Hindawi
Complexity
Volume 2022, Article ID 6758912, 11 pages
https://doi.org/10.1155/2022/6758912

Research Article

Blockchain-Based Contact Tracing and Information Sharing Model for COVID-19 Pandemic

Arwa Mashat and Aliaa M. Alabdali

Faculty of Computing & Information Technology, King Abdulaziz University, P.O. Box 344, Rabigh 21911, Saudi Arabia

Correspondence should be addressed to Aliaa M. Alabdali; amalabdali@kau.edu.sa

Received 19 March 2022; Accepted 29 April 2022; Published 7 June 2022

Academic Editor: Muhammad Ahmad

COVID-19 is the worst contagious disaster in the history of humankind, triggering a worldwide sickness pandemic. In lacking specialized treatments or immunizations, finding and eliminating the infection source is the best option to decrease disease transmission and lower sickness and degree of fatality among the general public. Generally, few significant barriers are present in the existing system of monitoring the contamination. One of the obstacles is regarding health-related data storage. The user's e-health data is kept in a traditional method that might have been compromised if shared with third parties. Secondly, the current disease tracking technologies fail to monitor diseases numerous ways. The tracing system is either personal or location-based. Apart from these, gathering individual consent and sharing their health data with unknown associations is a real-time problem. We propose a blockchain-based data system that maintains confidentiality with transparency. Users can acquire unlimited and nontampered vital routes as the suggested blockchain solution leverages to link the user/patient and approved solvers. Also, automatically executed smart contracts are constructed to desensitize the user ID and reallocation. The anonymous feature delivered by private blockchain with wireless technologies defends the customer's identity secrecy. We develop a matching approach using machine learning technology. Users may take safeguards in advance by employing our suggested analytical technique for predicting the risk due to infectious source presence.

1. Introduction

A new infirmity is known as COVID-19, and its variations are wreaking havoc throughout the globe. It was first originated in the Chinese Wuhan City in the province of Hubei. The virus's enormous proliferation has posed several obstacles, causing the foundations of human civilization to quiver. COVID-19 has infected about 11.5 million individuals and killed almost 529,090 people too far. South-East, in particular, has surpassed the United States as the country with the most known illnesses. Each country has its privacy policies to communicate information about sick patients [1–3]. Because various nations have their privacy policies for sharing the information of infected persons, sharing information across the world with reliable privacy protection is challenging. Users typically have slight control over the possible exploitation of personal data once uploaded to the cloud [4, 5]. If a comprehensive data security solution is not in place, the cloud's private user data might be stolen for any number of malicious objectives [6]. The Globe Health Institution (WHO), a worldwide organization, engages with governments to share information and improve epidemic preventive strategy. However, some nations are losing faith in WHO, and the organization cannot get sufficient funding. Other authorities may withhold, incorrectly report, or prevent pandemic data from being reported. For worldwide pandemic prevention, this might result in a considerable security weakness. As a result, not a single system is present to share their personal details or data while protecting their confidentiality. Administration departments and governments may have availed to all people's health medical data, which is outside their area of authority and obligation. Some public healthcare offices, for example, may track down sick people's personal information and keep it in a conventional

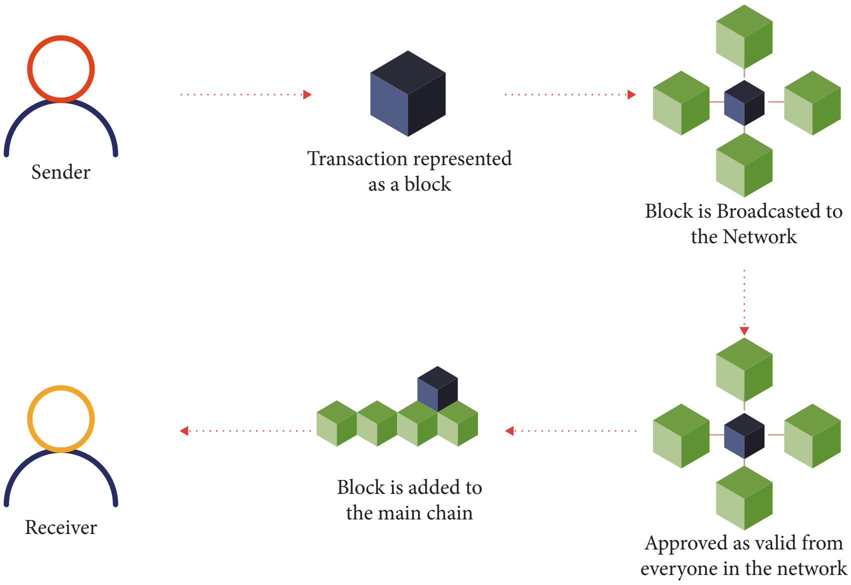

Sender
Transaction represented as a block
Block is Broadcasted to the Network
Approved as valid from everyone in the network
Block is added to the main chain
Receiver

Figure 1: The basic structure of blockchain network.

isolation place, so this process actually helps to increase secondary contaminations and limits delicate liberty [7]. Several large tech companies will release the info of infected persons with health authorities, implying that users' data confidentiality and HR (human rights) will be infringed without their awareness [7, 8].

There are presently two types of contact tracking systems available: location-based and individual-based contact tracking. Without knowing about infection migration, position-based contact tracking always offers a conversational service and data contaminations in specified places. Individual-based tracing solutions are solely concerned with person-to-person Bluetooth interaction and do not track where users become infected. According to the WHO, the virus may persist on various surfaces. Therefore, it impacts people's daily activities [9]. On the other hand, the identification method cannot track and quantify the COVID-19 effect at a specific place [10].

Blockchain could equip a decentralized solution for sharing information and protecting confidentiality right out of the box. Each computer node may bundle user data into transactions and store it on the blockchain. Even if one node's data is tampered with, it will not affect its integrity since the tampered info will fail to pass validated by existing blocks. A smart contract is a blockchain-based application that can execute instructions distributed while maintaining output consistency. Current viral monitoring service solutions examine infection transmission variables that are too simplistic. Figure 1 shows the basic structure of blockchain network.

The key features of blockchain are as follows:

(1) Efficiency: a blockchain is simple to use and it can stalk large amounts of information. Moreover, it can bypass any complicated system.

