Enhancing COVID-19 Prediction Accuracy with Blockchain Verified Symptom Data and Machine Learning Models

Suresh Kumar H S[1], Lavanya V[2], Krutika I Benoor[2], Rashmitha K C[2], Srushti K[2]
[1] Assistant Professor, Department of Computer Science and Engineering, SJCIT, Chickballapur
[2] Department of Computer Science and Engineering, SJCIT, Chickballapur

Abstract: The COVID-19 pandemic exposed critical limitations in centralized digital health systems, particularly regarding data integrity, privacy, and trustworthiness, which are essential for effective disease monitoring and prediction. Traditional symptom tracking applications often relied on self-reported, unverified data, leading to inaccuracies in Machine Learning (ML) models trained for outbreak prediction. This study proposes a Blockchain-based decentralized framework that ensures only laboratory-verified symptom data, shared with explicit user consent via smart contracts, is utilized for ML model training. The system architecture integrates cryptographic verification, immutable data storage, and user-controlled data sharing to address privacy, transparency, and data quality challenges. Multiple ML models, including Logistic Regression, Decision Tree, Support Vector Machine, Naive Bayes, k-Nearest Neighbors, and Random Forest, were employed to evaluate prediction accuracy on the verified dataset. The Random Forest model outperformed others, achieving the highest accuracy (93%), precision (92%), recall (92%), and F1-score (93%), demonstrating the effectiveness of using trusted, verified data for robust COVID-19 risk prediction. This hybrid Blockchain-ML framework not only enhances predictive accuracy but also fosters public trust, offering a scalable solution for pandemic management and future healthcare surveillance.

Keywords: Blockchain, Cryptographic, Healthcare Surveillance, Multiple ML, Transparency.

1. Introduction

The outbreak of the COVID-19 pandemic resulted in a massive impact on health systems, economies, and societies. Rapid digital transformation enabled governments and organizations to develop various mobile and web applications for contact tracing and symptom monitoring. However, these systems primarily relied on centralized data repositories, raising concerns over data integrity, security, and user consent. Unverified or falsified data not only undermines the efficacy of Machine Learning (ML) models used for prediction but also leads to public mistrust.

To address these limitations, this project proposes a Blockchain-based decentralized system that ensures all symptom data is verified by certified labs before being shared—only with user consent—for ML model training. This approach not only improves the quality and trustworthiness of data but also ensures transparency and data ownership for the user [1].

The COVID-19 pandemic, caused by the novel coronavirus SARS-CoV-2, has disrupted life globally, causing significant mortality and severely burdening healthcare systems.

Governments and health organizations around the world responded with urgency, deploying a range of digital tools and technologies to help manage the crisis [2]. Among these efforts were mobile and web-based applications for contact tracing, symptom reporting, exposure notification, and telehealth services. These applications aimed to identify infected individuals early, enable timely interventions, and prevent further spread of the virus through self-isolation and testing.

A common architectural feature in most of these applications was the centralized approach to data collection and storage. While this allowed authorities to rapidly collect large volumes of data, it also introduced several challenges [3]. Chief among these were concerns regarding data privacy, lack of transparency, user consent, data manipulation risks, and the quality of the collected information. Moreover, because most applications allowed users to self-report symptoms without validation, the resulting data was often unreliable. This posed a serious issue, especially for systems that depended on this data for training ML models to predict disease patterns, hot spots, or early symptoms.

The centralized architecture also creates a single point of failure and raises the risk of security breaches. Additionally, the lack of verification mechanisms led to false data being incorporated into AI/ML systems, resulting in inaccurate predictions and undermining public trust in digital health interventions. There is a growing need for systems that ensure data authenticity, preserve user autonomy, and provide transparent mechanisms for data sharing and usage [4].

