IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 June 2024, accepted 19 July 2024, date of publication 23 July 2024, date of current version 2 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3432662

RESEARCH ARTICLE

Fuzzy-Enhanced Secure Messaging Framework for Smart Healthcare System

NISHI PATEL[1], DHYAN PATEL[1], NILESH KUMAR JADAV[1], (Graduate Student Member, IEEE), TEJAL RATHOD[1], SUDEEP TANWAR[1], (Senior Member, IEEE), GIOVANNI PAU[2], (Senior Member, IEEE), GULSHAN SHARMA[3], FAYEZ ALQAHTANI[4], AND AMR TOLBA[5], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat 382481, India
[2]Faculty of Engineering and Architecture, Kore University of Enna, 94100 Enna, Italy
[3]Department of Electrical Engineering Technology, University of Johannesburg, Johannesburg 2006, South Africa
[4]Software Engineering Department, College of Computer and Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia
[5]Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia

Corresponding authors: Giovanni Pau (giovanni.pau@unikore.it) and Sudeep Tanwar (sudeep.tanwar@nirmauni.ac.in)

This work was supported in part by King Saud University, Riyadh, Saudi Arabia, under Grant RSP2024R509; and in part by the Kore University of Enna, Enna, Italy.

ABSTRACT The healthcare industry is exponentially growing its dependence on smart wearables and remote devices for efficient treatment and diagnosis. These smart devices benefit the healthcare industry, but they raise serious security and integrity concerns while exchanging healthcare data. These devices are primarily meant for data dissemination; hence, they are equipped with weak security protocols that are susceptible to attacks like distributed denial-of-service (DDoS), data injection, and man-in-the-middle (MiTM) attacks. To circumvent the aforementioned security challenges, this article proposed a secure and intelligent data exchange framework for smart healthcare systems. For that, we amalgamate artificial intelligence (AI) and blockchain technology to strengthen the security of data dissemination between smart medical devices. Further, we adopted fuzzy logic that extracts the essential features from the healthcare security dataset to enhance the detection rate of AI models. We used different AI algorithms such as logistic regression (LR), random forest (RF), decision trees (DT), stochastic gradient descent (SGD), and Gaussian naive Bayes (GNB) to classify healthcare data into malicious and non-malicious. The predicted data can still be maneuvered by adversaries that introduce subtle changes that skew the results to their advantage. Therefore, we employed blockchain technology that stores non-malicious healthcare data (predicted data) from data tampering attacks. The developed smart contract validates the non-malicious healthcare data and only allows them to be securely stored inside the interplanetary file system (IPFS)-based public blockchain. The proposed framework is evaluated by considering various evaluation metrics like recall, precision, accuracy, F1 score, area under the curve (AUC) score, and blockchain scalability.

INDEX TERMS Healthcare data security, blockchain, fuzzy logic, artificial intelligence, machine learning, wearable devices, smart contract.

I. INTRODUCTION

The healthcare sector is essential for a nation's overall well-being and plays a central role in strengthening the economy. Today's healthcare landscape is undergoing rapid transformation with the integration of cutting-edge technologies, such as the Internet of Things (IoT), that facilitate seamless communication through sensors. Smart healthcare devices are equipped with different sensors to sense patients' vital conditions and forward the patient's medical data to other sensors for comprehensive health monitoring and diagnosis [1]. However, these sensors often rely on legacy systems with potentially vulnerable protocols and weak security measures that jeopardize the performance

The associate editor coordinating the review of this manuscript and approving it for publication was Peter Langendoerfer.

of the smart healthcare system. Due to their size and energy constraints, these sensors cannot employ robust protocols, making them susceptible to threats like distributed denial-of-service (DDoS) and man-in-the-middle attacks. Further, due to the inherent openness of the public Internet, the potential for data breaches and system compromises increases exponentially. This vulnerability underscores the pressing need for a proactive security mechanism to safeguard our evolving healthcare ecosystem.

There are wide-ranging applications in the healthcare industry, like electronic health records, real-time monitoring of health data, securing patient data, research purposes, and medicine supply chains that assist in managing various operations of smart healthcare systems. However, there is a need to authorize and safely store health records that help in efficient prognosis and diagnosis of the patients. Real-time monitoring of patients can help to detect potential health issues early, give patients personalized treatment for specific problems, and improve patient health through continuous tracking. There are many applications in clinical research for new drug innovations and research about new diseases where data health management is required. As there are wide-ranging applications in the healthcare industry, we need a secure framework that effectively confronts different security threats in the healthcare sector.

Numerous researchers have proposed various solutions that address security issues in healthcare IoT devices. For example, Madavi et al. [2] have designed an advanced light-weight cryptography (LWC) technique tailored for healthcare wearables, which amalgamates various data metrics into a singular 64-bit plaintext, delivering improved encryption efficiency over existing LWC methods. Similarly, Fareed and Yassin [3] have developed a potent authentication method for wireless body area networks (WBANs) that adeptly mitigate impersonation and spoofing threats and employs both rigorous and heuristic analysis tools to traditional encryption protocols. Despite their merits, these solutions possess a notable drawback: their cryptographic techniques are susceptible to decryption by modern supercomputing capabilities, underscoring the need for alternative security strategies.

The transition to artificial intelligence (AI) signifies a significant shift, holding promise as a prevailing technology to address security challenges [4]. Ghazal [5] have proposed a pioneering solution, IoT-AIS, by fusing AI and IoT to bolster healthcare security through patient data encryption, remote access, and unmatched data transmission rates. Similarly, Almalawi et al. [6] leverages AI's prowess, presented lionized remora optimization and serpent encryption (LRO-S), elevating patient data understanding and cloud security with heightened efficiency. Nonetheless, AI's potential has limitations; it necessitates synergy with other technologies. The susceptibility to manipulated datasets poses a major drawback–misleading model training results in erroneous predictions. This underscores AI's vulnerability, prompting a cautious approach and emphasizing the significance of untainted data for its success.

Leveraging the integration of artificial intelligence and blockchain, Bhashini et al. [7] presents a pioneering approach to ensuring secure data exchange and privacy preservation in smart healthcare systems [8], [9]. This innovative integration employs data sanitization and restoration techniques for confidentiality across tiers. Complementing this, Mancer et al. [10] implements a blockchain-driven medical record system, securely collecting and sharing electronic health records while leveraging big data models, multi-agent systems, and cloud computing for optimal storage. However, recognizing computational constraints, a comprehensive solution necessitates amalgamating diverse technologies, including fuzzy logic, to address the challenges effectively [11].

In the evolving realm of healthcare technology, the fusion of AI, blockchain, IoT security solutions, and advanced cryptographic techniques holds great promise for bolstering healthcare system security [12]. The integration of fuzzy logic further enhances our proposed model by addressing uncertainties and complementing traditional encryption methods. This comprehensive approach aims to harness the strengths of each technology, potentially improving encryption efficiency, countering decryption threats, ensuring secure data transmission, and upholding patient privacy throughout the supply chain. This confluence of technologies underscores our commitment to creating an adaptable security solution aligned with the dynamic healthcare landscape's needs. Thus, in this research work, we have taken a high-dimensional dataset that passes through a fuzzy layer to efficiently select essential features, which will reduce the computational overhead. The processed data is then utilized by various AI algorithms like random forest, decision trees, logistic regression, Gaussian naive Bayes, and SGD classifier to classify the data as malicious or non-malicious. Our research work is achieving an accuracy of 98.98% from the random forest classifier. Afterward, the secure data is stored in the blockchain layer, where it is stored in the inter-planetary file system (IPFS) with the help of smart contracts. This approach not only enhances the efficiency and accuracy of the AI models but also ensures the security of healthcare data from malicious users or attackers.

A. MOTIVATION

The healthcare sector provides health services to millions of people, directly or indirectly, which benefit their health for the rest of their lives. All the healthcare facilities collect patients' information, such as name, age, address, health issues, reports, samples, and additional personal data. Thus, storing data securely and authorizing it becomes the most crucial task. There can be various attacks on the data where malicious users can modify the information, which can cause irregular treatment or wrong diagnosis of patients by healthcare professionals. After analyzing different literature, [13], [14] [15], we realized that the aforementioned works have used AI models but are prone to malicious attackers, which can hamper the integrity of predicted healthcare data. Thus, the overall efficiency of the smart healthcare system is deteriorating. Further, most of the existing works have not employed efficient feature extraction for the high dimensional dataset used in securing healthcare applications. Similarly, [7], [10], [16] have not integrated AI techniques in the blockchain network; due to this, the mining cost becomes expensive. Also, they have not adopted IPFS advantage in their proposed solution, resulting in higher response time and lower scalability. Therefore, we present a fuzzy-enhanced AI and blockchain model that enhances accuracy through fuzzy-based feature selection, which will improve the performance of AI models and the blockchain layer for safely securing patient data.

B. NOVELTY

In recent years, the healthcare sector has been adopting smart devices and wearables to improve patient care by enabling real-time monitoring and seamless data sharing. Although these technologies provide numerous benefits, they also pose significant security risks. These security risks mainly arise from the reliance on weak protocols that make these systems vulnerable to a variety of cyber-attacks, such as distributed denial of service (DDoS), data injection, and man-in-the-middle (MiTM) attacks. While traditional cryptographic methods have been effective, they are gradually becoming inadequate against the sophisticated attacks enabled by modern supercomputer capabilities. While numerous researchers have used AI to enhance data security, there is a gap in the proper feature selection method. The literature also shows that many researchers have not explored the integration of AI and blockchain to develop multi-layer security mechanisms for health data. Therefore, there is a stringent requirement for a secure architecture. Motivated by these, this paper proposes a framework that integrates fuzzy, AI, and blockchain-based security mechanisms. Fuzzy logic is used for better feature selection, AI is used to classify data into malicious and non-malicious, and blockchain technology is used to store non-malicious healthcare data from data tampering attacks. The developed smart contract validates the non-malicious healthcare data and only allows it to be securely stored inside the interplanetary file system (IPFS)-based public blockchain.

C. RESEARCH CONTRIBUTION

The following are the salient contributions of the paper:

- To propose a secure data exchange framework for smart healthcare systems by amalgamating AI and blockchain.
- We utilized different AI algorithms, such as logistic regression (LR), random forest (RF), decision trees (DT), stochastic gradient descent (SGD), and Gaussian naive Bayes (GNB) to classify malicious and non-malicious healthcare data. Further, to enhance the detection rate of AI algorithms, we employed fuzzy logic that efficiently selects essential features from the network dataset, improving the overall performance of the proposed framework.
- We adopted blockchain technology to tackle data integrity attacks, where we first deployed a robust smart contract that validates the non-malicious healthcare data from AI models. Upon successful validation, the data is forwarded to the interplanetary file system (IPFS) to improve the response time and blockchain scalability.
- To evaluate the performance of the proposed framework using various performance evaluation metrics, such as accuracy, F1-score, precision, recall, entropy value, and blockchain scalability.

