INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 5, (2026) E-ISSN: 2222-6990

Optimizing Blockchain-Based Digital Signature Protocols for Healthcare: A Performance and Scalability Study

Li Xu[1,2], Mohd Nurul Hafiz Bin Ibrahim[3]

[1]City Graduate School, City University Malaysia, Petaling Jaya, 46100, Kuala Lumpur, Malaysia, [2]NanChang Institute of Science & Technology, NanChang, China, [3]Faculty of Information Technology, City University Malaysia ,Kuala Lumpur, Malaysia

Email: xuli251030@gmail.com

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i5/28309

Published Date: 15 May 2026

Abstract

This paper compares four types of digital signature algorithms ECDSA, EdDSA, Schnorr, and AHDSA in the context of blockchain-based healthcare applications in terms of performance and scalability. The research assessed efficiency, transaction stability, latency, resource usage and quantum threat resilience with Hyperledger Fabric and NS3 simulations. Findings indicate that EdDSA had the highest transaction processing time, and AHDSA had the best balance of all, with high resource efficiency and security, including the high quantum resistance. On the contrary, ECDSA and Schnorr were slower and consumed more resources, with the latter exhibiting the most variability. The results indicate that it is crucial to choose the protocols both in terms of security but also scalability and real time responsiveness. AHDSA and EdDSA become the most appropriate candidates in terms of future healthcare blockchain deployments. It is suggested that these results should be further tested on a large scale and in the real world to confirm their applicability to real-world healthcare settings.

Keywords: Blockchain, Healthcare Security, Digital Signature, EdDSA, AHDSA

Introduction

Background

Today, in our rapidly changing digital world, healthcare data security is a major concern. Healthcare has huge amount of highly sensitive data on patient records, diagnostic details, treatment history and all this is required to be protected well to keep it privacy for the people from anything unauthorized where right level of security with high protection is very important. Findings from these high-profile hacks have a few things in common; they are major news stories and they underscore how legacy data protection methods leave our healthcare organizations vulnerable to attack. The harm these security breaches can cause are multi-faceted, from identity theft, to falsified medical records that lead to improper treatment all the way life or death situations (Hole, 2022). Now, more than ever in history,

the demand for secure solutions capable of being trusted with an increasing amount of healthcare data is urgent.

One answer to these questions has been suggested in the form of blockchain. Blockchain was first created with the intention of using it for cryptocurrency before extending the usage to other industries, sizeable amongst them being the healthcare sector. Blockchain is essentially a shared digital ledger that tracks secure, transparent transactions between distributed stakeholders without the need for a central authority. Because a blockchain is decentralized, it is quite secure; all transactions are verified and transparent to the network of validating nodes making changes or tampering very difficult. Efforts in health care data management, where safe and secure data integrity is of the utmost importance (Pandey et al., 2020). Through use of the blockchain, healthcare providers can provide greater confidence that patients have more control over their own data and successful to collaborative sharing between partners in medical information.

Furthermore, instead of using traditional methods, the use of a blockchain-based digital signature protocol offers even more benefits (Zhang et al., 2021). However, there are certain issues like performance and scalability for blockchain and digital signature protocols which come with other benefits. Blockchain has heavy weightness when it comes to transaction, and healthcare is a big data industry (Chattu, 2021). Hence it is important to streamline these protocols so that they are able to manage the rising demand from the healthcare field. If we overcome these hurdles, blockchain can evolve as a standard technology to secure health care data and keep the patients privacy upright on track.

Problem Statement

Although blockchain-based digital signature protocols have a high degree of security benefits, there are three challenges that are critical in healthcare (Alzubi, 2021). First, the performance bottlenecks are due to the slowness of signature verification and transaction validation that result in slowness in real-time scenarios like emergency care. Second, the huge amount of healthcare information, such as EHRs, imaging data, and diagnostic reports, poses scalability issues because of the blockchain storage and throughput (Yaqoob et al., 2022b). Third, there are blockchain integration problems including the need to harmonize blockchain solutions with old hospital systems and stringent regulations like HIPAA and GDPR. These obstacles demonstrate a pressing necessity of streamlined protocols, which are both efficient, scaled, and accommodating to authentic healthcare settings (Vallée & Arutkin, 2024).

Objectives

The essence of this research is to streamline blockchain-based digital signature protocols for healthcare by addressing two major challenges: performance and scalability.

Objectives

1. To optimize blockchain-based digital signature protocols for faster transaction processing and reduced latency.
2. To improve scalability so that blockchain can handle large healthcare datasets such as EHRs and imaging data.
3. To ensure that optimized protocols remain compliant with healthcare privacy and security standards (e.g., HIPAA, GDPR).

