

Security and privacy for Binance-based integrated blockchain for blood supply chain management systems

Rupa Ch¹, Sai Varshitha G.¹, Divya D.¹, Thippa Reddy Gadekallu^{2,3,4}, Mustufa Haider Abidi⁵ and Fahad Alasim⁶

¹ CSE, Siddhartha Academy of Higher Education Deemed to be University, VR Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India

² The College of Mathematics and Computer Science, A & F University, Hangzhou, China

³ Division of Research and Development, Lovely Professional University, Phagwara, India

⁴ Center of Research Impact and Outcome, Chitkara University, Punjab, India

⁵ Advanced Manufacturing Institute, King Saud University, Riyadh, Saudi Arabia

⁶ Department of Industrial Engineering, College of Engineering, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

The world faces a severe blood shortage, with a gap of 1.95 million units, highlighting the need for efficient blood allocation and management systems. Traditional cloud and blockchain approaches have been explored for blood bank management but faced implementation challenges. This study proposes designing and developing a decentralized Binance blockchain-based application framework to ensure transparency and security. It uses the AdaBoost algorithm to predict the availability of the nearest blood bank and blood donor. Supply chain management provides transparency without the intervention of third parties thereby preventing blood crimes. Metamask is incorporated for crypto transactions in the Binance Smart Chain test network (BSC). BSC stands out for its low transaction fees and high scalability, enabling swift transaction processing at a fraction of the cost compared to Ethereum. The smart contracts are deployed using hardhat configuration enabling BscScan as an Application Programming Interface (API) gateway to record transactions within the decentralized application (dApp). The proposed system achieved an accuracy of 99.5%, demonstrating the robustness of the AdaBoost model in predicting blood availability. The integration of blockchain technology ensures transparency, immutability, and secure traceability of blood transactions across the network.

Subjects Cryptography, Data Mining and Machine Learning, Security and Privacy, Cryptocurrency, Blockchain

Keywords Binance, Blood supply chain, AdaBoost, Hardhat, Smart contract, BscScan

INTRODUCTION

Blood is one of the main fluids in the human body. It helps to support the organs with the necessary and useful things needed for survival. As the demand for blood is exceeding all the medical requirements, the governments educate their citizens about blood donation by organizing awareness programs. The number of donors in the years 2018–2019 was estimated to be 136,908 donors, contributing to a total of 216,639 donations (*Mandal et al., 2023; Hawashin et al., 2021*). In general, every 56 days, mostly healthy individuals give

Submitted 20 January 2025
Accepted 22 July 2025
Published 23 September 2025

Corresponding author
Thippa Reddy Gadekallu,
thippareddy@ieee.org

Academic editor
Syed Hassan Shah

Additional Information and
Declarations can be found on
page 28

DOI 10.7717/peerj-cs.3123

© Copyright
2025 Ch et al.

Distributed under
Creative Commons CC-BY 4.0

OPEN ACCESS

blood donations. The World Health Organization estimates that the annual amount of blood donations collected is 112.5 million units, which is approximately 50 million liters, per year (Kim, Kim & Kim, 2020). However, the lack of blood donors has increased with the emergence of new diseases. The requirement to enable reliable and efficient blood donation management has been raised. Blood management for patients is a huge and complex task (Musamih et al., 2021). The current system of blood management contains various restrictions and gaps that limit the supply chain to perform efficiently. Hannon (Kumar et al., 2024) reported that the blood component wastage rates usually run from 1% to 5% and that the amount of disposal is not shared or visible to clarify the reason behind it. Therefore, any development or improvement in this regard is an important consideration in providing efficient health care globally.

Maintaining secure communications for sensitive healthcare information is paramount for both patients and providers. However, the widespread adoption of cloud-based solutions introduces significant concerns regarding data security, especially with the inclusion of third-party services (Nazir et al., 2023). Fundamental to managing data security is the Confidentiality, Integrity, and Availability (CIA) triad, which emphasizes confidentiality, integrity, and availability. Blockchain technology offers a promising solution to enhance the performance, management, and security of information systems, primarily due to its inherent non-repudiation feature (Ekanayake & Halgamuge, 2021). The Binance Smart Chain (BSC) has emerged as an ideal candidate for managing blood resources, thanks to its compatibility with the Ethereum Virtual Machine (EVM) and optimized transaction performance (Gia et al., 2023).

AdaBoost is vital in optimizing the prediction of available blood units concerning geographical location and blood type. AdaBoost combines many “weak classifiers” to get one strong predictive model. Similarly, calculations of geodesic distance are necessary to find nearby blood banks relative to the location of a user (Ramakrishna et al., 2023). These calculations show, among other things, the shortest distance between two points on the Earth’s surface, enabling the accurate filtering of blood banks within a specified radius from the user.

Motivation

India needs 15 million units of blood annually but has a shortage of about 4 million. It is also estimated that in this country, about 12,000 people die daily because quality blood is not available. This is the side of the coin, while on the other, it is indicated that India wastes approximately 6.5 lakh units of blood and blood components every year, just due to poor storage facilities. According to the World Health Organization (WHO), 54% of the countries have poor blood bank management systems (Vo et al., 2023).

Research contributions

Our main contributions can be summarized as follows:

- To analyse and identify the nearest blood banks and donors concerning the user.
- To collect and analyse the National AIDS Control Organization (NACO) standards required for a blood donor and design test data.

- To implement the AdaBoost algorithm for efficiently predicting the nearest blood bank and blood donor availability.
- To design and develop an integrated framework with a decentralized Binance blockchain in blood supply chain management (SCM).
- To test security algorithms to investigate the efficiency of blockchain in SCM and appropriate traceability of the blood bank supply chain.

Route map of the paper

The article is structured as follows: section 'Related Work' of the article explains the methodologies used in the existing studies followed by gap analysis. Section 'Methodology' contains the proposed methodology of the system and section 'Results and Discussions' justifies the results and discussions. Section 'Security Analysis' contains the security analysis followed by section 'Performance Analysis' which analyses the performance of the system. Finally, section 'Conclusion and Future Work' gives insights into the conclusion and future work of the system.

RELATED WORK

Hawashin et al. (2022) proposes a blockchain-based system for the management of the blood donation supply chain, ensuring transparency, security, and auditability. It uses a private Ethereum blockchain integrated with InterPlanetary File System (IPFS), used for storing large data files. It employs smart contracts for the core functionalities and dApp at the frontend interface, while software devices can be hooked with the former through Application Programming Interfaces (APIs). It is one of the permissioned Ethereum blockchain-based solutions providing all privacy and authorization controls. It has not been tested or deployed on the real network, it lacks analysis on performance and scalability, and very limited security analysis and details on what roles exist and the sort of access controls that would be required.

Fiore et al. (2023) proposes the current state of blockchain utilization in healthcare supply chains, pointing out that private/consortium blockchains have largely been implemented due to control, confidentiality, lower energy use, and cost benefits; Ethereum is a widely implemented platform; smart contracting is to support automation; and main blockchain principles regarding accountability, security, transparency, confidentiality, and reliability are covered. These proposed solutions are still not technologically mature and require many studies on scalability and real-world applications. Only one real-world application shows the potential of blockchain to reduce costs and enhance efficiency.

Imamoglu, Topcu & Aydin (2023) proposed an intense analysis of 265 articles in the Web of Science database, making use of bibliometric and network analyses to dissect the literature on the blood supply chain. Data visualization and statistical analysis tools help provide insights into deeper research trends and gaps within the blood supply chain research. The methodology used includes a mixed review methodology, which integrates technology-driven approaches toward providing a comprehensive understanding of the

literature on the blood supply chain, the identification of gaps within the research, and the future directions. The limitations of this study are that it is dependent on English-language publications, hence potentially excluding relevant research from linguistic diversity.

Roorkhosh, Pooya & Agarwal (2023) aimed at supply chain resilience improvement by predicting the blockchain acceptance rate in blood donation and supply chains. Herein, it makes a case for the hybrid combination of Hyperledger Fabric and Caliper with system dynamics in simulating the long-term behavior of blockchain acceptance rate (BAR) and machine learning techniques like Multilayer Perceptron (MLP) and Support Vector Regression (SVR) for its prediction. Ensuring that the issues of implementation challenges and data privacy and security, scalability, and performance limitations have been fully addressed, the study concludes by asserting that resilient supply chains are significantly influenced by inflationary control, R&D, exchange rates, and political risks, thereby underlining the need for effective analysis in these respects and eliciting proper policy making.

Emmanuel et al. (2023) proposed the use of machine learning in drug supply management chains in the case of outbreaks of infectious diseases, with a view of predictive parameters for spread of diseases like COVID-19, influenza, dengue, malaria, and Ebola. Some shared methods applied are neural networks, Bayesian networks, and reinforcement learning. Predictive parameters include demographic data, environmental factors, mobility data, and social media data; among them, demographic data is most used. The study would really increase the need for more efficacious research into the topic, especially in developing countries. It does not mention any blockchain technology or application, but only a systematic literature review on machine learning in drug supply chain management.

Le et al. (2022) propose BloodChain, a blockchain-based system using Hyperledger Fabric to manage blood information and improve the blood supply chain. It provides detailed information about blood consumption and its disposal to recipients. The implementation performance will be benchmarked through the transaction-per-second (TPS) metric by means of Hyperledger Caliper. BloodChain deploys a permissioned blockchain with an inbuilt governance model that assures trust among defined participants, doing away with the requirement of expensive mining. This might include governance and participant policy management, data privacy and security, and scalability and performance challenges, as indirectly reflected in latency results.

Trong et al. (2022) proposed a blockchain-based system for the management of the supply chain of blood using Hyperledger Fabric. The system provides a blockchain architecture for decentralized data storage, smart contracts for data control, and proof-of-concept implementation with evaluations that prove its benefits and feasibility. The current implementation, however, only covers a subset of processes, lacking an authorization mechanism across stakeholders. It potentially brings out the use of Hyper-ledge Fabric in enhancing transparency, security, and data integrity of the blood supply chain management but needs further work in bringing it fully to end-to-end.

Ben Elmir, Hemmak & Senouci (2023) aimed at proposing a smart platform for the enhancement of the blood supply chain. This will be achieved through the development of an information system that spans from the receipt of blood donation to the utilization stage. The model enhances coordination *via* a centralized database. The paper proposes the reduction in uncertainty related to blood demand through machine learning and time series forecasting models such as Autoregressive Moving Average (ARMA) and Autoregressive Integrated Moving Average (ARIMA). It also develops a blood donor classifier using artificial neural networks (ANN), Logistic Regression, Support Vector Machine (SVM), Decision Trees, K-Nearest Neighbors (KNN), and Naive Bayes. Limitations of the work include that there is a need for clear-cut statistical procedures considering resiliency and effectiveness, simplicity of the solution, and specialist expertise in some techniques.

Khalid et al. (2023) proposed blockchain-based decentralized storage systems, their benefits, solutions of challenges, and deployment strategies. It gives an analysis of applications such as Sia, Filecoin, and Storj against cloud storage, discussing various advantages and disadvantages. Security issues are addressed in the survey, some solutions are shown, and future research is suggested. However, it does not provide an in-depth analysis on the implementation challenges, detailed performance comparison, scalability issues, cost-effectiveness, and truly regulatory and legal implications. In a nutshell, the limitations include not discussing the regulatory and legal implications of using blockchain for decentralized data storage, which can turn out to be a big hindrance to its wide adoption.

Abdullah et al. (2022) proposed a decentralized blood donation system on the Ethereum blockchain to attain transparency, traceability, and safety in blood transfusion procedures. On this platform, peer-to-peer interactions can be facilitated because of token incentives to the donors through smart contracts. Since there are no hierarchical procedures, the turnaround time is reduced with full traceability through the blockchain. Along with that, some benefits include transparency and traceability of blood donations. The scalability challenges and the need for a wide adoption of the system among stakeholders might not permit the implementation of such a system's traceability.