D. PAPER ORGANIZATION

The flow of the remaining paper is described as follows. Section II discusses the related work done and the motivation behind the proposed work by comparing it with the existing work. The system model and the problem formulation are presented in Section III. The proposed framework is displayed in Section IV. The results are discussed in Section V. Lastly, Section VI provides concluding remarks and shows the future scope of this work.

II. RELATED WORKS

Misra et al. [13] have proposed a framework that introduces health recommendations in IoT-driven health systems named kea edge(KEdge). It utilizes data from different sensors to calculate the health condition index (CI). It uses a convolutional neural network for heart disease detection and a random forest (RF) model for respiratory analysis. KEdge specifically includes the sound of the digital stethoscope SkopEdge, enhancing its diagnostic capabilities. Its accuracy rate is 98.53% for cardiac arrhythmias and 98.68% for respiratory diseases, coupled with good memory, demonstrates its practicality in real-world clinical practice. Wazid et al. [15] provides an in-depth study of the growing threat of ransomware, particularly in areas such as smart healthcare. Varieties of malware lock files that demand ransom are causing serious problems across industries and across borders. Considering blockchain as a powerful and secure solution, the authors have introduced a blockchain-enabled security framework against ransomware attacks for smart healthcare (BSFR-SH). They have tested the framework using several machine learning algorithms, in which the decision tree approach achieved an accuracy of 98%. Their results underscored the superiority of BSFR-SH in terms of accuracy, F1-score, and overall performance against other existing mechanisms.

Ieracitano et al. [22] has addressed the challenge of interpreting chest x-rays (CXR) for the diagnosis of COVID-19 by presenting a convolutional neural network for Covid-19 (CovNNet) which is a hypothetical assumption that supports deep learning models. They combine fuzzy features obtained from CXR and edge detection algorithms; the model surpasses deep learning models and reaches 81% classification accuracy. In addition, CovNNet achieved a sensitivity of 76% and an accuracy of 75.6%, demonstrating its potential to integrate into clinical decision-making. More importantly, its best performance is found when CXR and fuzzy features are combined with 80.9% accuracy. In their study of cloud applications, PG Shynu et al. [23]

TABLE 1. Comparative analysis of the proposed work with the existing state-of-the-art works.

Authors	Year	Objectives	Pros	Cons
Proposed framework	2024	To store and secure the healthcare data into an IPFS after utilizing the fuzzy and AI layer.	The proposed scheme archives 98.97% accuracy	-
Abid *et al.* [17]	2024	To provide a distributed access control-based scheme for transparency and privacy	Their proposed scheme utilized smart contract-enabled framework	Their proposed framework not included AI capabilities
Rahman *et al.* [18]	2024	To facilitate timely healthcare and diagnosis for COVID 19	They utilized fuzzy logic with IoT for the intelligent healthcare system	Not incorporated blockchain for the smart healthcare system
Panja *et al.* [19]	2023	To provide real real-time monitoring system for COVID-19 19	They have provided fuzzy logic-based solutions for the COVID-19 identification, prediction, and remote diagnosis	They have not included a blockchain-based solution for to secure the smart healthcare system
Mishra *et al.* [13]	2023	Determining CI utilizing a two-step analytical framework and a multiple rules FIS in order to assess the patient's severity.	The system utilizes a two-stage fuzzy inference model with a multi-step AI approach, which gives high accuracy.	Not implemented blockchain for security and privacy.
Deveci *et al.* [14]	2023	To identify and evaluate the key factors influencing the adoption and diffusion of AI technologies within the healthcare supply chain	Efficient adoption of AI technologies and fuzzy model in healthcare supply chain process.	The system does not consider complexity and computational challenges to the model.
Ali *et al.* [20]	2023	Using a fuzzy logic with blockchain to address authentication and security challenges in the digital healthcare system	High Authentication success rates, and security while maintaining efficient response times	Less accuracy and will not be robust when an attack that poses a high risk is carried out.
Wazid *et al.* [15]	2022	A new blockchain-enabled security architecture for smart healthcare to identify and combat ransomware attacks	higher accuracy and F1-score, less computational time and more transactions per second	The proposed system does not use fuzzy logic for selecting features.
Zulkifl *et al.* [21]	2022	An innovative system integrating fuzzy logic and blockchain technology is developed to prioritize AAA services within healthcare IoT settings	Used Hyperledger Fabric to achieve distributed trust, fuzziness and remove single point of failure from AAA services.	The system does not include the AI capability of blockchain and the framework has been tested on fewer datasets.
Ieracitano *et al.* [22]	2022	To enhance COVID-19 diagnosis using Chest X-rays (CXR) through the CovNNet model, a fusion of fuzzy logic and deep learning techniques.	Achieving 81% accuracy in an image dataset.Providing valuable insights using occlusion-based saliency maps.	Used a small-size dataset, and the No-Covid-19 class only included acute interstitial pneumonia.
Shynu *et al.* [23]	2021	To develop a blockchain-based healthcare service utilizing a rule-based clustering method and fuzzy inference system to forecast disorders.	Uses blockchain and fuzzy logic and has higher accuracy than the existing systems	Small dataset of 800 samples, security, and privacy can be enhanced by using some hybrid clustering or classification model.

demonstrated new blockchain technology for medical use with a focus on diabetes and heart disease. They issued a special policy as a collaborative effort to improve the effectiveness of the medical records of the patients. Next, they used the adaptive neuro-fuzzy inference system (FS-ANFIS), a hybrid model combining Artificial neural network (ANN) and fuzzy logic for disease prediction. The comparison shows the superiority of their methods, achieving 81% prediction accuracy and outperforming other neural network algorithms. The model also shows admirable purity and normalized mutual information (NMI) values for both disease datasets, marking a major advance in medical technology.

Deveci [14] explores the integration of AI in different areas that highlight the disparity in AI adoption around the world. It highlights the historical struggle for new technology, comparable to the initial decision taken during the Eighth Industrial Revolution. They used the Aczel-Alsina-based decision model in their research for the healthcare market, with a particular focus on post-pandemic export distribution. Research based on the Turkish healthcare system shows that technical power, testing, and government support are important for the success of artificial intelligence. This insight has the potential to pave the way for policy reforms to leverage AI in the healthcare supply chain. Zulkifl et al. [21] have addressed the critical challenge of ensuring authentication, authorization, and audit logs (AAA) services in the IoT environment, highlighting the limitations of traditional security mechanisms. The proposed fuzzy and blockchain-based adaptive security for healthcare IoT (FBASHI) framework integrates fuzzy logic and blockchain using hyperledger. Focusing on the IoT of healthcare, this study proposes a security behavior change for AAA services. Comparing FBASHI's performance with other blockchain solutions shows its potential to increase and improve latency, especially in high-security healthcare environments. Secure data transfer is important. This highlights FBASHI's innovation and utility in IoT security regarding its impact on healthcare practices and the optimisation of blockchain to improve data integrity and privacy policies.

Ali et al. [20] presented an optimisation fuzzy logic combined with blockchain technology to solve authentication and consensus issues important in digital healthcare. By integrating fuzzy logic, the system minimizes negative and non-negative effects and improves protection against attacks. Additionally, the integration of blockchain technology provides a unified, tamper-proof infrastructure to securely store and manage original and important confirmation information. The evaluation of the proposed method using the special database highlights its superior performance over existing approaches. It achieves minimal false rejection rate (FRR), false acceptance rate (FAR), and response time, ensuring high authentication accuracy consistently above 95%. The simulation underscores the system's robustness, with over 90% of authentication attempts achieving successful identification.

Panja et al. [19] provided real time monitoring system for COVID 19. They have introduced fuzzy logic-based solutions for COVID-19 identification, prediction, and remote diagnosis. Then, Abid et al. [17] proposed a distributed access control solution-based framework that utilized smart contracts. They introduced a smart contract-enabled access control framework for transparency and privacy in smart healthcare systems. Rahman et al. [18] enabled timely healthcare and diagnosis for COVID-19. They proposed a fuzzy logic-based solution with IoT for the intelligent healthcare system. Their proposed solution facilitates accurate and cost-efficient solutions for the remote healthcare monitoring and diagnosis of COVID-19 patients. Table 1 shows the comparative analysis of the proposed scheme with the existing schemes of the healthcare system.

III. SYSTEM MODEL AND PROBLEM FORMULATION

In this section, we discuss the system model with the problem formulation of the fuzzy-based intelligent healthcare framework as shown in FIGURE 1.

A. SYSTEM MODEL

Every patient has a smart wearable device that tracks and monitors the patient's health data. The primary goal of the proposed system is to secure the data from various attacks and store the patient's health data in the blockchain so that only trusted and authorised users, like doctors or patients, can access the data. Therefore, healthcare network data is passed through fuzzy logic and certain AI techniques, which ensure important and non-attacked data is stored on the blockchain through smart contracts. The system model comprises different patients P and smart wearable S in the following way.

$$P = \{P_1, P_2, \ldots, P_k, \ldots, P_N\} \tag{1}$$

$$S = \{S_1, S_2, \ldots, S_j, \ldots, S_N\} \tag{2}$$

where j stands for a single smart wearable and N for the total number of all smart wearables so that $1 \leq j \leq N$. k stands for a single person, and each patient P_k is outfitted with a wearable device. S_k, such that each S_i has sharing capabilities by which they can share data, this is represented as follows.

$$D = \{d_1, d_2, \ldots, d_N\} \tag{3}$$

$$S_i \xrightarrow{d_i}; S_j \tag{4}$$

Health data D_j from P_j is gathered by W_k and sent to AI model M for evaluation.

$$S_i \xrightarrow{collects} D_i \tag{5}$$

$$M \xrightarrow{evaluates}; D_j \tag{6}$$

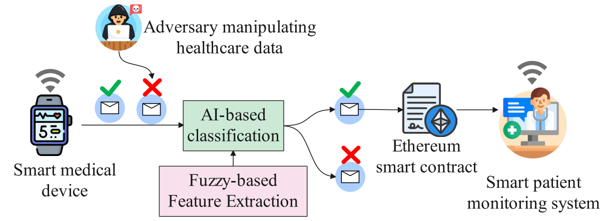

Adversary manipulating healthcare data
Smart medical device
AI-based classification
Fuzzy-based Feature Extraction
Ethereum smart contract
Smart patient monitoring system

FIGURE 1. System model.