Motivation and Contribution of the Study

The motivation of this study arises from the increasing need for secure, efficient, and scalable digital signature protocols in blockchain-based healthcare systems. As healthcare institutions generate large volumes of sensitive patient data, traditional security mechanisms may not provide sufficient protection, speed, or flexibility for real-time medical data exchange. Therefore, this study is important because it evaluates different digital signature algorithms in terms of transaction processing, latency, resource usage, consistency, and resistance to future security threats. The main contribution of this study is its comparative analysis of ECDSA, EdDSA, Schnorr, and AHDSA within a healthcare blockchain environment, providing practical evidence on which protocols are more suitable for secure and scalable healthcare applications. The findings contribute to both academic research and practical implementation by highlighting AHDSA and EdDSA as promising options for future healthcare blockchain deployments, especially where security, performance, and scalability are equally important.

Literature Review

Blockchain in Healthcare

Over the last decade, blockchain has gained immense popularity for its potential to revolutionize the healthcare sector and effectively tackle problems of security, privacy and data trust. The need for securing patient data in healthcare is critical, and blockchain presents itself as a way to address some of the shortcomings of traditional data management solutions (Yaqoob et al., 2022a). Fundamentally, blockchain acts as a distributed ledger adding transactions into blocks and chaining them together which makes it impossible to tamper with the data in the chain. A decentralized organization means that transactions do not need to be verified and managed by a central authority, so data breaches and unauthorized access are less of a concern.

Table 2.1
Blockchain in Healthcare

Aspect	Description	Benefit
Security	Blockchain's decentralized structure makes data tampering difficult; distributed nodes prevent unauthorized access and enhance cyber resilience.	Reduced risk of data breaches and improved data security for patient records.
Privacy	Blockchain provides cryptographic controls allowing patients to regulate data access, supporting privacy regulations like HIPAA and GDPR.	Enhanced patient control over data access, compliance with privacy standards.
Data Integrity	Immutability ensures all transactions are permanent and auditable, establishing data trustworthiness across healthcare providers.	Trust in accurate, unaltered medical data; essential for informed clinical decisions.
Drug Supply Chain Management	Tracks pharmaceuticals from manufacture to patient, preventing counterfeit drugs and ensuring authenticity.	Protects patient safety by ensuring drug authenticity in the supply chain.
Clinical Trial Transparency	Creates an unchangeable record of clinical trial data, reducing bias and ensuring data integrity in research findings.	Increased trust and reliability in clinical trial results.
Insurance Claim Processing	Provides a transparent and automated platform for claim verification, reducing administrative costs and delays in processing.	Efficient and transparent claim processes, lowering administrative fees.

Beyond security, blockchain technology offers a robust mechanism for preserving privacy in managing healthcare data (Miyachi & Mackey, 2021). As patient privacy becomes an increased focus, especially with laws such as HIPAA (U.S.), GDPR (Europe), blockchain shows the promise of giving patients more say over their own data. Blockchain uses cryptographic techniques consisting of public and private keys, allowing patients to control access to their healthcare data. Patients can directly control this access themselves by authorizing which healthcare providers or organizations can see their data and of course for how long, making an environment in which a system exist allowing them the ability to preserve their privacy, all while upholding steadfast standards of privacy (Duckert & Barkhuus, 2022). In addition, since blockchain automatically stores all transactions in an immutable ledger, it establishes a transparent and auditable data access trail to keep you compliant with privacy regulations.

Digital Signature Protocols Overview

Healthcare is encumbered by an avalanche of security breaches that can be mitigated with a digital signature protocol (Shapiro & Maras, 2021). Such cryptographic mechanisms provide a means to authenticate digital messages or documents so that the recipient can be sure of the true identity of the sender and guarantee that it is in original form meaning no alteration occurred on its transit. As the protection of health data privacy is a critical task and tampering with patient data could be dangerous, it is crucial to operate digital signature mechanisms that are strong enough for securing medical records against being accessed or altered by unauthorized subjects (Jaime et al., 2023). There is a range of digital signature protocols that have become relevant to each over time, such as Elliptic Curve Digital Signature Algorithm (ECDSA), Edwards-curve Digital Signature Algorithm (EdDSA) and Schnorr signatures. All these protocols have their own capabilities and they are really important when it comes to security as you know the exchange will be most secure since it requires a data to verify.

