sustainability

MDPI

Article

CoviBlock: A Secure Blockchain-Based Smart Healthcare Assisting System

Bhaskara S. Egala [1], Ashok K. Pradhan [1], Shubham Gupta [1], Kshira Sagar Sahoo [1,2], Muhammad Bilal [3,*] and Kyung-Sup Kwak [4,*]

[1] Department of Computer Science and Engineering, SRM University, Andhra Pradesh 522240, India
[2] Department of Computing Science, Umeå University, SE-901 87 Umeå, Sweden
[3] Department of computer Engineering, Hankuk University of Foreign Studies, Yongin-si 17035, Republic of Korea
[4] Department of Information and Communications Engineering, Inha University, Incheon 22212, Republic of Korea
* Correspondence: m.bilal@ieee.org (M.B.); kskwak@inha.ac.kr (K.-S.K.)

Abstract: The recent COVID-19 pandemic has underlined the significance of digital health record management systems for pandemic mitigation. Existing smart healthcare systems (SHSs) fail to preserve system-level medical record openness and privacy while including mitigating measures such as testing, tracking, and treating (3T). In addition, current centralised compute architectures are susceptible to denial of service assaults because of DDoS or bottleneck difficulties. In addition, these current SHSs are susceptible to leakage of sensitive data, unauthorised data modification, and non-repudiation. In centralised models of the current system, a third party controls the data, and data owners may not have total control over their data. The Coviblock, a novel, decentralised, blockchain-based smart healthcare assistance system, is proposed in this study to support medical record privacy and security in the pandemic mitigation process without sacrificing system usability. The Coviblock ensures system-level openness and trustworthiness in the administration and use of medical records. Edge computing and the InterPlanetary File System (IPFS) are recommended as part of a decentralised distributed storage system (DDSS) to reduce the latency and the cost of data operations on the blockchain (IPFS). Using blockchain ledgers, the DDSS ensures system-level transparency and event traceability in the administration of medical records. A distributed, decentralised resource access control mechanism (DDRAC) is also proposed to guarantee the secrecy and privacy of DDSS data. To confirm the Coviblock's real-time behaviour on an Ethereum test network, a prototype of the technology is constructed and examined. To demonstrate the benefits of the proposed system, we compare it to current cloud-based health cyber–physical systems (H-CPSs) with blockchain. According to the experimental research, the Coviblock maintains the same level of security and privacy as existing H-CPSs while performing considerably better. Lastly, the suggested system greatly reduces latency in operations, such as 32 milliseconds (ms) to produce a new record, 29 ms to update vaccination data, and 27 ms to validate a given certificate through the DDSS.

Keywords: digital medical records; blockchain; privacy; security; pandemic mitigation; smart healthcare systems

Citation: Egala, B.S.; Pradhan, A.K.; Gupta, S.; Sahoo, K.S.; Bilal, M.; Kwak, K.-S. CoviBlock: A Secure Blockchain-Based Smart Healthcare Assisting System. *Sustainability* **2022**, *14*, 16844. https://doi.org/10.3390/su142416844

Academic Editors: Iqram Hussain, MD Rashedul Hasan Sarker and Md Azam Hossain

Received: 5 September 2022
Accepted: 9 December 2022
Published: 15 December 2022

1. Introduction

The most recent pandemic (i.e., COVID-19) [1] has produced a global health emergency. The majority of nations enacted strict lockdowns, quarantines, and home isolation to limit the spread of the virus and the infection rate. Nonetheless, these actions had a significant influence on people's livelihoods and economies. All of these steps are necessary at the ground level for mitigation to be successfully implemented. Inconsistency, fragmentation, and unavailability of data render the mitigation plans obsolete. With access to a large amount of data, mitigation teams can develop the most effective measures to lower the

rate of new infections [2]. In addition, resources are assigned and managed in advance based on predictions derived from real-time contact tracking, quarantine, and isolation data. With the use of digital medical information, even vaccinations can be automated to reduce the gaps between the supply chain and consumption. Despite the fact that the digitalization of medical records aids in mitigating pandemics in numerous ways, it poses numerous data security and privacy concerns. Additionally, data stored on a single server suppresses the owner's rights due to the service provider's pre-eminence. The deployment of security and privacy features in a centralised model is simple and cost-effective. On the other hand, the data's privacy and security are questionable due to the involvement of other parties.

As the information resides on a single server, data availability is not guaranteed due to SPoF [3,4]. Figure 1 illustrates a cloud-centric intelligent healthcare system. To address the shortcomings of conventional pandemic mitigation systems, there is a need for more sensible SHS. The most recent developments in the decentralised computing paradigm present an opportunity for an SHS to become SPoF-resistant without sacrificing scalability or usability. We proposed an innovative blockchain-based decentralised system to aid mitigation teams in preserving data privacy and security during the digitization of 3T operations. However, there are numerous privacy and security concerns associated with decentralised computing due to the fact that it relies on untrusted network peers [5]. In contrast, blockchain technology provides decentralised applications with integrity, traceability, and transparency services. Nevertheless, blockchain-based operations are expensive and time-consuming. Moreover, blockchain provides complete privacy and anonymity by default. Due to this, an IPFS with customised lightweight cryptographic mechanisms is combined with blockchain to create DDSS, a decentralised peer-to-peer file-sharing platform. IPFS stores files in a peer-to-peer network and maintains an internal cache for faster response. Additionally, it provides a version control technique to keep track of different versions of the same file without duplication, thereby reducing the time required to locate a file. The proposed DDSS enables SHSs to maintain integrity, trust, transparency, and immutability while storing and distributing files on a peer-to-peer network. Due to this, neither individuals nor groups of users are able to modify the data on the DDSS network.

The digitalization of 3T begins with the registration of individuals, which contributes to the creation of a new digital pseudo-identities. Then, individuals undergo preliminary tests, for which the results are encrypted with a publisher access key and published to DDSS with a mapping to the corresponding pseudo-identity. Later, hybrid computing prepares and publishes non-personal information about each user in an encrypted format using an access key for hybrid computing. In the event that a test yields a positive result, the hybrid computing system sends alert messages to the corresponding user and local mitigation team. Concurrently, primary-level medical resources and facilities are allocated to the patient automatically. The medical team modifies the service type from normal to critical or vice versa based on the severity level. While concealing the patient's identity, the second layer monitors and tracks the treatment based on the severity of the various stages. The service identity and pseudo identity of the first layer are combined to produce a new treatment identity. When the test result is negative and the user is not immunised, the system notifies the user. After a successful vaccination, the system updates the user's medical records with the pertinent event details. In addition, it orders vaccines based on the local infection rate and available stock, thereby reducing the supply chain delay. Additionally, it decreases black market sales and vaccine waste. The patient receives a digital certificate for medical services and the medical data access code upon completion of treatment. In the meantime, the patient can monitor his/her treatment using their pseudonym (treatment). To optimise a patient's treatment, the DDSS serves as a common platform for knowledge exchange between medical services stakeholders.

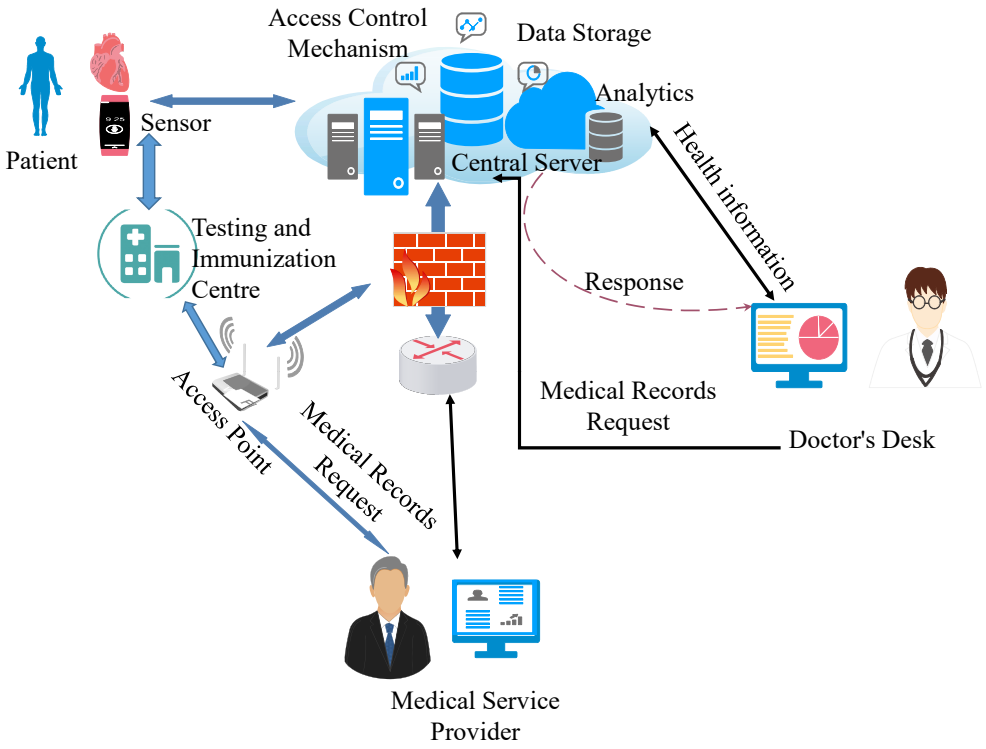


Figure 1. Overview of classical cloud-centric EHR management system architecture.