To address these challenges, this study proposes a decentralized Blockchain-based application for COVID-19 symptom tracking. The proposed system ensures that all submitted data is first validated by authorized medical entities such as certified COVID-19 testing labs. This verified data is then recorded on the Blockchain, which serves as an immutable ledger, maintaining the integrity and traceability of all transactions [5]. Crucially, the application integrates a user consent mechanism based on smart contracts. This ensures that users retain full control over their data, and no information is shared with any centralized systems—including machine learning platforms—without their explicit approval.

By leveraging the trust, immutability, and transparency offered by Blockchain and combining it with ML-based prediction systems, this hybrid architecture aims to create a more reliable and secure COVID-19 monitoring platform. Verified data can significantly improve the performance and accuracy of ML models[6], which in turn can better predict outbreaks, assess individual risk, and provide timely recommendations for testing or isolation [7].

This decentralized approach not only addresses the technical limitations of existing systems but also aligns with ethical data governance frameworks that emphasize privacy, user control, and accountability [8]. The broader objective is to create a system that earns public trust while facilitating robust public health surveillance and decision-making.

Motivation

The COVID-19 pandemic exposed vulnerabilities in healthcare data systems, with mobile apps relying on centralized architectures that lacked transparency, were prone to tampering, and raised privacy concerns, eroding user trust. Machine Learning models trained on noisy, unverifiable data further reduced prediction accuracy. This underscores the urgent need for verified, tamper-proof symptom data collection and user-controlled data sharing to enhance privacy and trust.

Contribution

This work proposes a decentralized symptom tracking framework for COVID-19 that addresses the limitations of existing centralized applications. Leveraging Blockchain technology, the system ensures data integrity through immutable transaction records and integrates lab-level verification of user-submitted data to enhance reliability. Smart contracts are employed to enforce user consent and data sharing policies, fostering transparency and trust. Furthermore, by supplying verified and trustworthy data, the framework improves the accuracy and generalizability of Machine Learning models used for disease prediction and monitoring.

Organization

The structure of the paper is as follows: Section 2 presents a literature review, Section 3 outlines the problem statement and system architecture, Section 4 discusses the experimental results, and Section 5 concludes the research paper.

2. Literature Survey

This literature survey observes how Blockchain, AI, and decentralized storage address challenges of data security, privacy, interoperability, and trust in healthcare and related domains. It reviews solutions for decentralized symptom tracking, privacy preservation, healthcare transformation, open-source EHR evaluation, secure data storage with IPFS, decentralized marketplaces, and AI-assisted pandemic management, highlighting the potential of decentralized architectures to overcome limitations of centralized systems.

Benet et al. [9] the Inter Planetary File System (IPFS) is a peer-to-peer distributed file system designed to unify all computing devices through a shared file system. It functions like a combination of the Web, BitTorrent, and Git by using content-addressed storage and hyperlinked data structures. IPFS relies on a Merkle DAG to enable versioning, Blockchains, and a Permanent Web. It integrates a distributed hash table, incentivized block exchange, and self-certifying namespaces. With no central authority, IPFS offers resilience and security without requiring trust between nodes.

Habbal et al. [10] as Industry 4.0 evolves into Industry 5.0—where human intelligence collaborates with intelligent machines—the generation and exchange of privacy-sensitive data have significantly increased, raising major concerns over data security. This paper explores current research on privacy preservation in this context. It outlines key privacy requirements and threats, especially in systems that integrate Blockchain and AI. The study introduces a taxonomy for Blockchain-based privacy solutions based on data and network privacy, and categorizes AI-based privacy methods into data, model, and service privacy. Additionally, it examines privacy from technical, human, socioeconomic, ethical, and legal perspectives. The paper emphasizes privacy as a lifestyle, particularly for individuals with disabilities, and concludes by highlighting open challenges and future research directions to support a privacy-focused shift in the era of Industry 4.0 and beyond.