Research gap

Existing studies exhibit significant limitations, including challenges in real-world deployment, the absence of machine learning integration for accurate blood availability prediction, minimal adoption of public blockchains such as BSC, and a lack of robust access control mechanisms to ensure secure data handling and system integrity ([Table 1](#)) gives a gist of existing studies.

METHODOLOGY

The proposed system architecture for the blood supply chain management system (B-SCM) is depicted in [Fig. 1](#). B-SCM comprises different entities that include Admin *i.e.*, National AIDS Control Organization (NACO), Collection Point (CP), Medical Centre

Table 1 Summary of the related work.

Author(s)	Blockchain	Coin	Scope	AIML	ACL	Application
<i>Hawashin et al. (2022)</i>	Private	ETH	Supply chain	No	No	Blood
<i>Fiore et al. (2023)</i>	Consortium	ETH	Supply chain	No	No	Healthcare
<i>Imamoglu, Topcu & Aydin (2023)</i>	Public	ETH	Supply chain	No	No	Blood
<i>Roozkhosh, Pooya & Agarwal (2023)</i>	Private	ETH	Supply chain	Yes	No	Blood
<i>Emmanuel et al. (2023)</i>	Public	ETH	Supply chain	Yes	No	Drugs
<i>Le et al. (2022)</i>	Private	ETH	Supply chain	No	No	Blood
<i>Trong et al. (2022)</i>	Private	ETH	Supply chain	No	No	Blood
<i>Ben Elmir, Hemmak & Senouci (2023)</i>	Private	ETH	Supply chain	Yes	No	Blood
<i>Khalid et al. (2023)</i>	Local	ETH	Stand alone	No	No	Networks
<i>Abdullah et al. (2022)</i>	Private	ETH	Supply chain	No	No	Blood
Proposed	Public	BNB	Supply chain	Yes	Yes	Blood

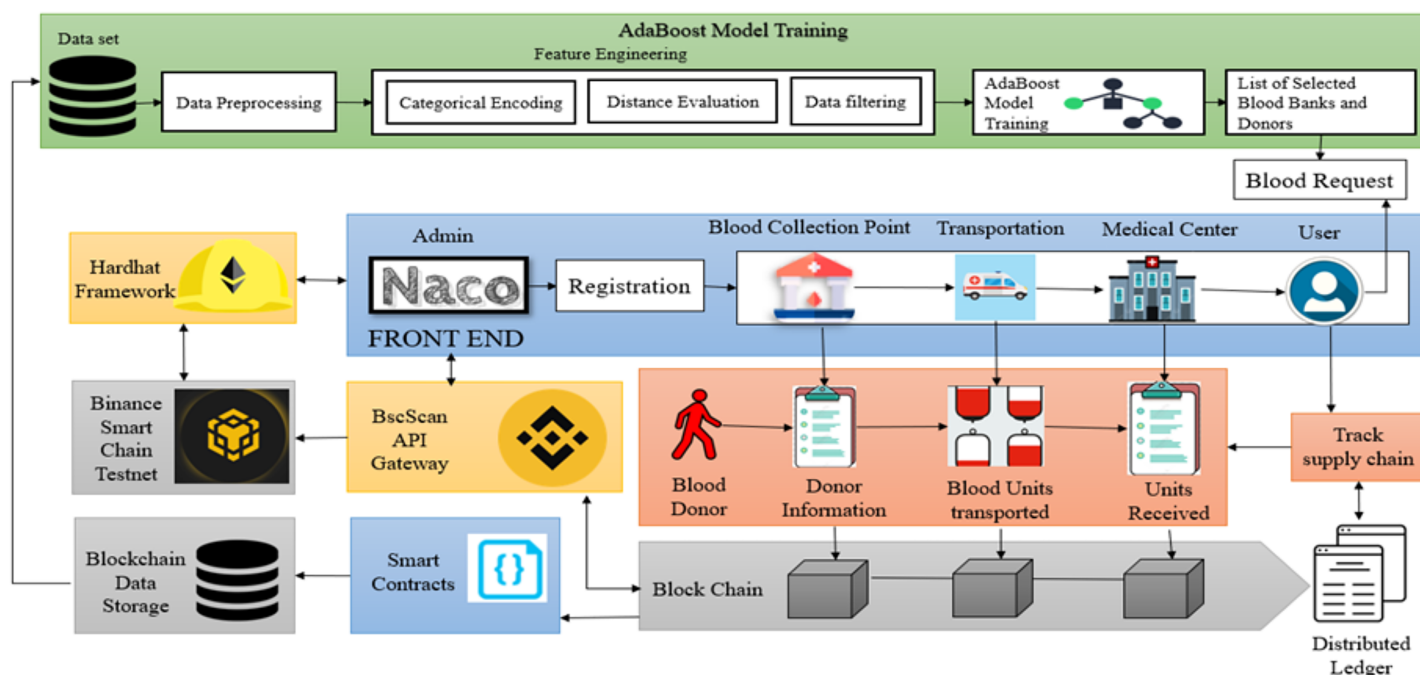


Figure 1 Proposed methodology for blockchain-based B-SCM (Bing, 2025d; Blockchains, 2025; Bing, 2025a; AltcoinsBox, 2025; Bing, 2025b; Google, 2025j; Flaticon, 2025; Google, 2025l, 2025i, 2025n, 2025b, 2025c, 2025f, 2025m, 2025e; Bing, 2025c).

Full-size DOI: 10.7717/peerj-cs.3123/fig-1

(MC), Transporter (TS), and Donor (DR). The system contains four phases—Registration phase, Login and authentication phase, Logistics Management, and User request (Eghtesadifard & Jozan, 2022). The model runs on a system equipped with an 11th Generation Intel Core™ i7-11390H processor, 16 GB RAM, a 64-bit Windows 10 operating system, and a 1 TB hard drive. The AdaBoost model was implemented using Python 3.9 with the scikit-learn library.

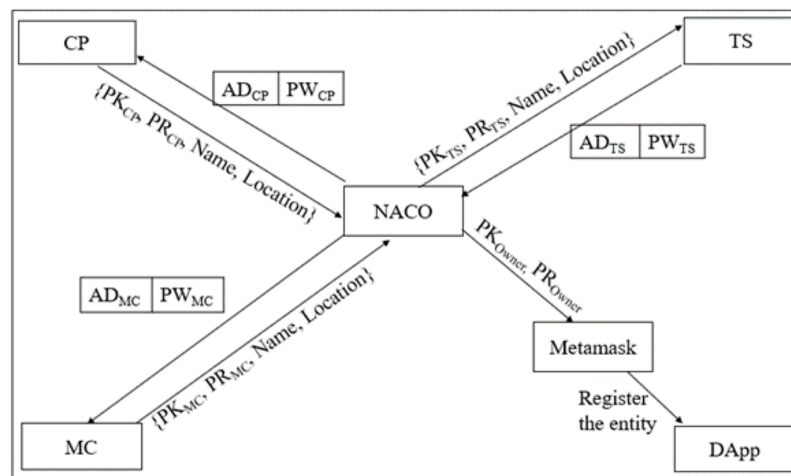


Figure 2 Entity registration phase of B-SCM.

Full-size DOI: 10.7717/peerj-cs.3123/fig-2

Registration phase

Entity registration phase

Figure 2 depicts the entity Registration phase which explains the process of each entity registration. B-SCM has three entities $\mathbb{E}$ as in Eq. (1) that are solely registered by the central authority NACO. Each entity has a wallet address that is technically analogous to the public key of the entity symbolically PK_E as represented in Eqs. (2) and (3).

$$\mathbb{E} = \langle CP, MC, TS \rangle \quad (1)$$

$$\langle \langle \text{Wallet Address} \equiv \text{Publickey}; PK_E \rangle \rangle \quad (2)$$

$$\langle \langle \text{Password} \equiv \text{Private Key}; PR_E \rangle \rangle. \quad (3)$$

Step 1: $NACO \iff \langle PK_{Owner} \parallel PR_{Owner} \rangle$; $NACO \rightarrow \langle PK_E \rangle$; NACO can access the dApp using $\langle PK_{Owner}, PR_{Owner} \rangle$. Once NACO registers into B-SCM, it is liable for registering $\mathbb{E}$ in B-SCM with $\langle PK_E \rangle$.

$$\text{Step 2: } \mathbb{E} \rightarrow \langle \langle PK_E \parallel PR_E \parallel \text{Name} \parallel \text{LOC} \rangle \rangle$$

$\mathbb{E}$ registers into the system with PK_E , Name, and Location. NACO validates the entity by considering the standards of the entity: (available (AV), accessible (AC), affordable (AF), safe (SF), and of standard quality (SQ)), i.e., $\mathbb{E}$ should possess the standards of NACO, and then it is considered to be valid as in Eq. (4).

$$\text{is Valid}(\mathbb{E}) \rightarrow \left\langle \begin{array}{ll} AV \rightarrow \text{True}; & AC \rightarrow \text{True}; \\ AF \rightarrow \text{True}; & SF \rightarrow \text{True}; \\ SQ \rightarrow \text{True} \end{array} \right\rangle. \quad (4)$$

$$\text{Step 3: } MM \rightarrow PK_{Owner};$$

The Metamask connected to PK_{Owner} will be initiated, and the transaction of registering $\mathbb{E}$ will be enforced.

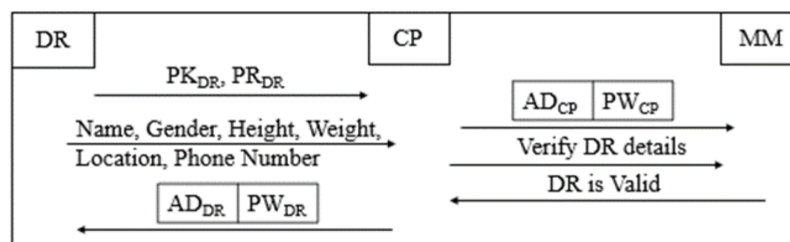


Figure 3 Donor registration phase of B-SCM.

Full-size DOI: 10.7717/peerj-cs.3123/fig-3

Step 4: If $\langle PK_{Owner}, PR_{Owner} \rangle$ is valid, the transaction will proceed further by processing $\mathbb{E}$ to MM and subsequently adding $\mathbb{E}$ into B-SCM. Otherwise, the access of $\mathbb{E}$ is denied, as illustrated in Eqs. (5), (6), (7).

$$\text{addEntity}(\mathbb{E}) \rightarrow (\mathbb{E} \mapsto MM) \cup (\mathbb{E} \bowtie B - SCM) \quad (5)$$

$$\text{denyEntity}(\mathbb{E}) \rightarrow (\mathbb{E} \not\bowtie B - SCM) \quad (6)$$

$$(PK_{Owner} \parallel PR_{Owner} == \text{Eq. (4)}) : \text{Eq. (5)}? \{ \text{Eq. (6)} \}. \quad (7)$$

Donor registration phase

CP registers DR in B-SCM, validating the DR as depicted in Fig. 3 and adhering to the regulatory standards of NACO (Rekha & Siddappa, 2023) as follows:

Step 1: $CP \rightarrow DR$;

$DR \rightarrow \sum (\text{name}, A, G, Wt, Ht, Loc, Phn)$; CP collects the details of DR, which include name, age, gender, weight, height, location, and phone number.

$$\text{isEligible}(DR) \rightarrow \left\langle \begin{array}{l} Wt \geq 50 \text{ kg} \cup A \geq 18 \\ \text{and } A \leq 75 \end{array} \right\rangle. \quad (8)$$

Step 2: After verifying whether the respective DR is eligible, as illustrated in Eq. (8), for donating blood by the details collected in Step 1, $\langle PK_{DR} \rangle$ is shared with CP and registered on B-SCM.

Step 3: $DR \rightarrow B\text{-SCM}$: DR can access B-SCM with $\langle PK_{DR}, PR_{DR} \rangle$ and then confirm their details. This ensures two-step authentication of DR details to ensure safe and secure blood maintenance (Ghadge et al., 2022).