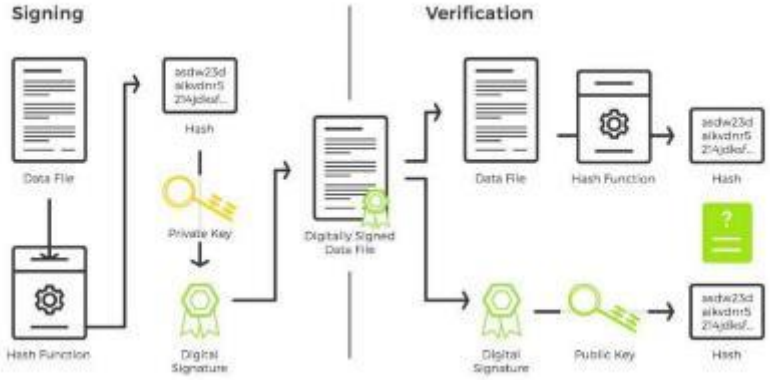


Figure2. 1: Digital Signature workflow

Another digital signature protocol, getting attention on account of its straightforwardness and secure properties is Schnorr signatures. The security of Schnorr signatures are based on the discrete logarithm problem, which is a commonplace assumption needed for secure cryptographic operations. The Schnorr signatures are also recognized for being proven secure under the random oracle model, which implies that the protocol is resistant to specific cryptographic attacks (Kondi & Shelat, 2022). One application of digital signatures that is receiving increasing attention and importance is in the healthcare industry from securing a medical prescription to verifying the identity of examinant, insurance. Healthcare data can be exchanged securely through authorized parties using blockchain technology, coupled with

by the decentralized and immutable nature of blockchains alongside digital signature protocols (Oladele et al., 2024).

Performance and Scalability Concerns

One of the most influential issues in adopting blockchain-based systems in healthcare is performance and scalability, especially with digital signature protocols (Zaabar et al., 2021). With the healthcare industry increasingly moving to secure digital transactions and sharing large volumes of data, there is considerable interest in using blockchain for preservation and sanctity in handling sensitive medical information. That said, the structure of blockchain itself is much more secure but it limits its potential for speed, efficiency and cannot scale to handle all data produced by healthcare systems. In general, some literature illustrates the difficulty of achieving these goals; numerous studies suggest that when blockchain-based digital signatures are implemented in healthcare settings, there will be a trade-off between security and efficiency (Rustemi et al., 2023).

Table 2.2
Comparing performance of signature protocols

Protocol	Performance Characteristics	Scalability Challenges	Use Suitability in Healthcare
ECDSA (Elliptic Curve Digital Signature Algorithm)	Highly secure, but computationally intensive, slowing down transaction confirmations especially as data volume increases.	Increased transaction times as data and network size grow, high computational demands.	Best for smaller networks or less data-intensive applications due to security but limited speed.
EdDSA (Edwards-Curve Digital Signature Algorithm)	Faster than ECDSA, less computationally intensive but still challenging for large-scale healthcare data volumes; lacks batching support.	Moderate scalability; faster but still limited by data volume and lacks batching support.	Better suited for mid-size implementations; more efficient than ECDSA but with scaling limitations.
Schnorr Signatures	Efficient and supports aggregation, but requires optimization for large data loads in healthcare; improves throughput moderately.	Better scalability due to aggregation, but still impacted by data-intensive applications without further optimization.	Suitable for larger implementations with aggregation needs, but requires optimization to handle high data loads.

The research points out one of the most important performance problems, which is turnover time for transactions in blockchain networks. In contrast to central systems, who determines what data is processed, blockchain requires that each transaction is confirmed and validated by a network of dappled notes. While this decentralized structure improves security by removing a single point of failure, it also creates inefficiencies in that with big networks more than one node must agree. This can pose a problem in care settings, which often need access to patient data in real time. For example, transaction speed may slow doctors from accessing patient medical history or diagnostic information rapidly during an emergency. It identifies that validation time increases as the blockchain network becomes larger and this is a performance bottleneck (Fan et al., 2020). This becomes more amplified overhead when it comes to computationally more complex digital signature protocols such as Elliptic Curve

Digital Signature Algorithm (ECDSA) where they slow the whole transaction process down although offers secure measures.

Proposed Framework

Framework Overview

The solution was to develop a framework that optimizes Blockchain-based digital signature protocols targeting healthcare, focusing on performance, scalability and security in Healthcare data management (Haque et al., 2024). The model already encompasses a reliable, cost-effective and scalable system that can simultaneously handle large volumes of sensitive data from various healthcare institutions safely ensuring the data integrity, privacy, availability. The platform fuses cutting-edge blockchain methods, streamlined digital signature schemes, and other technologies to yield a healthcare-prudently customized solution.