Then, the AI system S predicts whether the data is attacked or not.

$$AIP(D_i) = \begin{cases} 1 & \text{if } D_i \text{ is safe} \\ 0 & \text{if } D_i \text{ is attacked} \end{cases} \tag{7}$$

If the data D_j is safe ($AIP(D_j) == 1$) from the malicious user or attacker, it goes through the smart contract SC, where it is transmitted to IPFS I, and is stored in the blockchain B which is thus only accessible to those involved in the patient's treatment. Mathematically, it is defined as follows.

$$SC(D_j) = D_j \times AIP(D_j) \tag{8}$$

$$I \leftarrow SC(D_j) \tag{9}$$

$$B \leftarrow I \tag{10}$$

B. PROBLEM FORMULATION

Based on the aforementioned discussion, we formulated an objective function (O_b), which aims to mitigate the security aspects of the smart healthcare system.

$$O_b = \sum_{i=1}^{m}(d_i) + \max \sum_{i=1}^{m}(M)(d_i) \tag{11}$$

where,

- O_b is the objective function.
- d_i represents all the data collected from the smart wearables.
- $M(d_i)$ represents the AI model applied to each data instance d_i.
- $\sum_{i=1}^{m}(d_i)$ Represents all the data collected from the smart wearables.
- $\max \sum_{i=1}^{m}(M)(d_i)$ is intended to maximize the accuracy of the AI model.

The main aim of the objective function is to enhance the security of the smart healthcare system by using fuzzy-assisted AI and blockchain technology. It ensures safe data collection from all smart wearables. Additionally, it focuses on maximizing the accuracy of the AI model so that only non-malicious healthcare data is stored in the blockchain. By filtering malicious data, the system ensures the integrity and security of health information. This approach ensures that the data collected is secure and reliable, making it accessible only to trusted and authorized users, such as physicians and patients. Hence, it improves the overall effectiveness of the healthcare system.

IV. PROPOSED FRAMEWORK

This section discusses the proposed fuzzy logic-based intelligent framework for the healthcare system. As shown in FIGURE 2, the proposed framework comprises data, fuzzy, AI, and blockchain layers.

A. DATA LAYER

The proposed framework encompasses a data layer of medical devices, each equipped with an array of sensors responsible for monitoring various patient health metrics such as heart rate, blood oxygen level, and temperature. However, the communication between these sensors and medical practitioners is far from secure. Despite technological advancements, the devices often operate on legacy systems that utilize insecure or weak protocols like HTTP. This opens the door for attackers to infiltrate the network and manipulate patient data, making the healthcare system vulnerable to DDoS and man-in-the-middle attacks. Such manipulations can be life-threatening, especially in critical care scenarios where accurate data is imperative for diagnosis and treatment. To counter these security threats, an advanced AI mechanism is needed to identify and mitigate such vulnerabilities, thereby ensuring the integrity and reliability of patient data.

B. FUZZY LAYER

1) DATASET DESCRIPTION

In our proposed framework, we employ the IEEE IoT healthcare security dataset developed by Hussain et al. [24]. It contains both normal and malicious traffic data from IoT healthcare service applications. This dataset provides realistic traffic information for normal operations and various cyberattacks. It addresses specific security challenges such as intrusion detection, data integrity, and the availability of healthcare services. Including a wide range of attack scenarios, including specific DDoS and MQTT attacks, the dataset is valuable for developing and testing IoT-based security solutions. It features a comprehensive set of columns capturing network attributes and message queuing telemetry transport (MQTT) protocol parameters, such as time-related frames, internet protocol (IP) addresses, transmission control protocol (TCP) ports, and flags, as well as MQTT message types, client IDs, and quality of service levels, culminating in a 'label' column for binary classification. The dataset, comprising 188695 rows and 43 columns, is for a binary classification problem with class labels ranging from 0 to 1. This dataset enables us to robustly test our AI mechanisms for identifying and mitigating security vulnerabilities in healthcare IoT networks.

2) FEATURE EXTRACTION

When dealing with large and dimensional data, one often encounters problems with irrelevant features, missing values, and other discrepancies that affect the quality of model predictions. Selecting tree-based feature selection algorithms according to traditional rules is not enough and often leads to overfitting and putting too much emphasis on differences between different groups. To solve these problems, we use the fuzzy-based feature selection method. Unlike traditional algorithms, fuzzy-based methods provide a powerful technique for dealing with noise and uncertainty, allowing for a better understanding of values. This approach leads to a more efficient training process and improves the performance of our machine-learning models.

In the framework used in this study, the data is then split into training and test sets using the 80-20 distribution. In order to ensure the equality and comparability of the features in the training process, the min-max scaling method is used by keeping all the variables [0, 1] the same for many things.

In the feature selection phase, we incorporate a technique called fuzzification, which is derived from fuzzy logic. Various types of fuzzification functions are employed, such as Gaussian, triangular, and multiple forms of sigmoid functions. Each function is designed to suit data distributions, thereby optimizing the usefulness of each feature. For example, gaussian functions work well for features that follow a distribution, while sigmoid functions are more suitable for features with an s-shaped distribution curve. Through the fuzzification process, the dataset's crisp values are transformed into degrees of membership, providing nuanced representations that enhance the classifier's decision-making capabilities. After applying the preprocessing and fuzzification steps for the dataset, the subsequent stage involves computing entropy for each feature. Fuzzy entropy serves as a metric to evaluate how a feature distinguishes between different classes. The formula used to calculate entropy for a given feature is provided as follows.

$$\text{Fuzzy Entropy}(i) = \sum_{j=1}^{n} \mu_{ij} \cdot \log(\mu_{ij} + 1 \times 10^{-6}) + (1 - \mu_{ij}) \cdot \log(1 - \mu_{ij} + 1 \times 10^{-6}) \tag{12}$$

In this formula, n is the number of data points, μ_{ij} denotes the fuzzy membership value j^{th} data point for the i^{th}feature. Once the fuzzy entropy values are computed for each feature, they are ranked in descending order, starting with the top-ranked feature and gradually adding one additional feature at a time. To evaluate each composed feature set, we use regression models and employ 5-fold cross-validation to assess their

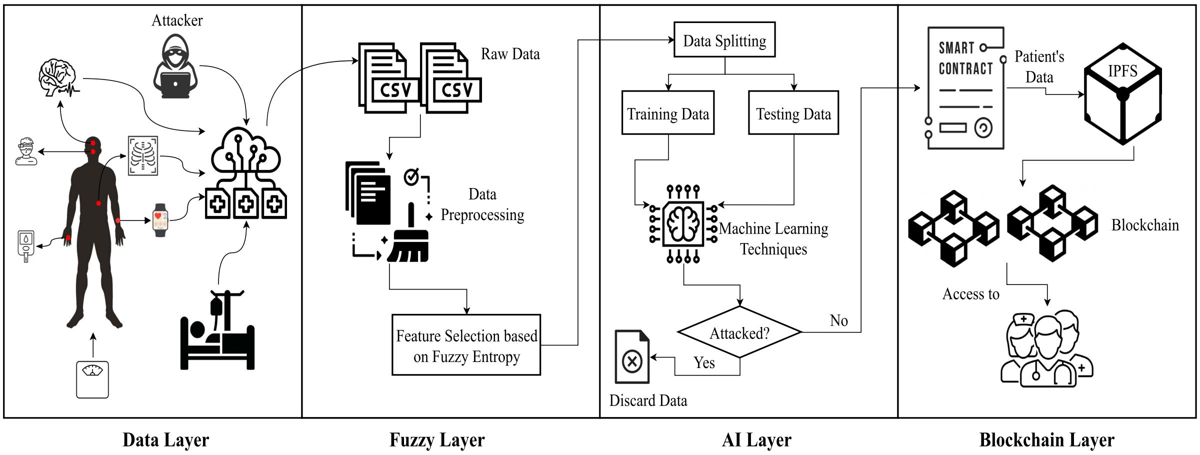


FIGURE 2. Proposed framework.

performance for each newly formed feature set. The study investigated various feature set sizes, ranging from the top 10 to the top 42 features, based on fuzzy entropy scores. It was observed that the mean cross-validated accuracy reached its peak at around 0.969 when utilising a set of 16 features. However, adding more features beyond this count led to a decrease in model accuracy, emphasising the importance of feature selection. Let D represent the size of the dataset used in our proposed framework. We D' from the fuzzy-based approach.

$$D = D^{188695\times 42} \xrightarrow{Fuzzification} D^{188695\times 16} = D' \tag{13}$$

The mean cross-validated accuracy achieved its zenith of approximately 0.968 with this reduced feature set of 16, reinforcing the importance of precise feature selection in achieving high classification performance. In the proposed architecture, we have used fuzzy entropy-based feature selection to pinpoint key features that help in distinguishing between attacked and non-attacked data. After feature selection in the fuzzy layer, the data will be sent and classified in the AI layer after training and testing of the data.

C. AI LAYER

In the AI layer of the pipeline, we experimented with various classifiers, including logistic regression (LR), stochastic gradient descent (SGD) classifiers, RF, gaussian naive Bayes (GNB), and decision trees (DT), to classify the pre-processed and feature-selected data. Then, we assessed this model using metrics such as accuracy, precision, recall, F1 score, and area under the curve (AUC). Notably, the RF achieved an accuracy of 0.992 while requiring a training time of only 0.345 seconds. The model also performed well on performance measures, with an F1 score of 0.992 and an AUC of 0.999. These outcomes highlight the effectiveness of our feature selection process.

In the proposed architecture, after AI algorithms are trained and validated on these selected features, which show high accuracy in classification tasks, all the data flagged as 'attacked' is promptly discarded to maintain system integrity. Meanwhile, the verified, non-attacked data is then sent to the blockchain layer for further secure processing and storage.

D. BLOCKCHAIN LAYER

The blockchain layer in the proposed framework ensures security, data integrity, and data validity. Blockchain is crucial in healthcare for safeguarding sensitive electronic records, including patient and billing information [25]. The core features of blockchain are transparency, immutability, and distributed networks, which enhance data security and trust. The technology also streamlines processes, from medication safety monitoring to credential verification, thereby reducing fraud and errors. The classified, non-attacked data from the AI layer is now routed through the blockchain network with the help of smart contracts, which validate the data. Then, the data is stored in the interplanetary file system (IPFS)-based public blockchain. In this blockchain layer, smart contracts are employed to exclusively permit access to the data by the patient and authorized medical practitioners. These smart contracts facilitate not only secure storage but also allow doctors to prescribe medication and suggest treatments based on verified data. Employing features like Merkle Trees and unique digital signatures, the blockchain layer ensures the integrity, security, and quick retrieval of healthcare data. Thus, this integrated approach enhances both privacy and the quality of patient care. Moreover, Algorithm 1 and 2 discuss fuzzy feature selection and health data security, respectively. FIGURE 3 shows the organizational flow of the proposed framework, where each layer briefly demonstrates its involvement in securing the data exchange of a smart healthcare system. Thus, the blockchain layer ensures the security of a smart healthcare system, and the data is accessed by authorized persons only. Smart Ambulance data collected from IoT devices would be safely stored in the IPFS system through smart contracts in the blockchain layer. This secure and streamlined process would be beneficial in emergency situations for the patients. Also, it helps the medical personnel to access the correct and authorized data which will result in effective treatment and care of the patients. This robust security mechanism thus plays a pivotal role in improving patient outcomes and fostering confidence in healthcare systems.