(2) Transparency: because it shares resource information with all connected mobile devices, a blockchain automatically opens all resource status and consumption data. This analysis looked at specific mobile devices' exclusive use of resources and infrastructure.

(3) Security: the security of a blockchain is superior to that of centralized data handling. Intruder invasions have the potential to do catastrophic damage to centralized data management. Giving misleading results is nearly tricky with a blockchain. It would need simultaneous control of all portable devices on which the data is disseminated, followed by a change to the data recorded in the machines.

1.1. Problem Definition. Because the epidemic had such a negative impact on Saudi Arabia's economy, it is necessary to decrease the pandemic's ramifications and restore it to normalcy. The primary guideline for probable illness outbreak prevention is a set of limits and confinements. Many Android-based applications have been developed to remind people of these limits to stay healthy [11–13]. Everyone should follow the health professionals' safety recommendations; yet, these are insufficient in any public gathering. The main motivations are mentioned as follows:

(i) There is a growing demand for accurate and updated real-time COVID-19 tracking and prevention-based solutions. Daily updates, visiting locations monitoring, physical symptoms screening (to use a question-and-answer technique), report uploading, and other features are available in multitasking programs.

(ii) As a result, present Android-based applications lack data security and dependability, consume more bandwidth, and result in requests overlapping in public locations, making them unable to meet the

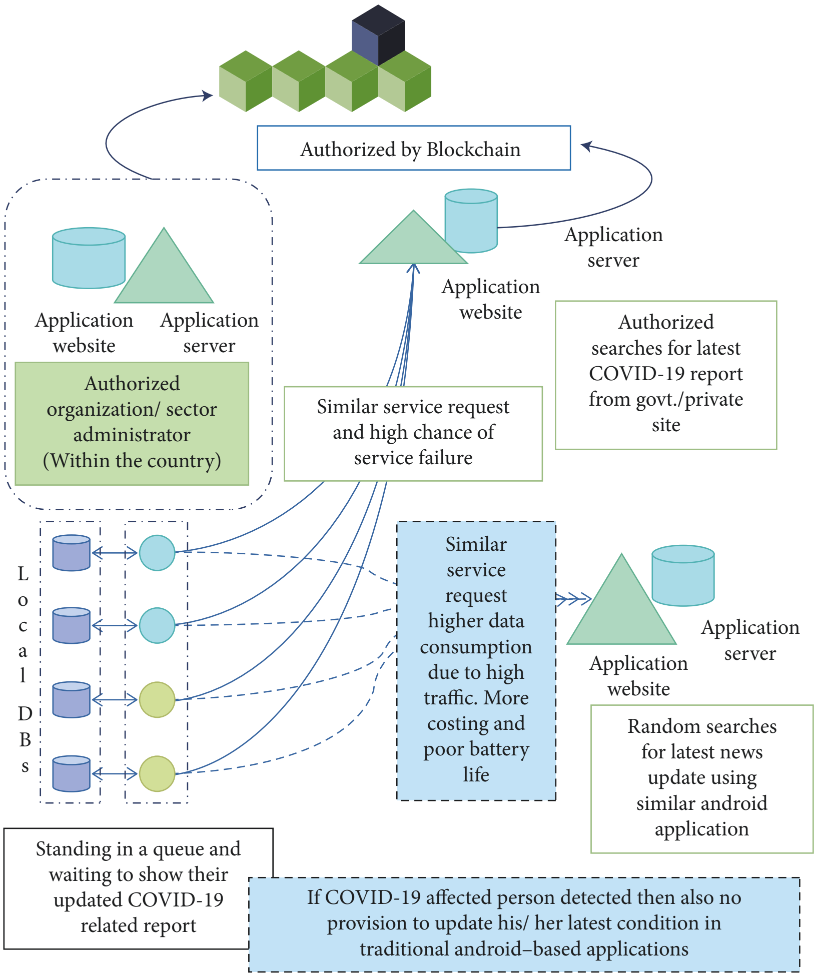

Authorized by Blockchain
Application website
Application server
Authorized organization/ sector administrator (Within the country)
Application server
Application website
Authorized searches for latest COVID-19 report from govt./private site
Similar service request and high chance of service failure
L o c a l D B s
Similar service request higher data consumption due to high traffic. More costing and poor battery life
Application website
Application server
Random searches for latest news update using similar android application
Standing in a queue and waiting to show their updated COVID-19 related report
If COVID-19 affected person detected then also no provision to update his/ her latest condition in traditional android–based applications

Figure 2: Request for in-country service avail.

extra quality of service (QoS) criteria [14]. We focused on two contemporary instances: admission into public meetings by people and customs checks.

(iii) Case 1: Figure 1 was added to the mix. Waiting in line to display their updated COVID-19 linked report, this gathering can expose people to infectious illnesses more seriously. An Android application was created to prevent this, although it has some security flaws. As a result, service failure is more likely when people in the queue/group make similar service requests. Due to increasing traffic, similar service requests can result in higher data usage. As a result, there is an increase in cost and a decrease in battery life. Figure 2 shows request for in-country service avail.

In this situation, the affiliations to which the user wishes to get access and the report supplier authorization/administrator each have their application website and application server (within the same country). As a result, we may delegate soul authority to a particular association/sector to scan every incomer, validate their provided report/information via direct access to that administrative website, and update the individual's most recent health clearance without requiring any human interaction. Hemayah provides this precise digital platform, which aids in the reduction of paper printed copy transfer during social assemblies.

(ii) Case 2: it is expanded into Figure 3 (request for outside-country service avail) waiting in line to show their updated COVID-19-related report in a country checkpoint after arriving from another country.

For storing and verifying proposals, a centralized system is also employed. As a result, there is a risk of data privacy, as data can be altered with or hacked. KSA is the authorized institution administrator. To monitor COVID-19, we also require a blockchain-based contactless notification system. The cloud is used to back up all of your data.

The major contributions are as follows:

(1) A blockchain-based decentralized system is proposed to get a better and contactless notification for COVID-19 contamination.

(2) A secure system order is used for escalation customer confidentiality, safety, and clearness.

