Journal of Soft Computing Paradigm (ISSN: 2582-2640)
www.irojournals.com/jscp/

A Scalable and Secure Data Analytics Framework for Decentralized Autonomous Healthcare Systems using Fuzzy Logic, Blockchain Sharding, Dynamic Network Slicing, and ECC

Venkata Surya Bhavana Harish Gollavilli[1], Kalyan Gattupalli[2], Harikumar Nagarajan[3], Poovendran Alagarsundaram[4], Surendar Rama Sitaraman[5]

[1]Under Armour, Maryland, USA

[2]Yash Tek inc, Ontario, Canada

[3]Global Data Mart Inc (GDM), New Jersey, USA

[4]Humetis Technologies Inc, Kingston, NJ, USA

[5]Intel Corporation, California, USA

E-mail: [1]venkataharish@ieee.org, [2]kalyangattupalli@ieee.org, [3]harikumarnagarajan@ieee.org, [4]poovendrana@ieee.org, [5]surendar.rama.sitaraman@ieee.org

Abstract

Healthcare systems are increasingly challenged by the complexity of managing scalable and secure data. Addressing this, the proposed novel framework integrates elliptic curve cryptography (ECC), dynamic network slicing, blockchain sharding, and fuzzy logic to enable efficient, adaptive, and secure data analytics. The framework processes healthcare data from IoT devices, wearable sensors, and patient records, ensuring real-time analytics, scalability, and robust security. By utilizing blockchain sharding for scalability, ECC for secure encryption, and fuzzy logic for decision-making, the architecture effectively overcomes the constraints of

DOI: https://doi.org/10.36548/jscp.2024.4.007
Received: 16.12.2024, received in revised form: 07.01.2025, accepted: 28.01.2025, published: 07.02.2025

traditional systems. The results demonstrate significant improvements, including enhanced security (98%), reduced latency (10 ms), and higher scalability (5000 TPS). These advancements establish a reliable, decentralized foundation for predictive healthcare insights, resource optimization, and adaptive governance, setting a benchmark for modern healthcare data management systems.

Keywords: Fuzzy Logic, Blockchain Sharding, Dynamic Network Slicing, Elliptic Curve Cryptography (ECC), Decentralized Healthcare.

1. Introduction

The way medical services are provided, administered, and optimized has been completely transformed by the quick development of digital technologies in the field. Innovative frameworks that guarantee safe, scalable, and effective data processing are becoming more and more necessary as the industry struggles with the flood of big data produced by wearable sensors, IoT devices, and smart healthcare systems. Technologies like Elliptic Curve Cryptography (ECC), Blockchain Sharding, Dynamic Network Slicing, Decentralised Autonomous Organisations (DAOs), and Fuzzy Logic are at the core of this change. When combined, they provide a strong basis for developing decentralised autonomous healthcare systems that combine state-of-the-art computational techniques with data analytics.

Fuzzy Logic is a mathematical technique that handles imprecise and uncertain data in a way that mimics human reasoning. This makes it ideal for dynamic healthcare contexts where data may be inconsistent or incomplete. Decision-making procedures like diagnosis and treatment planning can become more accurate and flexible by implementing fuzzy logic into healthcare systems. By splitting the ledger into smaller, more manageable sections, Blockchain Sharding, on the other hand, solves the scalability issues of conventional blockchain networks and permits quicker transaction processing and more effective data storage Hashim et al. [1].

A key component of 5G technology, dynamic network slicing enables the development of virtual network slices customized for certain healthcare uses, including emergency response, telemedicine, and remote monitoring. This guarantees high reliability, minimal latency, and optimal resource usage in crucial medical situations. As decentralised governance structures, DAOs lessen the need for centralized middlemen while facilitating smooth collaboration between healthcare stakeholders. Their automated and transparent character promotes efficiency and confidence in the administration of patient data and medical resources.

The complexity of healthcare data, the growing need for personalized therapy, and the strict regulations surrounding data security and privacy all point to the necessity for such a thorough framework. Because of problems like data storage, latency, and cyberattack susceptibility, traditional centralized systems frequently find it difficult to meet these expectations. Secure, interoperable, and scalable data management is ensured by a decentralised strategy that makes use of DAOs, Blockchain Sharding, and ECC. The system is further improved by incorporating fuzzy logic and dynamic network slicing, which allow for adaptive decision-making and effective resource use.

In the post-pandemic era, where telemedicine, remote patient monitoring, and smart medical equipment have become indispensable, the suggested paradigm is especially pertinent. Ensuring secure management and smooth data flow over-dispersed networks is essential as healthcare organizations throughout the world embrace IoT-enabled solutions. In addition to addressing these issues, this paradigm establishes the foundation for upcoming developments in self-governing healthcare systems, where data-driven insights and decentralised governance can lead to better patient outcomes.

The following objectives are:

- **Improve Scalability:** To effectively handle massive amounts of healthcare data, use Blockchain Sharding and Dynamic Network Slicing.
- **Assure Security and Privacy:** Integrate ECC to protect private medical information while keeping computing overhead to a minimum.
- **Facilitate Decentralised Governance:** Put DAOs into place to lessen dependency on centralised systems and expedite stakeholder collaboration.
- **Enhance Decision-Making:** To manage ambiguity in medical data and maximise diagnostic precision, apply fuzzy logic.
- **Enable Real-Time Analytics:** Make use of sophisticated data analytics methods to identify trends and gain predictive insights in healthcare systems.