Algorithm 1 Fuzzy Feature Selection

```
Input:
  • $data$: Dataset
  • $target$: Labels
  • $function\_mapping$: Mapping of features to fuzzification functions
Output:
  • Optimal feature set and corresponding accuracy
procedure FuzzyFeatureSelection($data$, $target$, $function\_mapping$)
    Divide $data$ into training and test sets
    Normalize both sets
    for each feature in training data do
        Fuzzify using $function\_mapping$
    end for
    for each feature do
        Compute fuzzy entropy
    end for
    Rank features by entropy
    for each possible feature subset do
        Select features
        Perform cross-validation
        Store subset and accuracy
    end for
    Choose the subset with the highest accuracy
    return selected subset and accuracy
end procedure
```

V. RESULTS AND DISCUSSION

The results are included in the analysis of various machine learning models and their performance metrics, providing insight into their effectiveness in specific contexts. An interesting aspect of evaluation is the integration of fuzzy logic, a method that captures approximate causes by considering the fact that things can happen in half at once. This approach reflects more concrete concepts than binary thinking and is particularly relevant to real-life situations where there is ambiguity and uncertainty. This section aims to provide a holistic understanding of the model's power, accuracy, and overall performance by juxtaposing fuzzy logic with traditional machine learning metrics. Through detailed illustrations and analysis, readers will gain insight into the integration of traditional methods and flexible fuzzy logic in predicting results.

A. EXPERIMENTAL SETUP AND SIMULATION ANALYSIS

We have used Anaconda Jupyter version 6.4.5 as a development environment for the implementation and simulation of fuzzy logic. Anaconda is a popular platform that is easier to use and provides integrated solutions for data science and scientific computing research. We have implemented the whole research work in the Python version (3.9.7). We have used it due to its adaptability and extensive support for the vast range of libraries available. Libraries like NumPy, Pandas, Scikit-Learn, Seborn, Matplotlib, and Time are used to implement our proposed work. NumPy (Version 1.19.5): NumPy is a fundamental library for numerical computing in Python. It enables efficient manipulation of large multi-dimensional arrays and provides essential mathematical functions to support various data analysis tasks. Pandas (Version 1.3.4) creates easy-to-use data frames for data analysis, time series, and statistics. Scikit-learn Sklearn (version 0.24.2): We have implemented this library for training and testing the data and also for preprocessing the data using the MinMaxScaler library present in it. Seaborn (Version 0.11.2): We have used Seaborn for statistical data visualization. Matplotlib (Version 3.4.3) was used to plot various graphs and to visualize and analyze the data. Time (Version 3.9.7): We have used the built-in time library to calculate the time taken for implementation.

Algorithm 2 Sequential Flow of AI Layer

```
Input:
  • $D = \{d_1, d_2, \ldots, d_N\}$: Input health data
  • $RF$: Trained random forest model
Output:
  • Secure health data stored in the blockchain $B$
procedure DataSecurityRandomForest($D$, $RF$)
    Data evaluation
    for each $d_i$ in $D$ do
        Evaluate $d_i$ using $RF$
        $AIP(d_i) \leftarrow 1$ if $d_i$ is safe, 0 otherwise
    end for
    Safety Check and Data Storage
    for each $d_i$ in $D$ do
        if $AIP(d_i) == 1$ then
            Process $d_i$ through smart contract $SC$
            Store $d_i$ in IPFS $I$
            Add $d_i$ to blockchain $B$
        end if
    end for
end procedure
```

For blockchain implementation, we used an Ethereum-based Remix integrated development environment (IDE) to develop a smart contract. The smart contract has different user-defined functions, such as submitData(), getPatientData(), transferOwnership(), and isDataValidated(), written in solidity language with version v0.8.25. The aforementioned functions assist in securing the patient's healthcare data, which is marked as non-malicious by the AI model. Further, the functions were compiled using a solidity compiler with version 0.8.26+commit.8a97fa7a and deployed on an Ethereum blockchain. To deploy, we used a MetaMask wallet (v11.16.13) and a Sepolia test

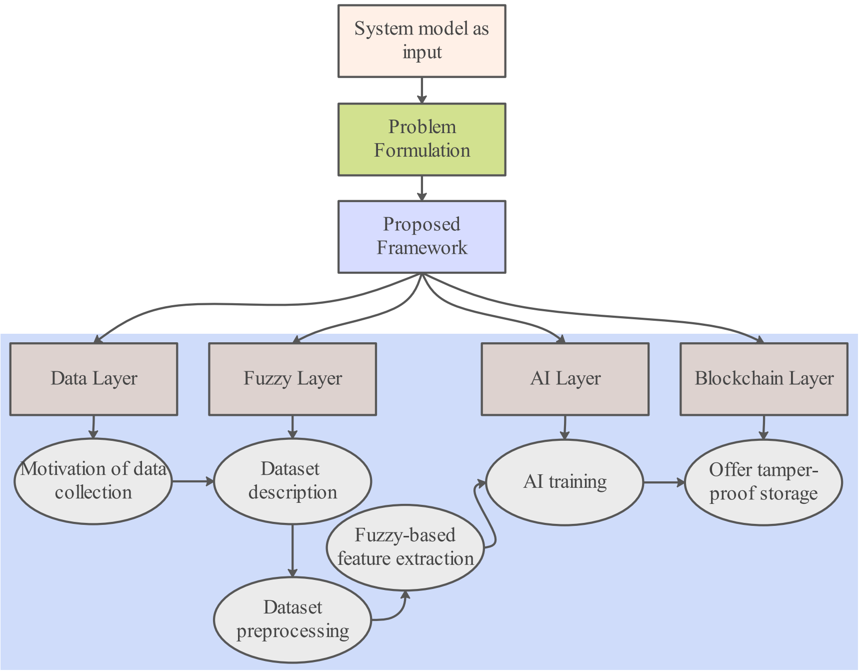


FIGURE 3. Organizational flow of the proposed framework.

TABLE 2. Experimental parameters used in the proposed framework.

Fuzzy logic parameters (for feature selection)	
Function	**Parameters**
fuzzify_gaussian	c: mean, sigma: std
fuzzify_sigmoid	a: 1, b: median
fuzzify_mirrored_sigmoid	a: 1, b: median
fuzzify_triangular	a: 25th, b: median, c: 75th
fuzzify_categorical	categories: unique values
AI model hyperparameters (for model training)	
Parameters	**Values**
max_depth	3
min_samples_split	10
min_samples_leaf	8
random_state	0
n_estimators	15
Blockchain parameters (for secure storage)	
Parameters	**Values**
Development environment	Remix (v0.50.0)
Programming language	Solidity (v0.8.25)
Compiler	Solidity compiler(0.8.26+commit.8a97fa7a)
Wallet	MetaMask wallet (v11.16.13)
Test network	Sepolia

c= Mean (center) of the Gaussian function, b = median (midpoint) of the sigmoid function, a = controls the slope (steepness) of the sigmoid function.

network - sepolia.etherscan.io. The entire proposed framework is implemented with a system with specifications such as 8GB RAM, Intel Core i7 processor with 8 CPUs, and DirectX 12. Table 2 shows all the experimental parameters used by each layer of the proposed framework.

B. EVALUATION METRICS

In this section, we have discussed the metrics to evaluate the proposed framework. In the context of health data security, true positive (s_j) means the AI model truly predicted the safe health data as safe; false positive (p_j) means the AI model wrongly predicted the attacked health data as safe; true negative (v_j) means the AI model truly predicted the attacked health data as attacked; false negative (m_j) means the AI model wrongly predicted the safe health data as attacked.

1) ACCURACY (OVERALL CLASSIFICATION ACCURACY)

Accuracy is defined as the ability of the model to correctly classify safe health data as "safe" and attacked health data as "attacked." It is the ratio of the sum of true positive and true negative samples ($s_j + v_j$) to all the samples of the prediction ($s_j + p_j + v_j + m_j$). Mathematically, it is expressed as follows.

$$\text{Accuracy} = \frac{s_j + v_j}{s_j + p_j + v_j + m_j} \tag{14}$$

2) PRECISION (DATA SAFETY IDENTIFICATION RATE)

Precision is defined as the model's ability to correctly identify safe health data among all instances classified as safe. It is the ratio of true positive samples (s_j) to the sum of true positive and false positive samples ($s_j + p_j$). Mathematically, it is expressed as follows.

$$\text{Precision} = \frac{s_j}{s_j + p_j} \tag{15}$$

3) RECALL (DATA SAFETY DETECTION RATE)

It is defined as the model's ability to correctly identify safe health data among all actual safe health data in the sample. It is the ratio of true positive samples (s_j) to the sum of true positive and false negative samples ($s_j + m_j$). Mathematically,

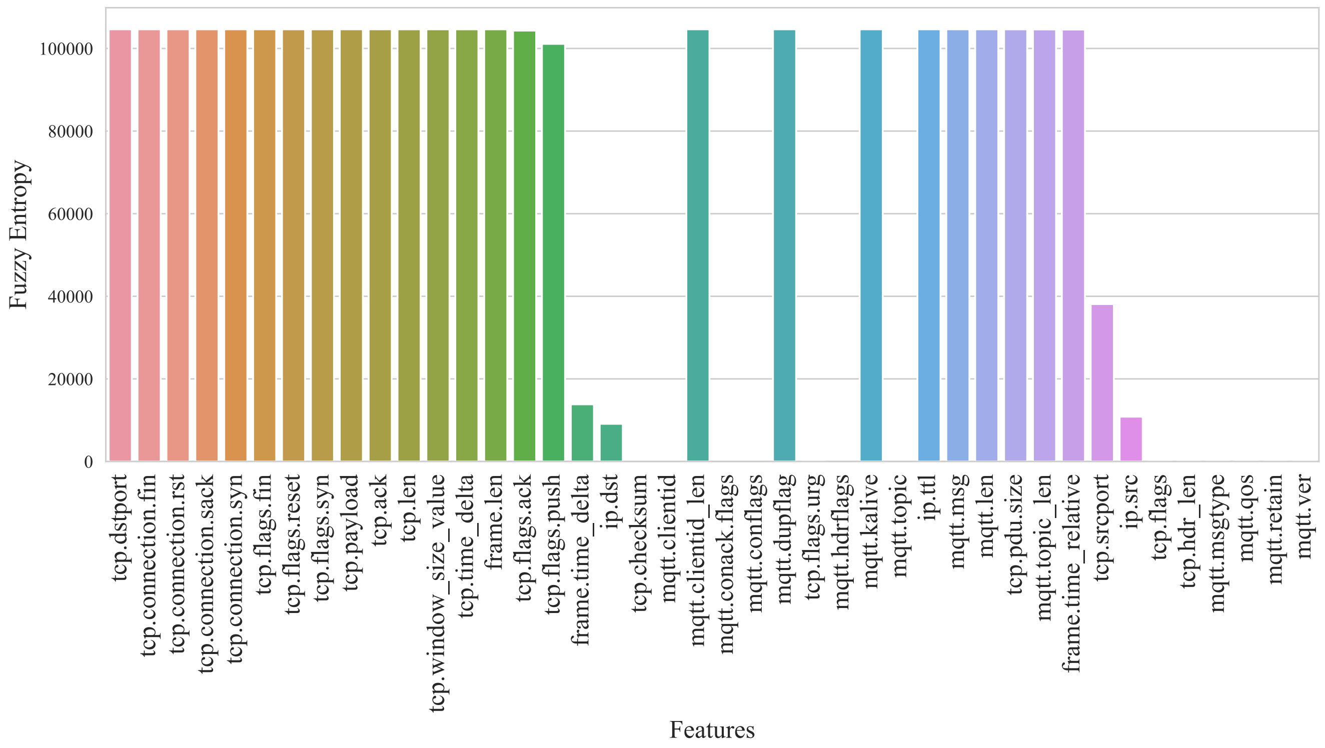


FIGURE 4. Entropy of features.