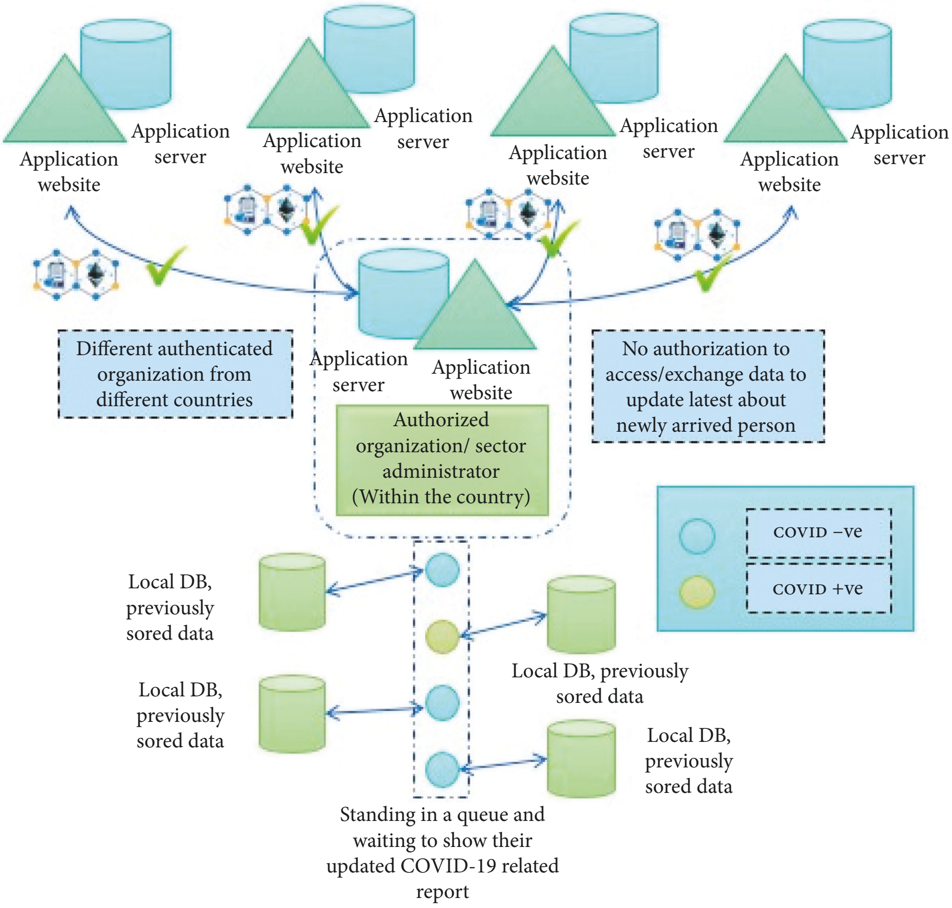

Application server
Application website
Application server
Application website
Application server
Application website
Application server
Application website
Different authenticated organization from different countries
Application server
Application website
Authorized organization/ sector administrator (Within the country)
No authorization to access/exchange data to update latest about newly arrived person
COVID –ve
COVID +ve
Local DB, previously sored data
Local DB, previously sored data
Local DB, previously sored data
Local DB, previously sored data
Standing in a queue and waiting to show their updated COVID-19 related report

Figure 3: Request for outside-country service avail.

(3) Encryption and decryption methods were also incorporated to generate both key pairs.

(4) Bluetooth is used for connecting one user to another user and generating a spontaneous and speed notification system.

1.2. Organization of Paper. The roadmap of this paper is mentioned in this section. Section 2 defines the background study of this present context. Section 3 formulizes our proposed system. Section 4 represents the simulation process along with evaluating scheme performance or outcome. Section 5 presents the result and discussion for this work. The last part of our work represents the conclusion for this paper

2. Related Work

MIT, Apple, and Google all have contact tracing-related products and initiatives. On the other hand, their remedies are either a centralized database incorporated into the system or insufficient data confidentiality for consumers. Such designs are unable to fulfill the demands of user privacy [15]. The smart contract ensures that operations are carried out consistently and that a consistent result is obtained in terms of data security. One study describes a trading platform for computer resources based on a smart contract-based edge computing network. This approach employs a tree-structured smart contract group similar to ours. However, their implementation focuses on matching users and completing resource trade. The goal of smart contracts, on the other hand, is to keep track of the infection state of sites. Some existing research uses differential privacy (DP) and completed their work [16]. Several publications employ DP algorithms on the Internet of Technology facts managing; however, DP approaches will yield a pretty precise outcome with impurity in it. This feature will not go to work with the property of decentralized technology like blockchain [17, 18]. While keeping information, the subsequent node should test the integrity of the preceding block's contents and cannot accept variances [19–21]. However, exploring how these two topics cross in the study might be fascinating. Table 1 represents a comparative analysis of different verification approaches with their advantages and disadvantages. Table 2 represents a descriptive discussion of decentralized blockchain approaches with their advantages and disadvantages.

Proposed technology can trace users' visits to other venues and their personal experiences with each other. When a user comes to know about the contaminated report, the proposed system will notify another person not to come in the major contacts either directly or indirectly and offer

Table 1: Verification approaches with their features.

Verification approaches	Benefit	Starfish
Fingerprint-based verification	More secure than other approaches and highly convincing	High-cost and difficult to implement and manage
Verification using hardware or software	More secure than the verification process using data or information	High threat of compromising sensitive data, entire data will be lost, one's terminal mislaid
Verification using information	Nominal cost with limited resources	Centralized control, prone to vulnerability
Others	Mantation higher safety, compact deception threat	High-cost and difficult to implement and manage

Table 2: Benefit and disadvantage of decentralized System.

Parameter	Benefit	Disadvantage
Within decentralize network	Immutability	High cost
	Clearness	Making possible forks
	Privacy	Complicated
	Trestles environment	Respectively slow
Database	Distributed	No centralized control

important information for the same. Lastly, the system tries to recognize that person who may contact unknowingly and get contaminated.