Login and authentication phase

Each entity upon registration goes through the login and authentication phase as shown in Fig. 4 by following the steps below:

Step 1: $\langle MM \rightarrow AD_E; AD_E \equiv PK_E; PW_E \equiv PR_E \rangle$; $\mathbb{E}$ enters $\langle AD_E, PW_E \rangle$ to log into B-SCM. It enables Metamask (MM) and performs a three-step mutual authentication. This includes verifying the existence of the address of $\mathbb{E}$ in MM and cross-checking the authenticity of $\mathbb{E}$.

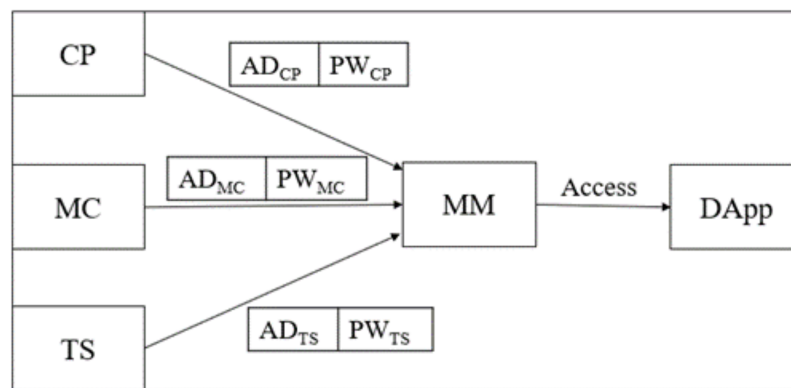


Figure 4 Login and authentication phase of B-SCM. Full-size DOI: 10.7717/peerj-cs.3123/fig-4

Step 2: $\langle MM \rightarrow AD_{CP}; AD_{CP} \equiv PK_{CP}; PW_{CP} \equiv PR_{CP} \rangle$; each $\mathbb{E}$ has its functions to perform in dApp. CP has $\langle AD_{CP}, PW_{CP} \rangle$ that are verified by MM for mutual authentication.

Step 3: $\langle MM \rightarrow AD_{MC}; AD_{MC} \equiv PK_{MC}; PW_{MC} \equiv PR_{MC} \rangle$; CP can receive blood from donors and supply it to MC as requested, whereas MC has $\langle AD_{MC}, PW_{MC} \rangle$ that are verified by MM for mutual authentication.

Step 4: $\langle MM \rightarrow AD_{TS}; AD_{TS} \equiv PK_{TS}; PW_{TS} \equiv PR_{TS} \rangle$; TS supplies the blood from CP to MC, whereas TS has $\langle AD_{TS}, PW_{TS} \rangle$ that are verified by MM for mutual authentication.

Logistics management

The blood inventory management ranges from the NACO to the user (*Kumaran & Mohan, 2023*), and all these logistics can be implemented by the entities in B-SCM as depicted in *Fig. 5*. The following steps outline the process:

Step 1: $MC \rightarrow CP$; $CP \rightarrow \langle ID_{CP} \parallel ID_{MC} \parallel N \parallel BG \rangle$; the supply chain process begins when a patient requires blood at a MC. The MC contacts the CP with the CP's identification number, the MC's own identification number for verification purposes, the number of blood units needed, and the required blood group (*Subramanian, 2024*).

Step 2: $CP \rightarrow MC$; CP evidences the MC and checks for availability of the intended blood group (BG) and required number of blood units as shown in *Eq. (9)*.

$$BG_{availability} \rightarrow \langle N_{available} > N \rangle \rightarrow \text{True}. \quad (9)$$

Step 3: $CP \rightarrow MC$; $MC \rightarrow \langle ID_{DR} \parallel ID_{MC} \parallel N \parallel DR_{Info} \rangle$; later, CP sends $\langle ID_{DR} \parallel ID_{MC} \parallel N \parallel DR_{Info} \rangle$ to MC, which ensures the safety, security, and quality of blood inventory management.

Step 4: $DR \rightarrow MC$; $DR_{Info} = \int \langle BG \parallel HIV \parallel LIV \parallel HB \parallel BP \rangle$; with the ID_{DR} , MC confirms the blood quality as illustrated in *Eqs. (10)* and *(11)* by verifying the DR_{Info} that comprises information about health standards according to NACO.

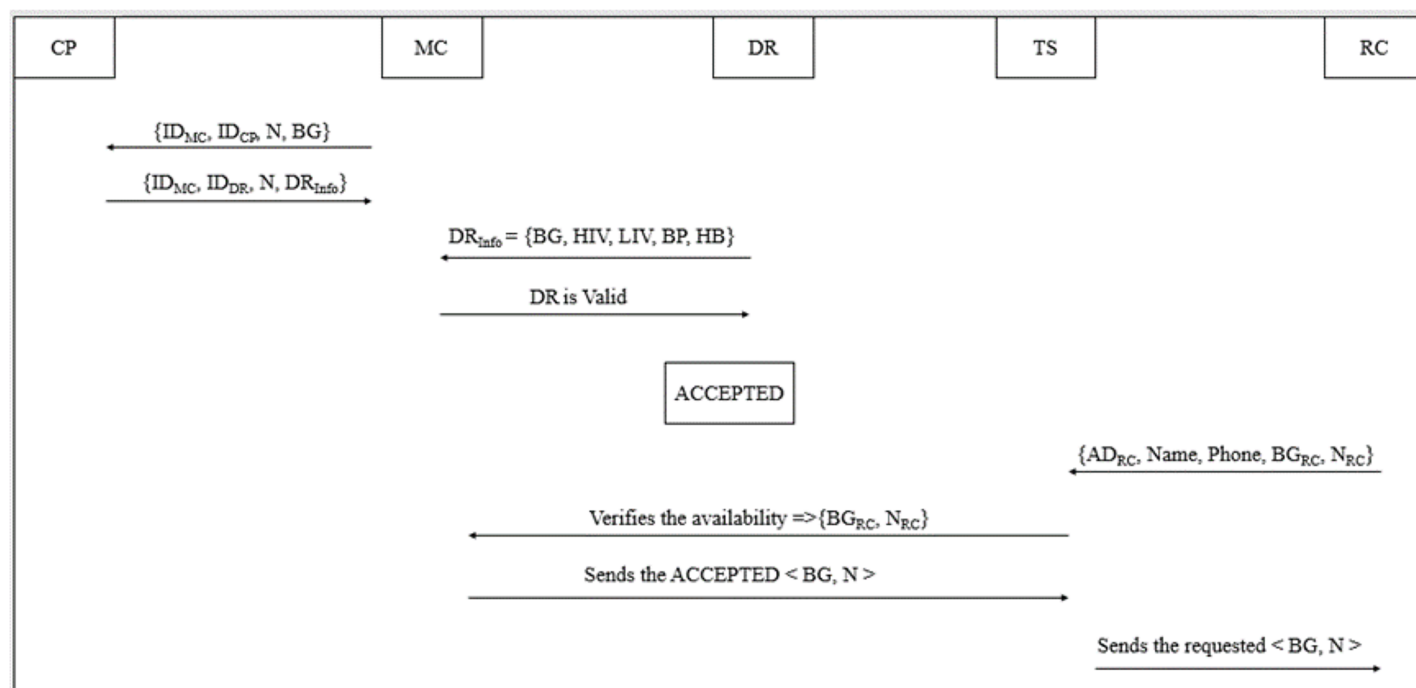


Figure 5 Logistics management phase of B-SCM.

Full-size DOI: 10.7717/peerj-cs.3123/fig-5

$$DR_{Standards} \rightarrow \langle \neg HIV \parallel \neg LIV \parallel \neg BP \parallel HB > 12 \rangle \quad (10)$$

$$BloodQuality(BU) \rightarrow (DR_{Info} \approx DR_{Standards}) : \text{True} ? \text{False}. \quad (11)$$

Step 5: On confirming the blood quality, MC assigns an ACCEPTED/REJECTED tag to the blood unit (BU) received as illustrated in Eq. (12).

$$BU \rightarrow (\text{Eq. (11)} == \text{True}) : \text{ACCEPTED} ? \text{REJECTED}. \quad (12)$$

Step 6: $TS \rightarrow User$; $RCInfo \Rightarrow \langle AD_{RC}, Name, Phone, BG_{RC} \rangle$; TS will send the ACCEPTED blood units to the end user. TS collects recipient information $\{RC_{Info}\}$ for safe and secure logistics management.

User request

The blood bank dataset utilized for this study was sourced from the central government's official website, eRaktKosh (*Ministry of Health and Family Welfare, Government of India, 2016*). The data was systematically organized into a structured format of rows and columns, enabling efficient preprocessing and model training. Specifically, the dataset comprises 106 entries across eight distinct attributes, providing a robust foundation for analysis and model development (*Ministry of Health and Family Welfare, Government of India, 2025*). This study employed a purposive sample of 106 participants, chosen for accessible direct engagement with the hospital system under evaluation. While the sample may seem limited, it aligns with similar exploratory research in health informatics. Future work will expand this to multiple institutions across different regions to improve

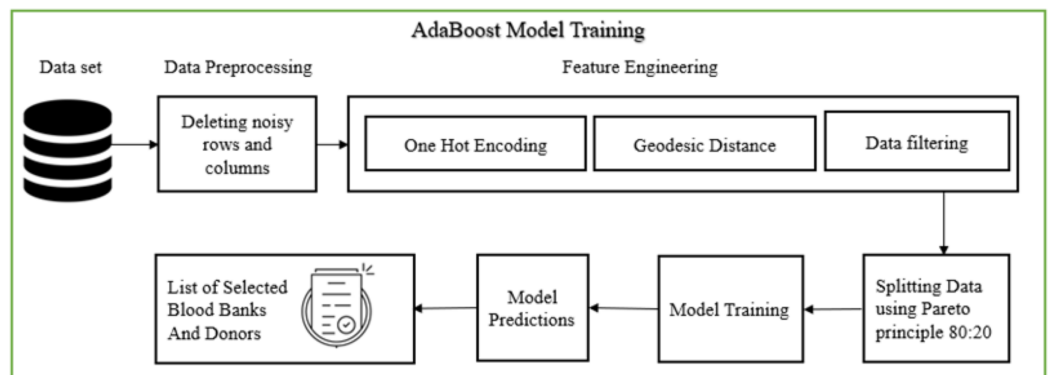


Figure 6 AdaBoost model training (Bing, 2025d).

Full-size DOI: 10.7717/peerj-cs.3123/fig-6

generalizability. The user can request the intended BG and search for the nearest blood banks (BB) as follows:

Step 1: $User \rightarrow Location$; $Location \Rightarrow \langle LAT_{User}, LON_{User} \rangle$; the user enables location services by logging into the dApp, which retrieves the user's latitude and longitude.

Step 2: $User \rightarrow \langle BG, N \rangle$; the user enters the required blood group and the number of necessary blood units into B-SCM. The $\langle LAT_{BB}, LON_{BB} \rangle$ of the blood banks are fetched, and the geodesic distance is calculated as shown in the following equations:

$$\alpha = \sin^2\left(\frac{\Delta\psi}{2}\right) + \cos(LAT_{User}) \times \cos(LAT_{BB}) \times \sin^2\left(\frac{\Delta\varphi}{2}\right) \quad (13)$$

$$\beta = 2 \times \arctan 2\left(\sqrt{\alpha}, \sqrt{1-\alpha}\right) \quad (14)$$

$$\gamma = \mathbb{R} \times \beta \quad (15)$$

$$\Delta\psi = (LAT_{User} - LAT_{BB}) \times \frac{\pi}{180} \quad (16)$$

$$\Delta\varphi = (LON_{User} - LON_{BB}) \times \frac{\pi}{180}. \quad (17)$$

Step 3: The AdaBoost model identifies the nearest blood banks to the user based on $\langle LAT_{BB}, LON_{BB} \rangle$ and filters the blood banks by checking blood availability $\langle BG, N \rangle$.

Step 4: The model filters blood banks based on the BG availability that matches with the user request along with the location that is nearest to the user's location.

