parameters.

RESULTS AND DISCUSSION

The comparison likely involves defining a set of methodologies and approaches to evaluate the algorithms. Assessing the security features offered by each algorithm, including encryption strength, resistance against attacks, and robustness. Measuring various performance metrics such as transaction time, memory usage and responsiveness to determine how efficiently the algorithms handle transactions and operations. Analyzing resource utilization metrics like memory usage and scalability to understand the algorithms' practical feasibility and economical aspects.Evaluating the complexity of implementation, operational complexity, and ease of integration into existing systems or frameworks. Utilizing methods to analyze collected data, compare results, and draw meaningful conclusions from the comparisons made between the algorithms.The main aim is to provide a comprehensive assessment of their strengths, weaknesses, and suitability for specific applications, thereby establishing the effectiveness and practicality of the proposed Hybrid Access Control Enabled Consensus Algorithm. The comparison between the proposed Hybrid Access Control Enabled Consensus Algorithm (HACBCA) with Triple DES encryption (Triple DES), Hash-Based Secret Key Encryption (HBSK), Certificate-less Signature Scheme (CLS), and Checkpoint Enabled Scalable Blockchain Architecture (CESBA) likely involved various methodologies and metrics to establish its effectiveness.

Comparative analysis based on block size

The structured representation of the analysis based on different block sizes (20, 40, 60, 80, 100) for transaction recovery time of various methods - Triple DES encryption algorithm, hash-based secret key encryption algorithm (HBSK), CLS, CESBA, and the proposed method hybrid access control blockchain-based consensus algorithm (HACBCA) as shown in table 2.

Table 2 Results of Blocksize verses Transaction Recovery Time

Block Size	20	40	60	80	100
Algorithms	Transaction Recovery Time in ms				
Triple DES	0.90	0.91	26.88	28.88	30.88
HBSK	0.89	0.89	21.88	23.88	25.88
CLS	0.88	0.88	16.88	18.88	20.88
CESBA	0.86	0.87	11.88	13.88	15.88
HACBCA	0.85	0.86	6.88	8.88	10.88

From figure 1 higher the block size, the longer it takes for transactions to recover across all algorithms. Different algorithms exhibit varying degrees of sensitivity to block size changes. For instance, Triple DES shows relatively steady and minor increases in Transaction Recovery Time with larger block sizes compared to HACBCA, which demonstrates more significant time increases as block size grows. Algorithms like HACBCA showcase a notable sensitivity to block size changes, resulting in a more rapid escalation of Transaction Recovery Time as the block size expands.

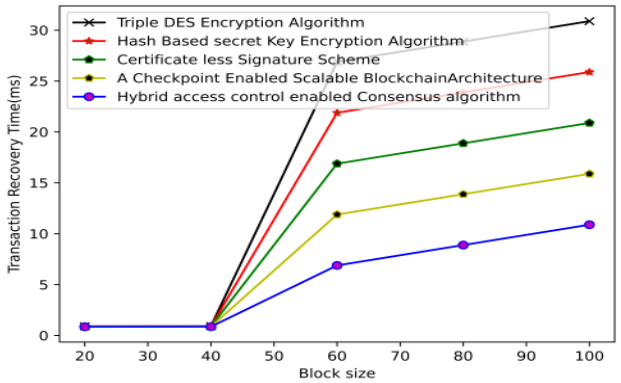


Figure 1 Block Size verses Trasaction Recovery Time

The data from table 2 portrays how alterations in block size directly impact Transaction Recovery Time across different algorithms. It highlights the importance of considering block size implications when choosing or designing an algorithm for transaction processing, as larger block sizes tend to elongate transaction recovery durations, potentially influencing the efficiency and speed of transactional processes within a given system or framework.