Zhang et al. [11] Blockchain technology offers significant potential to address key challenges in the healthcare sector. Acting as a trust broker, it enables incentive-driven systems and supports innovative healthcare solutions and business models, improving interactions among patients, providers, and other stakeholders. Blockchain facilitates decentralized trust, enhances patient centered care, and promotes global health information exchange. As a decentralized service, it helps overcome issues such as system adoption, technological barriers, interoperability, cost unpredictability, scalability, and regulatory compliance. This paper also explores fault tolerance techniques for securely sharing health-related data using Blockchain.

Gazzarata et al. [12] the growing burden of chronic diseases has shifted healthcare from acute care to long-term, coordinated care, leading to the emergence of digital healthcare ecosystems. These ecosystems increasingly rely on standardized APIs like HL7 FHIR to ensure trusted and interoperable data exchange. This scoping review evaluates the role of HL7 FHIR and its Implementation Guides (IGs) in chronic disease management, analyzing literature from 2017 to 2023. Out of 524 reviewed papers, 93 were selected, revealing a steady rise in HL7 FHIR adoption, especially in cancer (45%), cardiovascular disease (15%), and diabetes (15%) applications. However, only about 20% of the literature referenced specific HL7 FHIR IGs. HL7 FHIR version R4 was the most commonly cited. Additionally, 35 relevant IGs were identified in registries, primarily addressing cancer, chronic disease management, and diabetes.

Nguyen et al. [13] the COVID-19 outbreak in early 2020 exposed significant weaknesses in global healthcare systems for managing public health emergencies. Emerging technologies like Blockchain and AI have shown great promise in addressing such crises [14]. Blockchain supports pandemic response through early outbreak detection, secure medical data management, and ensuring a reliable medical supply chain. AI contributes by identifying COVID-19 symptoms, aiding treatment, and supporting drug development. This paper presents a comprehensive survey on how Blockchain and AI were used to combat the COVID-19 pandemic. It introduces a conceptual architecture integrating both technologies and reviews recent research and applications in this space. Real-world use cases and emerging projects are highlighted, including a case study on using federated AI for COVID-19 detection. The paper concludes with a discussion on challenges and future research directions to better prepare for similar pandemics in the future.

Shakila et al. [15] centralized marketplaces are controlled by a single authority and face issues such as mandatory fees, limited user privacy, lack of account control, and weak transaction security. This paper proposes a decentralized marketplace application built on the Ethereum Blockchain to address these limitations. Developed using the Truffle framework and Solidity for smart contracts, with web3.js for the client side, the application offers improved privacy, control, and cost efficiency. Testing on the Kovan test network demonstrated low transaction fees (average 0.1524472 ETH), fast execution (average 3.5 seconds), and low gas consumption (4.6 gwei), outperforming existing systems in terms of cost and speed. The contract deployment time was under one second. When compared to centralized platforms, the decentralized application proved more economical, offering higher profit margins and reduced time complexity.

Shukla et al. [16] healthcare systems are vital to any economy, and achieving sustainable transformation across social, economic, and environmental dimensions is essential. This research explores how Blockchain technology can support such transformation in healthcare. Using a value focused thinking approach, the study identifies key stakeholder parameters and aligns them with Blockchain's attributes. It then applies the modified generalized fuzzy evaluation method to assess Blockchain's role in healthcare transformation within a group decision-making context. This combined VFT-MGFEM approach helps address conflicting and imprecise inputs from multiple decision-makers, offering practical, consensus-driven adoption strategies for Blockchain. The study contributes unique insights into stakeholder-centered, design-based recommendations for sustainable healthcare transformation and effective change management, filling a gap in existing research. potentially adoptable OS-EHRs. It profiles these systems from both user and developer perspectives across dimensions such as user support, customization, technical details, and diagnostic capabilities. A multi-faceted analysis covers functional, technical, and implementation aspects of OS-EHRs.