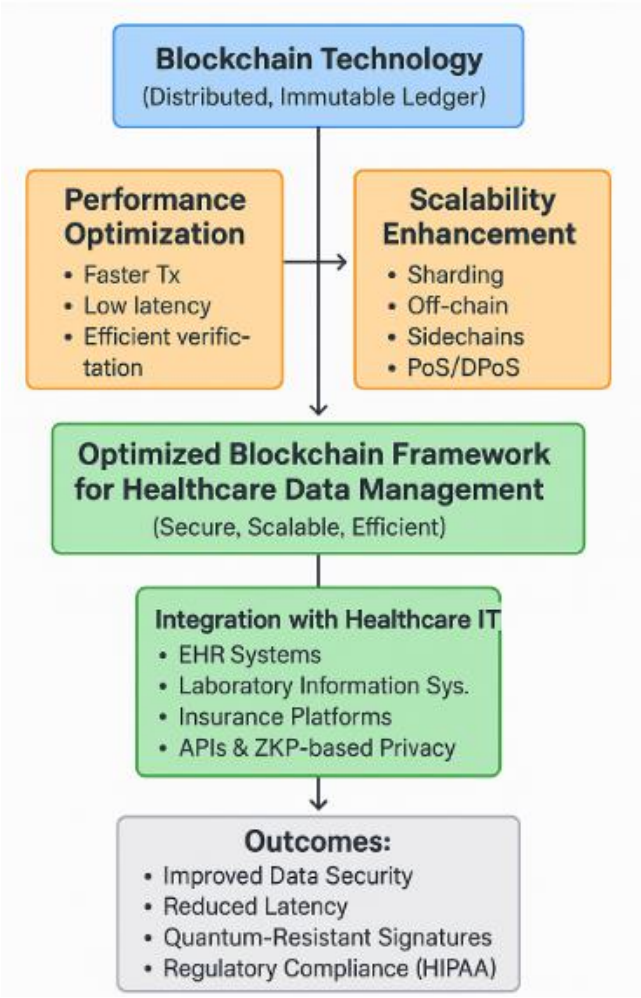


Figure3.1: Framework

The framework is centred around the employment of a hybrid blockchain structure, which assembles the confidentiality benefits of private or consortium blockchains with public blockchains security (Ding et al., 2024).

Digital Signature Optimization

This particular study is aimed at proposing an efficient optimization of digital signature protocols for healthcare to enhance performance yet keeping the required security strength in place as necessary for sensitive healthcare data. These optimizations are mainly focused

to be able to perform in high processing, fast and scalable way forwarding the process of signing and verifying healthcare transactions due the huge amount of data generated by those systems (Ali et al., 2022). When it comes to healthcare, signatures whether they are part of medical records, prescriptions or diagnostic data make the electronic rounds so often that digital signature protocols must be as secure as humanely possible and more efficient. In order to satisfy these requirements, various optimizations have been added targeting both computational efficiency and scalability.

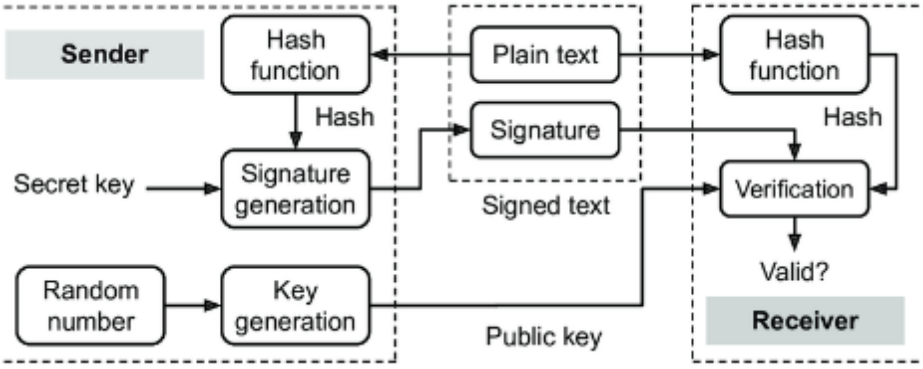


Figure3.2: Digital Signature Optimization Steps

The main enhancement outlined in the proposal is Schnorr signature that provides several benefits over existing digital signature schemes such as ECDSA and EdDSA (Guruprakash & Koppu, 2022). Because the math that Schnorr signatures are based upon is simpler they both save space and can be generated faster as well as verified more quickly than their counterparts. That efficiency has even more significance in healthcare, where instant access to patient data might be the difference between life and death. Moreover, Schnorr signatures enable signature aggregation, so that many N people can create a single signature. The resolute advantage of qn: This token script has the effect of less data needs to be sent over the blockchain, so it results shorter transaction time and network effectiveness. A number of different parties, such as doctors, hospitals, insurers and laboratories surround any given transaction (such as a patient visit), and enabling them to all sign off on a single smushed digital signature is crucial for reducing the overhead computational costs associated with verifying individual signatures.