2.1. End-to-End Tracking. Contacting trustworthy persons while using wireless technology can be possible in proposed smartphone-based method, which also uploads personal details to distributed, trustless blockchain systems. Wireless technology like Bluetooth can detect another present just approximately 4 to 8 meters. As a result, when the patient's smartphone receives Bluetooth signals, there are others around. When a person registers himself as contaminated, our system broadcasts their contamination situation to other customers, alerting them to their health condition; maybe they are in close interaction with this sick customer. Although viruses may adhere to water vapor and propagate via the aerosol, and users may be affected by other persons nearby, tracking the direct contact recorded by Bluetooth is critical. As a result, submitting customers' connection records will assist them in tracking the virus's invasion route and determining the likelihood of acquisition. Figure 4 represents the user logs on details to the corresponding site and records information in the blockchain database.

3. Health Tracing Service

3.1. Inflammation Possibility. As per WTO medical staff manual, healthy people can be infected both intrinsically and extrinsically, with the direct interaction being close person-to-person contact and the indirect interaction. The infection persisting on the object's external spreads the patient infecting healthy individuals after reaching the surface. As a result, the computer would assess the participant based on feature data collected from geographical tracking and individual contact tracings, such as the duration of interaction time among patients, the distance between patients, and the items in public spaces' risk from these aspects.

3.2. Infection Notice. After calculating the likelihood of contamination for this patient, the alerting function refers him a warning notification message, reminding him to either prepare for disease ahead of time or seek medical care before his health condition worsens. Whenever a client claims that they are contaminated, the proposed framework will publish their simulated individuality to other clients. The customers who get the warning notification can ask the native database to determine whether they have an infection or not by contacting directly or indirectly with the sick person, and the transmission risk will be calculated.

3.3. Tracing User Visited Locations. In a typical case, the customer may frequently meet numerous people in public locations in a single day, like workplaces, cafeterias, malls, or clubs; thus she may utilize the provided interaction tracking facility to upload her staying data, which she wants to include. Figure 4 shows the user logs on to the site and make the bunch of records and information in the blockchain-based database.

It informs our system about the time and place. The visitation data will be kept in the distributed blockchain system. Users may also verify the infection status before visiting to guarantee their protection. When a customer tested COVID-19 positive, a set of smart contracts incorporated in the proposed framework are responsible for updating the contamination condition of the spaces with modes of conveyance that the user visited or used, depending on their visit data.

4. Proposed Method

In this part, we have described and enlightened the proposed blockchain-based risk notification system with all components starting from the standpoint and different layers present in the system and the connections within it. Figure 5 defines the proposed blockchain-based architecture for contactless monitoring.

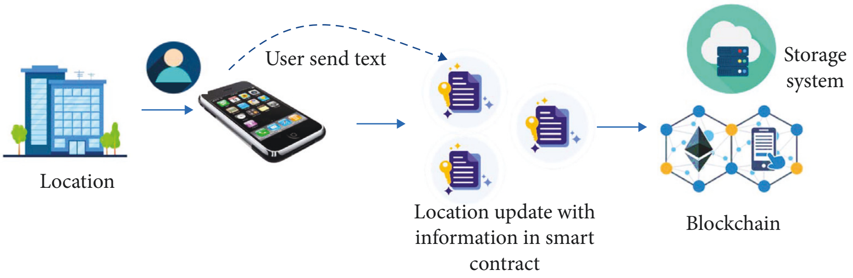


Figure 4: The user logs on to the site and records information in the blockchain database.

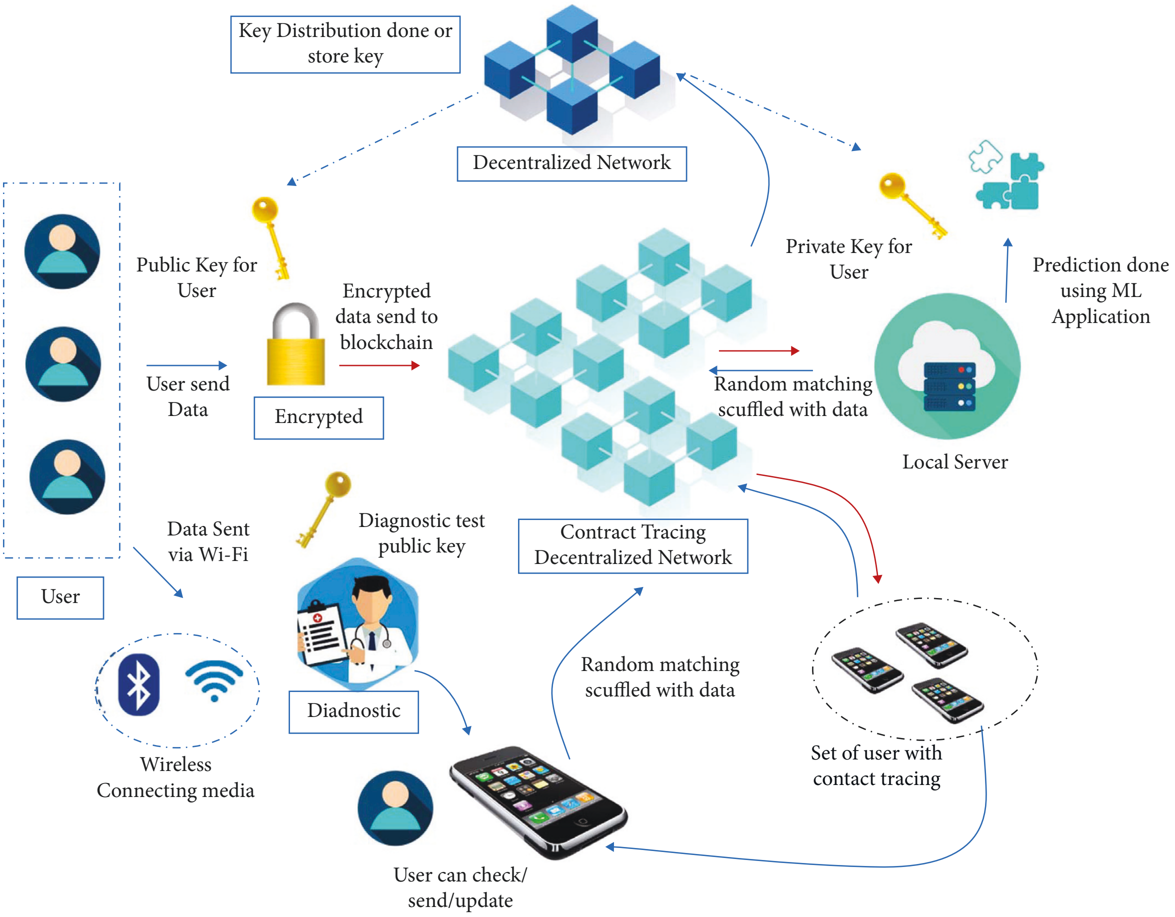

Key Distribution done or store key
Decentralized Network
Public Key for User
Private Key for User
Prediction done using ML Application
Encrypted data send to blockchain
User send Data
Encrypted
Random matching scuffled with data
Local Server
User
Data Sent via Wi-Fi
Diagnostic test public key
Contract Tracing Decentralized Network
Diadnostic
Random matching scuffled with data
Set of user with contact tracing
Wireless Connecting media
User can check/ send/update

Figure 5: Proposed blockchain-based architecture for contactless monitoring.