Our principal contributions are as follows:

- We propose a blockchain-based decentralised distributed assisting system for preserving medical record privacy and security in pandemic mitigation operations.
- We introduce system-specific DDRAC and privacy-preserving mechanisms.
- We suggest a prototype security analysis to demonstrate system-level security versus scalability and usability.
- We introduce a blockchain-based certificate management mechanism to introduce system-level transparency in medical resources utilization.

The rest of the paper is organised as follows: Section 2 highlights the related previous literature and its contributions. The proposed system architecture and its prototype model are introduced in Section 3. All major system functionalities are specified in Section 4. The experimental analysis with selected results is presented in Section 6. Finally, we conclude our work and listed the future directions in Section 7.

2. Related Work

The authors of [6] proposed a system to exchange the medical records over blockchain to help the mitigation teams. On the other hand, CoviChain, a framework for nonrepudiable contact tracing systems for pandemic outbreaks, is suggested in [7]. In a previous study [8], the authors proposed automating pandemic mitigation using cutting-edge technologies such as robotics to reduce the amount of human effort necessary for a streamlined mitigation process. The authors of [9] suggested a smart Real-Time Health Monitoring System for Stroke Prognostics where IoMT devices are connected to AI/ML models to predict the stroke possibility based on live data. As an extension, in the work in [10], researchers suggested stroke management using IoMT and AI/ML technologies. In [11], a game-theory-based vaccination distribution model is presented in order to reduce waiting times and forecast the required service providers. The authors of [12] discussed a blockchain-based smart, secure EHR sharing platform. In [13], the authors suggested blockchain-based privacy-preserving mechanisms for EHR over a decentralised platform. An improved

version of blockchain-based EHR privacy preserving methods is suggested in [14]. To improve intelligent real-time applications, researchers are focusing more on recent advances in cutting-edge technologies such as IoT, machine learning, and blockchain [15]. The authors of [16] recommended a quarantine management system based on blockchain technology. The authors of [17] proposed a blockchain-based decentralised system to address healthcare issues such as decentralised data security and confidentiality. In the majority of recent pandemic mitigation use-cases, blockchain technology plays a crucial role in data integrity and security, as demonstrated by researchers. A quarantine management system is proposed in [18] to aid mitigation teams in addressing the actions of individuals in quarantine. At the same time, blockchain has also proven its capabilities in the corporation and administration sectors to manage digital records for the manufacture and sale of drugs and goods [19]. A Privacy-Preserving and Incentivized Contact Tracing system for the COVID-19 pandemic is suggested using blockchain in [20]. Similarly, in [21], a blockchain-based IoT system is proposed for managing drug shipment, payments, and recipient validity. According to the authors of iblock [4], CovidWatch [22] blockchain could be used to create a decentralized contact-monitoring system on top of the current system. As security and privacy of the data matter in server-less environments, it is necessary to have pseudo-anonymity to eliminate confidentiality leakage attacks on records. In [23], Egala et al. introduced a blockchain-based contact recording system to support decentralised immutability, traceability, transparency, scalability, and privacy with the help of blockchain and cryptography mechanisms. BeepTrace [24], on the other hand, emphasized blockchain-based trust, transparency, and privacy in contact tracing. To support a community-level blockchain-based data exchange system, Bychain is introduced in [25]. The authors proposed better operational latency rates during message exchange, energy consumption, processing, and storage constraints. All the works mentioned previously solved different issues of digital data management using blockchain technology or some other approaches employing conventional cryptographic solutions [26,27]. However, 3T digital health certificate management (DHCM) and personal identity management are not addressed properly. Anonymous record management and record security are open challenges. In this paper, a new simplified DDSS-based SHS is introduced to assist the mitigation teams in 3T digitalization.

3. System Architecture and Identity Management

A three-layered decentralised computing infrastructure called the CoviBlock is depicted in Figure 2; in accordance with the sensitivity of the data, it ensures privacy and security. Figure 3 represents the internal system flow. The several sources used to obtain raw data are shown in the first layer. To create medical records with health information, smart health devices and IoMTs are positioned in this layer. The private DDSS network and edge computing are represented by the second layer. The second layer hosts data securely with the help of the DDRAC and PBFT protocols. In essence, this layer includes medical centres and labs that do diagnostic tests. Cloud computing and the public DDSS network make up the third tier. The mitigation teams and other engaged parties are covered by this layer. Users can dynamically join and depart the DDSS network using the first and third levels. The second layer DDSS network, by contrast, is a private network that controls access to electronic medical records to authorised hospital workers. It includes detailed information about the patient's health conditions and hospital-provided medical care. The peer-to-peer protocol used by the CoviBlock architecture links its layers together.

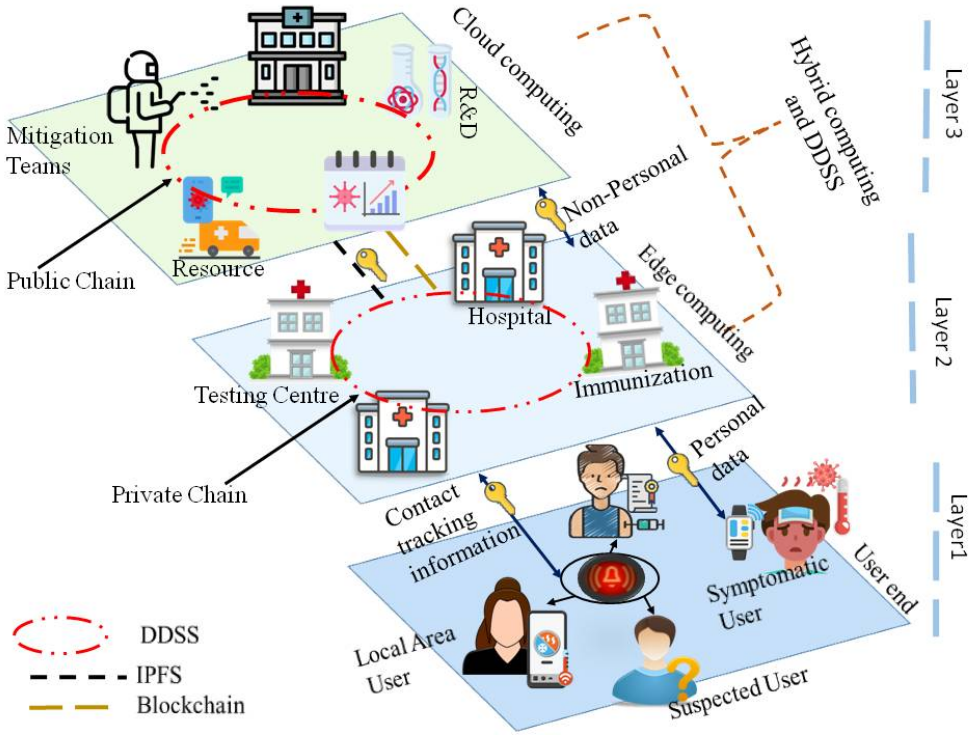


Figure 2. The proposed system architecture overview.

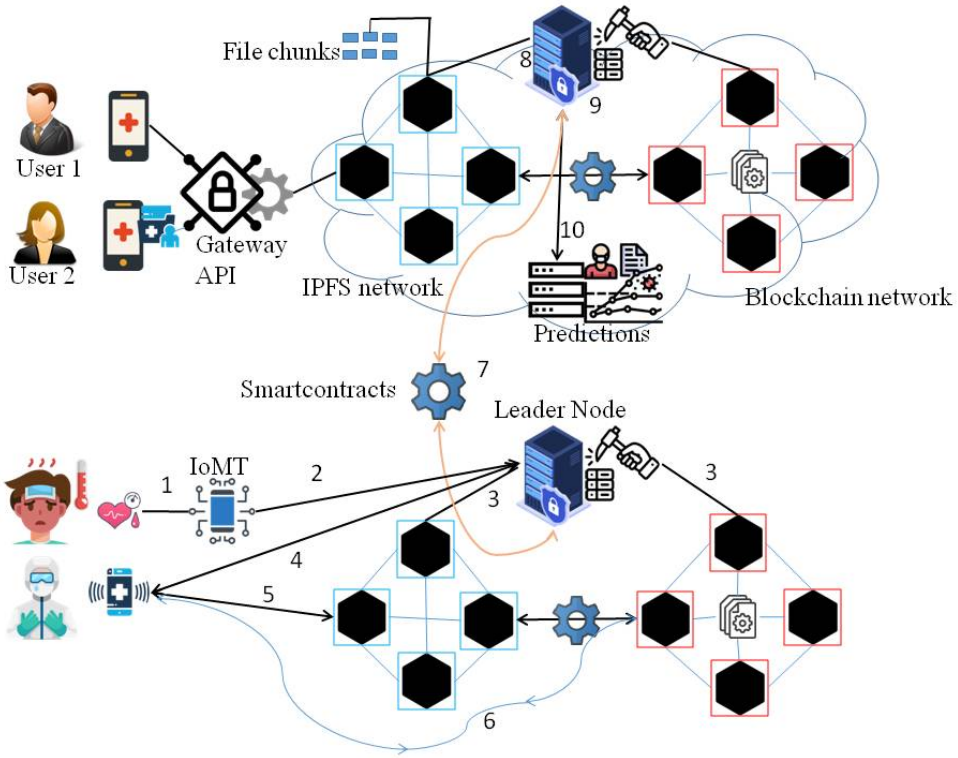


Figure 3. The proposed system's operational flow: (1) The sensor data are securely sensed from user. (2) The IoMT device securely uploads the data to DDSS using gateways. (3) The data are stored on the IPFS network, and its metadata are published to the blockchain network. (4) Business logic-based alerts are derived from DDSS. (5 and 6) EHR is only accessible to authorised users. (7) Non-personal data are published to a cloud-based DDSS using smart contracts. (8 and 9) Data are cached and process for predictions. (10) Time-to-time statistics are projected.