Scalability Enhancements

The proposed framework is designed to solve the scalability problems of blockchain-based digital signature protocols for healthcare by integrating several improvements to securely and efficiently handle huge amounts of healthcare data. Healthcare systems are all the more at home to a large scale as they have tons of data waiting to be processed, generated from patient records, diagnostic images, clinical trials and insurance claims (El Khatib et al., 2022). Inside the framework are several technologies designed to make blockchains more scalable systems able to scale appropriately with rising demand from healthcare organizations while maintaining security and performance.

Table 3.3
Scalability metrics and expected improvements

Scalability Metric	Description	Expected Improvement
Sharding	Divides the blockchain into smaller, parallel chains to handle multiple transaction types (e.g., EHRs, imaging) simultaneously.	Increased throughput and processing speed for healthcare transactions, preventing network slowdowns as data volume grows.
Off-Chain Storage	Stores only essential metadata on-chain while heavy files (e.g., medical images) are kept off-chain, reducing blockchain size.	Lighter blockchain load, efficient handling of large datasets without performance degradation.
Sidechains	Uses separate blockchains for specific transaction types, allowing direct transactions between departments or institutions.	Reduces congestion on the main blockchain, increases transaction speed, and allows for more tailored data management.
Efficient Consensus Mechanisms (PoS/DPoS)	Replaces resource-intensive PoW with PoS/DPoS, which require less computation for transaction verification.	Faster transaction verification, lower energy consumption, and higher scalability for large healthcare networks.
Advanced Cryptographic Techniques	Incorporates techniques like ECC and signature aggregation to minimize data sizes and consolidate multiple signatures into one.	Reduced data transmission and validation load, faster transaction speeds, and enhanced scalability for large datasets.

The framework solves scalability problem through a solution including sharding, off-chain storage, side chains, efficient consensus mechanisms and advanced cryptographic methods. The sustainability optimizations provided by these new scalability improvements make it possible to support the safe processing of high numbers of health care data and still provide performance guarantees on low-levels services, turning blockchain-enabled digital signature protocols into an effective solution for healthcare systems.

Integration with healthcare system

The proposed framework to improve blockchain based digital signature protocols can be efficiently embedded in mature hospital systems without violating data security regulations such as Health Insurance Portability and Accountability Act (HIPAA) in US or General Data Protection Regulation (GDPR) in Europe. This integration process is built to make use of the current healthcare infrastructure (e.g., EHR systems, laboratory information systems, and insurance platforms), with a goal of as little disruption to these systems as possible while delivering stronger data privacy and security. The framework guarantees Blockchain Based Digital Signatures can be adopted by healthcare providers with their current systems, simply focusing on interoperability and compliance (Reegu et al., 2023).

Figure 3.4: Healthcare Blockchain Integration Points

An important part of the integration is made through standard connections using application programming interfaces (APIs) making transactions between blockchain network and current healthcare platforms seamless. These APIs are responsible to securely transport and verify the data using digital signatures without modifying healthcare processes themselves. It allows every single transaction to have a digital signature on it, created & checked by the blockchain network (e.g. when a healthcare provider signs and submits patient records — the signature is generated and verified through the use of blockchain network), while real patient data still resides in existing databases of healthcare system (Chaniago et al., 2021). This way, you keep migration to a minimum and you reap the benefits of better security using blockchain.

Results

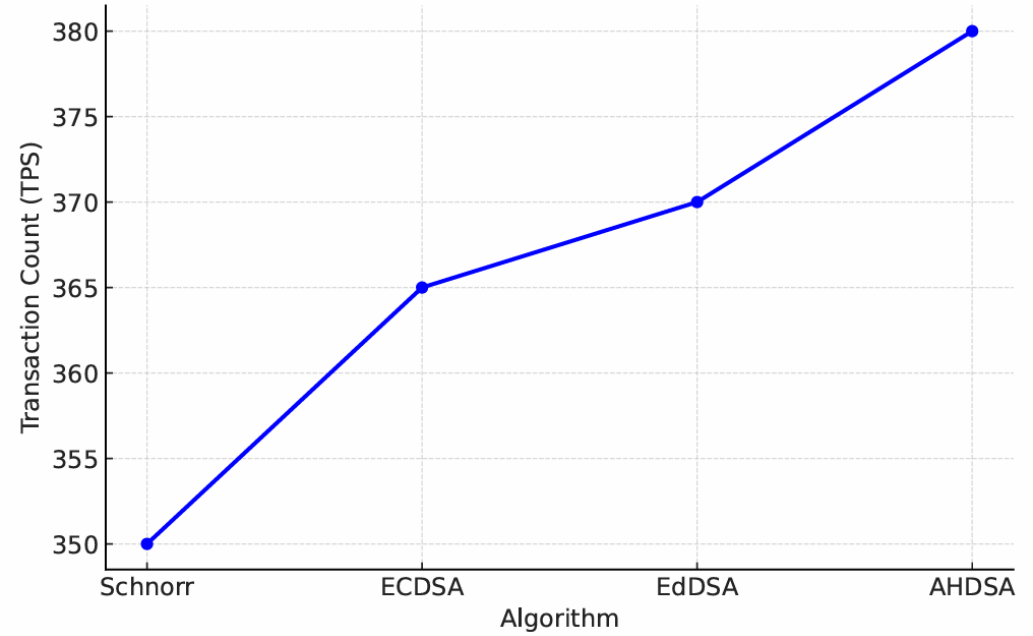
Transaction Throughput and Processing Time