Ensuring safe, scalable, and effective data management has become more difficult due to the increasing complexity of healthcare data and the broad use of IoT-enabled devices Gaikwad et al. [2]. Data storge, latency, and privacy concerns plague today's centralised

systems, emphasizing the essential need for a decentralised framework that incorporates cutting-edge technologies to successfully overcome these constraints.

Healthcare has investigated blockchain and IoT technologies Noori et al. [3], but current solutions frequently lack scalability, real-time analytics, and adaptive decision-making capabilities. A gap in the development of a unified, safe, and scalable framework for autonomous healthcare systems is caused by the underexplored integration of DAOs, ECC, Blockchain Sharding, Fuzzy Logic, and Dynamic Network Slicing.

2. Related Works

According to Hashim et al. [1], blockchain is relevant for healthcare applications where EHRs are central in healthcare services. Blockchain's advantages include increased privacy and security in data sharing; however, the scalability remains a limitation as it includes the replication of the ledger and mechanisms of achieving consensus. The partitioning of the network into shards for parallel processing addresses the limitations of sharding. A novel technique of patient care sharding across healthcare entities visits is presented which reduces overhead through cross-shard communication while optimizing latency, throughput, and improving the processing speed of an appointment.

According to Gaikwad et al. [2], the importance of medical record security is increasing, with the need for encrypted storage and transfer because of the sensitive nature of healthcare data. With advancing technology, doctors and patients can access medical services securely through mobile, computers, and wireless devices. This research presents an authentication protocol that is based on ECC for ensuring safe client-server communication. This authentication protocol aims at mitigating security threats while optimizing the computation time and cost and enhancing privacy and efficiency in medical systems.

Shetty et al. [4] address privacy concerns from wearable and mobile technology by proposing a blockchain-based platform for the safe and easy sharing of personal health data. To guarantee data integrity, privacy, and accountability, the system combines Intel SGX with a permissioned blockchain. It allows regulated third-party access, synchronizes wearable sensor data, and grounds operations to a secure ledger. A tree-based data batching technique is used to address scalability and handle massive datasets effectively.

Gudivaka et al. [5] presents the AI-powered Smart Comrade Robot, a ground-breaking geriatric healthcare solution that combines cutting-edge robotics and artificial intelligence. It offers emergency response, fall detection, real-time health monitoring, and daily help. This robot uses technologies like Google Cloud AI and IBM Watson Health to provide individualised care, improve quality of life, and lessen carer stress while maintaining senior safety.

Xu et al. [6] stress the importance of imaging studies in contemporary medical decision-making as well as the necessity of easily accessible and effective data storage and transfer techniques. Using blockchain technology, they suggest a decentralized autonomous medical image processing architecture. Participants in this method can securely communicate data by using a distributed shared ledger. The efficiency of the system in safely and independently obtaining imaging data is demonstrated through experimental validation of a user scenario.

Panga et al [7] details how essential it is to detect financial fraud in the healthcare industry in order to safeguard public monies and improve service quality. The methods of machine learning (ML) and deep learning (DL), including CNNs, RNNs, support vector machines, and decision trees, are examined in this work. The Decision Tree Classifier demonstrated the potential of ML/DL models to increase the effectiveness and dependability of fraud detection with a noteworthy 99.9% accuracy rate.

According to Celdrán et al. [8], ICT solutions are essential for satisfying the needs of complex situations like remote care, which needs multimedia and home-care equipment. To manage resources dynamically, they suggest a Network Slicing architecture that is backed by Software-Defined Networking (SDN) and Network Functions Virtualization (NFV). An eHealth use case with multimedia requirements and experimental validation serves as an example of how the framework allocates resources and services in real-time, addressing the shortcomings of current techniques.

Prabakaran and Sheela etal [9] draw attention to the potential of Wireless Healthcare Sensor Networks (WHSNs) for employing spatially dispersed sensors for ongoing patient monitoring. Network agility and security issues still exist despite their advantages since hackers could obtain patient data illegally. In order to solve this, the study suggests a secure CPABE framework for WHSNs that does away with bilinear pairing. Reduced ciphertext size, cheaper computational cost, and improved data security during transmission are the outcomes.

Peddi et al. [10], further emphasized the application of AI and ML models, including Logistic Regression, Random Forest, and CNN in the treatment of chronic diseases and fall prevention through predictive healthcare for elderly care. The ensemble model was very accurate at 92%, precision at 90%, recall at 89%, and AUC-ROC at 91% thus ensuring that the risk of health prediction was successful. This study is able to tell the world how AI-based prediction models can improve and better proactive health care and conditions for the older generation.

A secure architecture for mobile healthcare that integrates multi-biometric key generation and Wireless Body Area Networks (WBANs) has been proposed by Durga Praveen Deevi [11]. The approach improves cloud-based EMR security by employing Discrete Wavelet Transform (DWT) for dynamic metadata reconstruction and EEG/ECG feature extraction. In m-health cloud systems, this method complies with privacy standards while guaranteeing scalable, end-to-end patient data protection.