4.1. System Architecture. Users may utilize our four-layer trace and notification system to track individual Bluetooth connections, registration positions, also contamination question conditions with other patients on the applied decentralized platform. Figure 6 depicts different layers: patient communication layer, remote facility layer, service provided by SM layer, and record-keeping layer are the layers that make up the user interface. This system offers two main tracing and alerting services: Bluetooth-based individual contact tracking and position-based contact tracking. The data created by these two services are kept in distributed blockchain databases, and both services are built on the public blockchain. The smart contracts in the third tier coordinate the position-based contact tracking, while the wireless contact trace is handled by the next layer. Figure 6 represents the work flow diagram of proposed contactless monitoring.

4.2. Patient Communication Layer. Customer *C* and position *P* are both entities in the user interaction layer. Users are persons who have Bluetooth-enabled phones and fall into one of two categories of health: healthy or unhealthy. Both of you are infected; users who are not affected and those who are infected. In the second tier, users access cell phone services and update their health status regarding the medical

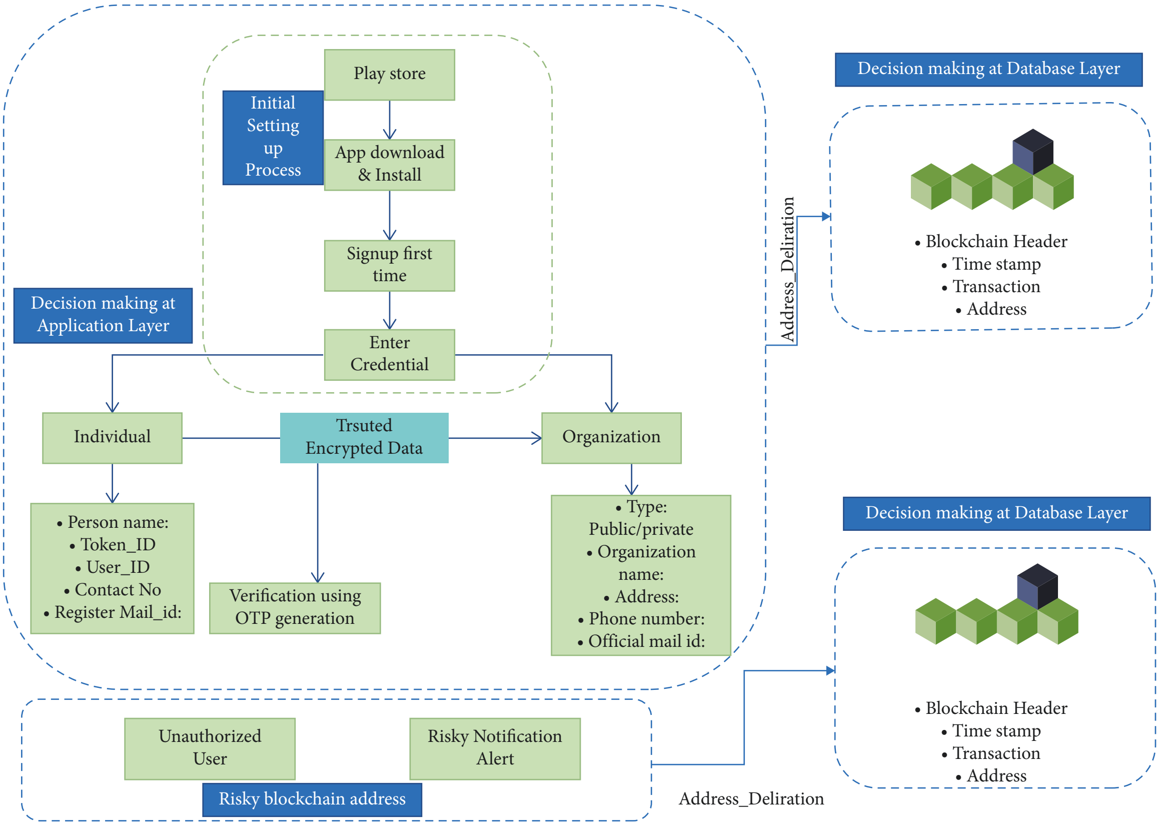


Figure 6: Proposed flow work for contactless monitoring.

assessments. We take it for granted that users constantly update our system with accurate information about their infection condition. A position P is a communal venue or mode of transport used by people in their everyday lives, such as workplaces, restaurants, stadiums, buses, and even aircraft. Uninfected position U_p normal and infected destination I_p infected are the two status kinds for position P. If this place P was visited by an infected user I_p infected, the system would record it as P contaminated.

4.3. Remote Facility Layer. Our system's primary handler, the mobile service Layer, communicates directly with the other three levels. In this layer, the remote facility Cell_p is our planned mobile phone application. The remote facility layer, in collaboration with different layers, such as an edge layer for delivering service to users, contains two major aspects: interaction tracking based on wireless or position and fitness tracking basis of information from the public blockchain.

4.4. Service Provided by SM Layer. Our system's second core is the smart contract service layer. The remote facility layer processes the check-in request rechecking created by the user visiting position P and forwards it to this smart contract facility layer, where the smart contract group manages it. The smart contract group ties contracts together based on the organizational structure scheme. The SM dedicated for the state level is SCont_state at the top of the hierarchy, followed through the county SCont_county Contract, the town SCont_city, and lastly, the minor unit location SCont_pos. $SCont\_city$ manages smart contracts based on location town contracts, SCont_county manages district contracts, and States SCont_state manages county-level contracts.