Table 3 Results of Blocksize verses Memory Usage

BlockSize	20	40	60	80	100
Algorithms	Memory Usage in KB				
Triple DES	109.22	110.22	110.30	110.02	109.74
HBSK	109.04	109.73	109.98	109.99	109.31
CLS	108.72	109.38	109.76	109.05	109.19
CESBA	108.63	109.07	109.71	108.80	108.88
HACBCA	107.18	107.91	109.46	108.40	108.17

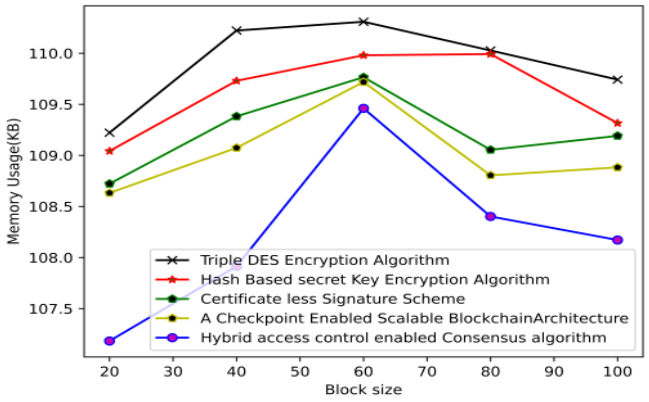


Figure 2 Block size verses Memory Usage

This data showcases in table 3 the memory usage for different algorithms at specific block sizes. It illustrates how the memory requirements change with varying block sizes for each encryption or consensus algorithm. From the data, it can be observed that the memory usage differs among algorithms at different block sizes.

Figure 2 shows at block size 20, the HACBCA algorithm has the lowest memory usage compared to other algorithms. The memory usage tends to fluctuate for each algorithm as the block size changes. In Triple DES and HBSK, there is a slight increase in memory usage with an increase in block size, while others may display different trends. The CESBA algorithm tends to maintain relatively consistent memory usage across different block sizes.

Table 4 displays the relationship between different block sizes (ranging from 20 to 100) and their corresponding Responsiveness (measured in milliseconds) for various algorithms: Triple DES, HBSK, CLS, CESBA, and HACBCA. Responsiveness, in this context, refers to the time taken by an algorithm to respond or execute a task within a given block size configuration. The table illustrates how changes in block size impact the responsiveness of each algorithm.

Across all algorithms, from figure 3 , as the block size increases from 20 to 100, there are fluctuations in the responsiveness values. For Triple DES, HBSK, and CLS algorithms, there is a general trend of increased responsiveness with larger block sizes, indicating that as the block size grows, these algorithms take more time to respond to tasks. CESBA shows a varied pattern where the responsiveness fluctuates with changing block sizes, demonstrating that its responsiveness is less affected by block size alterations compared to other algorithms.

Table 4 Results of Blocksize verses Responsiveness

Block Size	20	40	60	80	100
Algorithms	Responsiveness in ms				
Triple DES	46.71	54.29	79.99	108.09	138.43
HBSK	44.93	53.17	56.74	53.07	56.75
CLS	26.89	50.13	50.34	51.87	51.05
CESBA	26.84	31.03	32.23	35.10	35.09
HACBCA	26.20	26.96	26.43	27.17	33.54

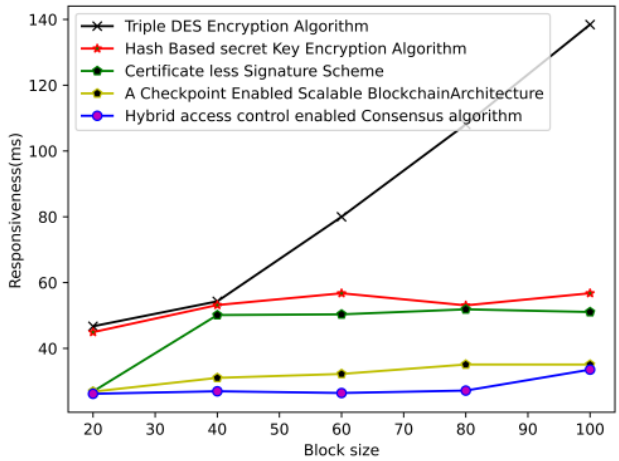


Figure 3 Blocksize verses Responsiveness

HACBCA exhibits a slightly different behavior, with fluctuations in responsiveness that do not consistently increase with larger block sizes. It initially shows a decrease in responsiveness before rising again with further block size increments.