Figure 6 illustrates the AdaBoost model training pipeline, which comprises several stages: data pre-processing, feature engineering, data splitting, model training, and displaying the final list of selected blood banks and donors. During data pre-processing, the dataset was first screened for missing values, duplicates, and outliers. Missing values in critical fields (e.g., blood group, geographic coordinates, or availability status) were either imputed using domain-informed defaults or removed if imputation risked introducing bias. Duplicate entries were eliminated using record linkage based on blood bank names and GPS coordinates. Outliers in numerical attributes (e.g., extreme or incorrect

Table 2 Considered factors in the index of blood donor profile.

Factors	Characteristics	Scoring mechanisms
Donor recruitment	Voluntary Non-remunerated, Low risk, Safe and healthy donors	
Name & Address		Govt. authorized Documents
Donor selection	Age	18 and 65 years
	Hemoglobin or packed Cell Volume (Hematocrit)	Hemoglobin more than 12.0 gm/dl or Hematocrit less than 36%
	Weight	45–55 Kg–350 ml collection 55 Kg–450 ml collection
	Blood pressure	Systolic blood pressure: 100 and 160 mm Diastolic pressure: 60–90 mm
	Temperature	37.5 C/99.5 F
	Pulse	60 to 100 beats per minute
Blood group	Temp & Expiry date	Use before 12 weeks
Medical history	Not suffering from any serious illness	Ex: malignant disease, epilepsy, bronchial asthma, diabetes, excessive menstrual bleeding, cardio-vascular conditions, renal disease, allergic diseases, abnormal bleeding tendency. Deferred permanently
	HIV, HBsAg/HCV	Deferred permanently
	Swollen glands, Persistent cough, Unexplained weight loss, Night sweats/fever, Skin rashes and skin infections, diarrhea	
	Alcohol, Any drug abuse	Not accepted if not providing reliable answers to the standard questionnaire

Table 3 Rules defined in access control lists.

Rule	Entity	Access control	Justification
R1	NACO	Register entities	NACO is authorized to register the central entities (CP, MC, TS) into B-SCM. This ensures that only authorized entities, validated by NACO, are included in the system, maintaining data integrity and regulatory compliance.
R2	CP	Register donors	CP can register donors into B-SCM after collecting and validating donor information. This rule ensures that only validated donors meeting regulatory standards can participate in the blood supply chain.
R3	E (CP, MC, TS)	Access B-SCM	Entities (CP, MC, TS) can access their respective operations within B-SCM using their public-private key pairs. This rule implements mutual authentication to ensure secure access and operation within the dApp.
R4	CP	Manage logistics	CP manages logistics such as blood inventory from collection points to medical centers. This rule allows CP to maintain efficient supply chain operations, verifying blood availability and quality before distribution.
R5	MC	Receive blood units	MC receives blood units from CP after verification of donor and blood quality. This rule ensures that only blood meeting specified health standards and donor eligibility criteria is accepted by MC.
R6	User	Request blood units	Users can request blood units based on blood group and location. This rule facilitates user access to critical blood supply information, ensuring efficient matching with available donors and blood banks.

latitude/longitude values) were detected using interquartile range (IQR) and Mahalanobis distance methods. Furthermore, categorical attributes were standardized to maintain consistency in labels (*e.g.*, “B+” and “B Positive” unified).

The cleaned dataset ensured higher model reliability and minimized noise during training. Feature engineering followed, involving one-hot encoding for blood groups and normalization of geospatial coordinates. Independent variables included user-provided latitude and longitude, the requested blood group (BG), and required units (N), while dependent variables were blood availability and system-generated selection of suitable blood banks. The model applied the Haversine formula for precise geodesic distance calculations, enabling spatial filtering of blood banks. The curated dataset was then partitioned into training and validation sets, and used to train the AdaBoost classifier—selected for its high accuracy in imbalanced datasets. The final output lists eligible blood banks based on both proximity and stock availability.

The AdaBoost algorithm was selected for its high classification accuracy and ability to handle imbalanced datasets, which are common in donor availability and blood stock prediction scenarios. Its ensemble learning approach, combining weak learners to form a strong predictor, makes it well-suited for our use case involving multiple features such as donor location, blood group, availability history, and urgency level. The AdaBoost model is implemented off-chain within the decision-support layer of the system. Performing such computations on-chain is not feasible due to gas cost constraints and the computational limitations of blockchain environments.

As shown in [Table 2](#), blood should only be collected by a licensed blood bank, considering certain factors. Blood should be drawn from the donor by a qualified physician or under their supervision by trained assistants. The blood is then stored over a blockchain using the proposed distributed application (dApp).

The implemented system incorporates predefined rules within Access Control Lists (ACLs), outlined in [Table 3](#), to safeguard the security and privacy of sensitive user, donor, and blood bank information. These rules ensure that digitalization processes are securely managed under authorized control, thereby protecting highly confidential details throughout the system. This comprehensive approach to access control ensures that only authorized entities can interact with specific functionalities, maintaining data integrity and regulatory compliance in the B-SCM system.

RESULTS AND DISCUSSIONS

The Home page of blood block supply chain management system (BB-SCM) shown in [Fig. 7](#) depicts the entities involved in BB-SCM where each entity has been provided with Login and Register options. The smart contracts written ensure that only the owner *i.e.*, NACO can register all the entities. [Figure 8](#) depicts all entities registered in BB-SCM by the Admin which details the public address, name, and contact number of each entity E. An entity is registered as a transaction initiated by the Admin that ensures authorization. As soon as the contract has been confirmed in Metamask, the dApp pops up a message showing the registration has been completed. CP can register donors since blood is collected by CP which can be seen in [Fig. 9](#) As per NACO standards, the details to be

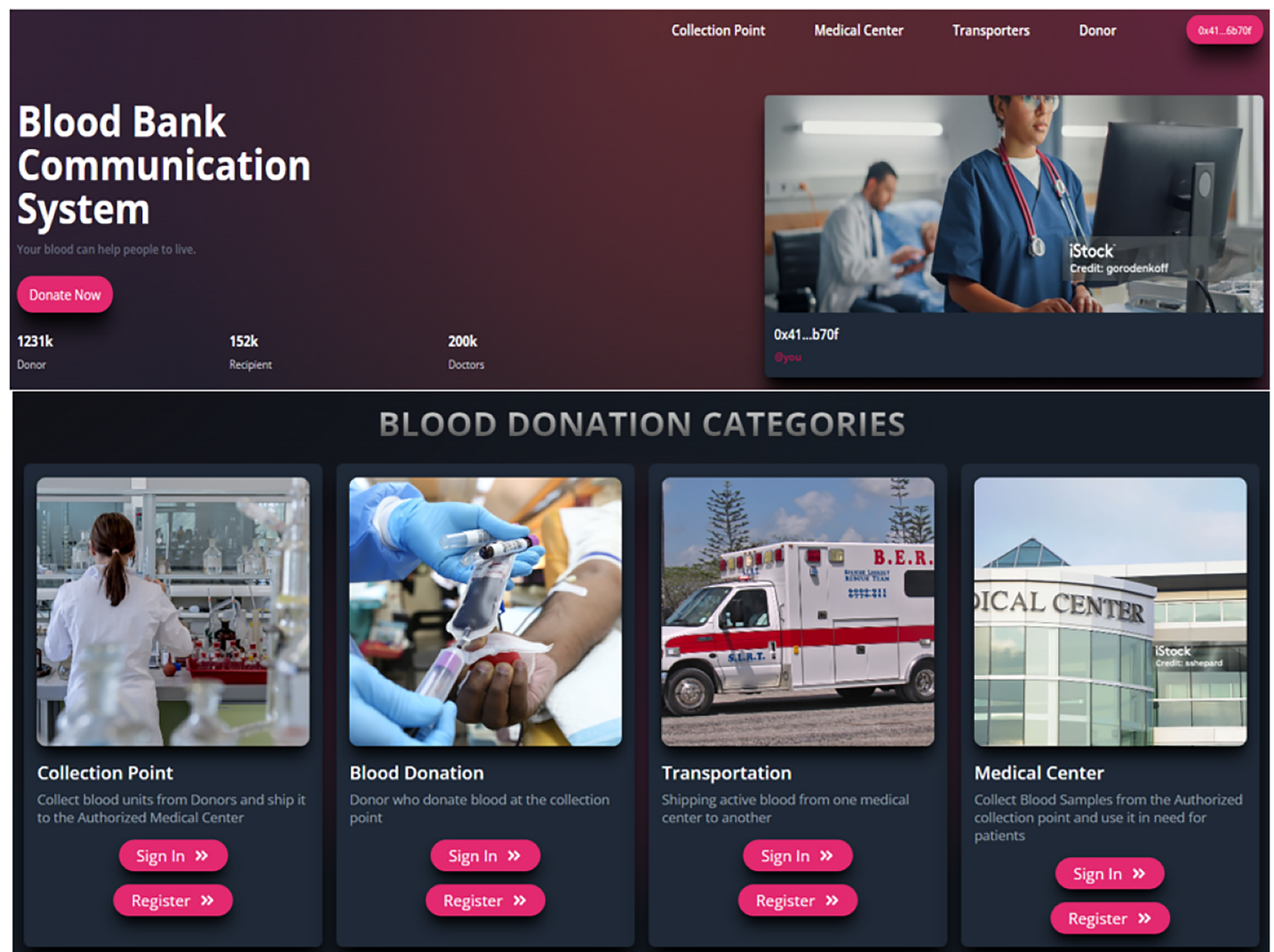


Figure 7 Home page of blood bank dApp (Google, 2025d, 2025a, 2025k, 2025h, 2025g).

Full-size DOI: 10.7717/peerj-cs.3123/fig-7

collected from the donor by CP are name, age, weight, gender, and mobile number. The public wallet address is collected in addition, to ensure donor authorization. Figure 10 depicts the process of distributing blood from the CP to the MC as requested by the MC to the CP. For initiating the transportation, CP requires the name of the intended MC, public address for authenticity, and volumes of blood required.

After the blood is transported to the MC, the second step of verification is presided over blood units by the MC. According to NACO standards, the following parameters of the DR are substantiated: $\langle BG, HIV, LIV, BP, HB \rangle$; if the DR meets all requirements specified by NACO, the blood unit is accepted. When the end user is in need of blood, the TS will receive the details of the RC and supply the blood unit from NACO to the end user. Later, the details of the RC are to be collected at the time of blood transportation. The end user can track the status of intended blood units to be received by logging in with their respective wallet address, as shown in Fig. 11.