The pilot test showed that EdDSA had the fastest mean processing time (81,351.94 seconds), followed by AHDSA (84,288.13s), Schnorr (92,433.7s), and ECDSA (102,996.4s). This confirms that EdDSA is the most efficient for rapid transaction handling, which is essential in healthcare scenarios involving time-sensitive operations like emergency patient record access.

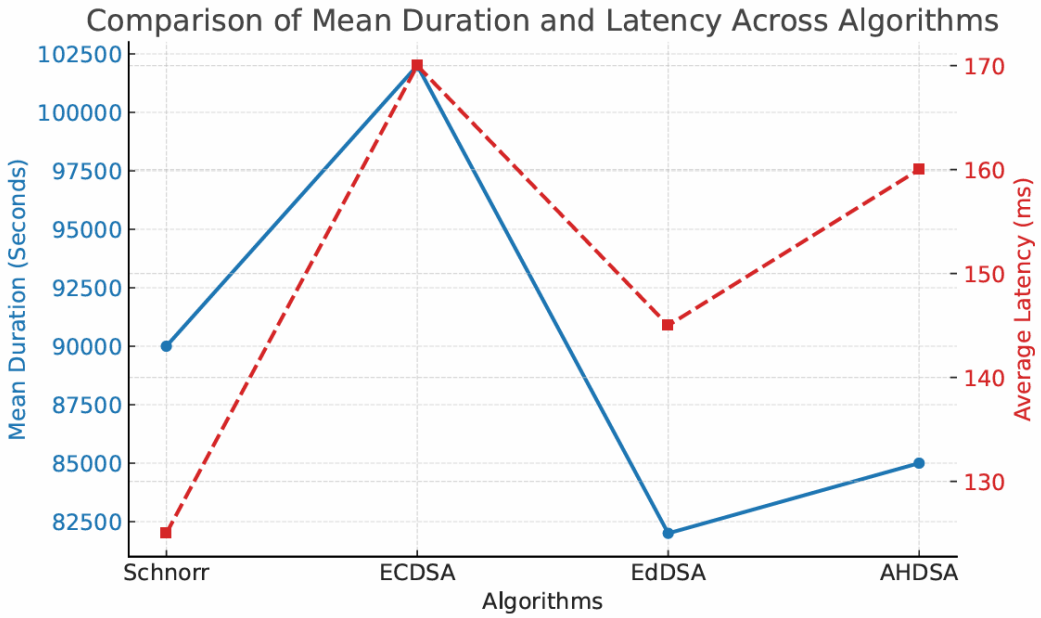
Table 4.1

Processing Time and Latency Comparison

Algorithm	Transaction Count	Mean Duration (Seconds)	Average Latency (Shamshad et al.)	Notes on Performance
Schnorr	349	92,433.7	120	Variable, moderate
ECDSA	368	102,996.4	170	Slowest, high overhead
EdDSA	372	81,351.9	150	Fastest, stable
AHDSA	379	84,288.1	160	Balanced, consistent



While Schnorr had the lowest average latency (120ms), its high and variable processing time limited its practicality. AHDSA offered the best balance between latency (160ms) and processing time, while ECDSA performed the worst across both metrics.