In order to maintain data privacy and security, we introduce DDRAC, which uses a three-layer identity management. The DDRAC mainly considers two instances: the first one is the sensitivity of information and the second one is users authorization. A simplified layered view of identity management is shown in Figure 4. After data have been generated, they are encrypted with the leader's public key and transmitted to the respective leader. In addition, leaders are responsible for maintaining the local cache in Layer Two in order to increase the system's throughput. In Layer Two, the edge computer prepares non-personal information for Layer Three. All transmissions between the second and third layers are encrypted using access codes. Edge computing on the second layer is responsible for DDRAC and DDSS maintenance.

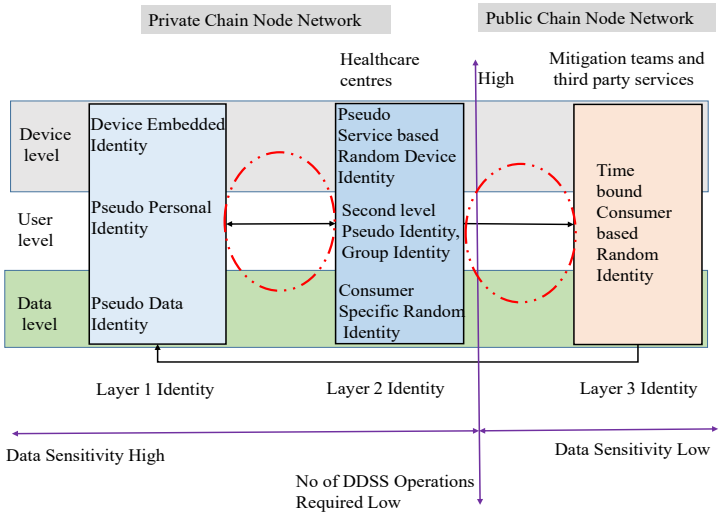


Figure 4. The layer identity model is divided logically into vertical and horizontal components. Vertical layers hold the layer-specific identifiers. Horizontal layers hold the different elements of the CoviBlock.

3.1. Three-Layered Identity and DDRAC

The distributed decentralised resource access control (DDRAC) multi-layered identification mechanism protects against backtracking attacks on a user's identity by associating digital healthcare activity with pseudo-identities.

DDRAC is considered to be founded on a three-layer identity management module and a selective ring-based access control system [23]. The edge computers perform hospital-level operations locally, thereby reducing the latency of analytics relative to cloud analytics. When an authorised user requests a medical record from a private DDSS, the system first checks its internal cache. If the cache is not available, it requests the medical files from the respective IPFS peers. In general, files are obtained from the network for the first time and then stored in a local cache; thereafter, the local cache is utilised instead of the network. The cache is updated every five minutes to preserve its integrity. The cache procedure facilitates CoviBlock's reducing the number of blockchain operations necessary for file access. This increases the overall throughput of CoviBlock and gives it an advantage over traditional centralised H-CPSs with blockchain. The primary identity for the first layer is determined by the embedded code of the device developer (E_{ID}), whereas the primary identity of actors is determined by a unique personal identity (P_{ID}). Because the P_{ID} contains sensitive personal information, CoviBlock conceals it with a new pseudo-identity. A first layer pseudo-identity for devices ($Prim_{Dev_{ID}}$ and actors $Prim_{Act_{ID}}$) is generated from their respective E_{ID} and P_{ID}, as shown in Equation (1), where device-embedded identity E_{ID} is XOR with its respective service identity S_{ID}. Thereafter, a left-shift operation $ls(input, shiftcount)$ is performed to make the newly generated identity anonymous. Additionally, a group key (G_{key}) is generated, as shown in Formula (2), to manage the devices and actors working for a specific service. Further, the second layer

identities are generated with the help of the Layer One identity, as shown in Formula (3). Finally, the third level of identities is generated with the help of the secondary identities, as shown in Equation (4).

$$\begin{aligned} Temp_{Dev_{ID}} &= E_{ID} \oplus S_{ID} \\ Temp_{Act_{ID}} &= P_{ID} \oplus S_{ID} \\ Prim_{Dev_{ID}} &= ls(Temp_{Dev_{ID}}, 3) \\ Prim_{Act_{ID}} &= ls(Temp_{Act_{ID}}, 3) \end{aligned} \tag{1}$$

$$G_{key} = 3^{N-1} \mod (N) \tag{2}$$

Second layer identity generation:

$$Scnd_{ID} = (((Prim_{ID} \oplus Rand_{num}) \oplus G_{ID}) \oplus G_{key}) \tag{3}$$

Third layer identity generation:

$$Publ_{ID} = (Scnd_{ID} \oplus Rand_{num}) \oplus Pub_{ser} \tag{4}$$

where N represents the number of actors in a group. A random number ($Rand_{num}$) is used in every identity generation to eliminate reverse engineering attacks. Every medical record is further encrypted with G_{key} and goes through the $E(G_{key}, Data) || hash(data)$ operation. The access permissions are created and updated by the group leaders on DDSS using smart contracts, due to which unauthorised modification to access rules is not possible. Simultaneously, the group leader generates a user-specific copy along with its decryption code. The credentials are only valid through the second layer and are only shared with the intended authorised users.

3.2. Group Formation and Leader Election

The proposed CoviBlock creates logical service groups for each patient by collaborating sensors, actuators, and edge nodes. As IoMT devices are incapable of participating in complex DDSS operations, the edge nodes of the second layer serve as gateways. By contrast, in a private DDSS network, all edge nodes participate in the election of new group leaders to prevent gateway attacks. These edge nodes maintain the local cache of medical records and their access rules in the private DDSS network to increase the scalability of CoviBlock.Hybrid computing uses PBFT protocol to maintain required number of nodes on every critical path to provide data availability. The group leaders are elected for both the private and public DDSS networks as shown in Figure 5. The leader election process considers the critical paths that mainly connect the most-influential nodes using pseudo-Algorithm 1. The overall process of leader election takes a few input parameters, such as path coverage rate (R_{CP}), competency rate (R_{CR}), offline rate (O_{RA}), elected history (R_{EH}), and history of blockage (R_{BH}).

i. Coverage rate is the ratio of the number of logical connections to the total number of nodes on the critical path. The device with the highest coverage rate is considered to be the new group leader. The availability of information can be ensured if a node has a greater number of connections.
ii. In the initial phase, the node with the greatest number of connections within the group is regarded as the interim leader. When the elected leader assumes control, the ledgers are transferred to the elected leader. In situations where only one node actively participates in the critical path and there is no competition for election, a temporary leader node is elected for the permanent position.
iii. A device with a low offline rate has a lower priority than a device with a high critical path coverage rate. It assists in preventing service interruptions and enhances service availability.

iv. In the event of a tie, a candidate's election history is taken into account to prevent the election from being biassed. In order to prevent a monopoly in the election, the system imposes a minimum threshold on each leader.

v. The election history is considered to identify valid nodes, thereby preventing the selection of a malicious device.

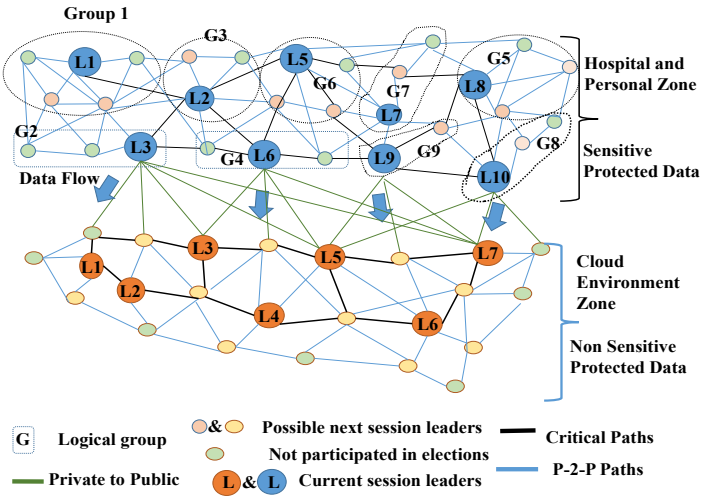


Figure 5. An overview of leader election and group management. Groups are created using service identity.