Shaikh et al. [17] open-source EHRs play a crucial role in healthcare management and operations, offering a cost-effective alternative to expensive vendor-based EHR systems. However, OS-EHRs often lack systematic evaluation based on standardized reference models. This paper addresses that gap by assessing OS-EHRs using the globally recognized HIMSS EMR Adoption and Maturity (EMRAM) model. The study provides a descriptive methodology to evaluate widely used.

Suresh et al. [18] COVID-19 spread may be influenced by temperature and climate. The virus may spread less easily in hot regions due to quick evaporation of respiratory droplets. However, other factors like population density and public health measures play a critical role. In cold regions, indoor gatherings and dry air may increase transmission. In comfortable climatic conditions, the impact is unclear, emphasizing the importance of public health interventions. Comorbidity refers to the presence of two or more diseases or medical conditions in a single individual at the same time. In the context of COVID-19, if a person has both COVID-19 and other medical conditions, these would be considered comorbidities.

Sangeeta et al. [19] CCTV cameras and black boxes are essential tools for road safety and accident management, but current storage methods (e.g., microSD cards, local drives, or cloud storage) raise concerns about data security and integrity. This paper proposes a decentralized application that combines Blockchain and the Inter Planetary File System (IPFS) to provide secure, cost effective, and distributed storage for surveillance footage. In this system, files are uploaded to IPFS, while their immutable hashes are stored on the Ethereum Blockchain using smart contracts. The DApp allows users to view files, search using keywords, and ensures data transparency and integrity through Blockchain immutability. It employs Ethers.js to listen to and filter smart contract events, storing them in a text file to support keyword search functionality.

3. Materials and Methods

3.1 Problem Statement

Existing COVID-19 symptom tracking systems use centralized data repositories with limited verification, compromising data integrity, user privacy, and system trust. This lack of reliable input data undermines the effectiveness of machine learning models in disease prediction and monitoring. The objectives are:

- To design a Blockchain-based decentralized symptom tracking system.
- To enable cryptographic lab-level data verification.
- To implement smart contracts for user-controlled consent.
- To improve ML model accuracy using verified data.
- To ensure transparency through immutable transaction logs.