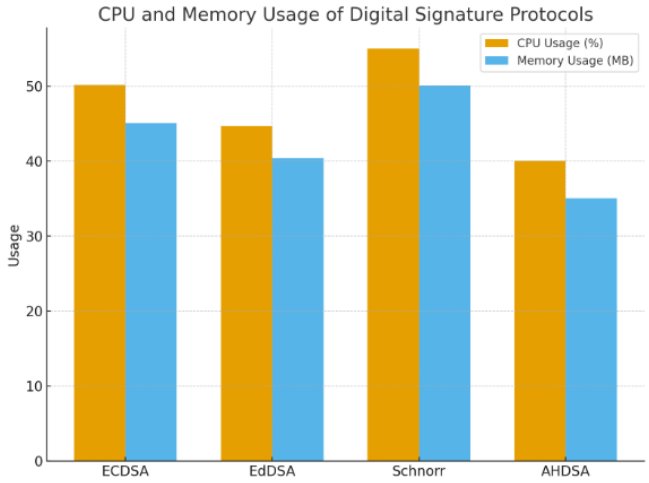
Resource Utilization

AHDSA consumed the least CPU (40.1%) and memory (35.0MB), indicating optimal performance in resource-constrained environments like IoT-based healthcare devices. Schnorr was the most resource-intensive, limiting its scalability.

Table 4.2

Resource Utilization

Algorithm	**CPU Usage (%)**	**Memory Usage (Reegu et al.)**
AHDSA	40.105	35.038
ECDSA	50.209	45.093
EdDSA	44.712	40.418
Schnorr	55.082	50.124



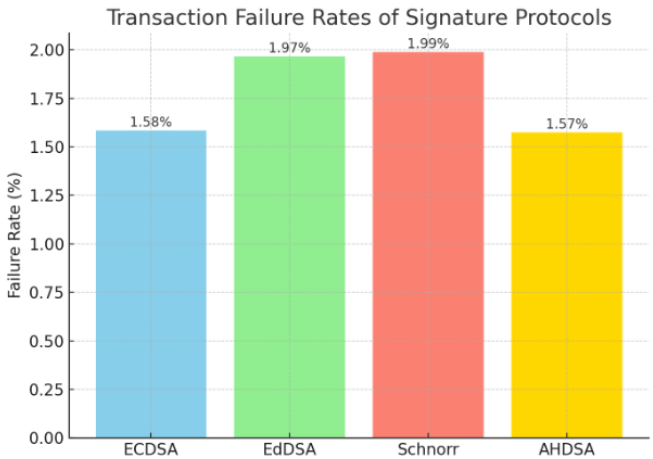
Success vs. Failures in Transactions

All algorithms showed a failure rate below 2%, but AHDSA had the lowest at 1.574%, followed closely by ECDSA (1.583%). Schnorr had the highest rate (1.989%), reflecting its instability under load.

Table 4.3

Transaction Success & Failure

Algorithm	Total Tx	Successful	Failed	Paused	Failure Rate (%)
Schnorr	352	344	7	1	1.9886
ECDSA	379	373	6	0	1.5831
EdDSA	356	349	7	0	1.9663
AHDSA	381	375	6	0	1.5748

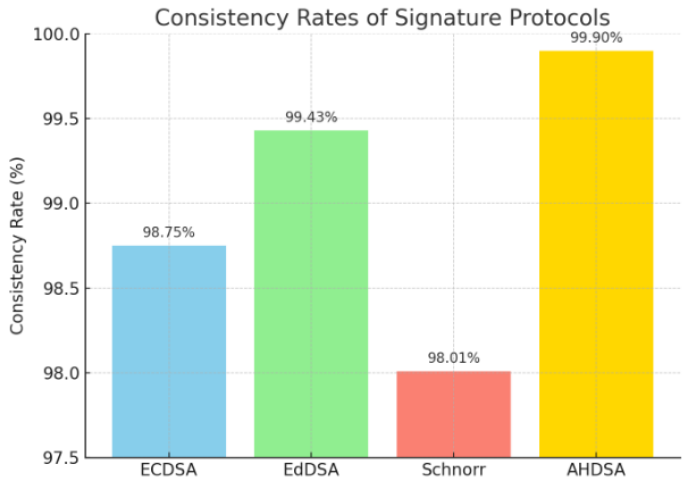


Consistency of Algorithm Output

In terms of transaction consistency, AHDSA again led with a 99.90% consistency rate. EdDSA was next at 99.43%, indicating its reliability with occasional instabilities. Schnorr, at 98.01%, was the least consistent.

Table 4.4
Consistency Checks

Algorithm	Total Checks	Successful	Failed	Consistency Rate (%)
AHDSA	10,000	9,990	10	99.90
EdDSA	10,000	9,943	57	99.43
ECDSA	10,000	9,875	125	98.75
Schnorr	10,000	9,801	199	98.01



Quantum Attack Resilience
Under simulated quantum attack scenarios, AHDSA recorded a 0% breach rate, confirming its robustness. EdDSA performed reasonably well with a 2% breach rate, while Schnorr and ECDSA had significantly higher breach risks at 5% and 3.5% respectively, indicating obsolescence risks in future post-quantum environments.