Algorithm 1 Leader Election

Data: $R_{CP-i...n}$,$R_{CR-i...n}$,$O_{RA-i...n}$,$R_{EH-i...n}$,$R_{BH-i...n}$ as array Input[]
Result: Elected Leader
Function `choseLeader()`:
  while *row in Input[n][5]* **do**
    compare i^{th} with its previous and next rows
     swap rows as per rules ; `// lower values towards bottom`
    row++
     go to step 2 ; `// recursive operation to sort the elements`
  return device at top of Input[] as new leader

4. 3T with CoviBlock

Algorithm 2 of CoviBlock operates the major functions of 3T. It enables the monitoring of a person's health status and suggests medications in real-time as needed. CoviBlock facilitates the creation of a medical record for vaccinated individuals. In another instance, it arranges a vaccination appointment at a nearby clinic. CoviBlock allots medical resources to infected individuals and organises them into groups based on their service identity. Due to this mechanism, mitigation teams are able to organise medical facilities in a real-time environment with minimal delays. Similarly, in the third layer, the system assists teams with mitigation based on real-time data. In addition, the proposed system utilises hybrid computing and data analytics to estimate the required immunisation doses and resources for in-hospital patient treatment on a regional basis. In Section 4.2, a service-based resource administration mechanism is introduced. The contact tracking and immunisation module in Section 4.3 takes care of tracking and alerting suspected connections with an infected person. Similarly, it sends awareness messages to the people in areas with a high infection rate to get vaccinated. It provides digital information to the DHC management module in Section 4.4 to create, update, and revoke digital health certificates.

Algorithm 2 Mitigation Assisting

Data: Actor identity, data, access control info, device identity
Result: Secure operation of 3T automation
Initialization: DDSS initialization with crypto primitives
choseLeader()
DDRAC: Check device identity and access permissions are valid **if** *Device is authorised* **then**
    Initiate requested 3T operations
    Start health monitoring and alerting
    Secure digital health data on DDSS
else
    Block device and add to the blocked-list
if *User has a chronic disease history and not vaccinated* **then**
    vacAuto() `// Immunization`
    dhc() `// Write DHC to DDSS`
else if *(suspected and vaccinated) or (suspected and not-vaccinated)* **then**
    Trace_alert() `// Track all exposed connections`
    Suggest vacAuto() for suspected close connections
    dhc() `// Write DHC to DDSS`
    subGroup() `// Allocate medical resources`
    Treat() `// In-person medical service`
else
    Generate DHC if a persion has recoverd or deceased after dhc() `// Write DHC to DDSS`

4.1. Electronic Health Record (EHR)

Using the first two layers, the electronic health record (EHR) or electronic medical record (EMR) is generated at the time of service registration. On the other hand, CoviBlock uses smart contracts to create EHR or EMR files. Typically, the EHR/EMR is generated utilising an IPFS empty object, such as heart rate, SpO2, and temperature, as depicted in Figure 6. To track the patient's health status, all specific user health information is linked to empty objects with different version names (e.g., HRv1, SpO2v1, TRv1, etc.). Each data version has its own hash value, represented as H1, H2, etc. The IPFS file chunks are denoted by the letters C1, C2, and C3. To simulate EHR/EMR operations, ten dummy actor accounts for each role were created. Fifty patient dummy data sets were utilised to simulate the 3T procedure. The EHR contains the pseudo-identity of the patient based on the layer in which the EHR is used. In addition, it includes information about daily services and events, such as service group information, service provider information, types of service and their unique information, known previous medical history, current health status, period of service information, etc. Figure 6 illustrates the process of conversion of medical data into a record format on DDSS.

Every IoMT device in the service group updates the information in the EHR through the edge devices. Every time the edge devices create a new file with received event data, the file is named according to the type of event. The heart rate observation files, for example, are linked to the $user - pesudo - idenity_{heart-rate}$ object on the DDSS network. When service providers change the service status, the information in the EHR is updated by adding a new file to $user - pesudo - idenity_{service}$. This can be improved by having this file link the tracking or history of a patient's treatment. The history of the data also provides the opportunity for medical examiners to perform analytics and predictions to gain more knowledge from the electronic health record.

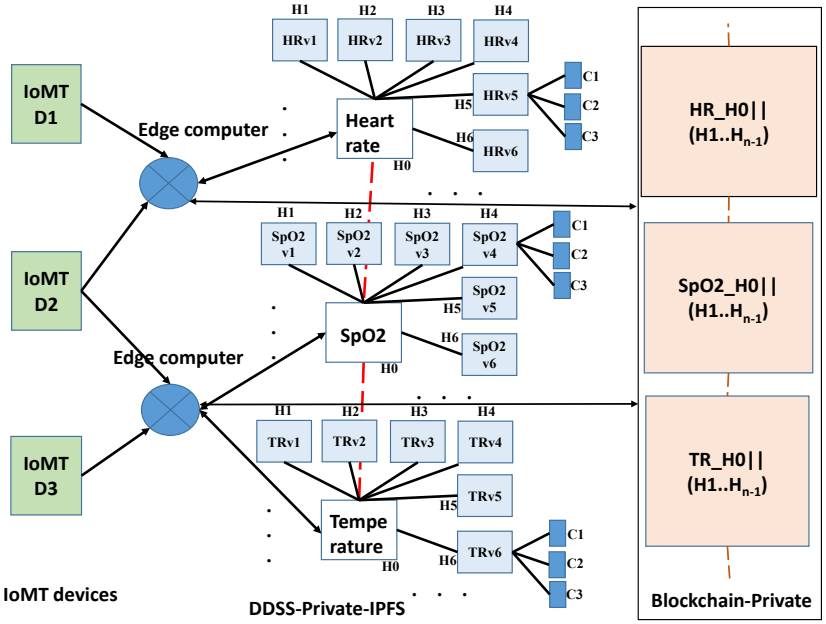


Figure 6. An abstract view of data-flow from the IoMT devices to DDSS-EHR. The edge computing devices perform DDSS operations. DDSS-IPFS meta-information is written to blockchain.

4.2. Resource Management

In an emergency, the system allocates the necessary medical resources and services to the affected patient automatically. It prevents false claims regarding the utilisation and allocation of medical resources. In addition, this mechanism aids patients by rapidly automating the clinical settlement process. In current systems, claim approval is performed manually, and due to human error, a genuine patient may not receive approval in a timely manner. The resource management system recognises data, healthcare personnel, and medical infrastructure as resources. In the proposed system, all resources are categorised as either critical, general, or open. As shown in Algorithm 3, the allocation of resources is solely determined by the severity of the patient's condition.

Algorithm 3 Resource Allocation

Data: user id, service level (S_{LE})
Result: resource group with S_{ID} and DDRAC
Function `subGroup()`:
  if *the service level is critical* **then**
    pull all required ICU resources and group them with S_{ID}
    register the group in DDRAC
  else if *service level is moderate* **then**
    pull the required general service resources and group them with S_{ID}
    register the group in DDRAC
  else
    allocate basic health monitoring resources and group them with S_{ID}
    register the group in DDRAC
  return group identity with S_{ID}

To care for patients in intensive care units (ICUs), a critical service level is made up of specialised medical professionals, trained healthcare workers, and intensive care medical equipment. Low-grade symptomatic and asymptomatic cases are typically treated by specially trained medical personnel. Lastly, the open level includes front-line employees, vaccine production labs, and other teams. The following are the four most common applications of blockchain technology and smart contracts.

i. Allocating ICU resources to patients in an emergency situation;
ii. Allocating a dedicated group of service providers for continuous monitoring;
iii. Patients' digital records are generated automatically based on the services and resources used during their treatments;
iv. Timely distribution of medical kits to front-line workers and other healthcare service providers.

4.3. Contact Tracing and Immunization

The components of a pandemic mitigation strategy are contact tracing, resource allocation, and immunisation. Using blockchain technology and decentralised web applications (DApps), our proposed CoviBlock can streamline the entire vaccination process. To maintain supply-chain transparency, the DApp records supply-chain events and vaccination procedures. In addition, it reduces the misuse of vaccines and their illegal distribution. Figure 7a depicts the geographical breakdown of COVID-19 cases and immunisation rates from the DDSS ledger. The information identifies the gaps in their mitigation plans, which facilitates their implementation in a real-world setting. The infection rate is computed using data from the previous week. Using the vaccination rate depicted in Figure 7b and the medical results, it is possible to predict the number of cases in a given area. As depicted in Figure 8a, the CoviBlock provides area-specific dosage information. In addition, it provides an estimated dosage count for the following two days based on slot registrations and the number of unvaccinated individuals in the region. It automatically assigns dosages based on the predictions using smart contracts. As depicted in Figure 8b, the dosage order transaction details are trackable on the blockchain test network using the block number. In addition, with the assistance of IoMT devices and smart contracts, human errors in record administration are nearly eliminated. With these safeguards in place, all eligible individuals receive the vaccine according to the vaccination program's schedule and on time. It also identifies high-density locations where the rate of infection spread is high in order to facilitate the deployment of mitigation teams. Using the seven-day infection rate from the previous week, future cases are predicted. In addition, the required inventory for the deployment is calculated based on the three-day gap between the most recent vaccination and the targeted vaccinations.