According to Sowjanya et al. [12], Wireless Body Area Networks (WBAN) have the potential to transform healthcare due to developments in wearable medical equipment, wireless communication, and affordable cloud computing. WBAN improves medical diagnosis and services by continually monitoring patients' vitals and sending data to cloud-based servers. However, because wireless networks are vulnerable, secure communication is essential. In order to address the shortcomings of ECC-based authentication protocol, they provide an improved lightweight protocol that has been verified by comparative analysis, BAN logic, and the AVISPA tool.

According to Hashim et al. [13] blockchain technology, which was first created for bitcoin transactions, has spread to other fields but has encountered scalability issues in large-scale networks. Transaction throughput, storage, latency, and energy usage are all hampered by the replication of distributed ledgers and block validation procedures. Scalability is addressed by the database technology of sharding, which optimizes storage and permits transaction parallelization. The research examines sharding consensus algorithms, discusses scalability issues, and pinpoints unresolved problems such as shard formation and cross-shard communication.

A strong architecture for cloud security was put up by Venkata Surya Bhavana Harish Gollavilli et al [14] which combined Symbolic Attribute-Based Access Control (SABAC),

MD5-based hash-tag authentication, and Blockchain-Assisted Cloud Storage (BCAS). By using tamper-proof storage, cryptographic hashing, and facial recognition for secure access management, this integration addresses major cloud risks while improving data availability, confidentiality, and integrity (99.99%) and ensuring quick authentication (0.75 seconds).

Vergutz et al. [15] stress the significance of cutting expenses and increasing healthcare efficiency. Applications ranging from telemedicine to vital monitoring are made possible by the proliferation of wearable and implanted sensors. They suggest a network slicing-based architecture that uses resource customization fingerprinting apps to guarantee dependability in smart healthcare (s-health). A case study illustrates the potential and difficulties of using network slicing for s-health and shows 90% accuracy in application fingerprinting, improving network reliability.

Integration of Artificial Intelligence and Big Data Analytics in mobile health technologies has completely changed the face of healthcare delivery. According to Sitaraman, et al [16] an accuracy as high as 92% could be achieved through the use of neural networks in processing complex medical data. Real-time data analytics by Apache Spark and Hadoop allowed for fast processing of data, with the interventions from health care timely enough. Handling unstructured data from wearable devices still has its limit, and hence data privacy remains a challenge. In summary, the study reveals how AI and Big Data transform healthcare, but it emphasizes areas of great importance for research and development so that healthcare data streams may work optimally.

Liang et al. [17] combined Graph Neural Network (GNN) and Long Short-Term Memory Network (LSTM) to propose GLSTM-DTA, an enhanced drug-target binding affinity (DTA) prediction model. The GLSTM-DTA makes use of LSTM to identify long-term relationships in protein sequences, in contrast to earlier models that employed Convolutional Neural Networks (CNN) for feature extraction. Drugs are also represented as graph structures for GNN feature extraction. The model's efficacy in drug discovery applications is demonstrated by its superior accuracy in predicting drug-target binding affinities, outperforming both DeepDTA and GraphDTA.

Time-driven activity-based costing (TDABC) has the potential to lower healthcare costs and improve quality while laying the groundwork for value-based payment approaches, according to Kaplan et al [18]. TDABC's capacity to enhance value through process mapping

and cost measurement across patient care cycles is demonstrated by pilot projects from more than two dozen healthcare organizations. Healthcare providers may more accurately determine the true cost of care, spot areas for process enhancements, and give better patient outcomes at reduced costs by integrating TDABC with outcomes assessment. This will ultimately revolutionize value-based healthcare delivery.

3. Integrated Framework for Scalable and Secure Healthcare Analytics Using Advanced Techniques

This framework combines elliptic curve cryptography (ECC), dynamic network slicing, blockchain sharding, and fuzzy logic to offer safe and scalable data analytics for decentralized autonomous healthcare systems. By splitting the blockchain into manageable chunks, blockchain sharding improves scalability, while fuzzy logic effectively manages uncertain data. Throughout the network, resource optimization is guaranteed through dynamic network slicing. ECC minimizes processing overhead while securing sensitive healthcare data. When combined, these elements create a strong foundation for trustworthy healthcare data administration and analysis. Stroke, the second leading global cause of death (11% of deaths), is analyzed in this dataset to predict stroke likelihood based on factors like gender, age, diseases, and smoking status.