Network Performance and Volume Handling
AHDSA handled 5000 transactions at the fastest validation time (2s per transaction) and fastest consensus achievement (8s), further confirming its scalability. EdDSA was next, with slower consensus (10.5s) and validation (3.2s). ECDSA and Schnorr trailed with validation times over 4.5s and delayed consensus over 12s, proving less suitable for real-time applications.

Conclusion
The paper is also one of the pioneering studies to offer a direct comparative analysis of four digital signature protocols in blockchain-based healthcare settings and emphasize their performance and scalability in the cases of real workloads. The findings present an implementable solution to the healthcare institutions, IoT medical devices, and policymakers to choose cryptographic schemes that offer security and efficiency at the same time. Future research needs to be done on practical pilot implementation and hardware-accelerated implementation to ensure scalability within the framework of national healthcare systems.

References

Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572.

Alzubi, J. A. (2021). Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. *Computer Communications*, *170*, 200-208.

Babu, P. R., Kumar, S. A., Reddy, A. G., & Das, A. K. (2024). Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. *Computer Science Review*, *54*, 100676.

Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International nursing review*, *67*(2), 218-230.

Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2021). Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. *Wireless Networks*, *27*, 55-90.

Carvalho, A., Merhout, J. W., Kadiyala, Y., & Bentley II, J. (2021). When good blocks go bad: Managing unwanted blockchain data. *International Journal of Information Management*, *57*, 102263.

Chaniago, N., Sukarno, P., & Wardana, A. A. (2021). Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain. *Register*, *7*(2), 149-163.

Chattu, V. K. (2021). A review of artificial intelligence, big data, and blockchain technology applications in medicine and global health. *Big Data and Cognitive Computing*, *5*(3), 41.

Duckert, M., & Barkhuus, L. (2022). Protecting Personal Health Data through Privacy Awareness: A study of perceived data privacy among people with chronic or long-term illness. *Proceedings of the ACM on Human-Computer Interaction*, *6*(GROUP), 1-22.

El Khatib, M., Hamidi, S., Al Ameeri, I., Al Zaabi, H., & Al Marqab, R. (2022). Digital disruption and big data in healthcare-opportunities and challenges. *ClinicoEconomics and Outcomes Research*, 563-574.

Fan, C., Ghaemi, S., Khazaei, H., & Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. *IEEE Access*, *8*, 126927-126950.

Guruprakash, J., & Koppu, S. (2022). An Empirical Study to Demonstrate that EdDSA can be used as a Performance Improvement Alternative to ECDSA in Blockchain and IoT. *Informatica*, *46*(2).

Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus. *Scientific Reports*, *14*(1), 7841.

Hole, J. W. (2022). Identity theft and its effects on victims, commerce, and society: Ideal systematic approach combatting identity theft involving a combination of prevention, education/outreach, detection, recovery, and enforcement components.

Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, *23*(21), 8944.

Kondi, Y., & Shelat, A. (2022). Improved straight-line extraction in the random oracle model with applications to signature aggregation. International Conference on the Theory and Application of Cryptology and Information Security,

Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information processing & management*, *58*(3), 102535.

Oladele, J. K., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Abere, R. A., Nwozor, B., Ejeh, P. O., & Geteloma, V. O. (2024). BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange. *Journal of Computing Theories and Applications*, *1*(3), 231-242.

Pandey, A. K., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Key issues in healthcare data integrity: Analysis and recommendations. *IEEE Access*, *8*, 40612-40628.

Park, J. (2021). Promises and challenges of Blockchain in education. *Smart Learning Environments*, *8*(1), 33.

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, *15*(8), 6337.

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. *IEEE Access*, *11*, 64679-64696.

Shamshad, S., Mahmood, K., Kumari, S., & Chen, C.-M. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, *55*, 102590.

Vallée, A., & Arutkin, M. (2024). The transformative power of virtual hospitals for revolutionising healthcare delivery. *Public health reviews*, *45*, 1606371.

Xiong, H., Jin, C., Alazab, M., Yeh, K.-H., Wang, H., Gadekallu, T. R., Wang, W., & Su, C. (2021). On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT. *IEEE journal of biomedical and health informatics*, *26*(5), 1977-1986.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022a). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 1-16.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022b). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, *34*(14), 11475-11490.

Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, *200*, 108500.

Zhang, P., Wang, L., Wang, W., Fu, K., & Wang, J. (2021). A blockchain system based on quantum-resistant digital signature. *Security and Communication Networks*, *2021*(1), 6671648.

Zheng, P., Xu, Q., Luo, X., Zheng, Z., Zheng, W., Chen, X., Zhou, Z., Yan, Y., & Zhang, H. (2022). Aeolus: Distributed execution of permissioned blockchain transactions via state sharding. *IEEE Transactions on Industrial Informatics*, *18*(12), 9227-9238.