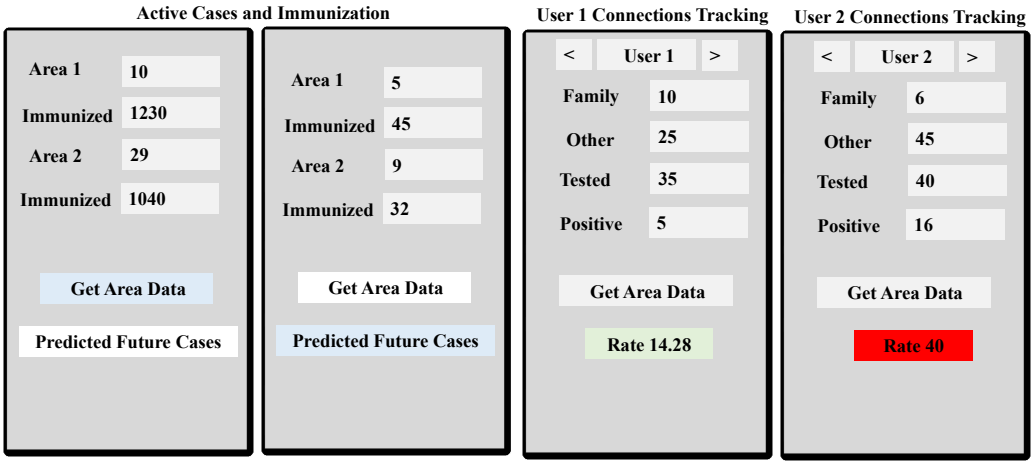
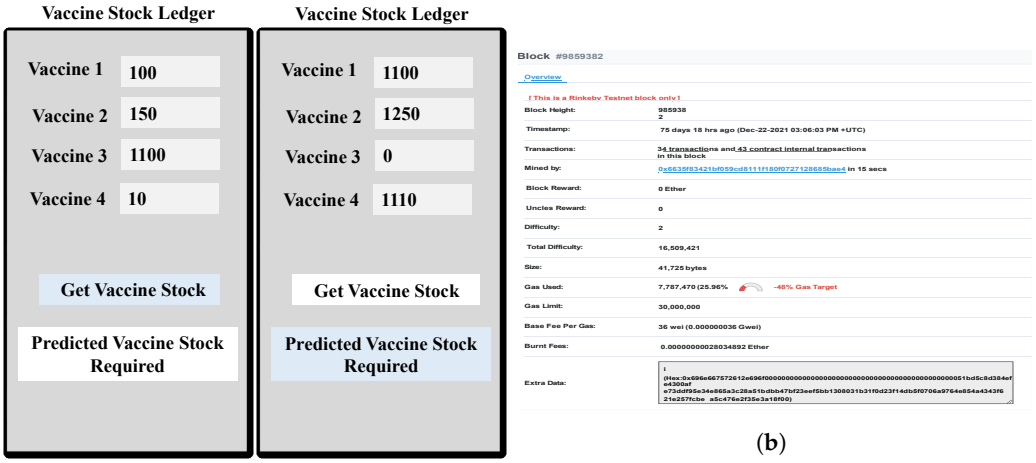


Figure 7. CoviBlock assisting in 3T operations. (**a**) Area-wise information from 3T on DDSS and number of possible cases and immunisation prediction based on the last 3–4 days' average. (**b**) The infection rate calculation for different patients uses different parameters to deploy medical services.



(**a**) (**b**)

Figure 8. CoviBlock in run-time with transaction details. (**a**) CoviBlock automatically allots doses to different areas based on the last seven days' consumption versus the total eligible population. (**b**) DDSS operation transaction details on test network.

Consequently, vaccine manufacturers and government agencies will have a clear understanding of the requirements and will be able to take the necessary precautions in advance. Pseudo-Algorithm 4 is proposed to achieve COVID-19 prescriptions for drug supply and use. The CoviBlock performs contact tracing with the aid of IoMT devices and smart contracts. The system registers all users with a pseudo-identity and prevents the disclosure of sensitive information, including unique personal identifiers, demographic data, and personal smart-device security codes.

Algorithm 4 Immunization

Data: Personal identity, area, health state
Result: Automated distribution of vaccinations and predefined slots
Function `vacAuto()`:
  Get the last two days' vaccination data from DDSS
  Find vaccination stocks in highly infected areas
  Find the gaps in the supply chain and initiate supply requests
  Divide the received vaccinations into batches to supply as per prediction
  Monitor and record the supply and immunization events
  Do vaccination for authorised users
  return In-time supply-chain initiation and record management

4.4. Digital Health Certificate Management

Using the suggested three-layer identity approach, the proposed system automates digital health certificate life-cycle operations such as enrolment, distribution, validation, and revocation. The digital health certificate manager function *dhc*() has two sub-functions: certificate life-cycle administration and validation. As depicted in Figure 9, the *dhc*() function generates a QR-code-based, tamper-resistant DHC certificate for each authorised user. Using DApp, anyone can demonstrate his/her identity and authenticity without disclosing personal information. To validate a user's digital health certificate, a second user (the "validator") must scan the QR code and initiate the validation process as shown in Figure 10. In addition, *dhc* prevents the use of forged or duplicate certificates by implementing a public ledger system. With the aid of pseudo—Algorithm 5, an acknowledgment is generated for each successfully validated QR code.

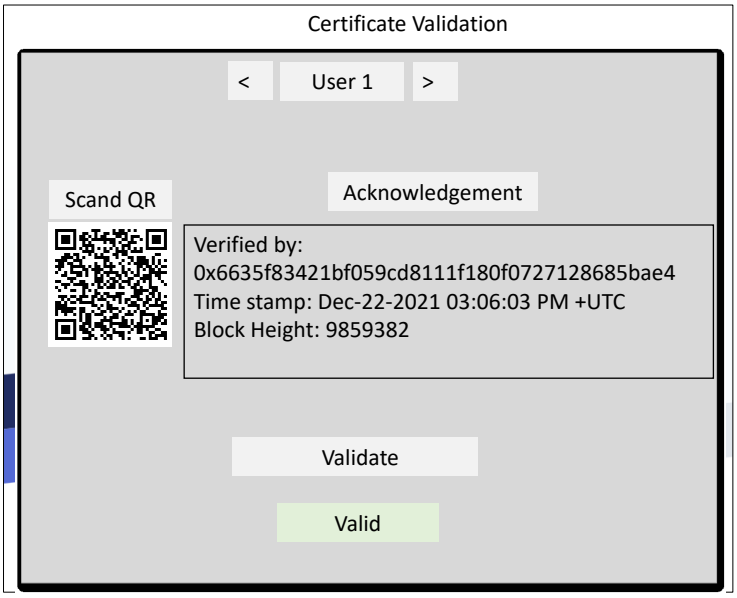


Figure 9. Sample digital certificate validation.

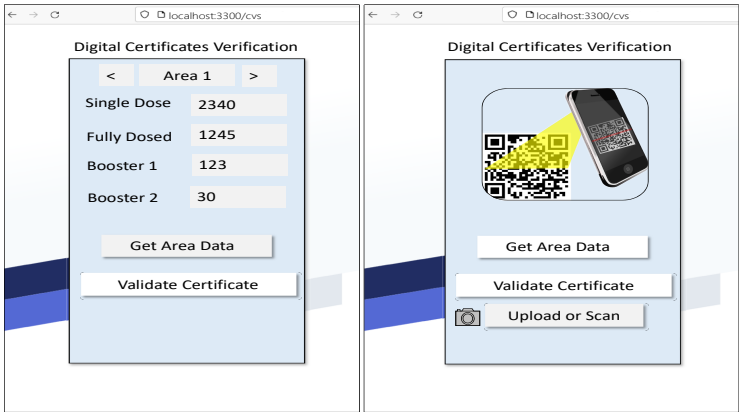


Figure 10. QR-code-based digital certificate validation.

Algorithm 5 Digital Health Certificate

Data: QR code, layer identity, group identity, service identity
Result: Digital health certificate life-cycle administration
Function `dhc()`:
- **if** *User is new to the system* **then**
  - Generate dhc
  - update the records
- **else if** *User is availed services* **then**
  - Update certificate
  - Validate user information
  - Initiate claim if user is opted
- **else**
  - deny claim
- **else if** *patient is deceased* **then**
  - Update certificate
  - Generate death certificate
  - Initiate compensation
- **else if** *User is nonexistant* **then**
  - Revoke the certificate
- **return** DHC to DDSS

When a critical event occurs, such as successfully registering for a vaccination, being released from the hospital, or being declared deceased, the *dhc*() smart contract module generates digital certificates for users. Users can validate by simply providing the verifier with a certificate QR code. The validator verifies the QR code and grants access to the services for the authorised user. Considering the aforementioned scenarios, the applicant must demonstrate that he/she is fully immunised in order to receive an e-visa. The applicant simply shares the QR code with immigration authorities to obtain approval. On the other hand, the DApp handles data security and validates without any additional human intervention. The entire system relies on a non-transferable digital certificate for identity validation. The receiver executes the identity extraction procedures and initiates the validation process with the help of the *validation*() sub-function. Three inputs are necessary for the validation procedure. The first is the identity associated with the certificate, the second is the public identity of the requester, and the third is the location of the requester. Validation aids the system in identifying its local users and devices in order to prevent malicious attacks from the outside network.