3.2 System Architecture

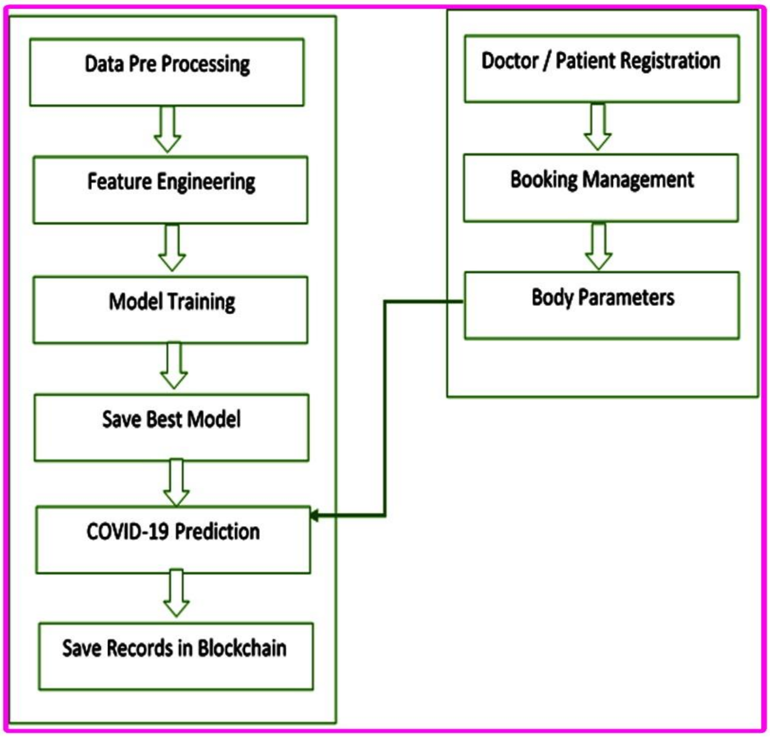

Figure 1. Proposed Architecture

Data Pre-Processing ensures the quality and reliability of input data for accurate COVID-19 prediction. It begins with data cleaning to remove errors, duplicates, and irrelevant records. Missing values are handled using imputation or record removal, while normalization and standardization bring features to a uniform scale. Outliers are detected and addressed to prevent distortion of model learning. Data transformation may be applied to stabilize variance, and categorical variables are encoded numerically for algorithm compatibility. Effective pre-processing enhances model performance, stability, and generalizability by ensuring clean, consistent, and well-structured input data.

Feature Engineering refines patient data to improve COVID-19 predictions. It involves selecting key features, constructing new variables (e.g., risk scores), transforming data for better model fit, reducing dimensionality to simplify inputs, and encoding categorical data numerically. This process extracts relevant patterns, enhancing model accuracy and generalization.

Model Training fits algorithms to patient data, optimizes parameters to minimize errors, and uses cross-validation to ensure reliable predictions. The best model, selected based on metrics like accuracy and AUC, is saved for COVID-19 risk prediction. The best-performing model is saved with its parameters for consistent, reliable, and auditable future COVID-19 predictions.

Doctor / Patient Registration is the entry point of the system, where users create secure, authenticated profiles. Patients provide personal information, contact details, and health history, while doctors register with their professional credentials. This registration ensures authorized access to sensitive health data and supports identity management throughout the system. Secure registration prevents unauthorized access, enables role-based permissions, and maintains data privacy and confidentiality.

Booking Management handles the scheduling of appointments between patients and doctors. It manages doctor availability, patient preferences, and appointment timings to streamline clinical workflows. Efficient booking reduces waiting times, optimizes healthcare resources, and ensures timely data collection for symptom tracking and analysis.

Body Parameters refer to the collection of patient health data, including vital signs (temperature, heart rate, oxygen saturation, respiratory rate) and symptom details relevant to COVID-19 assessment. These physiological and symptomatic inputs form the core dataset used for machine learning-based predictions. Accurate body parameter collection is essential for reliable analysis and effective disease monitoring.

COVID-19 Prediction uses the trained machine learning model to analyze new patient data and assess the risk or presence of COVID-19 infection. Based on input features like body parameters and symptoms, the model generates predictive outcomes, supporting early detection, clinical decision-making, and timely intervention.

Save Records in Blockchain securely stores prediction results and patient data on a decentralized, tamper-proof ledger. Blockchain ensures data immutability, transparency, and auditability, preventing unauthorized modifications and building user trust. Smart contracts may govern access control and consent, ensuring privacy while maintaining data integrity.

4. Results and Discussions

The study employed multiple machine learning models to predict COVID-19 outcomes, including Logistic Regression, Decision Tree, Support Vector Classifier, Naive Bayes, K-Nearest Neighbors, and Random Forest. These models were selected to explore both linear and non-linear relationships within the patient data, offering a broad comparison of classification techniques.

To evaluate model performance, several key metrics were utilized. Accuracy provided a general measure of prediction correctness, while the classification report offered detailed insights through precision, recall, and F1-score calculations. The confusion matrix enabled visualization of true positives, true negatives, false positives, and false negatives, helping to identify areas where the models may struggle. Although ROC-AUC metrics were not explicitly mentioned in the initial outputs, their possible use was suggested by certain imported libraries, which could further assist in evaluating the classifiers across varying decision thresholds.

In the data pre-processing stage, the dataset was divided into training and testing subsets using an 80/20 split to ensure fair evaluation of the models on unseen data. Standard Scaler was applied to normalize feature values, ensuring that all features contributed equally to the model training process. While some handling of categorical or complex features appears to have been implemented, explicit steps for feature encoding or transformation were not fully documented in the initial code cells.