Every agreement or smart contract may only inherit from one superior contract, and it cannot be a part of two excellent contracts simultaneously. One of these three states must be present at each site: $\{E_{\text{status}}, Af_{\text{status}}, \text{Neg}_{\text{status}}\}$ and the smart contract that goes with it. Contract location dynamically records the infection status of position P. This place P is deemed infected by this customer C infected if an infected customer I_c infected visits it or if a user who has seen it reports that he is affected. The position P is regarded as a $\text{Neg}_{\text{status}}$ only if it has been cleansed or fourteen days after being contaminated. The subsequent requests will reduce the smart contract SCont_pos operation costs while maintaining the correctness of the position P status record. Requirements cause the smart contract SCont_pos to check and update the infection state of position P. Otherwise, the SM SCont_pos will not vigorously detect the contamination condition of position P. This approach guarantees that customers obtain the most up-to-date location status for their requests while eliminating smart contract activities.

4.5. Record-Keeping Layer. In the record-keeping layer, we have deployed a distributed blockchain database DB. Every customer and compute block in this system may be synced to

```
(1) Initiation for setup
(2) System setup for Mobile Application installation and get the credential
(3) Check Login credential working or not
(4) If yes
(a) .Then end
(5) Else repeat line 2
(6) Generate User_id_temp with geo location
(7) Apply for verification and validation
(8) Once validate users get User_id
(9) If get error
(a) Then apply line 8
(10) Update user device to the network
(11) Get device_pair_id ready to connect with others via Bluetooth
(12) User will broadcast User_id
(13) Users can connect multiple times but need to match a dd ress_i d
(14) Start Testing by Miner
(15 )req_sample from the user and identify COVID-19 in the lab
(16 )if,req_sample == POV
(a) Then
(b) reg_id user details and generate new id
(c) Key_pairs is generated by the applied method
(d) .Provide treatment by the health unit
(e) .Find any Local_match nearest to the user
(f) .Generate alert_warning and broadcast it to the author
(g) Update contaminated info blockchain
(17) Else declare re_sample == NOV
(a) Update user info into blockchain
(18) End
(19) Only Updated and users can access the data while using keys
(20) Gov. can only check the numbers of COVID tested req_sample == POV to confirm the user's confidentiality
```

Algorithm 1: Proposed blockchain-based secured data sharing algorithm.

Table 3: Overall comparison of existing work with proposed work.

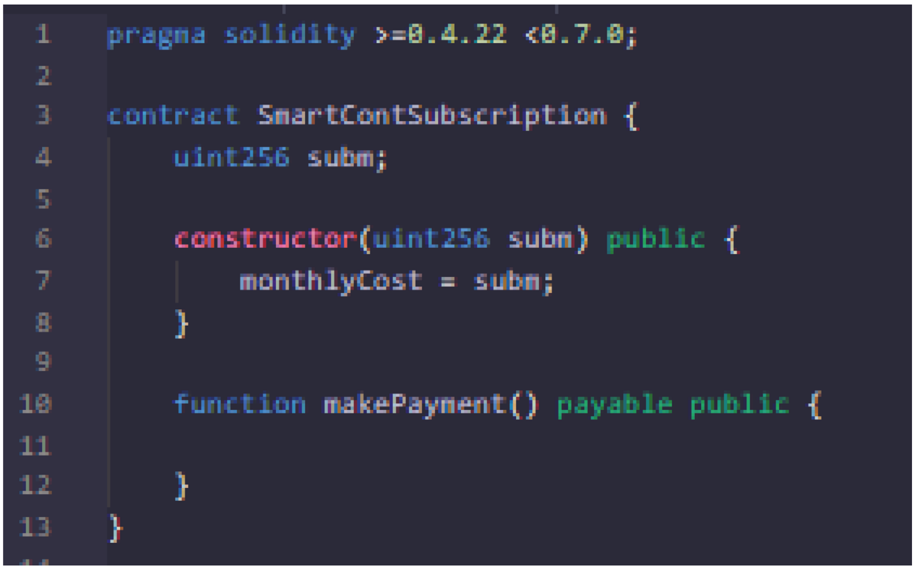
Paper name	Decentralized	Authentication of user	Data confidentiality	Availability	Tractability	Integrity
Azzaoui [3]	Yes	Yes	Yes	No	No	No
Sharma et al. [4]	Yes	Yes	No	No	No	Yes
Kim et al. [2]	Yes	Yes	Yes	No	No	Yes
Abouyoussef et al. [5]	Yes	No	Yes	No	No	No
Dhaliwal et al. [12]	No	No	Yes	Yes	No	No
Gupta et al. [18]	No	Yes	Yes	Yes	Yes	No
Proposed work	Yes	Yes	Yes	Yes	Yes	Yes

receive a comprehensive database consistent with all others. Typically centralized databases hold all data in a single data server center, whereas conventional distributed records store information in numerous data server centers; however, each storage system may not contain entire worldwide information. Database systems need an essential block to execute input and keep the output of operations in the database. In contrast, a blockchain-based database never requires a central module because all users may query the same database locally for consistency.

The blockchain database in our system will hold all transaction processing, such as customers' Bluetooth commerce data, registration info for the frequented position, and changes in the user's general medical status, except for position-based contact tracking, which requires SM to upload, update, and keep contamination report condition in the DB. For other services like tracking facilities, position-based contact tracking, wireless contact tracking, and e-health tracking facilities, customers can ask questions to the decentralized database unswervingly for private contacts and staying data.

5. Result Analysis

We create a working demo and test its work in the following tests, which employ the Poisson distribution equation to replicate users' daily contact and check-in actions. The average cost of submission requests and the overall cost of



```
pragma solidity >=0.4.22 <0.7.0;

contract SmartContSubscription {
    uint256 subm;

    constructor(uint256 subm) public {
        monthlyCost = subm;
    }

    function makePayment() payable public {

    }
}
```

Figure 7: Example of pragma.