5. Experimental Setup

A CoviBlock prototype is simulated on four virtual computers (VC) connected via a virtual local area network (VLAN). Each VC includes a node.js-based decentralised application (DApp) for interacting with DDSS and DDRAC smart contracts. Figure 11 illustrates an overview of the DApp testbed. The RikBay testnet is used to validate and test the DApp smart contracts; the local setup consists of MetaMask, the Truffle framework, and Ganache; and the Infura platform is being considered for the public DDSS network. The web3.js API enables interaction between DApps and smart contracts on DDSS. The testbed VCs are equipped with 8 GB of RAM, an Intel i5 @2.30 GHz processor, and 150 GB of storage space. A network address translation (NAT) protocol is used to link the public DDSS network to the local infrastructure. In contrast, for the gateway use case, two mobile devices with 3 GB of RAM, an octa-core @2.0 GHz processor, and 16 GB of storage space are considered. In addition, we have published the experimental setup details in a github repository [28].

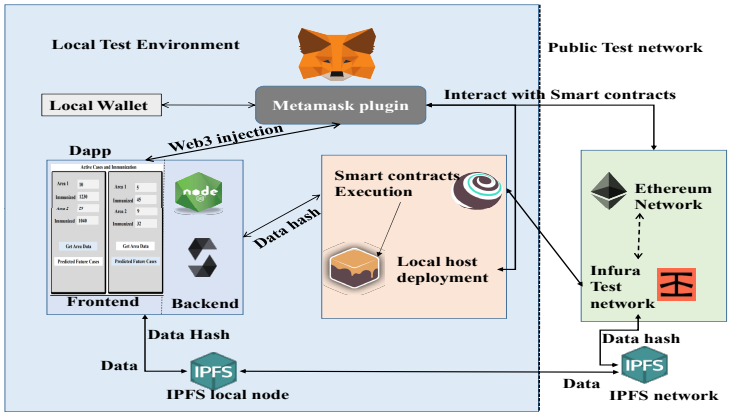


Figure 11. The proposed system experimental setup.

6. Results and Analysis

This section discusses system performance and security analysis to support CoviBlock's objectives. The section that follows discusses theoretical security analysis with respect to performance, reliability, availability, scalability, and confidentiality, respectively.

6.1. Security Analysis

This section summarises CoviBlock's DDSS communication protocol security validation using security protocol description language (.spdl) and the Scyther tool. The outcomes demonstrated that the protocol is resistant to data leakage attacks. Figure 12 demonstrates the outcomes of the Scyther tool analysis. The pseudo-code of the CoviBlock security

protocol is presented in the next section, along with a tool that verifies whether or not sensitive data are disclosed. The *Nisynch* and *Niagree* algorithms are used to detect man-in-the-middle and replay attacks, respectively. The parameters asserting confidentiality are the *SessionKey* keys. To establish the DDSS protocol use case, a protocol is established between one leader (*Lead*) node and two IoMT devices (DA and (DB). The symbols *msg*, *DIsig*, *MATdiv*, and *const*, for example, stand for the initial communication between nodes, the digital signature, mutually agreed-upon keys for one-to-one communication, and constant values, such as various identities, respectively.

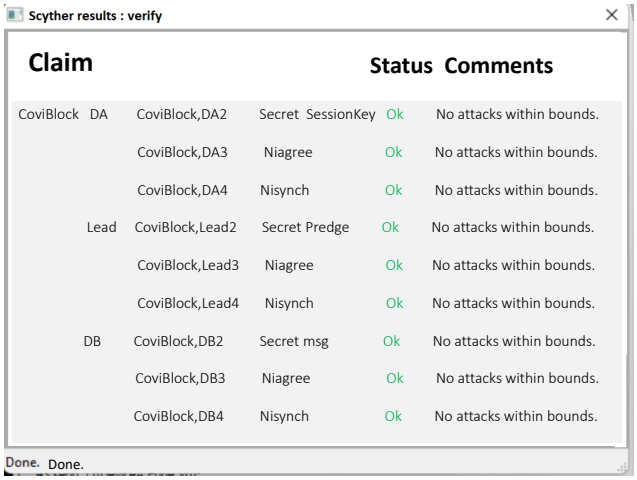


Figure 12. The proposed system security protocol analysis. No communication leakage is identified between Device A, Leader, and Device B.

The Microsoft Threat Modeling Tool (MTMT) is utilised (Figure 13) to identify security threats at the system architecture level. Using the STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege) methodology, MTMT generates a list of potential threats. The MTMT tool highlights several known system attacks, such as cache and data spoofing, data tampering, actuator configuration tampering, repudiation, information disclosure at the storage level and transmission level, and escalation of actor privileges. Clearly, the DDSS and tamper-proof ledger protect the system from non-repudiation attacks. Following is a discussion of the theoretical security analysis of the proposed system.

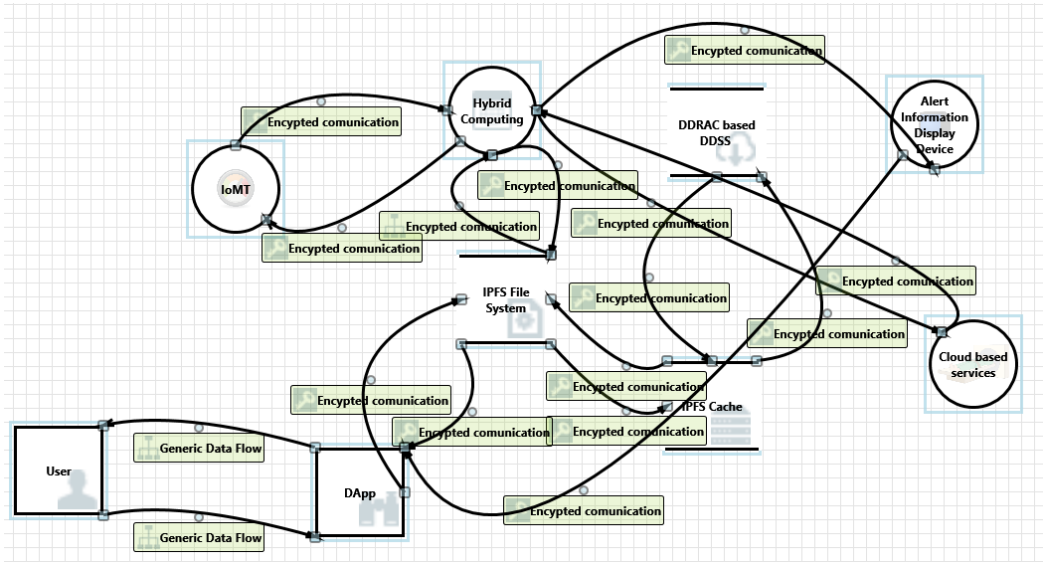


Figure 13. CoviBlock architecture model vulnerability assessment on MTMT platform.

6.2. Privacy and Anonymity

The CoviBlock enables the exchange of session keys, mutual authentication tokens (MAT), and signed data during node-to-node communication. In addition, it enforces dual encryption to conceal data and key information across a peer-to-peer DDSS network. System-specific access control adds an additional layer of confidentiality and only permits chosen users to view the data. The session keys and mutual authentication tokens ensure data privacy and confidentiality, respectively.

Using a three-layer pseudo-identity model, DDRAC protects the user's digital information at the user, group, and public DDSS levels. The user's public key is used to encrypt and store private data on the DDSS, whereas the group key is used to encrypt group information. The public information is encrypted using a hybrid computing symmetric key and is only shared with authorised users upon request. In order to compromise the DDRAC, an attacker must calculate three distinct encryption keys, including a private key, a group key, and a hybrid computing symmetric key, which is not practically feasible in a limited amount of time. Since the identities are dynamic and mapped in a unidirectional manner, it is not possible to generate Layer One and Layer Two identities using Layer Three data. This mechanism aids the system in reducing identity theft or leakage attacks.

6.2.1. Integrity and Version Control

The CoviBlock generates a hash for each block, which is appended to the encrypted block for integrity checking. In addition, the blockchain ledger assures data integrity on the DDSS network and tracks the integrity of multiple versions using IPFS. Every version is uniquely identified by its hash value. The versions help the system to track the authorised changes in real time. The appended hash value is used to check the received data's integrity before using them for system operations.

6.2.2. Accountability and Authorization

Before granting a user access to DDSS network information, the three-tier DDRAC verifies the user's identity and authorization. All actions and events are recorded in DDSS to prevent non-repudiation attacks, thereby ensuring individual accountability. The CoviBlock ensures that only authorised users are permitted to participate in system operations.

6.3. DDoS and Availability

The DDSS system ensures data and system operations availability for authorised users by distributing operations over a peer-to-peer network. A Byzantine Fault Tolerance (BFT) consensus ensures the required number of nodes are available all the time. The combination of the access control system and transactional costs determines the attacker. A DDoS attack is not allowed by the PBFT protocol while 51 percent of nodes are offline. Local cache management further guarantees data availability for the group nodes. Due to a lack of version control and redundancy control, data cached in numerous locations in non-DDSS systems leads to redundancy and inconsistency. Even though the local cache strategy adds data redundancy to the system, it also speeds up operations. The model links all the data versions to the same empty IPFS object to preserve the version history and data. The IPFS module in DDSS increases system throughput and availability all the time without any data redundancy. The blockchain-based access control system prevents unauthorised DDSS operations, allowing CoviBlock to preserve its integrity and availability. Even if a successful attack on 50 percent of nodes renders information unavailable, the records cache at the leaders ensures the information's availability because the PBFT protocol guarantees the availability of at least two-thirds of the nodes at all times. Furthermore, for an intruder to modify the ledger on the DDSS, at least 51 percent of nodes must be compromised, which is practically impossible in a short period of time. To predict the CoviBlock response to a DDoS attack, a 40-node testbed was used to simulate a DDoS attack. The relationship between availability and percentage of compromised nodes is depicted in Figure 14. CoviBlock with

PBFT and local cache maintained 80 percent data availability when 50 percent of its nodes were unavailable per experimental analysis.