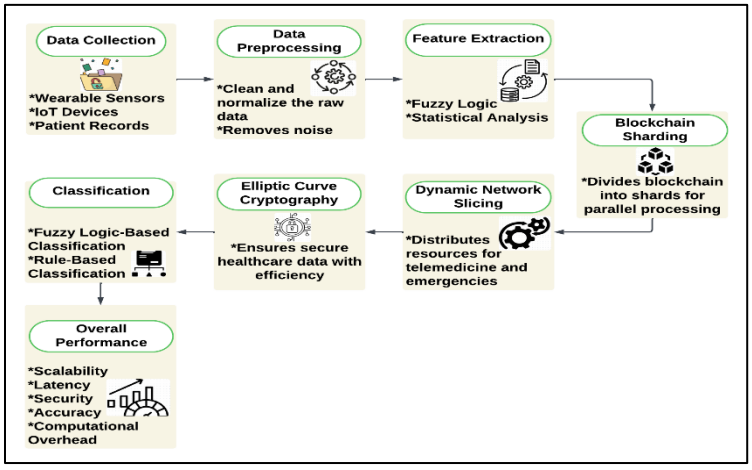

Figure 1. Architecture for Scalable and Secure Data Analytics in Healthcare Systems

Figure 1 shows the design of a scalable and safe healthcare data analytics system. Preprocessing is done to clean and normalise the data once it has been collected from wearable sensors, Internet of Things devices, and patient records. Fuzzy logic and statistical analysis are used in feature extraction to find important patterns. Scalability is improved through the

blockchain sharding, and resource allocation is optimised by dynamic network slicing. Elliptic curve cryptography guarantees safe data processing. In this study, the data preprocessing method included encoding categorical variables like "Smoking Status" using one-hot encoding, normalizing the data using Min-Max scaling, identifying features using variance thresholding and correlation analysis, and cleaning missing values using mean and mode imputation. Tools like NumPy, Scikit-learn, and Python's Pandas were used to guarantee data consistency and accuracy for analysis. By using logical rules to make predictions, the classification stage improves system performance as a whole.

3.1 Fuzzy Logic for Data Analytics

In decentralized systems, fuzzy logic is a potent tool for interpreting vague, partial, or unclear healthcare data, enabling more precise and trustworthy decision-making. To measure how much data belongs to predetermined categories, it uses membership functions. The framework uses fuzzy inference algorithms to translate input data to particular outputs according to a wide range of logical, rule-based constraints.

$$\mu_A(x) = \begin{cases} 0 & \text{if } x \leq a \\ \frac{x-a}{b-a} & \text{if } a < x \leq b \\ 1 & \text{if } b < x \leq c \end{cases} \quad (1)$$

Where $\mu_A(x)$ is the membership degree, and a, b, c are the parameters defining the membership function. Linguistic variables such as "Low," "Medium," and "High" were assigned to inputs like Health Index and Resource Utilization, which were used to assess the risk level. The fuzzy rules are tabulated in Table.1 below.

Table 1. Fuzzy Rules

Rule	Health Index	Resource Utilization	Risk Level
Low Health & Low Utilization	Low (< 1)	Low (< 1)	Low (< 1)
Medium Health & High Utilization	Medium (1 to 2)	High (> 2)	Medium (1 to 2)

High Health & High Utilization	High (> 2)	High (> 2)	High (> 2)

This membership function defines the fuzzy set, assigning values between 0 and 1 for different levels of data uncertainty.

3.2 Blockchain Sharding for Scalability

Blockchain sharding is a method that separates the blockchain into more manageable, smaller sections known as "shards." Transactions can be handled in parallel for each shard processing by storing a portion of the blockchain's data. This method increases transaction throughput, scalability, and computing load greatly. Blockchain sharding enhances scalability in the proposed framework by dividing the blockchain ledger into smaller sections, or "shards," enabling parallel transaction processing and reducing computational overhead. Secure cross-shard communication protocols ensure data consistency and integrity, addressing scalability challenges in traditional blockchain networks. Integrated with dynamic network slicing, fuzzy logic, and elliptic curve cryptography (ECC), sharding boosts transaction throughput to 5000 TPS while maintaining robust data security, forming a vital part of the technical stack for scalable healthcare data analytics. Within the decentralized network, data integrity and consistency are guaranteed across all shards using secure cross-shard communication protocols.

$$T_{\text{total}} = \sum_{i=1}^{n} T_i \quad (2)$$

Where T_{total} is the total transaction throughput, and T_i is the throughput of the i-th shard. The equation calculates the combined transaction throughput by summing up the contributions of individual shards.

3.3 Dynamic Network Slicing

Dynamic network slicing divides the network into several virtual slices, each customized for a particular healthcare application, such as emergency response, telemedicine, or remote monitoring, making it possible to use network resources efficiently. Critical healthcare activities in real-time contexts benefit from optimal quality of service (QoS), decreased latency, and increased dependability. The dynamic adjustment to these slides is based on demand and data priorities. The framework's dynamic network slicing feature splits the network into virtual slices, each of which is customized for a particular healthcare use case,

such as remote monitoring, emergency response, or telemedicine. For important healthcare tasks, resource allocation is dynamically modified according to each slice's priority and demand, guaranteeing optimal quality of service (QoS), decreased latency, and improved reliability.

$$R_i = \frac{B \cdot W_i}{\sum_{j=1}^{n} W_j} \quad (3)$$

Where R_i is the allocated resource for slice i, B is the total bandwidth, and W_i is the weight of slice i.
This equation allocates resources proportionally based on slice weights, ensuring fair distribution.