DISCUSSION

The comprehensive assessment of the proposed Hybrid Access Control Enabled Consensus Algorithm (HACBCA) against existing algorithms involves an in-depth analysis of various methodologies and metrics, including security features, performance metrics, resource utilization, complexity of implementation, and practical feasibility.

Security Features: The security of any algorithm is of paramount importance in transaction systems. In the context of encryption strength, the comparison considered the Triple DES encryption algorithm, Hash-Based Secret Key Encryption (HBSK), Certificate-less Signature Scheme (CLS), Checkpoint Enabled Scalable Blockchain Architecture (CESBA), and HACBCA. While the provided data focuses more on performance metrics, it is crucial to note that encryption strength and resistance against attacks are critical aspects that are assumed to be maintained across algorithms for fair comparison.

Transaction Recovery Time: The analysis based on block size reveals insights into the Transaction Recovery Time across different algorithms. As presented in Table 2 and Figure 1, it is evident that larger block sizes generally result in longer transaction recovery times for all algorithms. However, the sensitivity of each algorithm to block size changes varies. HACBCA, in particular, exhibits a more significant increase in Transaction Recovery Time with larger block sizes compared to Triple DES, which shows a steadier rise. This suggests that HACBCA may have a more pronounced impact on efficiency as block size grows, emphasizing the importance of considering block size implications when designing or choosing an algorithm.

Memory Usage: Table 3 and Figure 2 provide insights into the memory usage of different algorithms at varying block sizes. HACBCA consistently demonstrates lower memory usage, especially at smaller block sizes. The fluctuations observed in memory usage across block sizes for Triple DES and HBSK may indicate their sensitivity to changes, while CESBA maintains relatively consistent memory usage. The presented data underscores the importance of memory efficiency, especially in resource-constrained environments, and positions HACBCA as a promising algorithm in this regard.

Responsiveness: Table 4 and Figure 3 highlight the responsiveness of algorithms across different block sizes. The general trend indicates that as block size increases, Triple DES, HBSK, and CLS algorithms exhibit increased responsiveness, implying a longer time taken to respond to tasks. CESBA, on the other hand, shows a more varied pattern, suggesting that its responsiveness is less affected by block size alterations. Notably, HACBCA displays fluctuations in responsiveness, initially decreasing before rising again with further block size increments. This unique behavior may be attributed to the adaptive nature of HACBCA in handling varying block sizes.

Practical Feasibility: The consideration of memory usage, scalability, and responsiveness contributes to the assessment of the algorithms' practical feasibility. Lower memory usage, consistent performance, and adaptive responsiveness position HACBCA as a promising solution in terms of resource efficiency. Scalability is crucial in transaction systems, and HACBCA's ability to handle varying block sizes makes it adaptable to evolving demands, emphasizing its practical feasibility in real-world applications.

Implementation Complexity and Ease of Integration: While the presented data primarily focuses on performance metrics, the complexity of implementation and ease of integration are vital considerations. The Hybrid Access Control Enabled Consensus Algorithm's sensitivity to block size changes may contribute to its complexity of implementation, but this is offset by the adaptability it offers. Integrating HACBCA into existing systems or frameworks may require careful consideration of these sensitivities but presents an opportunity for tailoring the algorithm to specific use cases.

The comparison of the Hybrid Access Control Enabled Consensus Algorithm with established algorithms provides a nuanced understanding of its strengths and areas for improvement. The analysis based on block size illuminates the impact of this factor on transaction recovery time, memory usage, and responsiveness. HACBCA exhibits unique characteristics, such as its sensitivity to block size changes, which may be both an advantage and a consideration in specific scenarios. The lower memory usage and adaptive responsiveness make HACBCA a compelling choice, especially in resource-constrained environments.