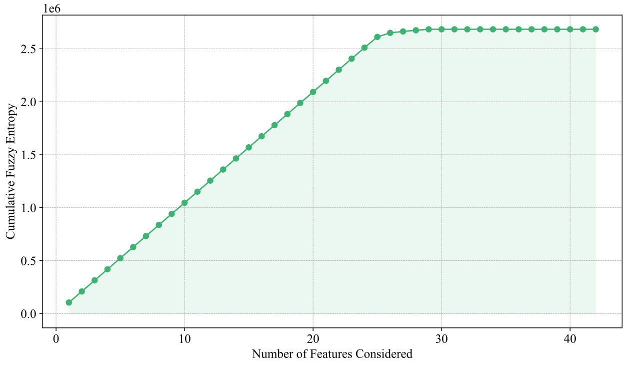


FIGURE 5. Cumulative fuzzy entropy.

it is expressed as follows.

$$\text{Recall} = \frac{s_j}{s_j + m_j} \tag{16}$$

4) F1 SCORE (HARMONIC MEAN OF SAFETY IDENTIFICATION AND DETECTION RATES)

The F1 Score is the harmonic mean of precision and recall. It describes the balance between the precision and recall for both safe and attacked health data. Mathematically, it is expressed as follows.

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{17}$$

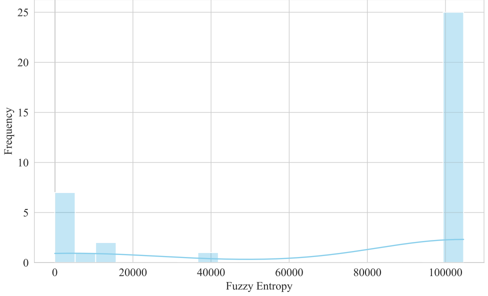


FIGURE 6. Distribution of fuzzy entropy values.

C. PERFORMANCE ANALYSIS OF THE FUZZY AND AI LAYER

FIGURE 4 illustrates the relationship between features and their corresponding calculated fuzzy entropy. Higher entropy values indicate features that capture more complex data patterns, while lower values suggest more deterministic patterns. This graph serves as a roadmap, highlighting the significance of utilizing high-entropy features to enhance the predictive capabilities of the model. FIGURE 5 shows how fuzzy entropy builds up across a group of characteristics in descending order. The x-axis represents the number of features considered, whereas the y-axis depicts the cumulative fuzzy entropy. There is an initial spike, but it gets stabilized after 25 features, which suggests that adding more features after this point would not be beneficial. To gain a more detailed understanding of the fuzzy entropy

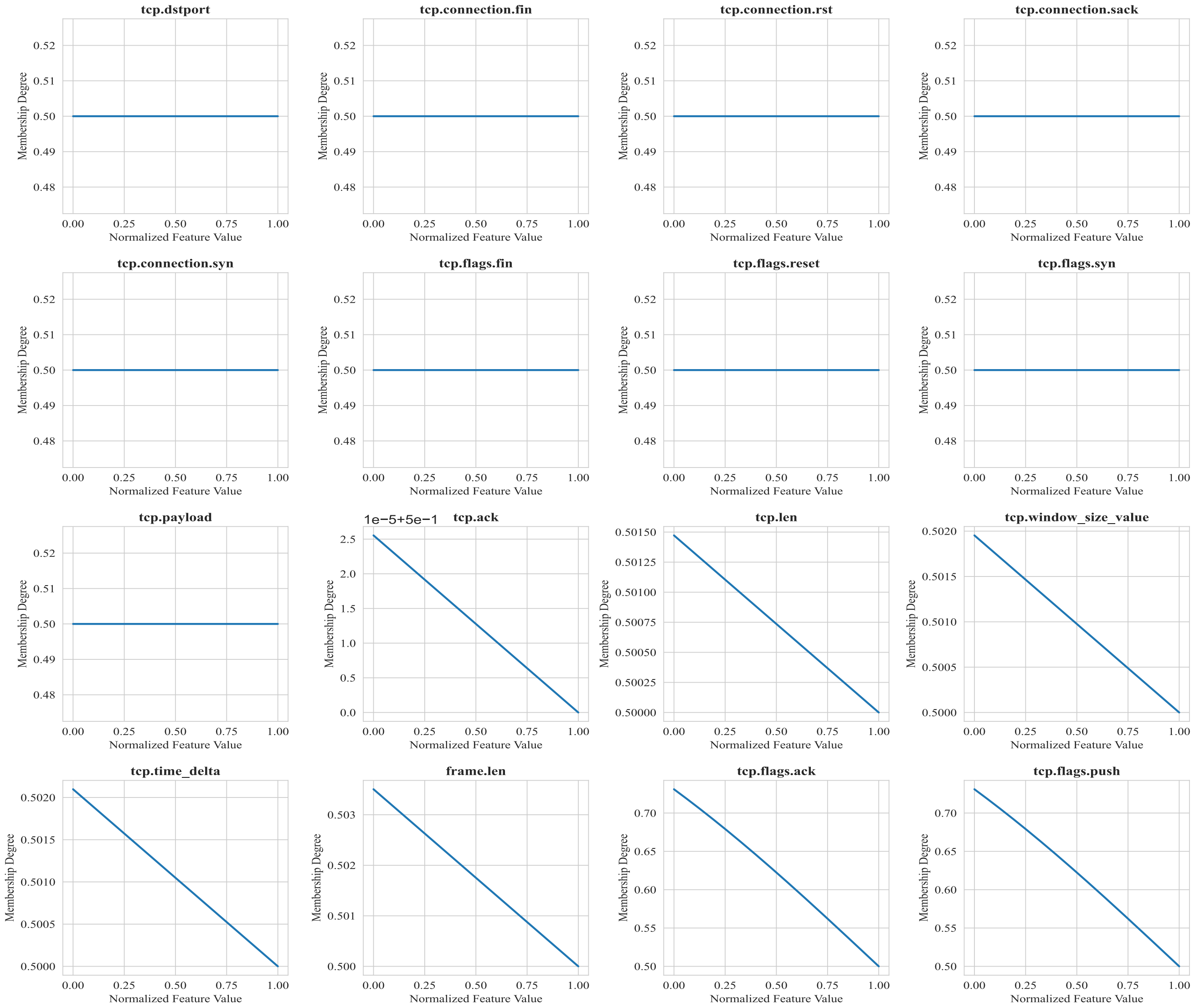


FIGURE 7. Feature values.

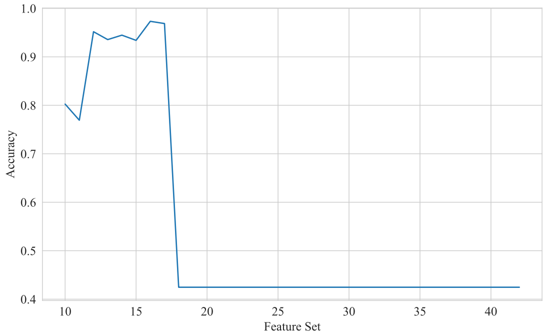
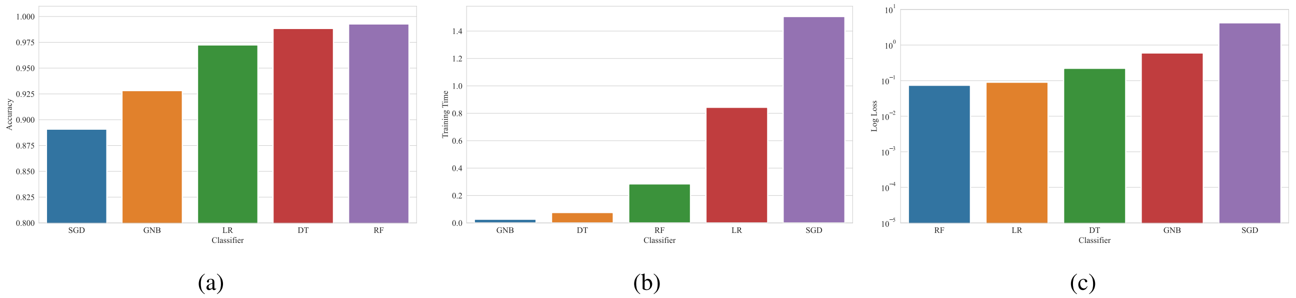


FIGURE 8. Accuracy of different feature sets.

distribution, a histogram combined with kernel density estimation (KDE) was constructed in FIGURE 6. The distribution exhibits considerable variability, with a distinct peak of about 104,633 entropy values. This peak indicates that a significant subset of features share high entropy values, which can indicate high prediction power. In contrast, low entropy peaks, especially around 13,838 and 9,119, indicate features with limited predictive power. This statistical insight enhances the feature selection method, potentially increasing the prediction accuracy of the model.

As depicted in FIGURE 7, the visualization shows the membership functions of various selected features, demonstrating the degree to which each normalized feature value belongs to a certain fuzzy set. The x-axis indicates the normalized feature value, whereas the y-axis represents the membership degree. Moreover, FIGURE 8 demonstrates the feature selection process undertaken using fuzzy entropy, starting with an initial set of 10 features. As the number of characteristics that are integrated varies, the graph shows a shifting trend in the mean cross-validated accuracy. Notably, optimal performance is achieved with a



(a)

(b)

(c)

FIGURE 9. Performance of AI classifiers - (a) Accuracy. (b) Training time. (c) Log loss.

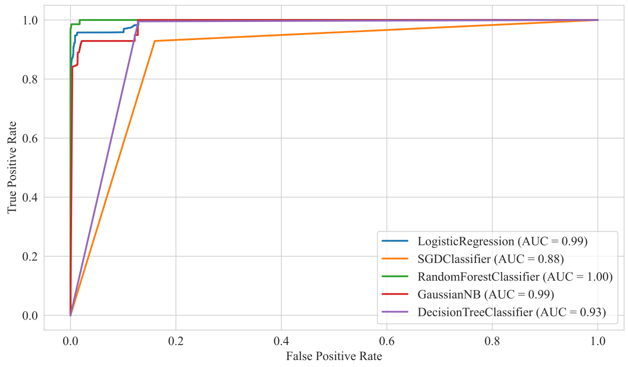


FIGURE 10. ROC curve of different AI classifiers.