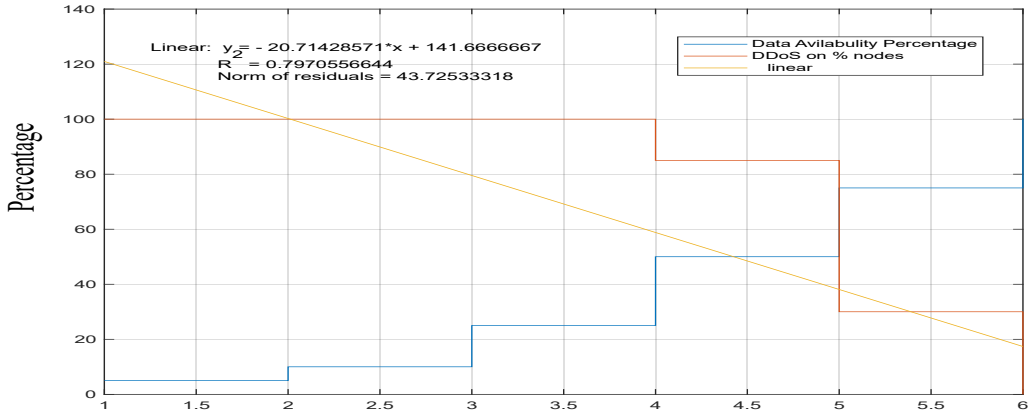


Figure 14. DDoS vs. data availability. The proposed system availability increases when the number of participating nodes increases.

6.4. Cost and Response-Rate Analysis

This subsection presents a formal cost and latency analysis of the proposed system. To determine system responses in real-time, the major system operations, such as identity generation, immunisation tracking, subgroup generation, new leader election, and access rule updating, are evaluated. The respective observations are shown in Table 1. In addition, DDSS data operational behaviour concerning file sizes is presented in Table 2. Response time is the time between the request and the DDSS's response to the request. From Table 1, it is evident that the proposed system is cost-effective and feasible in real-time. In addition, the proposed system reduces the cost of blockchain data storage with the IPFS file system (DDSS). The CoviBlock only stores the hash value of the data on the blockchain, and the data are stored on an IPFS peer-to-peer network to reduce the DDSS data operational cost and latency. In addition, a straightforward comparison of file storage costs is presented in Table 3. According to the results, the proposed system achieves satisfactory transaction throughput and halves the time required to access files from the cache.

Table 1. Healthcare dataset file storage operation cost and time interval.

Smart Contract	Transaction Fee (Ether)	Max Gas Fee (Gwei)	Execution Time (ms)	Response Time In (ms)	Cost in USD (Dollar)
User Registration	0.00010504	2.500000011	27.2	32.26	0.12
Immunization Tracking	0.000155366	2.500000018	20.6	29.64	0.17
SubGroup Generation	0.000155611	2.600000102	28.73	34.64	0.17
Electing New Leader	0.000019348	2.600001102	40.23	49.12	0.022
New Digital Certificate	0.000011826	2.500000002	22.65	26.93	0.013
Access Rule Update	0.000012214	2.400000180	34.1	42.5	0.014
Pseudo-Identity Generation	0.000019309	2.600000002	38.06	45.43	0.022
Public Identity Generation	0.000010116	2.500001110	26.7	29.7	0.011

Table 2. Selected CoviBlock DDSS data operations.

Data Size	Data Writing (ms)	Data Reading (ms)	Response Time (ms)	Local Cache Response Time (ms)
40 kb	135	790	350	120
70 kb	238	1160	410	145
100 kb	290	1436	490	156
130 kb	320	1570	540	163
160 kb	350	1610	565	171
190 kb	390	1690	589	183
220 kb	423	1740	603	193

Table 3. Storage cost with respect to file size.

System Name	20	25	30	35	40
H-CPS with Blockchain	16.32	19.38	21.21	21.98	23.72
CoviBlock with DDSS	0.020	0.041	0.059	0.082	0.093

6.5. Transparency

The DDSS system implements smart contracts for resource distribution and administration based on the mitigation department's business logic. The transaction is validated in accordance with the smart contract standards. To automate the static behaviours of system processes, DDSS smart contracts and three-layer identities are utilised. The vaccination supply chain is automated using smart codes, and public access to the data is restricted using DDRAC, where only authorised users are issued access codes based on the SRAC access tables.

6.6. Scalability

This subsection describes the scalability of Coviblock. Multiple tests were conducted by increasing the number of peers and concurrent transactions each time. The analysis of the results revealed that the proposed system was more scalable than blockchain-based H-CPSs. In addition, the proposed DDSS fabrication produced data operations with low latency when compared to PoW-based blockchain H-CPSs. The results are depicted in Figure 15. In its best case, the CoviBlock outperformed an H-CPS based on a bare blockchain nearly fourfold, and in its worst case, it was nearly threefold. Additionally, we present experimental analysis regarding group management in relation to the increase in participating nodes (Ls). CoviBlock manages low latency while initialising service groups and updating the group-level cache, as shown in Figure 16. CoviBlock requires more time during the initial stages of group creation due to device validation and crypto primitive generation.

Finally, we present a comprehensive feature comparison between our proposed CoviBlock and selected related works in Table 4.

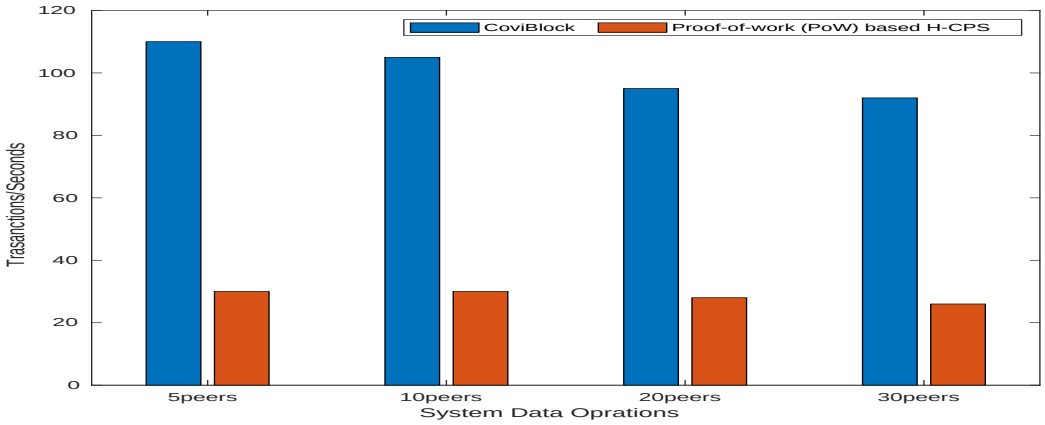


Figure 15. Transactions per second vs. peers.

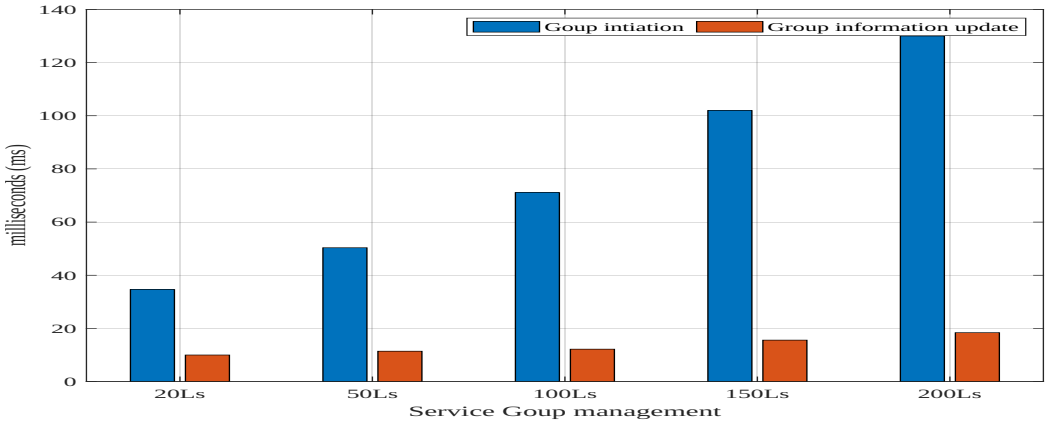


Figure 16. Service group management.

Table 4. Feature comparison with other frameworks.