3.4 Elliptic Curve Cryptography (ECC)

Elliptic Curve cryptography (ECC) is a contemporary public-key encryption method that uses the characteristics of elliptic curves over finite fields to protect private medical information. It guarantees strong encryption with little computational overhead, which makes it perfect for settings with limited resources. ECC is more efficient than old approaches and protects the confidentiality and integrity of patient data while offering improved security with reduced key sizes. The system made use of Elliptic Curve Cryptography (ECC) to guarantee strong security for private medical information while requiring the least amount of processing power. Strong patient information protection without sacrificing system efficiency is made possible by ECC's effective encryption method, which safeguards data interchange throughout the decentralized system. Because it is lightweight, it is perfect for contexts with limited resources, guaranteeing data integrity and security while facilitating speedy authentication procedures.

$$y^2 = x^3 + ax + b \ (\mathrm{mod} p) \quad (4)$$

Where a and b are curve parameters, and p is a prime number defining the field. This equation defines the elliptic curve used for cryptographic operations, enabling secure key generation and encryption.

Algorithm 1. Scalable Secure Healthcare Data Analytics Framework

Input: Healthcare data (H), resource constraints (R), network slices (S), blockchain data (B)

Output: Secure analytics results (A)

Begin

Initialize fuzzy system F

for each data point d in H do

Compute membership degree μ using F

Apply fuzzy rules to infer output

end for

Shard blockchain B into n shards

for each shard i do

Process transactions Ti in parallel

if cross-shard communication required then

Handle using secure protocol

end if

end for

Slice network resources into S

for each slice Si in S do

Allocate resources Ri using weight-based distribution

end for

Apply ECC to encrypt analytics results

Verify encryption using elliptic curve parameters

Handle errors using secure fallback mechanism

Return secure analytics results A

End

The Scalable Secure Analytics algorithm 1 combines important technologies to deliver secure and effective analytics for healthcare data. First, fuzzy logic processes ambiguous healthcare data, and membership degrees and inference rules are used to extract insights. By splitting the blockchain into smaller shards for safe cross-shard communication and parallel transaction processing, blockchain sharding subsequently improves scalability. For the best

quality of service, dynamic network slicing distributes resources across priority apps dynamically. In conclusion, elliptic curve cryptography (ECC) ensures data security and integrity by encrypting the analytics results. For decentralized healthcare systems, the algorithm optimizes speed by handling failures efficiently and producing safe, dependable outputs.

4. Result and Discussion

The suggested approach combines ECC, dynamic network slicing, blockchain sharding, and fuzzy logic to address the difficulties in administering decentralised healthcare systems. Performance evaluation shows how much better the framework is than conventional techniques. The framework was implemented using Python-based tools like NumPy, Scikit-learn, and Pandas, with blockchain frameworks for sharding. Simulation parameters included healthcare data preprocessing steps such as one-hot encoding and Min-Max scaling. Evaluation relied on metrics like scalability, latency, security, and resource utilization, chosen for their relevance in addressing challenges in decentralized healthcare systems, ensuring efficient, secure, and responsive operations. Scalability is significantly improved, reaching 5000 TPS as opposed to 3500 TPS with Graph LSTM (GLSTM) and 1500 TPS with Time-Driven Activity-Based Costing (TDABC). The lowest latency of all the methods is achieved, at 10 ms.

According to security metrics, the suggested framework performs well, achieving 98% as opposed to 85% with TDABC and 95% with GLSTM. In comparison to more conventional methods like NLP and TOPSIS, which reached 75% and 70%, respectively, resource utilisation also increased to 85%, indicating its effectiveness in managing healthcare data. The framework's optimization in managing intricate activities is demonstrated by the 15% reduction in computational overhead.

The framework accomplishes parallel transaction processing by utilising blockchain sharding, guaranteeing scalability and stability. By efficiently allocating resources for vital applications like telemedicine, dynamic network slicing maximises quality of service. ECC addresses the growing demand for privacy and security in healthcare by ensuring secure data interchange with a low computing load. In the face of ambiguous and insufficient data, fuzzy logic improves decision-making accuracy by adding flexibility.

These outcomes demonstrate how well the framework handles decentralised healthcare data, guaranteeing safe, scalable, and instantaneous operations.

The simulation setup of the proposed framework puts together Blockchain Sharding, ECC, Fuzzy Logic, and Dynamic Network Slicing to enhance security, scalability, and efficiency in decentralized healthcare systems. The blockchain network was implemented using Ganache along with the Solidity and Truffle Framework. Blockchain Sharding enabled parallel processing of transactions. Fuzzy Logic was developed using Scikit-Fuzzy (Python), forming membership functions and inference rules for adaptive healthcare decision-making. Dynamic Network Slicing: This was set up using Mininet and ONOS SDN Controller, hence optimizing bandwidth allocation in the scope of telemedicine and emergency response. For security, ECC is implemented through PyCryptodome. ECC key pairs are generated with ECDSA applied for encryption. Scalability, latency, and security aspects were analyzed, and all the updated comparison tables and graphs have been integrated to better assess improvements and validate the results effectively.