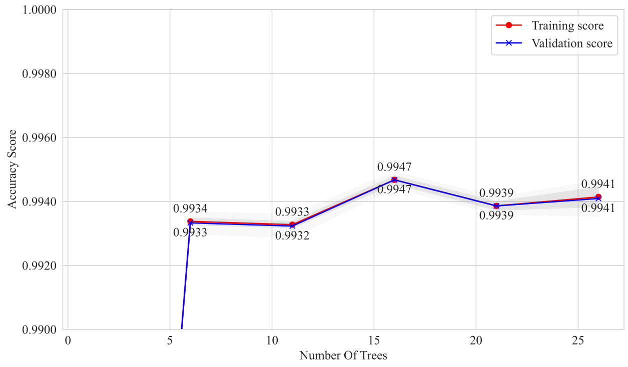


FIGURE 11. Validation curve of RF.

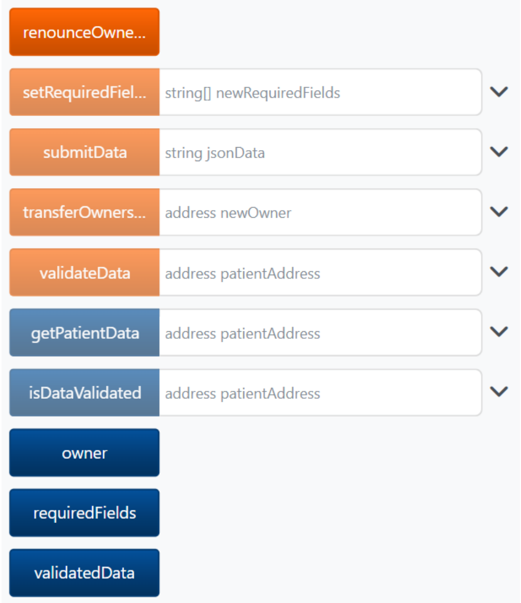


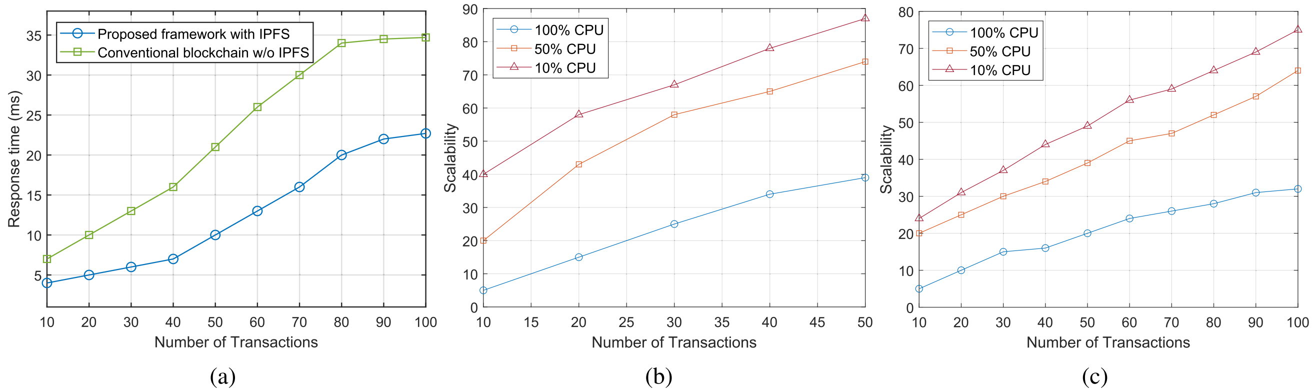
FIGURE 12. Smart contract interface.

TABLE 3. Comparison of accuracy and incorporation of fuzzy logic and blockchain technology in different studies.

Authors	Accuracy	Fuzzy	Blockchain
[15]	98.98	✗	✓
[13]	98.53	✓	✗
[20]	95.08	✓	✓
[22]	80.10	✗	✗
Proposed	98.97	✓	✓

subset of 16 distinct features, registering a mean accuracy of approximately 96.86%. We can conclude that not all features contribute equally, so selecting the subset would be appropriate. After thorough analysis, it's evident that not all features in the dataset hold equal weight, with the first 16 features accounting for half of the total fuzzy entropy, highlighting their significance. FIGURE 9a showcases the accuracy scores of several machine learning classifiers like LR, SGD classifier, RF, GNB, and DT. Among these, RF emerges as the most accurate and precise, delivering an accuracy of approximately 98.97%. However, efficiency is also of paramount importance. As illustrated in FIGURE 9b, the Gaussian Naive Bayes is the quickest, completing training in just over 0.026 seconds. LR and SGD classifiers perform fairly accurately but are the most time-consuming. These variations in training times showcase the computational trade-offs inherent in different models.Thus, Table 3 shows the comparison of the proposed framework with the existing state-of-the-art approaches where we can see that the proposed framework is achieving 98.97% accuracy in which we have integrated fuzzy and blockchain layer.

Similarly, FIGURE 9c displays the log loss values for several classifiers, notably LR, SGD classifier, RF, GNB, and DT. The log loss measures the uncertainty of predictions, with lower values denoting better performance. Remarkably, the RF classifier achieves the lowest log loss of about 0.07411,



(a) (b) (c)

FIGURE 13. (a) Comparison of blockchain's response time. Scalability performance with 100%, 50%, and 10% CPU utilization (b) at 50 data transactions. (c) at 100 data transactions.

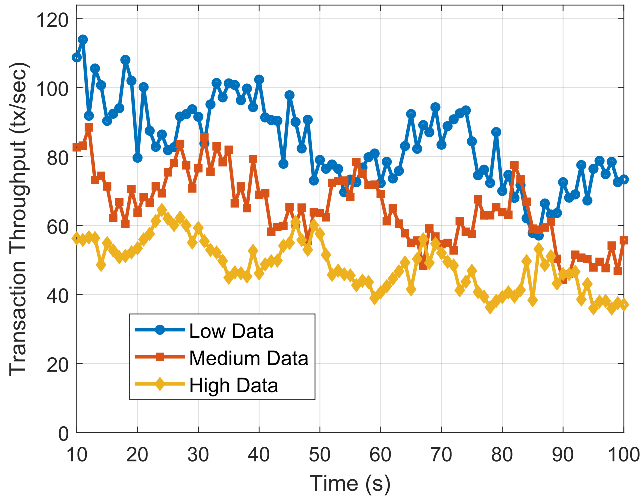


FIGURE 14. Transaction throughput comparison with dynamic data size.

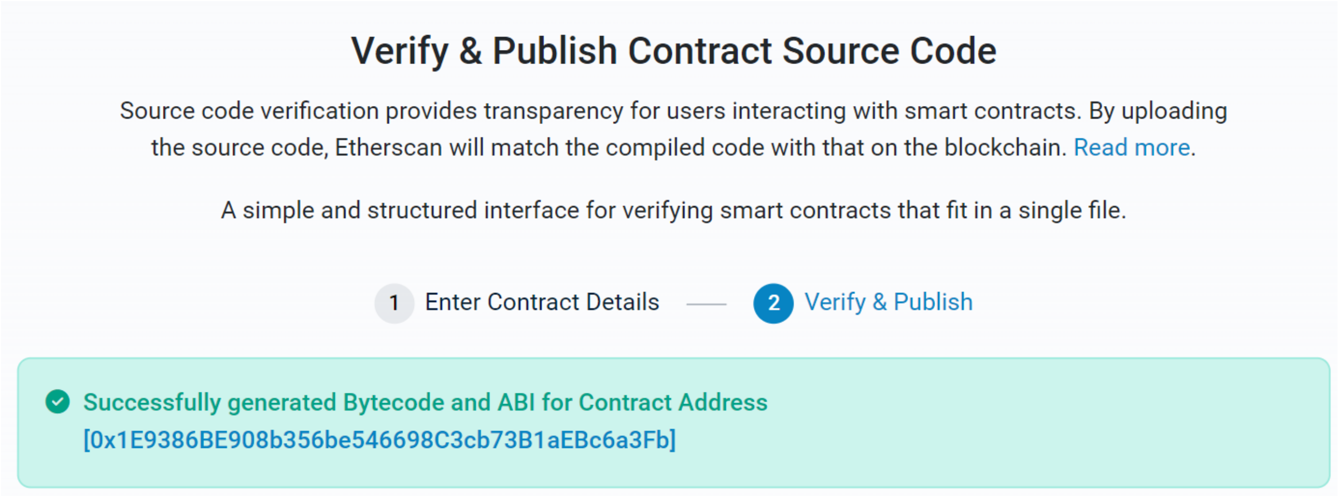
TABLE 4. Performance evaluation metrics of different AI classifiers.

Model	Precision	Recall	F1 Score	AUC
LR	0.99617	0.95757	0.97649	0.99475
DT	0.85082	0.99532	0.91741	0.93325
SGD classifier	0.90523	0.82898	0.86542	0.8845
RF	0.99867	0.98602	0.99231	0.99998
GaussianNB	0.98170	0.84676	0.90925	0.98823

indicating high-confidence predictions. On the other end, the SGD classifier logs a value of approximately 4.2198, pointing to increased prediction uncertainty. Thus, this graph points to the dual importance of accuracy and prediction confidence in model assessment.

Further, FIGURE 10 represents the receiver operating characteristic (ROC) curve, which offers a comparative visualization of different classifiers' performance. The AUC score of RF is around 0.9997, which indicates that it handles classification well. LR and GNB also perform well, with AUC scores of 0.9946 and 0.9882, respectively. On the other hand, the decision tree classifier and SGD's low AUC value for the model highlight its poor ability to distinguish between classes and indicate a need for a significant improvement in its classification performance. Table 4 depicts the performance metrics of five different classifiers: LR, DT, SGD classifier, RF, and Gaussian classifier. We have produced results using metrics like precision, recall, F1 score, and AUC. In terms of classifier performance, RF emerged as a frontrunner, boasting superior accuracy, optimal log loss, and a commendable AUC score. While GNB was the swiftest in training, the RF not only excelled in accuracy but also demonstrated efficient training time. Thus, considering both precision and efficiency, the RF stands out as the most promising model for this dataset.