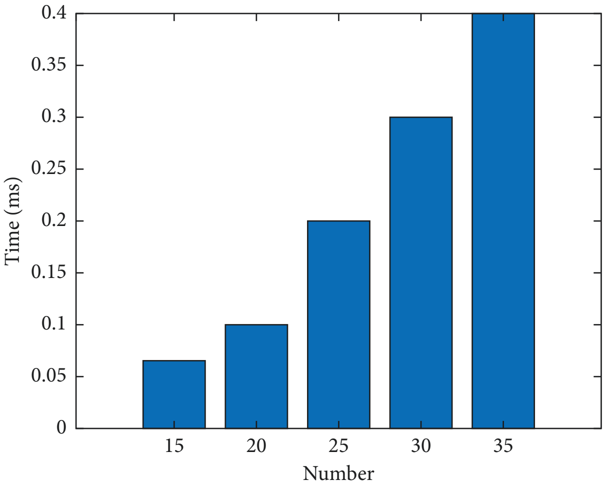


Figure 8: Time to create a block.

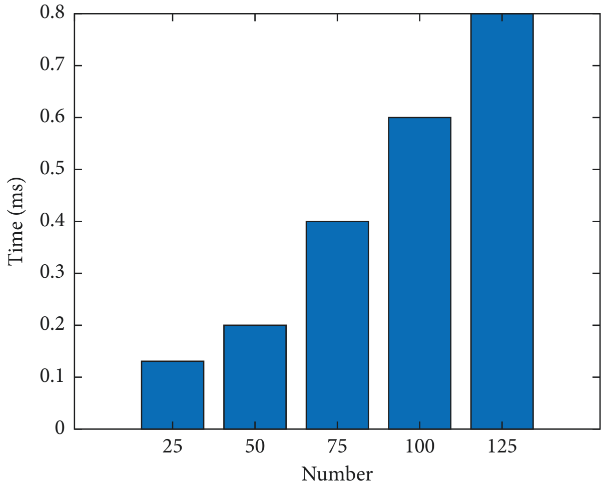


Figure 9: Time to validate a block. Calculate overhead in the system. The expenses of interaction between remote facility and patients and the operational expenses of smart contracts are quantified by Ethereum gas.

operating the proposed prototype framework are the studies' subjects. We begin by setting the stage for the tests. The service's security and adaptability are next evaluated and analyzed. The proposed system may set up and create benchmarks in the future to assess while the actual dataset becomes accessible.

Implementation of the System Experiments is carried out using an HP with Windows 10 operating system. This computer features a 2.3 GHz Intel i3 processor and eight gigabytes of RAM. The SM set is established and implemented using the Solidity programming language, and it is implemented on a sample Ethereum blockchain modeled using Ganache software. The script for data analysis is then written in Python [22]. Table 3 defines the overall comparison of existing work with proposed work. A sample code is displayed in Figure 7.

To calculate the average submission cost, we calculate the average gas cost of all requests and the standard deviation on the average cost of fifteen iterations of tests using three measures of arranged smart contracts and five different numbers of submissions ranging from one hundred to six hundred. The average request gas consumption is lowered by a factor of five from two hundred thousand Wei to four hundred thousand Wei. The variance of request cost is lowered by five times as the number of requests increases. The actual overhead is relatively minimal, even though the gas volume and deviation in Figures 8 and 9 are rather large. We understand that the lowest gas unit in the Ethereum system is the Wei and that one ether equals 1011 Wei.

It shows that as the number of applications rises from 50 to 200 and the contract rises from 15 to 25, the system's total gas usage rises linearly, taking into account the case of the same number of applications with different figures of

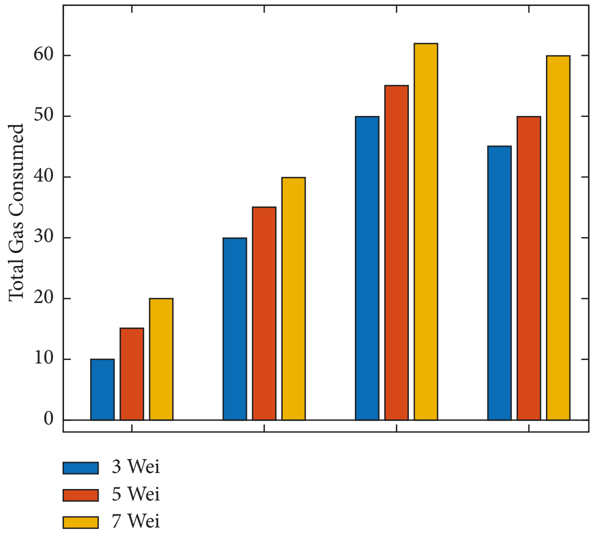


FIGURE 10: The amount of gas used by the remote facility, smart contracts, and consumers combined.

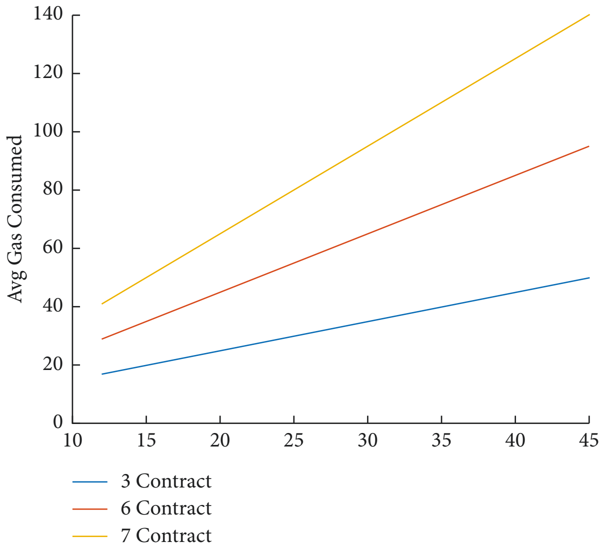


FIGURE 11: The average gas consumption.

contracts, as well as the case of the equal number of agreements with varying numbers of requests. A comparison is also demonstrated in Figure 10 of gas consumption by remote facility, smart contracts, and consumers combined.

Our suggested scheme has high stability and scalability based on the three measures [23]. The demand cost, which is the most significant overfit in the framework functioning, has been steadily approaching a lower threshold as the number of requests and contracts has increase. Lastly, Figure 11 shows an average gas consummation for the entire system.