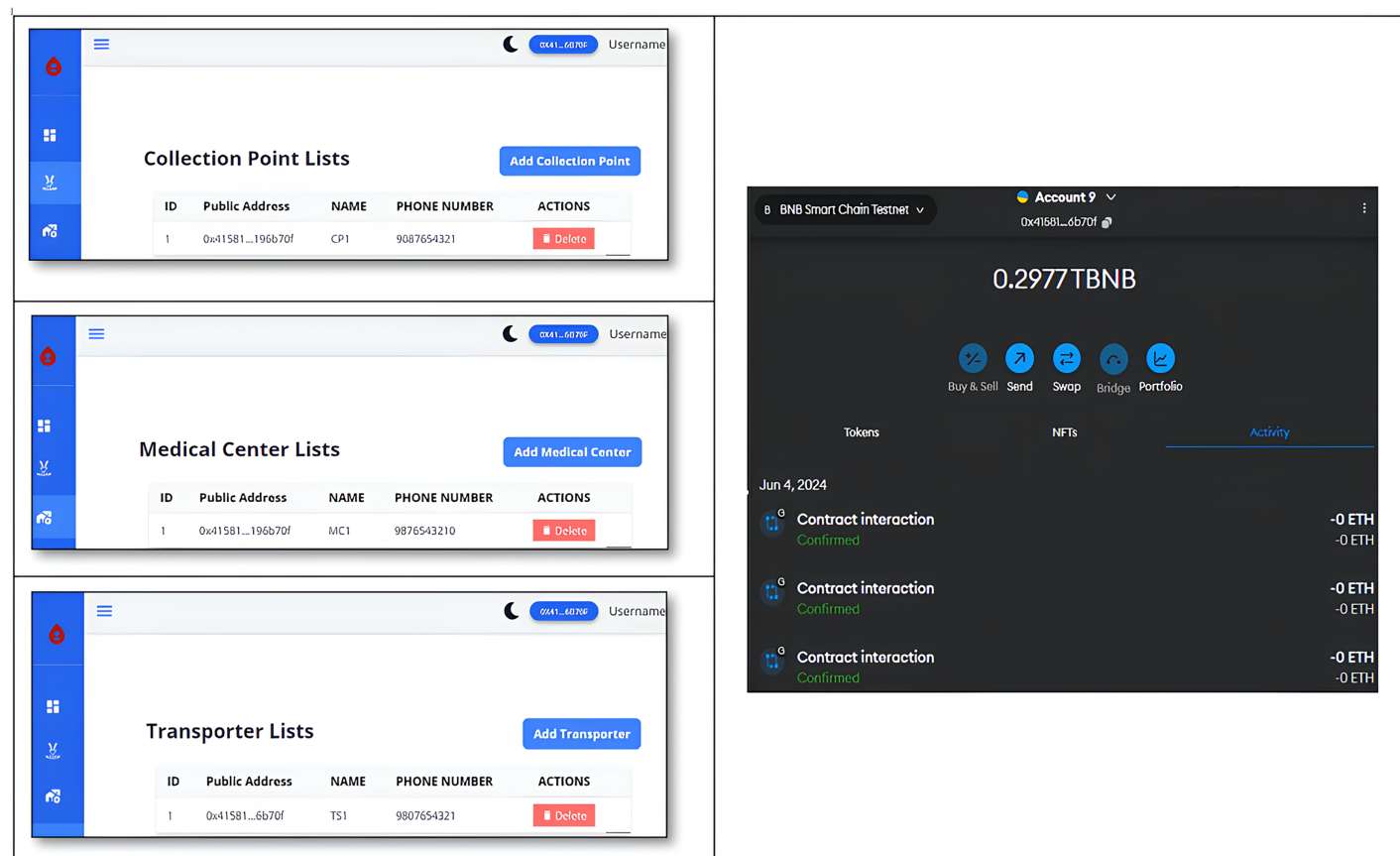


Figure 8 Registered entities in B-SCM.

Full-size DOI: 10.7717/peerj-cs.3123/fig-8

Figure 12 describes a user interface where the user is prompted to enter their blood type and location by providing the latitude and longitude. When the user clicks the “Search Blood Banks” button, the system calculates the nearest blood banks using the geodesic distance method. Based on this data, it lists the blood banks closest to the user, ensuring that the user can quickly find available blood supplies.

SECURITY ANALYSIS

Formal analysis

Theorem: The security and privacy of the data are provided in the B-SCM by implementing a Byzantine Fault Tolerance (BFT) system for the nodes in the system (*Al-Farsi, Rathore & Bakiras, 2021*). The nodes in the system, namely NACO, DR, CP, TS, and MC, are interconnected in the network as shown in Fig. 13.

Proof: Let $N = 5$ be the total number of nodes in the network. For a Byzantine Fault Tolerance system to function correctly, it must tolerate up to f faulty nodes where $N > 3f$. The BFT consensus algorithm used is Practical Byzantine Fault Tolerance (PBFT), which ensures consensus if at least $\frac{2N}{3}$ nodes agree on the validity of a transaction. Given $N = 5$,

Register Donor

✕



Figure 9 Donor registration at CP in B-SCM.

Full-size  DOI: 10.7717/peerj-cs.3123/fig-9

the maximum number of tolerated Byzantine nodes is f , which satisfies (Eq. (18)). Therefore, we get the f value as evaluated in Eq. (19):

$$N > 3f \quad (18)$$

$$f < \frac{N}{3} = \frac{5}{3} \approx 1.67. \quad (19)$$

To analyze the relationship between correct nodes and faulty nodes, consider the following inequality derived from Eq. (18):

$$N - f > 3f - f. \quad (20)$$

Simplifying Eq. (20), we get:

$$N - f > 2f. \quad (21)$$

Therefore, from Eqs. (19) and (21), we get:

$$N - f > \frac{2N}{3}. \quad (22)$$

Distribute Blood To MedicalCenter

Medical Center Name:

Donor Public Address:

Donated Volume (in ML):

[Register](#)

Complete Blood Checking

Blood Type:

HIV Test:

Liver Fever:

Blood Pressure

HemoglobinLevel

Blood Test Results:

[submit](#)

Full Fill Blood To Recipient

Recipient Public Address:

Name

Recipient Phone Number:

Blood Type:

[Full Fill](#)

Figure 10 Distributing blood from the collection point to the medical center.

Full-size  DOI: 10.7717/peerj-cs.3123/fig-10

Blood Donation Transaction

S/N	TRANSACTIONID	DONOR	TRANSPORTER	RECIPIENT	BLOODTYPE	VOL. (IN ML)	DONAT DATE	STATUS	BLOODTESTRESULT	ACTIONS
1	1730625375	DR1	0X00000...00000	0X922FC...4AC34	A+	12	1730625375	FULLFILLED	ACCEPTED	Complete FullFill Supply
2	1730625506	DR1	0X00000...00000	0X00000...00000	--	12	1730625506	SHIPPED	NO RESULT	Complete FullFill Supply

Figure 11 Tracking the stages of blood unit in supply chain management.

Full-size  DOI: 10.7717/peerj-cs.3123/fig-11

To validate the number of correct nodes required for consensus, we calculate:

$$\frac{2N}{3} = \frac{2 \times 5}{3} = \frac{10}{3} \approx 3.33 \approx 4. \quad (23)$$

Hence, the system can tolerate up to 1 faulty node ($f = 1$). For a transaction T (e.g., blood donation, transport, or utilization) to be validated, each node i (where $i \in \{1, 2, \dots, 5\}$) independently validates T . The transaction T is considered valid if at least the number of nodes as computed in Eq. (23) vote in favor of it. This ensures that even if up to 1 node is malicious or faulty, the system remains secure. Therefore, from Eqs. (22)

Find Blood Banks

Blood Type

A+

Latitude Longitude Required Units

17.3860712
78.3511362
2

Use Current Location
Search Blood Banks

Connect Wallet

Ramesh Hospital Blood Center

Distance: 0.01 km

Blood Type: A+

Net Units Available: 7

Location: Ward 33D, Ground floor, Ring Road, ITI Bus stop, Vijayawada, Krishna, Andhra Pradesh

Phone: 9640123234

Coordinates: 16.4801,80.6881

Kamineni Health Care Pvt. Ltd. Blood Centre

Distance: 1.01 km

Blood Type: A+

Net Units Available: 3

Location: 102 Feet Road, New Auto Nagar, Poranki, Vijayawada, Krishna, Andhra Pradesh

Phone: 8333993002

Coordinates: 16.4798,80.697575

Andhra Hospital Blood Bank

Figure 12 Prediction of the nearest blood banks.

Full-size  DOI: 10.7717/peerj-cs.3123/fig-12

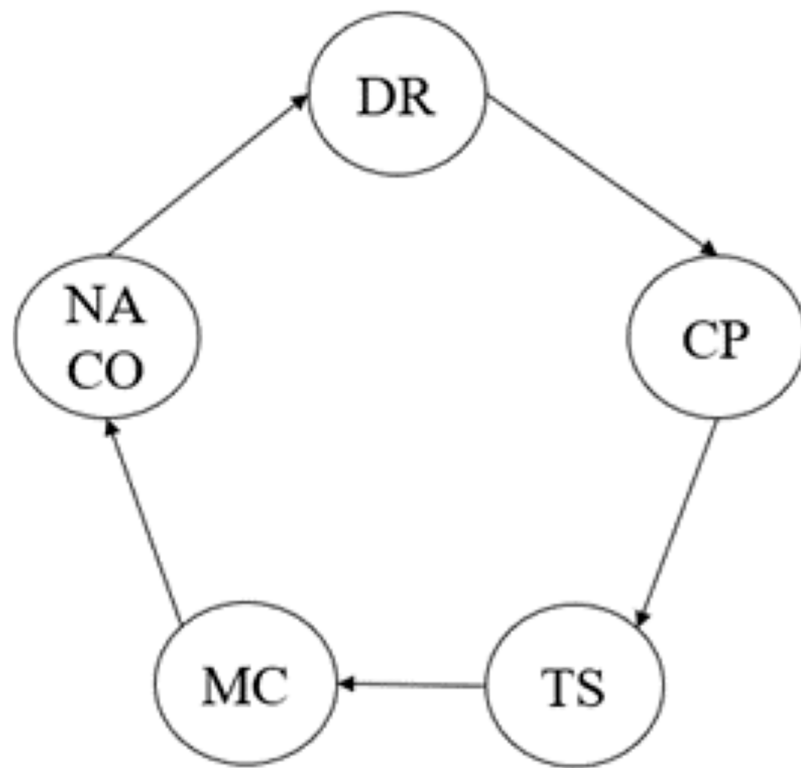


Figure 13 Nodes in B-SCM.

Full-size DOI: 10.7717/peerj-cs.3123/fig-13

and (23), if four nodes agree, T is added to the blockchain. Additionally, in the case where TS submits conflicting transport data, the other nodes (NACO, DR, CP, and MC) identify the inconsistency and reject TS's transaction. Continuous misbehavior by TS leads to its removal from the consensus process by a majority vote, ensuring system integrity.

Lemma 1: In a PBFT system, consensus is reached.

Proof: In a PBFT system, f is the maximum number of faulty nodes the system can tolerate. Since $N > 3f$, there are always at least $N - f$ correct nodes. The consensus requires $\frac{2N}{3}$ votes, thereby from Eq. (22) ensuring that a majority of correct nodes can reach consensus even if up to f nodes are faulty.

Lemma 2: The system ensures data integrity and privacy.

Proof: The data is stored and transmitted using blockchain technology, which leverages cryptographic techniques inherent in blockchain systems to ensure that data cannot be altered once it is committed to the ledger. Each transaction is digitally signed by the submitting node, and the integrity of the data is verified by all participating nodes. The immutable audit trail on the blockchain ensures that all transactions are verifiable and traceable, further ensuring data integrity and privacy. This system implements this framework by maintaining a ledger that records every crypto transaction.

Informal analysis

Proposition 1: The proposed B-SCM model can prevent a 51% attack.

Proof: A 51% attack in blockchain systems involves an adversary gaining majority control of the network's hashing power, enabling them to manipulate transactions and undermine network integrity. The B-SCM system achieves consensus through a decentralized Proof of Authority (PoA) mechanism (Manolache, Manolache & Tapus, 2022). Validators, comprising entities $\mathbb{E} = \{CP, MC, TS\}$, are selected based on their authority and reputation within the supply chain network. Let N denote the total number of validators, and n denote the number of validators required to approve a transaction. By design, the B-SCM system ensures that n is sufficiently large to prevent any single entity or coalition from controlling more than $\frac{n}{N}$ of the network's validation power. Therefore, through the distributed authority and consensus mechanism, the B-SCM model ensures that the network remains secure and resilient against such attacks, preserving the integrity of blood supply chain transactions.

Proposition 2: The proposed blockchain model is resilient to Eclipse attacks.

Proof: An Eclipse attack aims to isolate a target node V in a blockchain network by surrounding it with malicious nodes controlled by an attacker (Jabbar et al., 2021). Let $G = (V, E)$ denote the blockchain network graph, where V represents nodes, $\mathbb{N} = \{CP, MC, TS\}$, and E denotes edges representing communication links. Each node $v_i \in V$ maintains connections with a set of neighboring nodes $N(v_i) \subseteq V$ and updates this set periodically using decentralized protocols. To prevent Eclipse attacks, the B-SCM system employs a consensus mechanism $\mathcal{C}$ enforced by smart contracts, ensuring that each transaction T initiated by nodes in V undergoes validation by a subset $N(T) \subseteq V$ comprising multiple nodes. Formally, for any transaction T initiated by node v_i , $N(T)$ verifies T according to $\mathcal{C}$, ensuring $|\{v_i \in N(T) \mid v_i \text{ validates } T\}| \geq \tau$, where τ is a consensus threshold. This decentralized validation approach, coupled with cryptographic signatures and secure communication protocols, ensures that the B-SCM system maintains network integrity, effectively resisting Eclipse attacks by preventing malicious nodes from controlling the information seen by targeted nodes and maintaining robustness in transaction verification across the decentralized network.