FIGURE 11 illustrates the validation curve for the RF classifier, demonstrating the model's performance as a function of the number of trees. The x-axis represents the range of the hyper-parameter "Number of Trees" varying from 1 to 31 in increments of 5. The y-axis shows the model's accuracy score, confined to a narrow range between 0.9790 and 0.9994 for enhanced visibility of variations. The red and blue lines represent average accuracy scores for training and validation sets, respectively. The shaded area around these lines represents the standard deviation of the scores and provides a measure of the consistency of the sample. Notably, both training and validation accuracy display a trend of improvement as the number of trees increases, converging around an accuracy score of approximately 0.99. The fact that the standard deviation is particularly narrow for large trees indicates that the model is robust with little overfitting. Based on a comprehensive evaluation of ML models, RF stands out as a superior model due to its performance on several metrics. RF has the highest accuracy at about 98.97%. Although GNB was the fastest, it completed the training in just over 0.026 seconds. Despite the speed, its lower accuracy compared to RF makes it unsuitable for this application. Moreover, RF has a minimum log loss value of about 0.07411. The validation curve illustrates the robustness of the RF with minimum overfitting, and an AUC score of almost 0.9997 shows its high classification efficiency. Given its high accuracy, reasonable training time, and strong predictive reliability, RF stands out as the best model for classification.



Verify & Publish Contract Source Code

Source code verification provides transparency for users interacting with smart contracts. By uploading the source code, Etherscan will match the compiled code with that on the blockchain. Read more.

A simple and structured interface for verifying smart contracts that fit in a single file.

1 Enter Contract Details — 2 Verify & Publish

Successfully generated Bytecode and ABI for Contract Address [0x1E9386BE908b356be546698C3cb73B1aEBc6a3Fb]

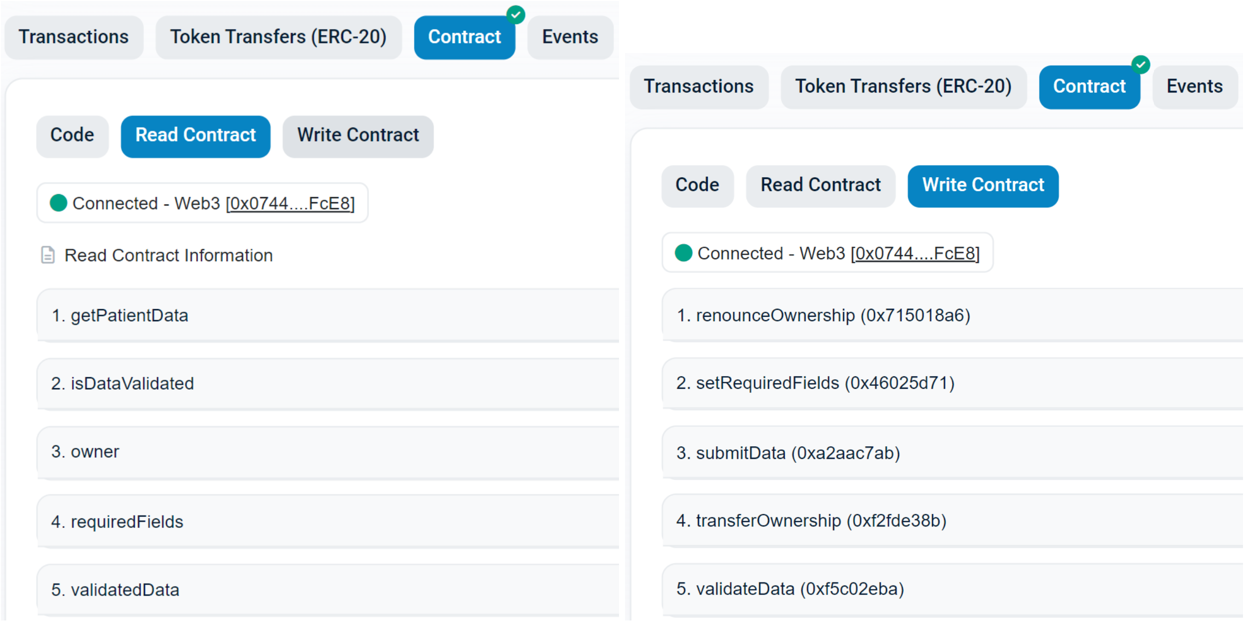
FIGURE 15. Verification of the deployed smart contract.

D. PERFORMANCE ANALYSIS OF THE PROPOSED BLOCKCHAIN

Further, we evaluated the performance of the proposed framework by analyzing the blockchain's transaction cost and IPFS bandwidth utilization. In the blockchain layer, we implemented a smart contract to validate the non-attack data of healthcare systems (e.g., smart wearable) to protect them from data manipulation/injection attacks. FIGURE12 shows the smart contract interface with different user-defined functions, such as owner(), setRequiredFields(), validateData(), submitData(), and getPatientData(). These functions act as data validators by which each entity of the proposed framework has to verify the healthcare data that is going to be stored in the blockchain nodes. Conventionally, it is verified by the intermediaries; however, it can be tainted to manipulate the data and jeopardize the entire healthcare system. Therefore, smart contracts play an essential role in verification and data validation and enforce access control to ensure data privacy and integrity.

Once the data is validated, it is forwarded to the IPFS container using IPFS application programming interfaces (APIs) and storeDataOnIPFS() function. It computes the hash for each incoming validated data and simultaneously forwards it to the immutable blockchain ledger. Here, we used Filebase APIs to get the IPFS bucket, where each healthcare data gets a unique IPFS content identifier (CID) for storage and retrieval purposes. It is to be noted that the use of IPFS improves the response time and performance of the blockchain network. Since only hash is stored in the blockchain instead of the original healthcare data, the blockchain's response time is reduced. FIGURE 13a shows the response time comparison between the conventional blockchain (without IPFS) and the blockchain with IPFS. Based on the aforesaid discussion, it is evident from FIGURE 13a that the proposed framework with IPFS has a lesser response time compared to the conventional blockchain. It can be observed that the blockchain's processing capacity is directly influenced by the response time. In essence, the shorter the response time, the greater the number of data transactions the blockchain can effectively process. Hence, a scalability parameter is utilized to measure blockchain performance under the influence of CPU utilization. FIGURE 13b and FIGURE 13c shows the scalability performance with 10%, 50%, and 100% CPU utilization when data is transacted (stored and retrieved). From the graphs, it becomes evident that the integration of IPFS represents a significant and transformative advantage in the context of scalability within blockchain ecosystems. In addition to that, we also evaluated our smart contract with dynamic data size for scalability assessment. From smart contract, we send different chunks of data to IPFS, such as low data, medium data, and high data of sizes, ∼100-200 KB, ∼1.83- 2.16 MB, and ∼ 4.56 - 7.38 MB, respectively. Based on such dynamic transactions in the blockchain, we found that due to the incorporation of IPFS, the response time becomes minimal and eventually improves scalability. FIGURE 14 illustrates the transaction throughput comparison with different data sizes. From the graph, we can observe that low data has higher transaction throughput at the initial time (10-20 (s)), but later, it gradually decreases due to the high IPFS bandwidth utilization by other participants. Similarly, medium and high data have better throughput at the initial timespan, but since it has a huge amount of data (in MBs) traversing through the blockchain network, it has lower transaction throughput compared to low data (shown in the black line). Overall, the blockchain network offers a transaction throughput of ∼ 60 tx/sec while storing and retrieving the transaction from IPFS storage. The transaction and response time are directly related to scalability, and since the proposed framework has higher transaction throughput and minimum response time for storing and retrieving healthcare data, it has higher scalability compared to the conventional blockchain.

Furthermore, we verified the developed smart contract on a Sepolia test network via a MetaMask wallet. Smart



Connected - Web3 [0x0744....FcE8]

Read Contract Information

1. getPatientData
2. isDataValidated
3. owner
4. requiredFields
5. validatedData

(a)

Connected - Web3 [0x0744....FcE8]

1. renounceOwnership (0x715018a6)
2. setRequiredFields (0x46025d71)
3. submitData (0xa2aac7ab)
4. transferOwnership (0xf2fde38b)
5. validateData (0xf5c02eba)

(b)

FIGURE 16. **(a) Read contract and (b) write contract on Sepolia Etherscan.**

contract verification ensures that the contract is free from potential security risks. Additionally, it provides transparency and ensures that the contract's logic is correct and developed for the intended behavior. This verification ensures that the contract's logic correctly implements the intended behavior, reducing the risk of unexpected behavior or errors. Toward this goal, we deployed the smart contract on Sepolia.etherscan.io with the contract hash address - 0 × 1E9386BE908b356be546698C3cb73B1aEBc6a3Fb as shown in FIGURE 15. From the verified smart contract, we can access both the read and write smart contract functionalities. FIGURE 16 shows the read and write contract of the deployed smart contract, which has all the functions related to get() and set() that secures the predicted healthcare data.

VI. CONCLUSION AND FUTURE SCOPE

In this article, we proposed a novel secure data dissemination framework to secure healthcare data in smart healthcare systems. For that, we amalgamate AI and blockchain technology that first classifies healthcare data, i.e., malicious and non-malicious data, and then offers secure data storage. Firstly, we pre-processed the data and performed feature scaling on the standard network security dataset by applying fuzzy logic. Then, we trained the AI algorithms, such as LR, RF, DT, Gaussian classifier, and SGD, on this specific dataset to classify malicious and non-malicious healthcare data. Fuzzy logic reduces the computation overhead from the AI algorithms since it efficiently selects the crucial features from the dataset and only allows them to partake in AI training. However, since the non-attacked predicted data can be maneuvered by the attackers, there is an imperative requirement for tampered-proof storage to tackle data integrity issues in the healthcare domain. Therefore, the non-attacked predicted data is forwarded to the blockchain network, where we developed a smart contract that takes the data from the AI model to offer secure data storage in the immutable ledger. To improve the scalability performance of the blockchain network, we employed IPFS, which computes the hash of each raw healthcare data and forwards the hash to the immutable ledger. Lastly, the proposed framework is evaluated against several performance metrics like accuracy, log loss curve, ROC curve, and validation curve. The results show that the RF classifier achieves 98.97% accuracy compared to other classifiers.

In future work, we will enhance the performance of the proposed framework by incorporating the imperative benefits of the 5G network. We will also address the integration challenges that lie across all the layers of the proposed framework, which will be crucial in strengthening the security of the proposed framework. It will make the proposed framework more robust and enhance efficiency. In the data layer, work should be done in order to make the heterogeneous data more synchronous and secure, which can be integrated with the fuzzy layer. In the future, we will work in the fuzzy layer to decrease the computational overhead of feature extraction and also maintain the accuracy of AI models. While integrating the AI layer, we can encounter challenges like scalability issues of ML models, computational resources with DL models, latency, and synchronization challenges with the blockchain layer. Therefore, in the future, we will focus on reducing these integration problems.

REFERENCES

[1] S. Chaudhary, R. Kakkar, N. K. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, M. D. Alshehri, R. Sharma, G. Sharma, and I. E. Davidson, "A taxonomy on smart healthcare technologies: Security framework, case study, and future directions," *J. Sensors*, vol. 2022, pp. 1–30, Jul. 2022.

[2] B. M. KP and N. Patwari, "Embedded light-weight cryptography technique to preserve privacy of healthcare wearable IoT device data," in *Proc. Int. Conf. Distrib. Comput. Electr. Circuits Electron.*, Apr. 2023, pp. 1–6.