This discussion emphasizes the importance of a holistic evaluation, considering not only performance metrics but also security features, resource utilization, and practical feasibility. As technology evolves, the Hybrid Access Control Enabled Consensus Algorithm stands as a promising contribution to the landscape of transaction systems, with its adaptability and efficient resource usage paving the way for further exploration and refinement in real-world applications.

CONCLUSION

The surge in Internet of Things (IoT) integration has improved online payment system usage, demanding robust security measures. This study focused on enhancing transaction security and efficiency through a hybrid access control-enabled consensus algorithm and checkpoint-enabled blockchain model (BECM). BECM utilizes smart contracts for automated agreements, enhances security with checkpoints, and ensures authorized access through the consensus algorithm.

This approach ensures safe banking transactions using a hybrid access control-enabled consensus algorithm on a checkpoint-enabled blockchain. Blockchain technology, essential in privacy preservation applications, offers enhanced privacy, security, traceability, detailed data provenance, and precise time-stamping. The checkpoint-enabled blockchain facilitates new block creation and storage maintenance.

The hybrid access control-enabled consensus algorithm efficiently preserves privacy and transaction security. Implementing blockchain benefits banking sectors, reducing

friction, delays, and enhancing operational efficiency across various sectors. Compared to existing methods, the proposed approach significantly reduced transaction recovery times (10.88 milliseconds), memory consumption (108.17 kilobytes), and responsiveness (33.55 milliseconds).

ACKNOWLEDGMENTS

The authors are thankful to Computer Science Engineering Department, G. H. Raisoni University, Amravati, Maharashtra, INDIA for providing all state-of-art facilities to carry out the research work in Research Laboratory.

CONFLICT OF INTEREST

Authors do not have any conflict of interest in publishing of this work. No Academic or financial interest to be declared for this work.