Proposition 3: The proposed model can prevent a Sybil attack.

Proof: A Sybil attack involves creating multiple fake identities to gain disproportionate influence in a network. The proposed B-SCM system uses identity certification to counter this attack. The Central Authority (NACO) registers all entities in the system, ensuring that each entity has a verified and unique identity. This prevents malicious actors from creating multiple fake identities to manipulate the system. NACO checks each entity's credentials, such as private key of entity (PRE), wallet address of entity (ADE), and transhash, to ensure their authenticity. This certification process effectively mitigates the risk of Sybil attacks by ensuring that only legitimate entities can participate in the network (Choudhury et al., 2021).

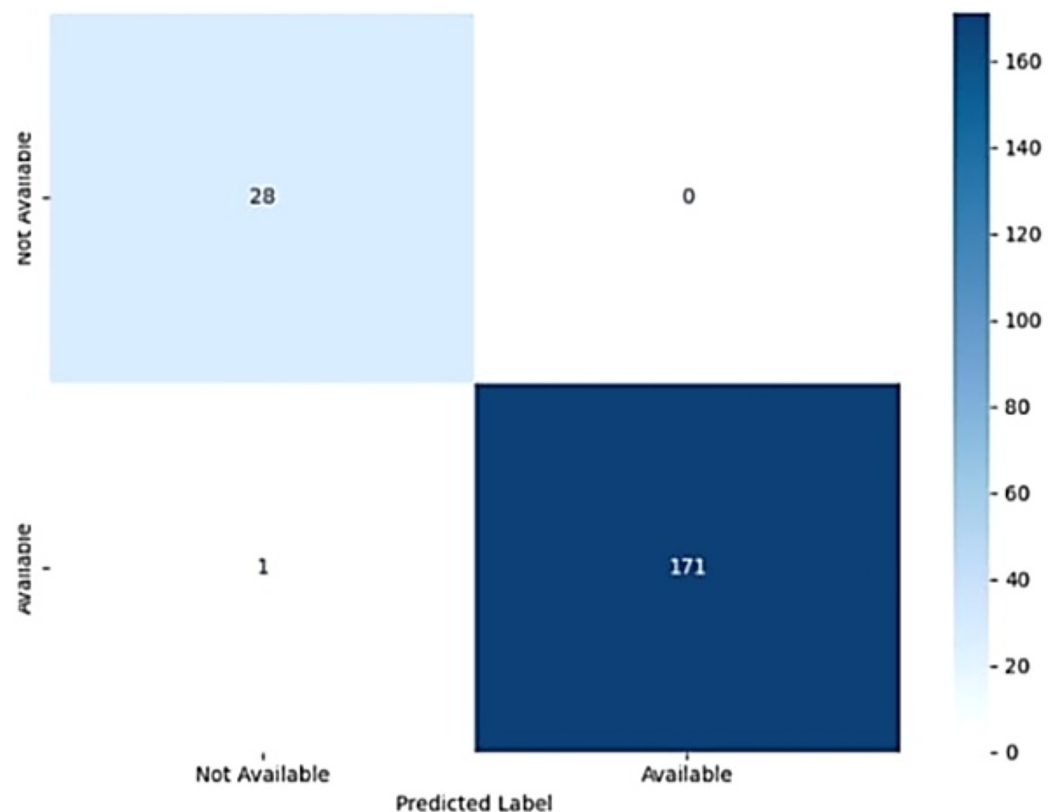


Figure 14 Confusion matrix of the AdaBoost model. Full-size [DOI: 10.7717/peerj-cs.3123/fig-14](https://doi.org/10.7717/peerj-cs.3123/fig-14)

Proposition 4: The proposed model is resilient to man-in-the-middle attacks.

Proof: A man-in-the-middle (MITM) attack involves an attacker intercepting and possibly altering the communication between two parties. In the B-SCM system, communication between entities $\mathbb{E} = \{CP, MC, TS\}$ is secured using cryptographic techniques. Each transaction is hashed using a cryptographic hash function hash of entity (HE). The hash value is kept confidential and is not included in the application binary interface (ABI) file, preventing attackers from gaining access. For an attacker to successfully intercept the communication, they would need to provide valid credentials PRE, public key of entity (PKE) matching the hashed values of the legitimate entities. Since these values are kept secret, an attacker can't perform an MITM attack (Maroun, Daniel & Fynes, 2019).

PERFORMANCE ANALYSIS

The model's performance was assessed using a confusion matrix, as shown in Fig. 14. In Eqs. (24), (25), (26) and (27) blood availability (BA) is analogous to True Positives, indicating the number of correct predictions of blood supply availability when it was indeed available. Blood unavailability (BU) corresponds to True Negatives, representing correct predictions of unavailability when the blood supply was unavailable (Younis et al., 2021). False blood availability (FBA) represents False Positives, where the model incorrectly predicted availability when the blood supply was unavailable. Similarly, false

blood unavailability (FBU) corresponds to False Negatives, indicating incorrect predictions of unavailability when the blood supply was available. This evaluation provides a comprehensive breakdown of the model's accuracy in predicting blood supply availability within the given context (Rupa et al., 2025).

The model achieved an accuracy of 96%, demonstrating its effectiveness in predicting the availability of blood from nearby blood banks and donors. The study possesses a precision of 97.95%, highlighting the model's ability to accurately identify true positive blood availability predictions. The recall was also 97.95%, indicating the model's effectiveness in detecting actual blood availability. Similarly, the F1-score was 97.95%, reflecting the balance between precision and recall and confirming the model's overall high performance in predicting blood supply availability.

$$\text{Accuracy} = \frac{BA + BU}{BA + BU + FBA + FBU} \quad (24)$$

$$\text{Precision} = \frac{BA}{BA + FBA} \quad (25)$$

$$\text{F1-score} = \frac{2 \times BA}{2 \times BA + FBA + FBU} \quad (26)$$

$$\text{Recall} = \frac{BA}{BA + FBU} \quad (27)$$

where:

- BA = True Positives (Blood Available)
- BU = True Negatives (Blood Unavailable)
- FBA = False Positives (False Blood Available)
- FBU = False Negatives (False Blood Unavailable)

B-SCM includes entities such as NACO, CP, MC, TS, and DR, as shown in Fig. 15. These entities interact and access data according to specific rules defined by Access Control Lists (ACLs), as illustrated in Table 2. To represent and enforce these rules, we use two matrices: a Binary Connection Matrix A and a Weighted Connection Matrix W .

The Binary Connection Matrix A in Eq. (28) indicates whether there is access (1) or no access (0) between entities. The rows and columns represent the entities, and each element a_{ij} shows if entity i has access to the resources of entity j .

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (28)$$

where in Eq. (28):

- rows and columns represent the entities in the order: NACO, CP, MC, TS, DR.
- Each element a_{ij} indicates whether entity i has access to the resources of entity j .

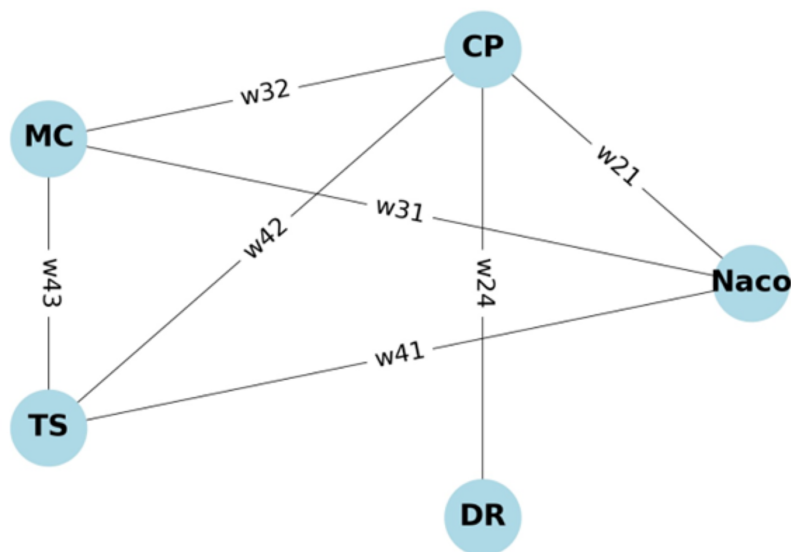


Figure 15 Graph representing entities in B-SCM.

Full-size DOI: 10.7717/peerj-cs.3123/fig-15

The Weighted Connection Matrix W assigns weights to the access permissions, representing the priority or level of access. These weights could be based on transactional data, security levels, and access frequency.

$$W = \begin{bmatrix} 0 & W_{12} & W_{13} & W_{14} \\ W_{21} & W_{22} & W_{23} & W_{24} \\ W_{31} & W_{32} & W_{33} & W_{34} \\ W_{41} & W_{42} & W_{43} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (29)$$

This study has successfully implemented Access Control Lists (ACLs) and priority scores were assigned for the entities for secure communication. The performance analysis of ACLs, priorities of entity operations, alongside the security and privacy requirements are clearly stated as follows:

$$ACL_{i,j} = \begin{cases} 1 & \text{if } a_{ij} = 1 \\ 0 & \text{if } a_{ij} = 0 \end{cases} \quad (30)$$

$$P_{i,j} = \begin{cases} W_{ij} & \text{if } a_{ij} = 1 \\ 0 & \text{if } a_{ij} = 0 \end{cases}. \quad (31)$$

To ensure ACLs are maintained, we sum the priority scores for all granted accesses as depicted in Eqs. (32) and (33). To illustrate the enforcement of ACLs, we use the priority scores of each entity along with the access level assigned to each entity.

For $ACL_{i,j} = 1$

$$\sum_{i \in E_j} \sum_{j \in E} ACL_{i,j} \cdot P_{i,j} = \sum_{i \in E_j} \sum_{j \in E} P_{i,j}. \quad (32)$$

For $ACL_{i,j} = 0$

Table 4 Quantitative comparison of BSC, ethereum, and hyperledger fabric.

Criteria	BSC	Ethereum (Mainnet)	Hyperledger fabric
Average transaction fee	≈ \$0.10	\$5–\$10	None (permissioned)
Transaction throughput (TPS)	55–100 TPS	15–30 TPS	1,000+ TPS
Block confirmation time	3 s	13–15 s	~1 s
Public/Private	Public	Public	Permissioned
Development complexity	Low (EVM-compatible)	Medium	High
Use case suitability	Scalable public DApps	Public DApps with high trust	Enterprise-grade apps

$$\sum_{i \in E_j} \sum_{j \in E} ACL_{i,j} \cdot P_{i,j} = \sum_{i \in E_j} \sum_{j \in E} 0 \cdot P_{i,j} = 0. \quad (33)$$

To strengthen the rationale for selecting Binance Smart Chain (BSC) over other platforms such as Ethereum and Hyperledger Fabric, a quantitative comparison is presented in [Table 4](#). The comparison evaluates core parameters including transaction fees, throughput, confirmation time, development complexity, and use case suitability. BSC offers significantly lower transaction costs (approximately \$0.10) compared to Ethereum’s \$5–\$10 range, making it highly cost-effective for frequent interactions in decentralized applications. While Hyperledger Fabric provides higher throughput, it is a permissioned network, making it less suitable for publicly accessible systems like ours. Additionally, BSC achieves a good balance between scalability, development simplicity (due to EVM compatibility), and public accessibility. These factors make BSC a more practical and efficient choice for the implementation of a decentralized blood supply chain management system.