[3] M. Fareed and A. A. Yassin, "A lightweight and secure multilayer authentication scheme for wireless body area networks in healthcare system," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 13, no. 2, p. 1782, Apr. 2023.

[4] K. Chauhan, S. Jani, D. Thakkar, R. Dave, J. Bhatia, S. Tanwar, and M. S. Obaidat, "Automated machine learning: The new wave of machine learning," in *Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 205–212.

[5] T. M. Ghazal, "Internet of Things with artificial intelligence for health care security," *Arabian J. Sci. Eng.*, vol. 1, no. 1, pp. 1–23, 2021.

[6] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing security of healthcare data for a modern healthcare system," *Sensors*, vol. 23, no. 7, p. 3612, Mar. 2023.

[7] K. P. Bhashini, K. Nalini, and P. Lalitha, "An end-to-end secured blockchain framework for Internet of Things based smart healthcare," in *Proc. 5th Int. Conf. Electr., Comput. Commun. Technol.*, Feb. 2023, pp. 1–4.

[8] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain technology for secure supply chain management: A comprehensive review," *IEEE Access*, vol. 10, pp. 85493–85517, 2022.

[9] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for Industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, pp. 69160–69199, 2022.

[10] M. Mancer, K. M. Akram, E. Barka, K. Okba, S. Sihem, S. Harous, B. Athamena, and Z. Houhamdi, "Blockchain technology for secure shared medical data," in *Proc. Int. Arab Conf. Inf. Technol. (ACIT)*, Nov. 2022, pp. 1–6.

[11] N. K. Jadav, R. Gupta, R. Kakkar, and S. Tanwar, "Intelligent onion routing and UAV-based electronic health record sharing framework for Healthcare 4.0," in *Proc. IEEE Conf. Comput. Commun. Workshops*, May 2023, pp. 1–6.

[12] D. Jadav, N. K. Jadav, R. Gupta, S. Tanwar, O. Alfarraj, A. Tolba, M. S. Raboaca, and V. Marina, "A trustworthy healthcare management framework using amalgamation of AI and blockchain network," *Mathematics*, vol. 11, no. 3, p. 637, Jan. 2023.

[13] S. Misra, S. Pal, P. K. Deb, and E. Gupta, "KEdge: Fuzzy-based multi-AI model coalescence solution for mobile healthcare system," *IEEE Syst. J.*, vol. 17, no. 2, pp. 1721–1728, Jun. 2023.

[14] M. Deveci, "Effective use of artificial intelligence in healthcare supply chain resilience using fuzzy decision-making model," *Soft Comput.*, vol. 1, pp. 1–14, Jul. 2023.

[15] M. Wazid, A. Kumar Das, and S. Shetty, "BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Trans. Consum. Electron.*, vol. 69, no. 1, pp. 18–28, Feb. 2023.

[16] A. Verma, P. Bhattacharya, M. Zuhair, S. Tanwar, and N. Kumar, "VaCoChain: Blockchain-based 5G-assisted UAV vaccine distribution scheme for future pandemics," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1997–2007, May 2022.

[17] A. Abid, S. Cheikhrouhou, S. Kallel, Z. Tari, and M. Jmaiel, "A smart contract-based access control framework for smart healthcare systems," *Comput. J.*, vol. 67, no. 2, pp. 407–422, Feb. 2024.

[18] M. Z. U. Rahman, M. A. Akbar, V. Leiva, C. Martin-Barreiro, M. Imran, M. T. Riaz, and C. Castro, "An IoT-fuzzy intelligent approach for holistic management of COVID-19 patients," *Heliyon*, vol. 10, no. 1, Jan. 2024, Art. no. e22454.

[19] S. Panja, A. K. Chattopadhyay, A. Nag, and J. P. Singh, "Fuzzy-logic-based IoMT framework for COVID19 patient monitoring," *Comput. Ind. Eng.*, vol. 176, Feb. 2023, Art. no. 108941.

[20] A. Ali, T. Tin, B. Al-rimy, T. A. E. Eisa, H.-S. Gan, and J. Chaw, "Revolutionizing digital healthcare: Unlocking the power of blockchain with an optimized fuzzy logic approach to authentication and key agreement," *Preprints*, pp. 1–33, Jul. 2023.

[21] Z. Zulkifl, F. Khan, S. Tahir, M. Afzal, W. Iqbal, A. Rehman, S. Saeed, and A. M. Almuhaideb, "FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs," *IEEE Access*, vol. 10, pp. 15644–15656, 2022.

[22] C. Ieracitano, N. Mammone, M. Versaci, G. Varone, A.-R. Ali, A. Armentano, G. Calabrese, A. Ferrarelli, L. Turano, C. Tebala, Z. Hussain, Z. Sheikh, A. Sheikh, G. Sceni, A. Hussain, and F. C. Morabito, "A fuzzy-enhanced deep learning approach for early detection of COVID-19 pneumonia from portable chest X-ray images," *Neurocomputing*, vol. 481, pp. 202–215, Apr. 2022.

[23] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing," *IEEE Access*, vol. 9, pp. 45706–45720, 2021.

[24] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, and E. Zdravevski, "A framework for malicious traffic detection in IoT healthcare environment," *Sensors*, vol. 21, no. 9, p. 3025, Apr. 2021.

[25] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, "Blockchain and quantum blind signature-based hybrid scheme for Healthcare 5.0 applications," *J. Inf. Secur. Appl.*, vol. 56, Feb. 2021, Art. no. 102673.

NISHI PATEL is currently pursuing the Bachelor of Technology degree in computer engineering with the Institute of Technology, Nirma University. Her current research interests include deep learning, data science, fuzzy logic, and explainable AI.

DHYAN PATEL is currently pursuing the Bachelor of Technology degree in computer engineering with the Institute of Technology, Nirma University. His current research interests include deep learning, data science, and blockchain.

NILESH KUMAR JADAV (Graduate Student Member, IEEE) received the bachelor's and M.Tech. degrees from Gujarat Technological University (GTU), Gujarat, India, in 2014 and 2018, respectively. He is currently a full-time Ph.D. Research Scholar with the Department of Computer Science and Engineering, Nirma University, Ahmedabad, Gujarat. He is an Active Member with the ST Research Laboratory. He has authored/co-authored publications (including papers in SCI-indexed journals and IEEE ComSoc-sponsored international conferences). Some of his research findings are published in top-cited journals and conferences, such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE OPEN JOURNAL OF VEHICULAR TECHNOLOGY, *Digital Communications and Networks* (Elsevier), *Computers and Electrical Engineering* (Elsevier), IEEE INFOCOM, IEEE ICC, and IJCS. His research interests include artificial intelligence, network security, 5G communication networks, and blockchain technology.

TEJAL RATHOD is currently a full-time Ph.D. Research Scholar with the Department of CSE, Institute of Technology, Nirma University, Ahmedabad, India, under the supervision of Sudeep Tanwar. Her research interests include big data analytics and modeling artificial intelligence for wireless network applications.

SUDEEP TANWAR (Senior Member, IEEE) is currently a Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, India. He is a Visiting Professor with Jan Wyzykowski University, Polkowice, Poland; and the University of Piteşti, Piteşti, Romania. He has authored two books, edited 13 books, and more than 270 technical papers, including top journals and top conferences, such as IEEE Transactions on Network Science and Engineering, IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Informatics, IEEE Wireless Communications, IEEE Network, ICC, GLOBECOM, and INFOCOM. He initiated the research field of blockchain technology adoption in various verticals, in 2017. His H-index is 68. He actively serves his research communities in various roles. His research interests include blockchain technology, wireless sensor networks, fog computing, smart grids, and the IoT. He is a member of the Technical Committee on Tactile Internet of the IEEE Communication Society. He is a Senior Member of CSI, IAENG, ISTE, and CSTA. He has been awarded the Best Research Paper Award from IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He served many international conferences, as a Member of the Organizing Committee, such as the Publication Chair for FTNCT-2020, ICCIC 2020, and WiMob2019; a member of the Advisory Board for ICACCT-2021 and ICACI 2020; the Workshop Co-Chair for CIS 2021; and the General Chair for IC4S 2019 and 2020 and ICCSDF 2020. He is serving on the Editorial Board for *Frontiers in Blockchain*, *Cyber Security and Applications*, *Computer Communications*, *International Journal of Communication Systems*, and *Security and Privacy*.

GIOVANNI PAU (Senior Member, IEEE) received the bachelor's degree in telematic engineering from the University of Catania, Italy, and the master's degree (cum laude) in telematic engineering and the Ph.D. degree from the Kore University of Enna, Italy. He is currently an Associate Professor with the Faculty of Engineering and Architecture, Kore University of Enna. He is the author/co-author of more than 100 refereed papers published in journals and conference proceedings. His research interests include wireless sensor networks, fuzzy logic controllers, intelligent transportation systems, the Internet of Things, smart homes, and network security. He is a member of IEEE (Italy Section) and has been involved in several international conferences, as the session co-chair and a technical program committee member. He serves/served as the Leading Guest Editor for special issues on several international journals and is an Editorial Board Member and an Associate Editor of several journals, such as IEEE Access, *Wireless Networks* (Springer), *EURASIP Journal on Wireless Communications and Networking* (Springer), *Wireless Communications and Mobile Computing* (Hindawi), and *Sensors* (MDPI), to name a few.

GULSHAN SHARMA received the B.Tech., M.Tech., and Ph.D. degrees. He is currently a Senior Lecturer with the Department of Electrical Engineering Technology, University of Johannesburg. He is also a Y Rated Researcher with NRF, South Africa. His research interests include power system operation and control and application of AI techniques to the power systems. He is an Academic Editor of *International Transactions on Electrical Energy Systems* (Wiley) and a Regional Editor of *Recent Advances in Electrical and Electronic Engineering* (Bentham Science).

FAYEZ ALQAHTANI was appointed as the Director of the Computer Division, Deanship of Student Affairs. He is currently a Full Professor with the Software Engineering Department, College of Computer and Information Sciences, King Saud University (KSU). He has conducted research projects in several areas of information and communication technology, such as web 2.0, information security, enterprise architecture, software process improvement, the Internet of Things, and fog computing. He has participated in several academic events. He is also a member of a number of academic and professional associations, such as the Association for Computing Machinery (ACM), Australian Computer Society, and the Association for Information Systems.

AMR TOLBA (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees from the Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Egypt, in 2002 and 2006, respectively. He is currently a Full Professor of computer science with King Saud University (KSU), Saudi Arabia. He has authored/co-authored over 180 scientific papers in top ranked (ISI) international journals and conference proceedings. His research interests include artificial intelligence (AI), the Internet of Things (IoT), data science, and cloud computing. He serves as a technical program committee (TPC) member for several conferences. He served as an associate editor/guest editor for several ISI journals.

Open Access funding provided by 'Università degli Studi di Enna "KORE"' within the CRUI CARE Agreement