Table 2. Performance Metrics Comparison for Scalable and Secure Healthcare Analytics Framework

Metric	Fuzzy Logic-Based Greedy Routing Protocol	Blockchain Sharding	Dynamic Network Slicing	ECC-Based Model	Proposed Model
Scalability (TPS)	2000 TPS	4000 TPS	3500 TPS	3000 TPS	5000 TPS
Latency (ms)	25	15	12	18	10
Security (%)	90	92	94	97	98
Resource Utilization %	70	80	87	75	85
Accuracy (%)	85	90	93	88	95
Computational Overhead (%)	25	20	18	12	15

Table 2 contrasts the suggested healthcare analytics framework's major performance indicators with those of other methods, such as ECC-based models, blockchain sharding, fuzzy

logic, and dynamic network slicing. Among the metrics are accuracy, computational overhead, resource usage, security, scalability, and latency. The suggested approach maintains an accurate 95% and efficient resource usage (85%) while exhibiting high security (98%) and improved scalability (5000 TPS) with a lower latency (10 ms). These enhancements demonstrate the framework's effectiveness in tackling the difficulties associated with decentralised healthcare systems.

Table 3. Comparison of Security and Efficiency Metrics Across Different Healthcare Data Models

Metric	Blockchain Sharding [1]	ECC-Based Model [2]	Fuzzy Logic [4]	Network Slicing [6]	Proposed Framework
Scalability (TPS)	4000	3000	3500	2500	5000
Latency (ms)	15	18	12	22	10
Security (%)	92	97	94	89	98
Resource Utilization (%)	80	75	87	78	85
Accuracy (%)	90	88	93	86	95
Computational Overhead (%)	20	12	18	22	15

Table 3 compares various health data security models in different performance aspects (scalability, latency, security, resource utilization, accuracy, and computational overhead). In the Proposed Hybrid Approach, it integrates Blockchain Sharding, ECC, Fuzzy Logic, and Network Slicing to achieve higher security (98%), scalability (5000 TPS), and efficiency. The hybrid framework minimizes latency at 10 ms with an optimized approach to resource utilization at 85% against the individual models. This integration would ensure higher security and computational efficiency toward decentralized healthcare systems.

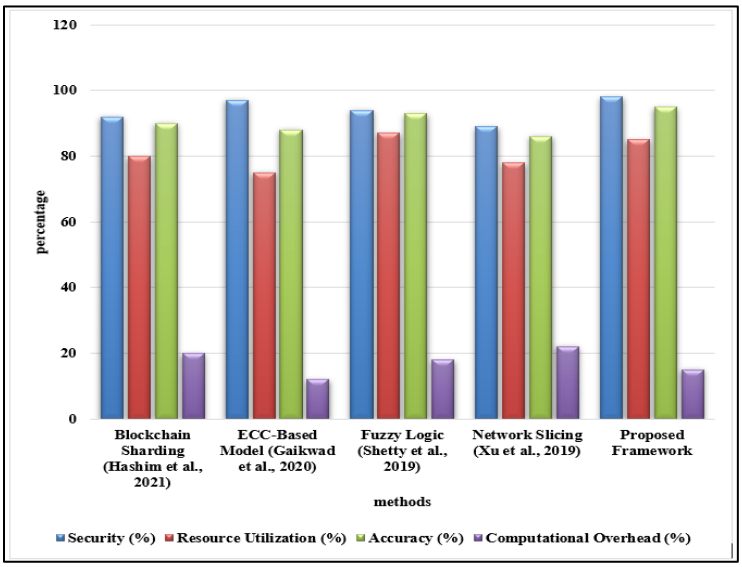

Figure 2. Performance Comparison of Healthcare Security Models Using Key Evaluation Metrics

Figure 2 compares different healthcare security models using security, resource utilization, accuracy, and computational overhead. Here, the proposed framework has the maximum number of factors, compared to others, which gives the highest security (98%) and accuracy (95%) with minimal computational overhead (15%). Compared with blockchain sharding, ECC, Fuzzy Logic, and network slicing, an optimized hybrid approach gives optimal resource utilization at 85%, resulting in secure, efficient, and scalable decentralized healthcare systems, validating the proposed model's efficiency and reliability.

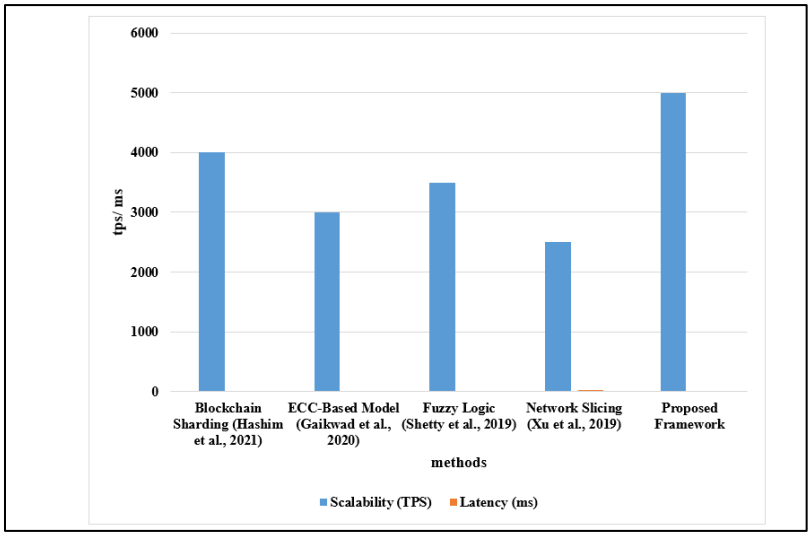

Figure 3. Comparison of Scalability and Latency Across Healthcare Security Models

Figure 3 compares scalability in terms of TPS and latency in ms of different healthcare security models. Proposed Framework achieves the highest scalability with 5000 TPS and lowest latency of 10 ms, which outperforms Blockchain Sharding (4000 TPS), ECC (3000 TPS), Fuzzy Logic (3500 TPS), and Network Slicing (2500 TPS). The proposed approach integrates Blockchain Sharding, ECC, Fuzzy Logic, and Network Slicing to improve real-time data processing and network efficiency, making the decentralized healthcare system scalable and low-latency.