Work Name	Proposed Solution	Computing Platform	Features	DDoS Proof
[12]	Blockchain-based EHR management system	Centralised	Security and Privacy management	No
[13]	Blockchain-based EHR management system	Decentralised	Privacy management	Yes
[14]	Blockchain-based EHR management system	Hybrid (centralised)	Privacy management	No
[16]	Blockchain-based quarantine management system	Partially decentralised	records sharing	No
[18]	quarantine records management system	Centralised	Data sharing	No
[19]	Blockchain-based records management system	Partially decentralised	Supply-chain management	No
[20]	Privacy-preserving and incentivized contact tracing for COVID-19	Decentralised	Privacy management	No
CoviBlock	Blockchain-based EHR security and privacy management system	Hybrid (de-centralised)	Privacy, security, traceability, scalability, anonymity, digital certificates	Yes

6.7. Reliability

We performed CoviBlock reliability analysis using different factors such as data confidentiality, integrity, availability, and privacy versus cost and usability. Our proposed system is cost effective while providing the blockchain services (Table 1). Further, it is con-

sistent while delivering dynamic services to different groups (Figures 15 and 16). Moreover, the availability of medical records is ensured by PBFT and the cache mechanism (Figure 14). When cost and dependability trends are noted, they are directly proportional to each other.

6.8. Limitations

Operational and access control aspects of the CoviBlock DDSS are vulnerable to 51% attacks. In order to keep the necessary real and legitimate devices, CoviBlock requires extra mechanisms. Larger user populations improve system performance; smaller user populations may not have the same advantages.

7. Conclusions and Future Work

CoviBlock is a proposal for a decentralised, distributed, intelligent healthcare support system. The proposed system facilitates the management of digital records by mitigating teams by providing traceability, transparency, and anonymity. The decentralised, distributed, blockchain-based DDRAC ensures data privacy and confidentiality. The proposed system-specific characteristics facilitate the digitalization of contact tracing, vaccination, and treatment (i.e., resource allocation and management). CoviBlock offers digital health certificate services to verify the patient's health status in order to expedite services. The system analysis demonstrated that the proposed DDSS-based digital medical records base services are more efficient than traditional blockchain-based H-CPSs. The CoviBlock allocates vital resources automatically based on real-time needs to optimise the mitigation process. In multiple respects, the proposed CoviBlock outperforms the blockchain-based non-DDSS H-CPS. The analysis of the system revealed that it is four times faster than a non-DDSS H-CPS and also extremely cost-effective. CoviBlock with DDSS and DDRAC managed system-level digital data privacy, transparency, and security without sacrificing usability. In the event of a future pandemic, the CoviBlock system can be further deployed to support the mitigation teams. In our future work, we intend to investigate the most efficient ways to incorporate lightweight federated learning into the CoviBlock.

Author Contributions: Formal analysis, B.S.E.; Investigation, B.S.E.; Methodology, B.S.E.; Project administration, A.K.P., K.S.S. and M.B.; Validation, S.G.; Visualization, B.S.E.; Writing—original draft, B.S.E.; Supervision, K.-S.K. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported in part by the National Research Foundation of Korea grant funded by the Korean Government (Ministry of Science and ICT)—NRF-2020R1A2B5B02002478), in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea Government (MSIT)—No. 2019001816, and in part by the Science and Engineering Research Board (SERB)—grant number TAR/2019/000286.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: Thank you for the support provided by the Wallenberg AI, Autonomous Systems and Software Program (WASP) and Kempe Foundation.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yu, L.J. Study on the impact and Countermeasures caused by International Public Health Emergency response measures–based on COVID-19. In Proceedings of the 2021 International Conference on Public Health and Data Science (ICPHDS), Chengdu, China, 9–11 July 2021; pp. 139–147. [CrossRef]
2. Sahraoui, Y.; Korichi, A.; Kerrache, C.A.; Bilal, M.; Amadeo, M. Remote sensing to control respiratory viral diseases outbreaks using Internet of Vehicles. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4118. [CrossRef]

3. Egala, B.S.; Priyanka, S.; Pradhan, A.K. SHPI: Smart Healthcare System for Patients in ICU using IoT. In Proceedings of the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 16–19 December 2019; pp. 1–6. [CrossRef]
4. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. iBlock: An Intelligent Decentralised Blockchain-based Pandemic Detection and Assisting System. *J. Signal Process. Syst.* **2021**, *94*, 595–608. [CrossRef] [PubMed]
5. Bilal, M.; Pack, S. Secure Distribution of Protected Content in Information-Centric Networking. *IEEE Syst. J.* **2020**, *14*, 1921–1932. [CrossRef]
6. Christodoulou, K.; Christodoulou, P.; Zinonos, Z.; Carayannis, E.G.; Chatzichristofis, S.A. Health Information Exchange with Blockchain amid Covid-19-like Pandemics. In Proceedings of the 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, CA, USA, 15–17 June 2020; pp. 412–417. [CrossRef]
7. Vangipuram, S.L.T.; Mohanty, S.P.; Kougianos, E. CoviChain: A Blockchain Based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems During Pandemic Outbreaks. *SN Comput. Sci.* **2021**, *2*, 346. [CrossRef] [PubMed]
8. Magid, E.; Zakiev, A.; Tsoy, T.; Lavrenov, R.; Rizvanov, A. Automating pandemic mitigation. *Adv. Robot.* **2021**, *35*, 572–589. [CrossRef]
9. Hussain, I.; Park, S.J. HealthSOS: Real-Time Health Monitoring System for Stroke Prognostics. *IEEE Access* **2020**, *8*, 213574–213586. [CrossRef]
10. Hussain, I.; Park, S.J. Big-ECG: Cardiographic Predictive Cyber-Physical System for Stroke Management. *IEEE Access* **2021**, *9*, 123146–123164. [CrossRef]
11. Bidkhori, Y.Y.H.; Rajgopal, J. Optimizing vaccine distribution networks in low and middle-income countries. *Omega* **2021**, *99*, 714–725.
12. Faroug, A.; Demirci, M. Blockchain-Based Solutions for Effective and Secure Management of Electronic Health Records. In Proceedings of the 2021 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 2–3 December 2021; pp. 132–137. [CrossRef]
13. Tahir, S.; Tahir, H.; Sajjad, A.; Rajarajan, M.; Khan, F. Privacy-preserving COVID-19 contact tracing using blockchain. *J. Commun. Netw.* **2021**, *23*, 360–373. [CrossRef]
14. Tan, L.; Yu, K.; Shi, N.; Yang, C.; Wei, W.; Lu, H. Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 271–281. [CrossRef]
15. Jabarulla, M.Y.; Lee, H.N. A Blockchain and Artificial Intelligence-Based, Patient-Centric Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications. *Healthcare* **2021**, *9*, 1019. [CrossRef] [PubMed]
16. Zhang, J.; Wu, M. Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine. *Electronics* **2020**, *9*, 1746. [CrossRef]
17. Hasanat, R.T.; Arifur Rahman, M.; Mansoor, N.; Mohammed, N.; Rahman, M.S.; Rasheduzzaman, M. An IoT based Real-time Data-centric Monitoring System for Vaccine Cold Chain. In Proceedings of the 2020 IEEE East-West Design Test Symposium (EWDTS), Varna, Bulgaria, 4–7 September 2020; pp. 1–5. [CrossRef]
18. Dell'Atti, S.F.G.D.V.; Tatullo, M. Blockchain in healthcare: Insights on COVID-19. *Int. J. Environ. Res. Public Health* **2020**, *17*, 853–865.
19. Manoj, M.; Srivastava, G.; Somayaji, S.R.K.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. An Incentive Based Approach for COVID-19 planning using Blockchain Technology. In Proceedings of the 2020 IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
20. Naren; Tahiliani, A.; Hassija, V.; Chamola, V.; Kanhere, S.S.; Guizani, M. Privacy-Preserving and Incentivized Contact Tracing for COVID-19 Using Blockchain. *IEEE Internet Things Mag.* **2021**, *4*, 72–79. [CrossRef]
21. Yong, B.; Shen, J.; Liu, X.; Li, F.; Chen, H.; Zhou, Q. An intelligent blockchain-based system for safe vaccine supply and supervision. *Int. J. Inf. Manag.* **2020**, *52*, 102024. [CrossRef]
22. Ranisch, R.; Nijsingh, N.; Ballantyne, A.; van Bergen, A.; Buyx, A.; Friedrich, O.; Hendl, T.; Marckmann, G.; Munthe, C.; Wild, V. Digital contact tracing and exposure notification: Ethical guidance for trustworthy pandemic management. *Ethics Inf. Technol.* **2020**, *23*, 285–294. [CrossRef]
23. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [CrossRef]
24. Xu, H.; Zhang, L.; Onireti, O.; Fang, Y.; Buchanan, W.J.; Imran, M.A. BeepTrace: Blockchain-Enabled Privacy-Preserving Contact Tracing for COVID-19 Pandemic and Beyond. *IEEE Internet Things J.* **2021**, *8*, 3915–3929. [CrossRef]
25. Lv, W.; Wu, S.; Jiang, C.; Cui, Y.; Qiu, X.; Zhang, Y. Towards Large-Scale and Privacy-Preserving Contact Tracing in COVID-19 Pandemic: A Blockchain Perspective. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 282–298. [CrossRef]
26. Bilal, M.; Kang, S.G. An Authentication Protocol for Future Sensor Networks. *Sensors* **2017**, *17*, 979. [CrossRef]
27. Bilal, M.; Kang, S.G. A secure key agreement protocol for dynamic group. *Clust. Comput.* **2017**, *20*, 2779–2792. [CrossRef]
28. Santhosh, B.; Pradhan, A.K. CoVID-19Block. 2022. Available online: https://github.com/BhaskaraSanthosh/Fortified-Chain (accessed on 1 December 2022).