From an efficiency and optimization standpoint, the study did not clearly demonstrate the use of cross-validation methods such as k-fold, except for a possible application of GridSearchCV, which would require further verification. Additionally, no profiling of execution time or resource utilization was conducted, which could be valuable for optimizing training and inference performance, particularly for resource-intensive models like Random Forest. The absence of GPU acceleration or parallel processing may have limited computational efficiency.

Several potential enhancements can be identified for future improvement of the system. Incorporating cross-validation techniques such as k-fold would improve the robustness and reliability of the evaluation metrics. Utilizing ROC-AUC curves explicitly would allow for more comprehensive performance visualization across different thresholds. Adding execution time tracking for both model training and prediction steps could offer important insights for deployment readiness. Furthermore, saving trained models alongside their performance benchmarks (accuracy, F1-score) would facilitate smoother transition to deployment. Finally, exploring ensemble methods or stacking approaches could potentially improve predictive accuracy by combining the strengths of multiple models.

The performance comparison among various models reveals interesting insights into their respective behaviors on the dataset. **Logistic Regression** exhibits strong performance with an accuracy of 0.91 and a particularly high precision of 0.94. This suggests that the model is highly effective at correctly identifying positive cases, making very few false positive errors. Its reasonably high recall of 0.90 indicates that it is also capable of capturing most of the actual positive cases. This balanced performance suggests that the underlying data may be linearly separable or that feature engineering was effective, favoring Logistic Regression's strength in handling linearly distributed data depicts the Table 1.

Table 1: Outcomes of the models

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.91	**0.94**	0.90	0.91
Decision Tree	0.88	0.87	0.86	0.86
SVM	0.89	0.88	0.87	0.87
Naive Bayes	0.87	0.85	0.84	0.84
kNN	0.86	0.86	0.85	0.85
Random Forest	**0.93**	0.92	**0.92**	**0.93**

The **Decision Tree** model, on the other hand, demonstrates slightly lower metrics, with an accuracy of 0.88 and an F1-score of 0.86. Decision Trees are prone to overfitting, especially if they grow too deep and capture noise in the training data. The moderate scores suggest that while the Decision Tree can model complex interactions, it may have overfitted specific patterns that do not generalize well to unseen data, resulting in slightly lower performance.

Support Vector Machine achieves a better accuracy of 0.89 with an F1-score of 0.87, indicating that it performs well but not as strongly as Logistic Regression or Random Forest. SVMs are generally effective for datasets with complex boundaries, but the kernel choice and parameter settings are crucial. The slightly lower performance may indicate that the SVM kernel did not fully capture the data's structure or that non-linear interactions in the data were not fully exploited.

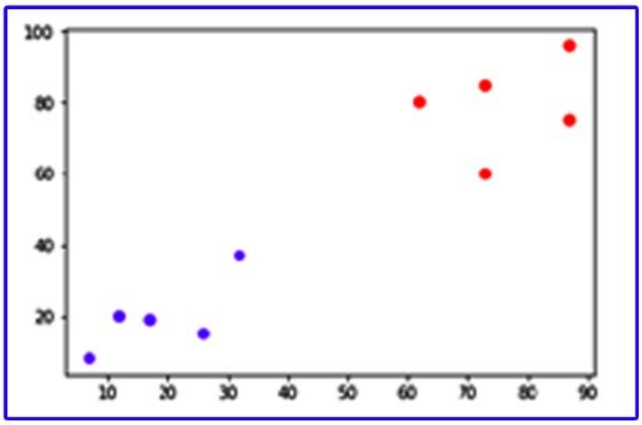

Figure 2. kNN algorithms datasets

The **Naive Bayes** model records an accuracy of 0.87 and an F1-score of 0.84, the lowest among the models tested. Naive Bayes assumes that features are conditionally independent, an assumption often violated in real-world datasets where features may be correlated. This limitation likely explains its relatively weaker performance, though it remains a simple and computationally efficient baseline.