6. Conclusions

In this work, we propose a tracking and alerting framework based on blockchain and smart contracts that offer three types of services: position-based contact tracking, wireless tracking, and smart contract-based tracking. Solutions for health tracing our technology can track a customer's travel and interaction record, as well as reminding them of previous infections they may have had. The health tracking program also allows users to evaluate their chances of becoming sick. Customers can securely transmit their visit data and health condition to the blockchain network to secure their confidentiality. Users may also utilize a massive set of arbitrary physical addresses generated by wireless technology as a provisional identity to preserve their anonymity even more.

Furthermore, the set of smart contracts was integrated into the framework to keep the contamination condition of each and every place. It executes the equivalent order of check-in procedures to guarantee that each patient receives the location's contamination findings consistently. We also simulate user contact with the proposed prototype organization before assessing its performance, including gas consumption, operating constancy, and request handling speed. Our system offers high scalability and stability in a simulated environment. We plan to have actual data regarding customer contact data to assess our technology in the forthcoming.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the financial support provided by King Abdulaziz City for Science and Technology (General Directorate for Financing and Grants) to King Abdulaziz University, Rabigh to implement this work through Fast Track Program for COVID-19 Research Project no. 5-20-01-009-0092.

References

[1] D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey," *IEEE Access*, vol. 9, no. 2021, pp. 95730–95753, 2021.

[2] H.-W. Kim and Y.-S. Jeong, "Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 11–13, 2018.

[3] A. E. L. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A quantum approximate optimization algorithm based on blockchain heuristic approach for scalable and secure smart logistics systems," *Human-centric Computing and Information Sciences*, vol. 11, 2021.

[4] A. Sharma, S. Bahl, A. K. Bagha, M. Javaid, D. K. Shukla, and A. Haleem, "Blockchain technology and its applications to

combat COVID-19 pandemic," *Research on Biomedical Engineering*, vol. 38, no. 1, pp. 173–180, 2020.

[5] M. Abouyoussef, S. Bhatia, P. Chaudhary, S. Sharma, and M. Ismail, "Blockchain-enabled online diagnostic platform of suspected patients of COVID-19 like pandemics," *IEEE Internet of Things Magazine*, vol. 4, no. 4, pp. 94–99, 2021.

[6] A. K. Das, B. Bera, D. Giri, and D Giri, "AI and blockchain-based cloud-assisted secure vaccine distribution and tracking in IoMT-enabled COVID-19 environment," *IEEE Internet of Things Magazine*, vol. 4, no. 2, pp. 26–32, 2021.

[7] M. Shuaib, N. Hafizah Hassan, S. Usman et al., "Identity model for blockchain-based land registry system: a comparison," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–17, Article ID 5670714, 2022.

[8] Y. Kim and J. Park, "Hybrid decentralized PBFT blockchain framework for OpenStack message queue," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 31–12, 2020.

[9] K. Dev, S. A. Khowaja, A. S. Bist, V. Saini, and S. Bhatia, "Triage of potential COVID-19 patients from chest X-ray images using hierarchical convolutional networks," *Neural Computing & Applications*, pp. 1–16, 2021.

[10] P. Zhai, Y. Ding, X. Wu, J. Long, Y. Zhong, and Y. Li, "The epidemiology, diagnosis and treatment of COVID-19," *International Journal of Antimicrobial Agents*, vol. 55, no. 5, Article ID 105955, 2020.

[11] R. Guha and S. Narayana, "A blockchain-based cyber attack detection scheme for decentralized Internet of things using software-defined network," *Software: Practice and Experience*, vol. 51, no. 7, pp. 1540–1556, 2021.

[12] P. Dhaliwal, P. Kumar, and P. Chaudhary, "An approach for concept drifting streams: early dynamic weighted majority," *Procedia Computer Science*, vol. 167, pp. 2653–2661, 2020.

[13] Y. Xiong, H. K. S. Lam, A. Kumar, E. W. T. Ngai, C. Xiu, and X. Wang, "The mitigating role of blockchain-enabled supply chains during the COVID-19 pandemic," *International Journal of Operations & Production Management*, vol. 41, no. 9, pp. 1495–1521, 2021.

[14] L. Ricci, D. D. F. Maesa, A. Favenza, and E. Ferro, "Blockchains for covid-19 contact tracing and vaccine support: a systematic review," *IEEE Access*, vol. 9, no. 2021, pp. 37936–37950, 2021.

[15] S. Bhatia, A. K. Dubey, R. Chhikara, P. Chaudhary, and A. Kumar, *Intelligent Healthcare*, Springer International Publishing, Berlin, Germany, 2021.

[16] M. H. Kassab, V. V. G. Neto, G. Destefanis, and T. Malas, "Could blockchain help with COVID-19 crisis?" *It Professional*, vol. 23, no. 4, pp. 44–50, 2021.

[17] W. Alkhader, K. Salah, A. Sleptchenko, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain-based decentralized digital manufacturing and supply for COVID-19 medical devices and supplies," *IEEE Access*, vol. 9, no. 2021, pp. 137923–137940, 2021.

[18] R. Gupta, P. Pandey, S. K. Chaudhary, and S. K. Pal, "Technological and analytical review of contact tracing apps for COVID-19 management," *Journal of Location Based Services*, vol. 15, no. 3, pp. 198–237, 2021.

[19] M. Khalid Imam Rahmani, F. Taranum, R. Nikhat, M. Rashid Farooqi, and M. Arshad Khan, "Automatic real-time medical mask detection using deep learning to fight COVID-19," *Computer Systems Science and Engineering*, vol. 42, no. 3, pp. 1181–1198, 2022.

[20] G. F. Frederico, "Towards a supply chain 4.0 on the post-COVID-19 pandemic: a conceptual and strategic discussion for more resilient supply chains," *Rajagiri Management Journal*, vol. 15, no. 2, pp. 94–104, 2021.

[21] T. P. Mashamba-Thompson and E. D. Crayton, "Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing," *Diagnostics*, vol. 10, no. 4, p. 198, 2020.

[22] P. Gandhi, S. Bhatia, and K. Dev, Eds., *Data Driven Decision Making Using Analytics*, CRC Press, Florida, USA, 2021.

[23] S. Basheer, S. B. Bhatia, and S. B. Sakri, "Computational modeling of dementia prediction using deep neural network: analysis on OASIS dataset," *IEEE Access*, vol. 9, pp. 42449–42462, 2021.