[Table 5](#) describes the comparison between the proposed system with the existing studies. The proposed system, utilizing AdaBoost, demonstrates superior performance across all metrics, achieving an accuracy of 99.5%, which is the highest among the compared models. In terms of precision, recall, and F1-score, the proposed system consistently scores 0.99, 0.96, and 0.98, respectively, surpassing the performance of models like SVM, KNN, and MLP. These results indicate that the proposed AdaBoost system is not only more accurate but also more reliable in correctly identifying positive instances and capturing all relevant instances, making it the best-performing model in this comparison. This comprehensive improvement across all evaluation criteria underscores the robustness and effectiveness of our proposed approach. The superior performance of the proposed system can be demonstrated graphically in [Fig. 16](#).

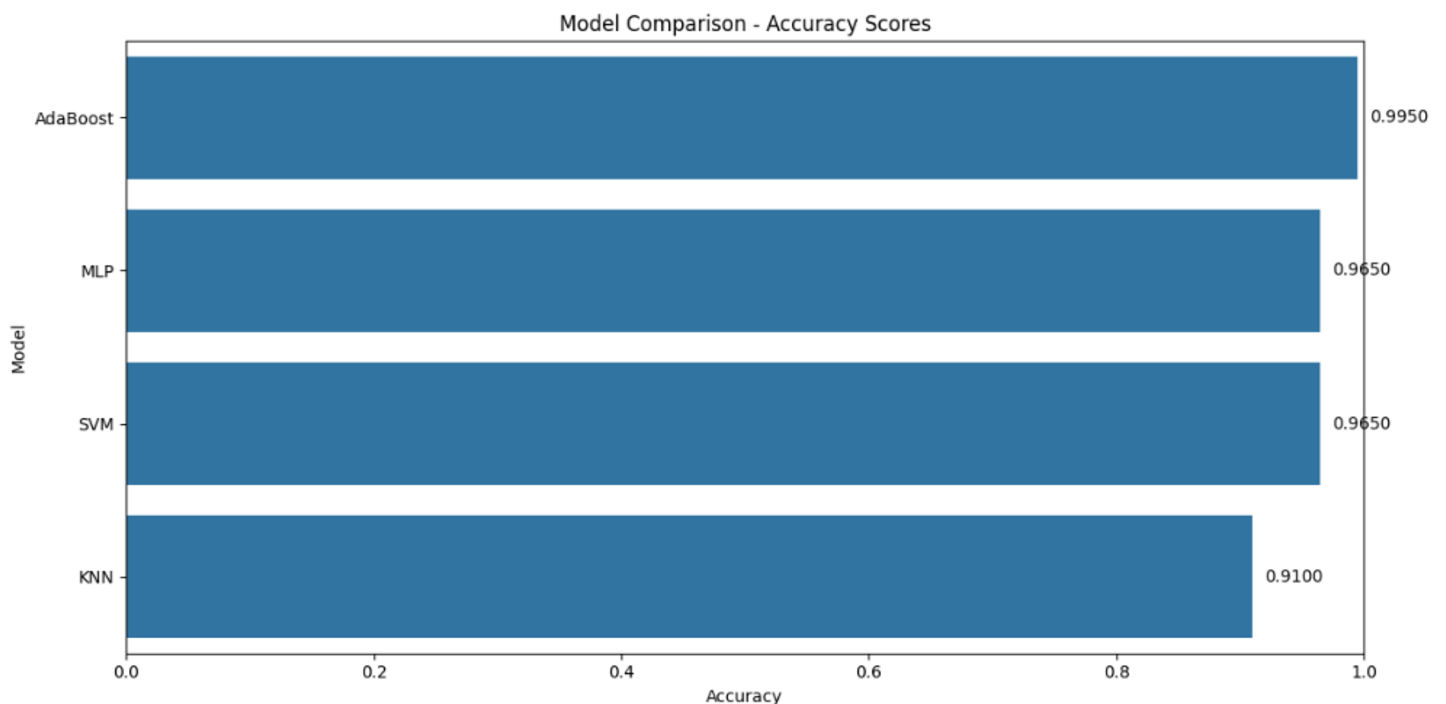
The comparative analysis demonstrates the AdaBoost model’s superiority over alternative approaches, achieving 99.5% accuracy compared to 96.5% for SVM and MLP models. Beyond prediction performance, BSC provides distinct advantages over other blockchain platforms: its \$0.10 average transaction cost is 50–100× lower than Ethereum’s \$5–\$10 range, while maintaining 3-s confirmation times vs Ethereum’s 13–15 s. Although Hyperledger Fabric offers higher throughput (1000+ TPS vs. BSC’s 100 TPS), its permissioned nature limits suitability for public health applications. This balance of low

Table 5 Comparison with different models.

Model	Accuracy	Precision	Recall	F1-score
MLP	96.5 (%)	0.82	0.63	0.71
SVM	96.5 (%)	0.84	0.94	0.89
KNN	91.0 (%)	0.89	0.91	0.91
AdaBoost	99.5	0.99	0.96	0.98

Note:

Since AdaBoost algorithm is used in the proposed methodology because of its highest performance, it is highlighted in bold. This is to mention that AdaBoost is utilized in the proposed work which stands as best fit model.


Figure 16 Comparative analysis with different models.

[Full-size !\[\]\(e474458956c9a37fbf9586ddb60a7fa1_img.jpg\) DOI: 10.7717/peerj-cs.3123/fig-16](https://doi.org/10.7717/peerj-cs.3123/fig-16)

cost, developer-friendly EVM compatibility, and public accessibility makes BSC ideal for decentralized blood supply chains.

This study aimed to develop an intelligent and secure blood supply chain management system by integrating the AdaBoost machine learning algorithm with a blockchain-based infrastructure. The rationale behind this integration is to overcome key limitations of traditional systems, such as low accuracy in predicting donor and blood bank availability, and the absence of secure, transparent data handling. Existing centralized systems are often prone to data tampering and lack the intelligence needed for real-time decision-making. The proposed system addresses these gaps by using the AdaBoost algorithm off-chain to provide high-accuracy predictions for locating the nearest eligible donors and available blood banks, outperforming conventional models like SVM, KNN, and MLP in terms of both accuracy and speed. Simultaneously, the blockchain layer is deployed on the Binance

Smart Chain, ensuring immutable and verifiable records of all supply chain events, from donor registration to blood unit tracking, using smart contracts. By combining predictive intelligence with decentralized trust, the proposed framework offers superior performance, enhanced transparency, and greater reliability compared to existing centralized or siloed approaches, thereby meeting the core research objectives effectively.

CONCLUSION AND FUTURE WORK

The blockchain system configured for blood supply chain management integrates nodes with different levels of access, thereby enhancing authorization mechanisms and ensuring secure handling of sensitive information. By configuring the Binance Coin (BNB) gas price through the Hardhat environment, the system avoids high transaction costs, as demonstrated in the experiments. The integration of the AdaBoost algorithm achieves a 99.5% prediction accuracy, significantly enhancing user experience by efficiently identifying suitable donors and blood banks. The use of BscScan validates the reliability of public blockchain operations, while essential security features such as immutability *via* access control, confidentiality, integrity of records, and non-repudiation through distributed ledgers strengthen the trustworthiness of the system.

In contrast to traditional centralized systems that are often prone to data tampering, single-point failures, and limited transparency, our system offers decentralized trust, traceability, and predictive intelligence. The comparative analysis demonstrates significant advantages: AdaBoost outperforms alternative models (SVM, KNN, MLP) by 3–8.5% in accuracy, while Binance Smart Chain reduces transaction costs 50–100x compared to Ethereum. However, limitations including potential integration challenges with existing healthcare infrastructure (particularly regarding HL7/FHIR interoperability and HIPAA/GDPR compliance), dependency on public blockchain gas fees during network congestion, and limited deployment across diverse geographic regions need to be addressed in future iterations.

From a practical perspective, deploying such a system in real-world healthcare environments presents several benefits, including increased transparency, improved traceability, and faster, data-driven decisions. However, challenges may arise, such as integrating with legacy hospital systems, complying with healthcare data privacy regulations, managing blockchain scalability, and ensuring affordability of gas fees under high-volume transactions. Although the current system is built on a public blockchain, future adaptations may consider private or consortium blockchains for enhanced data safety and interoperability. Specific infrastructure compatibility solutions will include developing standardized API gateways and hybrid architectures that maintain backward compatibility with existing hospital systems.

In addition, scalability studies using more advanced machine learning models will be undertaken to optimize performance further. Future work will specifically address current limitations through: (1) multi-institutional trials across diverse healthcare ecosystems, (2) implementation of Layer-2 scaling solutions for gas optimization, (3) expansion of training datasets *via* partnerships with national blood networks, and (4) smart contract modularization for regulatory adaptation across jurisdictions. This work lays the

foundation for a scalable, secure, and intelligent blood supply chain management system, with promising implications for broader healthcare applications, including secure e-blood donation platforms and digital payment integration.

ABBREVIATIONS

The following Table 6 lists the abbreviations used in this manuscript:

Table 6 Nomenclature.

Acronym	Description
CP	Collection point
MC	Medical centre
TS	Transporter
DR	Donor
RC	Recipient
E	Entities = {CP, MC, TS}
PKE	Public key of E $\{\forall E \text{ in Entities}\}$
PRE	Private key of E $\{\forall E \text{ in Entities}\}$
PKOwner, PROwner	Public key and Private key of NACO
PKDR, PRDR	Public key and Private key of Donor
MM	Metamask
ADE, PWE	Wallet address and Password of E $\{\forall E \text{ in Entities}\}$
IDCP, IDMC, IDDR	Unique ID of CP, MC, and DR
N	Number of blood units
BG	Blood group
DRInfo	Personal information of DR
ADRC	Wallet address of recipient
BGRC	Blood group of recipient
HIV	HIV test
LIV	Liver fever test
BP	Blood pressure
HB	Hemoglobin
LATUser, LONUser	Latitude and longitude of the user
LATBB, LONBB	Latitude and longitude of the blood bank
$\equiv$	Identical
(Condition): $x ? y$	If condition is true then return x else y

DATA SOURCE

The dataset was compiled using information sourced from the official e-RaktKosh platform of the Ministry of Health and FamilyWelfare, Government of India: <https://eraktkosh.mohfw.gov.in/BLDAHIMS/bloodbank/transactions/bbpublicindex.html>. The dataset has been curated and published with an assigned DOI via the Zenodo repository: <https://doi.org/10.5281/zenodo.15667720>.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

This work was supported by Research Institute Supporting Program (RICSP-25-2), King Saud University, Riyadh, Saudi Arabia. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Grant Disclosures

The following grant information was disclosed by the authors:

Research Institute Supporting Program (RICSP-25-2), King Saud University, Riyadh, Saudi Arabia.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Rupa Ch conceived and designed the experiments, performed the experiments, authored or reviewed drafts of the article, and approved the final draft.
- Sai Varshitha G. conceived and designed the experiments, performed the experiments, prepared figures and/or tables, and approved the final draft.
- Divya D. conceived and designed the experiments, performed the experiments, prepared figures and/or tables, and approved the final draft.
- Thippa Reddy Gadekallu analyzed the data, authored or reviewed drafts of the article, and approved the final draft.
- Mustufa Haider Abidi analyzed the data, performed the computation work, authored or reviewed drafts of the article, and approved the final draft.
- Fahad Alasim performed the computation work, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

Raw data is available at: <https://eraktkosh.mohfw.gov.in/BLDAHIMS/bloodbank/transactions/bbpublicindex.html>

Data is also available at Zenodo:

Gondela, S. V., Durgempudi, D., & Dr Chiramdasu, R. (2025). Blood bank dataset [Data set]. Zenodo. <https://doi.org/10.5281/zenodo.15667720>.

Supplemental Information

Supplemental information for this article can be found online at <http://dx.doi.org/10.7717/peerj-cs.3123#supplemental-information>.