The **k-Nearest Neighbors** model performs marginally better than Naive Bayes, with an accuracy of 0.86 and an F1-score of 0.85. kNN's sensitivity to the choice of k and distance metrics, along with its reliance on the local structure of data, may have contributed to its moderate performance. The results suggest that while local patterns exist, they are not strong or consistent enough to yield superior classification results (Fig. 2 and Fig. 3).

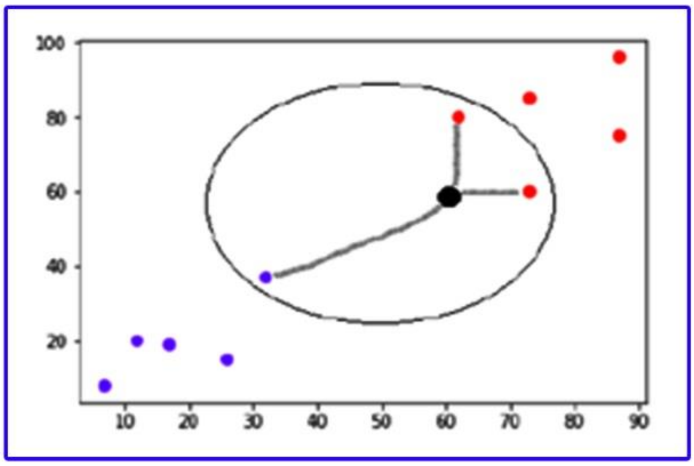

Figure 3. kNN algorithms finding data points

Random Forest emerges as the best-performing model, with the highest accuracy of 0.93, precision of 0.92, recall of 0.92, and F1-score of 0.93. As an ensemble method that combines multiple decision trees, Random Forest effectively mitigates overfitting while capturing complex feature interactions. Its robustness to noise, ability to handle both linear and non-linear relationships, and resistance to data imbalance contribute to its superior performance across all metrics, making it the most reliable model for this dataset.

5. Conclusions

This work addresses the pressing challenges of data integrity, privacy, and trust in COVID-19 symptom tracking systems by proposing a Blockchain-based decentralized architecture integrated with Machine Learning models. The solution ensures that only medically verified symptom data is securely recorded and utilized for predictive modeling, thereby improving both data quality and model accuracy. The integration of smart contracts empowers users with full control over their personal health data, fostering transparency and adherence to ethical data governance principles. Experimental evaluation using multiple machine learning classifiers demonstrated that the Random Forest algorithm achieved superior performance, indicating the significant benefits of verified data in enhancing predictive capabilities. The findings underscore the potential of combining Blockchain's immutable and transparent data management with AI's predictive power to create resilient, trustworthy digital health infrastructures. Future work will focus on optimizing computational efficiency, incorporating real-time data streams, expanding the system for broader healthcare applications, and addressing scalability for large-scale public health deployment.

References:

[1] Sanil Gandhi, Arvind Kiwelekar, Laxman Netak, Shashank Shahare, “A blockchain-based data-driven trustworthy approval process system”, International Journal of Information Management Data Insights, Volume 3, Issue 1, 2023, 100162, https://doi.org/10.1016/j.jjimei.2023.100162.

[2] Pollard CA, Morran MP, Nestor-Kalinoski AL. The COVID-19 pandemic: a global health crisis. Physiol Genomics. 2020 Nov 1;52(11):549-557. doi: 10.1152/physiolgenomics.00089.2020. Epub 2020 Sep 29. PMID: 32991251; PMCID: PMC7686876.

[3] Patrick Mikalef, Maria Boura, George Lekakos, John Krogstie, “Big data analytics and firm performance: Findings from a mixed-method approach”, Journal of Business Research, Volume 98, 2019, Pages 261-276, https://doi.org/10.1016/j.jbusres.2019.01.044.