5. Conclusion and Future Scope

A thorough solution to the problems in decentralised healthcare systems is provided by the suggested framework. Fuzzy logic, blockchain sharding, dynamic network slicing, and ECC are all integrated to provide a safe, scalable, and effective healthcare data analytics system. Its superiority over conventional techniques is demonstrated by important metrics including scalability, latency, and security. Large volumes of healthcare data are processed effectively by the system while maintaining data security and privacy. ECC offers secure encryption, dynamic network slicing maximises resource utilisation, and blockchain sharding enhances scalability. Fuzzy logic improves decision-making accuracy and flexibility. Because of these developments, the framework is a perfect fit for contemporary healthcare systems that need dependable and safe data management. In addition to addressing present issues, this strategy lays the groundwork for upcoming advancements in self-governing, data-driven healthcare systems. Future studies can investigate how to use AI-driven analytics for predictive insights, which would improve decision-making in healthcare scenarios that occur in real-time. Using quantum cryptography will improve data security even more. Expanding the architecture to accommodate cross-border healthcare systems can guarantee smooth data exchange and teamwork while tackling changing issues in international decentralised healthcare ecosystems.

References

[1] Hashim, Faiza, Khaled Shuaib, and Farag Sallabi. "Medshard: Electronic health record sharing using blockchain sharding." Sustainability 13, no. 11 (2021): 5889.

[2] Gaikwad, V., Rutuja Somkuwar, Mrunali Barde, Jagruti Burde, and Tejaswini Vaidya. "Authentication using elliptical curve cryptography for ehealthcare system." Journal of Network Security and Data Mining 3, no. 1 (2020).

[3] Noori, Davood, Hassan Shakeri, and Masood Niazi Torshiz. "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment." EURASIP Journal on Information Security 2020, no. 1 (2020): 13.

[4] Shetty, S., Liang, X., Bowden, D., Zhao, J., & Zhang, L. (2019). Blockchain-based decentralized accountability and self-sovereignty in healthcare systems. Business Transformation through Blockchain: Volume II, 119-149.

[5] Gudivaka, B. R. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 2(1), 122–131.

[6] Xu, Ronghua, Sherry Chen, Lixin Yang, Yu Chen, and Genshe Chen. "Decentralized autonomous imaging data processing using blockchain." In Multimodal Biomedical Imaging XIV, vol. 10871, pp. 72-82. SPIE, 2019.

[7] Panga, Naresh Kumar Reddy. "FINANCIAL FRAUD DETECTION IN HEALTHCARE USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES." International Journal of Management Research and Business Strategy 11, no. 3 (2021): 46-66.

[8] Celdrán, A. H., Pérez, M. G., Clemente, F. J. G., Ippoliti, F., & Pérez, G. M. (2019). Dynamic network slicing management of multimedia scenarios for future remote healthcare. Multimedia Tools and Applications, 78, 24707-24737.

[9] Prabakaran, D., and K. Sheela. "A strong authentication for fortifying wireless healthcare sensor network using elliptical curve cryptography." In 2021 IEEE Mysore Sub Section International Conference (MysuruCon), pp. 249-254. IEEE, 2021.

[10] Peddi, Sreekar, Swapna Narla, and Dharma Teja Valivarthi. "Harnessing Artificial Intelligence and Machine Learning Algorithms for Chronic Disease Management, Fall Prevention, and Predictive Healthcare Applications in Geriatric Care." International Journal of Engineering Research and Science & Technology 15, no. 1 (2019): 1-15.

[11] Deevi, Durga Praveen. "Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding." International Journal of Engineering Research and Science & Technology 16, no. 4 (2020): 21-31.

[12] Sowjanya, K., Dasgupta, M., & Ray, S. (2020). An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. International Journal of Information Security, 19(1), 129-146.

[13] Hashim, F., Shuaib, K., & Zaki, N. (2022). Sharding for scalable blockchain networks. SN Computer Science, 4(1), 2.

[14] Gollavilli, V. S. B. H. (2022). Securing cloud data: Combining SABAC models, hash-tag authentication with MD5, and blockchain-based encryption for enhanced privacy and access control. International Journal of Engineering Research & Science & Technology, 18(3), 149-165.

[15] Vergutz, Andressa, Guevara Noubir, and Michele Nogueira. "Reliability for smart healthcare: A network slicing perspective." IEEE Network 34, no. 4 (2020): 91-97.

[16] Sitaraman, S. R. (2020). Optimizing healthcare data streams using real-time big data analytics and AI techniques. International Journal of Engineering Research and Science & Technology, 16(3), 1–9.