REFERENCES

- Abdullah CM, Kamal M, Shaiara F, Kamal ARM, Hossain MA. 2022. BloodComm: a peer-to-peer blockchain-based community for blood donation network. In: *2022 25th International Conference on Computer and Information Technology (ICCIT)*, 218–223.

- Al-Farsi S, Rathore MM, Bakiras S. 2021. Security of blockchain-based supply chain management systems: challenges and opportunities. *Applied Sciences* 11(12):5585 DOI 10.3390/app11125585.
- AltcoinsBox. 2025. Binance smart chain testnet logo. Available at <https://altcoinsbox.com/wp-content/uploads/2023/01/bnb-chain-binance-smart-chain-logo.jpg> (accessed 27 April 2025).
- Ben Elmir W, Hemmak A, Senouci B. 2023. Smart platform for data blood bank management: forecasting demand in blood supply chain using machine learning. *Information* 14(1):31 DOI 10.3390/info14010031.
- Bing. 2025a. Bscan api gateway image. Available at <https://tse3.mm.bing.net/th?id=OIP.35RX7Fv-M1gvrO-sojpFagHaFj&pid=Api&P=0&h=180> (accessed 27 April 2025).
- Bing. 2025b. Blockchain data storage image. Available at https://tse2.mm.bing.net/th?id=OIP.r7KjL_GhK8vhDoTl2CktzQHaHa&pid=Api&P=0&w=300&h=300 (accessed 27 April 2025).
- Bing. 2025c. Blockchain image. Available at <https://tse4.mm.bing.net/th?id=OIP.9WaVvFzkDrYVtOt8BIgLvWHaEN&pid=Api&P=0&h=180> (accessed 27 April 2025).
- Bing. 2025d. Database image. Available at https://tse2.mm.bing.net/th?id=OIP.r7KjL_GhK8vhDoTl2CktzQHaHa&pid=Api&P=0&w=300&h=300 (accessed 27 April 2025).
- Blockchains. 2025. Hardhat framework image. Available at <https://101blockchains.com/wp-content/uploads/2022/08/hardhat-1-300x300.png> (accessed 27 April 2025).
- Choudhury B, Dewri N, Das P, Nag A. 2021. Blockchain-IoT based blood supply chain management system. In: *International Conference on Network Security and Blockchain Technology*. Singapore: Springer Nature Singapore, 356–368.
- Eghtesadifard M, Jozan F. 2022. A systematic literature review on the blood supply chain: exploring the trend and future research directions. *Journal of Ambient Intelligence and Humanized Computing* 13(2):1173–1200 DOI 10.1007/s12652-021-03563-5.
- Ekanayake OAS, Halgamuge MN. 2021. Lightweight blockchain framework using enhanced master-slave blockchain paradigm: fair rewarding mechanism using reward accuracy model. *Information Processing & Management* 58(3):102523 DOI 10.1016/j.ipm.2021.102523.
- Emmanuel G, Ramadhan A, Zarlis M, Abdurachman E, Trisetyarso A. 2023. Machine learning in drug supply chain management during disease outbreaks: a systematic review. *International Journal of Electrical & Computer Engineering* 13(5):5517–5533 DOI 10.11591/ijece.v13i5.pp5517-5533.
- Fiore M, Capodici A, Rucci P, Bianconi A, Longo G, Ricci M, Sanmarchi F, Golinelli D. 2023. Blockchain for the healthcare supply chain: a systematic literature review. *Applied Sciences* 13(2):686 DOI 10.3390/app13020686.
- Flaticon. 2025. Blood collection point icon. Available at https://www.flaticon.com/free-icon/blood-bank_4265085 (accessed 27 April 2025).
- Ghadge A, Bourlakis M, Kamble S, Seuring S. 2022. Blockchain implementation in pharmaceutical supply chains: a review and conceptual framework. *International Journal of Production Research* 61(19):6633–6651 DOI 10.1080/00207543.2022.2125595.
- Gia KH, Huong HL, Phuc NT, Khoa TD, Khanh HV, Quy LT, Triet NM. 2023. A comprehensive system for managing blood resources leveraging blockchain, smart contracts, and non-fungible tokens. *International Journal of Advanced Computer Science and Applications* 14(10):959–969 DOI 10.14569/ijacsa.2023.01410101.
- Google. 2025a. Blood donation icon. Available at <https://images.app.goo.gl/WQZ5BqZ5pQrnW7sD8> (accessed 27 April 2025).
- Google. 2025b. Blood donor icon. Available at <https://images.app.goo.gl/vsbW15ehpfpSGBtn7> (accessed 27 April 2025).

- Google. 2025c.** Blood units icon. Available at <https://images.app.goo.gl/T6ywF8LxNWbSqQzx7> (accessed 27 April 2025).
- Google. 2025e.** Distributed ledger icon. Available at <https://images.app.goo.gl/AtSUxdzuf1hnoxg79> (accessed 27 April 2025).
- Google. 2025d.** Collection point icon. Available at <https://images.app.goo.gl/2CqnsArpR2M49Ra88> (accessed 27 April 2025).
- Google. 2025f.** Donor information icon. Available at <https://images.app.goo.gl/6DW4cXLAcP2LQ4tU6> (accessed 27 April 2025).
- Google. 2025g.** Main image icon. Available at <https://images.app.goo.gl/9F2aoYniwtxEpUkh8> (accessed 27 April 2025).
- Google. 2025h.** Medical center icon. Available at <https://images.app.goo.gl/XfLtJhwtN1qJMWaMA> (accessed 27 April 2025).
- Google. 2025i.** Medical center image. Available at <https://images.app.goo.gl/yihvmdTnfwRXWpn87> (accessed 27 April 2025).
- Google. 2025j.** Smart contracts image. Available at <https://images.app.goo.gl/xW4LVfVEZWudUY8r8> (accessed 27 April 2025).
- Google. 2025k.** Transportation icon. Available at <https://images.app.goo.gl/RBPSgMM6m4wQWDTj8> (accessed 27 April 2025).
- Google. 2025l.** Transportation image. Available at <https://images.app.goo.gl/o9y65s7hZSLyViqi6> (accessed 27 April 2025).
- Google. 2025m.** Units received icon. Available at <https://images.app.goo.gl/6DW4cXLAcP2LQ4tU6> (accessed 27 April 2025).
- Google. 2025n.** User icon. Available at <https://images.app.goo.gl/vsbW15ehpfpsGBtn7> (accessed 27 April 2025).
- Hawashin D, Mahboobeh DAJ, Salah K, Jayaraman R, Yaqoob I, Debe M, Ellahham S. 2021.** Blockchain-based management of blood donation. *IEEE Access* **9**:163016–163032 DOI 10.1109/access.2021.3133953.
- Hawashin D, Mahboobeh DAJ, Salah K, Jayaraman R, Yaqoob I, Debe M, Ellahham S. 2022.** Blockchain-based management of blood donation. *IEEE Access* **9**:163016–163032 DOI 10.1109/access.2021.3133953.
- Imamoglu G, Topcu YI, Aydin N. 2023.** A systematic literature review of the blood supply chain through bibliometric analysis and taxonomy. *Systems* **11**(3):124 DOI 10.3390/systems11030124.
- Jabbar S, Lloyd H, Hammoudeh M, Adebisi B, Raza U. 2021.** Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia Systems* **27**(4):787–806 DOI 10.1007/s00530-020-00687-0.
- Khalid MI, Ehsan I, Al-Ani AK, Iqbal J, Hussain S, Ullah SS. 2023.** A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access* **11**:10995–11015 DOI 10.1109/ACCESS.2023.3240237.
- Kim S, Kim J, Kim D. 2020.** Implementation of a blood cold chain system using blockchain technology. *Applied Sciences* **10**(9):3330 DOI 10.3390/app10093330.
- Kumar A, Chatterjee I, Pallavi, Sharma K, Thakur M. 2024.** Real-time-based blood wastage management using iot and blockchain technology. *SN Computer Science* **5**(3):310 DOI 10.1007/s42979-024-02613-x.
- Kumaran N, Mohan JSS. 2023.** BRDO: blockchain assisted intrusion detection using optimized deep stacked network. *Cybernetics and Systems* **55**(8):2071–2092 DOI 10.1080/01969722.2023.2175153.

- Le HT, Nguyen TTL, Nguyen TA, Ha XS, Duong-Trung N. 2022. Bloodchain: a blood donation network managed by blockchain technologies. *Network* 2(1):21–35 DOI 10.3390/network2010002.
- Mandal S, Massand H, Kamboj S, Kaur S. 2023. Decentralized blood bank management system. In: *Proceedings of the KILBY 100 7th International Conference on Computing Sciences*, 1–6 DOI 10.2139/ssrn.4489012.
- Manolache MA, Manolache S, Tapus N. 2022. Decision making using the blockchain proof of authority consensus. *Procedia Computer Science* 199:580–588 DOI 10.1016/j.procs.2022.01.071.
- Maroun EA, Daniel J, Fynes B. 2019. Adoption of blockchain technology in supply chain transparency: Australian manufacturer case study. In: *Proceedings of the 10th European Decision Sciences Institute (EDSI)*.
- Ministry of Health and Family Welfare, Government of India. 2016. e-raktkosh: about blood bank management information system. Available at <https://eraktkosh.com/> (accessed 10 January 2025).
- Ministry of Health and Family Welfare, Government of India. 2025. Dataset from e-raktkosh blood bank transactions. Zenodo. DOI 10.5281/zenodo.15667720.
- Musamih A, Salah K, Jayaraman R, Arshad J, Debe M, Al-Hammadi Y, Ellahham S. 2021. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* 9:9728–9743 DOI 10.1109/access.2021.3049920.
- Nazir T, Ahmed RH, Hussain M, Zahid S. 2023. Transforming blood donation processes with blockchain and IoT integration: a augmented approach to secure and efficient healthcare practices. In: *2023 International Conference on IT and Industrial Technologies (ICIT)*. Chiniot, Pakistan, 1–8 DOI 10.1109/ICIT59216.2023.10335787.
- Ramakrishna MT, Venkatesan VK, Izonin I, Havryliuk M, Bhat CR. 2023. Homogeneous adaboost ensemble machine learning algorithms with reduced entropy on balanced data. *Entropy* 25(2):245 DOI 10.3390/e25020245.
- Rekha H, Siddappa M. 2023. Blockchain mechanism-based attack detection in IoT with hybrid classification and proposed feature selection. *Cybernetics and Systems* 56(3):1–26 DOI 10.1080/01969722.2023.2166266.
- Roorkhosh P, Pooya A, Agarwal R. 2023. Blockchain acceptance rate prediction in the resilient supply chain with hybrid system dynamics and machine learning approach. *Operations Management Research* 16(2):705–725 DOI 10.1007/s12063-022-00336-x.
- Rupa C, Varshitha GS, Divya D, Gadekallu TR, Piran MJ. 2025. Blockchain-based dapp for drug supply chain with AI-driven drug recommender system. In: *IEEE Consumer Electronics Magazine*, 1–6 DOI 10.1109/mce.2025.3536326.
- Subramanian N. 2024. An optimal modified bidirectional generative adversarial network for security authentication in cloud environment. *Cybernetics and Systems* 158:1–33 DOI 10.1080/01969722.2024.2343988.
- Trong NP, Vo HK, Huong LH, Gia KH, Dang KT, Quoc DNT, Khanh BL, Tuan KL. 2022. Blood and product-chain: blood and its products supply chain management based on blockchain approach. *International Journal of Advanced Computer Science and Applications* 13(11):743–750 DOI 10.14569/ijacsa.2022.0131186.
- Vo HK, Tran BQ, Doan HM, Le KT, Trong ND, Le HV, Phu LV. 2023. Blood and blood products management system based on blockchain, and NFT technologies. In: *International Conference on Database Systems for Advanced Applications*. Cham: Springer Nature Switzerland.
- Younis M, Lalouani W, Lasla N, Emokpae L, Abdallah M. 2021. Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access. *IEEE Systems Journal* 16(3):3746–3757 DOI 10.1109/jsyst.2021.3092519.