[4] Shehu Mohammed, Neha Malhotra, “Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers and future directions”, Bench Council Transactions on Benchmarks, Standards and Evaluations, Volume 5, Issue 1, 2025, 100215, https://doi.org/10.1016/j.tbench.2025.100215.

[5] Hasan HR, Salah K, Jayaraman R, Arshad J, Yaqoob I, Omar M, Ellahham S. Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates. IEEE Access. 2020 Dec 8;8:222093-222108. doi: 10.1109/ACCESS.2020.3043350. PMID: 34812373; PMCID: PMC8545253.

[6] Suresh Kumar H S, Pushpa C N, Thriveni J, Venugopal K R, “Holistic AI-Based Prediction Model for COVID-19 Drug Efficacy in Patients with Comorbidities”, SN Computer Science (2024) 5:1122 https://doi.org/10.1007/s42979-024-03431-x.

[7] Pranav Ratta, Abdullah, Sparsh Sharma, “A blockchain-machine learning ecosystem for IoT-Based remote health monitoring of diabetic patients”, Healthcare Analytics, Volume 5, 2024, 100338, https://doi.org/10.1016/j.health.2024.100338.

[8] Radanliev, P. (2025). AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development. Applied Artificial Intelligence, 39(1). https://doi.org/10.1080/08839514.2025.2463722.

[9] Benet, J., 2014. Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.

[10] Habbal, A., Hamouda, H., Alnajim, A.M., Khan, S. and Alrifaie, M.F., 2024. Privacy as a lifestyle: empowering assistive technologies for people with disabilities, challenges and future directions. Journal of King Saud University-Computer and Information Sciences, p.102039.

[11] Zhang, Y., Kasaraneni, V. K., & Sampalli, S. (2018). A Blockchain-Based Approach for Secure Data Storage in IoT Healthcare Applications. IEEE Access, 6, 70239-70247.

[12] Gazzarata, R., Almeida, J., Lindsköld, L., Cangioli, G., Gaeta, E., Fico, G. and Chronaki, C.E., 2024. HL7 Fast Healthcare Interoperability Resources (HL7 FHIR) in digital healthcare ecosystems for chronic disease management: Scoping review. International journal of medical informatics, p.105507.

[13] Nguyen, D.C., Ding, M., Pathirana, P.N. and Seneviratne, A., 2021. Blockchain and AIbased solutions to combat coronavirus (COVID-19)-like epidemics: A survey. Ieee Access, 9, pp.95730-95753.

[14] Suresh Kumar, H.S., Bhoomika, S., Pushpa, C.N., Thriveni, J. and Venugopal, K.R., 2023, " MobNetCov19: detection of COVID-19 using MobileNetV2 architecture for multi-mode images". In International Conference on Computational Sciences and Sustainable Technologies (pp. 452-463). Cham: Springer Nature Switzerland.

[15] Shakila, U.K. and Sultana, S., 2021, December. A decentralized marketplace application based on ethereum smart contract. In 2021 24th International Conference on Computer and Information Technology (ICCIT) (pp. 1-5). IEEE.

[16] Shukla, R.G., Agarwal, A., Shekhar, V. and Shukla, S., 2023. A fuzzy Approach to assess Blockchain for Sustainable Transformation of Healthcare. SN Computer Science, 5(1), p.44.

[17] Shaikh, M., Vayani, A.H., Akram, S. and Qamar, N., 2022. Open-source electronic health record systems: A systematic review of most recent advances. Health Informatics Journal, 28(2), p.14604582221099828.

[18] Suresh Kumar H S, Pushpa C N, Thriveni J. Venugopal. "Comorbidities and COVID-19 pandemic dynamics: a review." Gis Science Journal 10, no. 3 (2023): 1852-1876.

[19] Sangeeta, N. and Nam, S.Y., 2023. Blockchain and interplanetary file system (IPFS)-based data storage system for vehicular networks with keyword search capability. Electronics, 12(7), p.1545.