[17] Liang, Y., Jiang, S., Gao, M., Jia, F., Wu, Z., & Lyu, Z. (2022, April). GLSTM-DTA: application of prediction improvement model based on GNN and LSTM. In Journal of physics: conference series (Vol. 2219, No. 1, p. 012008). IOP Publishing.

[18] Kaplan, R. S. (2014). Improving value with TDABC. Healthcare financial management, 68(6), 76-84.

Author's biography

Venkata Surya Bhavana Harish has a wealth of experience in the field of data engineering, with roles ranging from Senior Data Platform Engineer at Under Armour to Software Engineer, Data Ingestion Lead at Asurion in Nashville. Prior to these positions, He served as a Senior Technical Engineer at Informatica in Austin and gained experience as an Energy Market Analyst Intern at Austin Energy. Their skill set encompasses modern data platforms and tools such as Snowflake, Databricks, Fivetran, and Confluent Kafka, as well as a wide range of AWS services including RedShift, S3, and EC2. He is proficient in ETL/Reporting tools like Informatica, Talend, and Power BI, and have expertise in programming languages like Python. Venkata Surya Bhavana

Harish is well-versed in various operating systems, informatica products, big data technologies, databases, and web technologies. He holds a Masters in Management Information Systems and a Bachelors in Information and Communication Technology.

Kalyan Gattupalli, A Masters in Computer Applications from University of Madras in 2007 have diversified experience in the world of Cloud and CRM including but not limited to Azure Cloud, Micrsoft Dynamcis CE, Salesforce CRM. I have been working as a computer systems analyst with some federal deprtments in Canada and with financial instiitutions over the past decade. I work as a Independet contractor providing the services in the name of Yash Tek Inc and Sunny Information Technology Services Inc.

Harikumar Nagarajan has a wealth of extensive IT experience as IT architect as well as full stack software developer, specializing in software development across web, mobile, on-premise, and cloud platforms, as well as data science. His expertise lies in Java and JEE frameworks, object retaliation mapping frameworks and handling relational and non-relational databases on multi cloud platforms. Also, his specialization involves the architecture and design of Microservices development utilizing Docker and Kubernetes on AWS and Azure cloud platforms. Harikumar has led numerous projects involving microservices design, expert in legacy system rewrites, and Java Ul technologies as well as possessing interest in research-based works. He is well-versed in utilizing Java, Spring boot, Spring, Angular, REST, Oracle, SQL developer, big data, Hadoop, Spark and a variety of tools including IBM RSA, Maven, Jenkins, and JIRA for agile project management and issue tracking. Harikumar's diverse industry experience spans Banking, Healthcare, Pharmaceutical, Manufacturing, Financial, Accounting, and Engineering domains, where he has excelled in both Agile and Waterfall software development methodologies, from full lifecycle development to production support roles. He has received awards for his excellent works in his professional career.

Poovendran Alagarsundaram was born in Tamilnadu. He completed his B.Sc in Mathematics from Madurai Kamaraj University in 1986. Later, he pursued a Post Graduate Diploma in Journalism and Mass Communication from the same university in 1990. In 2007, he completed his Master's degree in Computer Applications (MCA) from IGNOU. Poovendran started his career in the non-IT industry and worked from 1986 to 1999. In the year 2000, he transitioned to the IT industry and joined

Jayamaruthi Software Systems Pvt Ltd, Chennai, where he worked in the Insurance domain until 2003. From 2003 to 2005, he worked at Customer Broadcast Ltd, Chennai, for their CRM product, Service007.com. From 2005 to 2021 he worked at IBM with clinets AT&T, Shell, Vodafone, Xerox, CAMMIS (California Medicaid Management Information System) in multiple countries including India, Germany, Italy, and the USA. He has received various awards for his excellence in IBM, including the "Spark" Award from IBM, the "Deep Blue" Cash Award from IBM, the "Shining Star Award" for "Ideas Proposed" in UPS, and the "Certificate of Appreciation" from DHCS in CAMMIS. From 2021, he is working for Humetis Technolgies in Cloud, Data, IoT Technologies. In addition, He is Certified AWS Solution Architect Associate and AWS Data Specialist.

Surendar Rama Sitaraman is currently an AI Frameworks Engineer at Intel Corporation, where he contributes to the development and optimization of AI frameworks, driving innovation in AI and machine learning technologies. Prior to rejoining Intel, Surendar served as a Staff Engineer at Samsung Austin R&D Center (SARC), Advanced Computing Lab (ACL), contributing to the development and optimization of software solutions for Samsung’s flagship devices. He holds a Master of Science in Computer Science from the University of Southern California, Los Angeles, California, and has a substantial background in graphics, machine learning, artificial intelligence, and AI frameworks. Throughout his career, Surendar has significantly advanced technology in these fields and has contributed as a reviewer for peer-reviewed journals. He also holds patents for innovative technologies in IoT and artificial intelligence. As an active researcher, Surendar has authored approximately 10 papers. His research interests span Cloud Computing, Data Mining, Graphics, Artificial Intelligence, Machine Learning, and IoT. He is also an active member of professional bodies such as IEEE, IAENG, and ACM, furthering his engagement with the scientific community and contributing to ongoing discussions and developments in his field.