REFERENCES

1. W. Liu, X. Wang, W. Peng. State of the Art: Secure Mobile Payment. *IEEE Access* **2020**, 8, 13898–13914.
2. K. Fan, H. Li, W. Jiang, C. Xiao, Y. Yang. Secure Authentication Protocol for Mobile Payment. *Tsinghua Sci. Technol.* **2018**, 23 (5), 610–620.
3. R. Venkatesan, B. Anni Princy, V.D. Ambeth Kumar, et al. Secure online payment through facial recognition and proxy detection with the help of TripleDES encryption. *J. Discret. Math. Sci. Cryptogr.* **2021**, 24 (8), 2195–2205.
4. L. Yu, M. He, L. Xiong, Q. Luo, X. Niu. A Blockchain-Based Decentralized Privacy-Preserving Mobile Payment Scheme Using Anonymous Credentials. In *Proceedings - 24th IEEE International Conference on High Performance Computing and Communications*, Hainan, China, **2022**; pp 1517–1524.
5. P. Williams, I.K. Dutta, H. Daoud, M. Bayoumi. A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things (Netherlands)* **2022**, 19, 100564.
6. J. Li, J. Wang, S. Wangh, Y. Zhou. Mobile Payment with Alipay: An Application of Extended Technology Acceptance Model. *IEEE Access* **2019**, 7, 50380–50387.
7. M. Masoud, Y. Jaradat, A. Manasrah, I. Jannoud. Sensors of smart devices in the internet of everything (IOE) era: Big opportunities and massive doubts. *J. Sensors* **2019**, 2019, 6514520.
8. S. Desai, O. Deshmukh, R. Shelke, et al. Blockchain based secure data storage and access control system using cloud. In *Proceedings - 2019 5th International Conference on Computing, Communication Control and Automation, ICCUBEA 2019*; India,IEEE, Pune, **2019**.
9. N. Agarwal, P. Wongthongtham, N. Khairwal, K. Coutinho. Blockchain Application to Financial Market Clearing and Settlement Systems. *J. Risk Financ. Manag.* **2023**, 16 (10), 452.
10. D. Li, W.E. Wong, M. Chau, S. Pan, L.S. Koh. A Survey ofNFC Mobile Payment: Challenges and Solutions using Blockchain and Cryptocurrencies. In *Proceedings - 2020 7th International Conference on Dependable Systems and Their Applications, DSA 2020*; Xi'an, China, **2020**; pp 69–77.
11. B. Shrimali, H.B. Patel. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *J. King Saud Univ. - Comput. Inf. Sci.* **2022**, 34 (9), 6793–6807.
12. D. Guha Roy, P. Das, D. De, R. Buyya. QoS-aware secure transaction framework for internet of things using blockchain mechanism. *J. Netw. Comput. Appl.* **2019**, 144, 59–78.
13. H.D. Zubaydi, P. Varga, S. Molnár. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors* **2023**, 23 (2), 788.
14. S. Zhang, J.H. Lee. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, 6 (2), 93–97.
15. P. Chorey, N. Sahu. Enhancing efficiency and scalability in Blockchain Consensus algorithms: The role of Checkpoint approach. *J. Integr. Sci. Technol.* **2024**, 12 (1), 706.
16. Q. Wang, Y. Liu. Blockchain for public safety: A survey of techniques and applications. *J. Saf. Sci. Resil.* **2023**, 4 (4), 389–395.
17. R. Nair, S.N. Zafrullah, P. Vinayasree, et al. Blockchain-Based Decentralized Cloud Solutions for Data Transfer. *Comput. Intell. Neurosci.* **2022**, 2022.
18. U. Javaid, B. Sikdar. A Checkpoint Enabled Scalable Blockchain Architecture for Industrial Internet of Things. *IEEE Trans. Ind. Informatics* **2021**, 17 (11), 7679–7687.
19. A. Vuppala, R.S. Roshan, S. Nawaz, J.V.R. Ravindra. An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm. *Procedia Computer Science*. 2020, pp 1054–1063.
20. A. Šilenskytė, J. Butkevičienė, A. Bartminas. Blockchain-based connectivity within digital platforms and ecosystems in international business. *J. Int. Management*. **2023**.
21. C. Alcaraz, J. Lopez. A Cyber-Physical Systems-Based Checkpoint Model for Structural Controllability. *IEEE Syst. J.* **2018**, 12 (4), 3543–3554.
22. C. Wu, H. Huang, K. Zhou, C. Xu. Cryptanalysis and improvement of a new certificateless signature scheme in the standard model. *China Commun.* **2021**, 18 (1), 151–160.
23. R. Toorajipour, P. Oghazi, V. Sohrabpour, P.C. Patel, R. Mostaghel. Block by block: A blockchain-based peer-to-peer business transaction for international trade. *Technological Forecasting and Social Change*. 2022.
24. Y. Qian, Y. Jiang, J. Chen, et al. Towards decentralized IoT security enhancement: A blockchain approach. *Computers and Electrical Engineering*. 2018, pp 266–273.
25. A. Ali, A.H.S. Saad, A.H. Ismael. Data Hiding Technique Based on NFC-Enabled Smartphones; Procedia Computer Science, **2020**, 171, 2400-2409.
26. M. Zulfiqar, M. Kamran, M.B. Rasheed. A blockchain-enabled trust aware energy trading framework using games theory and multi-agent system in smat grid. *Energy*. **2022**.
27. S. Chorey, N. Sahu. Failure recovery model in big data using the checkpoint approach. *J. Integr. Sci. Technol.* **2023**, 11 (4), 564.
28. S. Chorey, N. Sahu. Rapid Recover Map Reduce (RR-MR): Boosting failure recovery in Big Data applications. *J. Integr. Sci. Technol.* **2024**, 12 (3 SE-Engineering), 773.
29. E. Politou, F. Casino, E. Alepis, C. Patsakis. Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Trans. Emerg. Top. Comput.* **2021**, 9 (4), 1972–1986.