Noname manuscript No.
(will be inserted by the editor)

iBlock: An Intelligent Decentralised Blockchain-based Pandemic Detection and Assisting System

Bhaskara S. Egala · Ashok K. Pradhan* · Venkataramana Badarla · Saraju P. Mohanty

the date of receipt and acceptance should be inserted later

Received: date / Accepted: date

Abstract The recent COVID-19 outbreak highlighted the requirement for a more sophisticated healthcare system and real-time data analytics in the pandemic mitigation process. Moreover, real-time data plays a crucial role in the detection and alerting process. Combining smart healthcare systems with accurate real-time information about medical service availability, vaccination, and how the pandemic is spreading can directly affect the quality of life and economy. The existing architecture models are become inadequate in handling the pandemic mitigation process using real-time data. The present models are server-centric and controlled by a single party, where the management of confidentiality, integrity, and availability (CIA) of data is doubtful. Therefore, a decentralised user-centric model is necessary, where the CIA of user data is assured. In this paper, we have suggested a decentralized blockchain-based pandemic detection and assistance system (iBlock). The iBlock uses robust technologies like hybrid computing and IPFS to support system functionality. A pseudo-anonymous personal identity is introduced using H-PCS and cryptography for anonymous data sharing. The distributed data management module guarantees data CIA, security, and privacy using cryptography mechanisms. Furthermore, it delivers useful intelligent information in the form of suggestions and alerts to assist the users. Finally, the iBlock reduces stress on healthcare infrastructure and workers by providing accurate predictions and early warnings using AI/ML.

Keywords Pandemic Detection and Control · Collaborated Medical Database (CMD) · Health Cyber-Physical Systems (H-CPS) · Artificial Intelligence (AI) / Machine Learning (ML) · Blockchain · Fog Computing

Bhaskara S. Egala
Dept. of Computer Sci. and Eng., SRM University-A.P, IN
E-mail: bhaskara_santhosh@srmap.edu.in

Ashok K. Pradhan (Corresponding Author)
Dept. of Computer Sci. and Eng., SRM University-A.P, IN
E-mail: ashokkumar.p@srmap.edu.in

Venkataramana.Badarla
Dept. of Computer Sci. and Eng., IIT- Tirupathi
E-mail: ramana@iittp.ac.in

Saraju P. Mohanty
Dept. of Computer Sci. and Eng., University of North Texas, USA
E-mail: smohanty@ieee.org

I Introduction

The outbreak of COVID-19 impacted people's health, livelihood, food system, and economy. With these circumstances, the healthcare system is facing enormous stress in terms of service capabilities. In addition to that, many are at risk of falling into the extreme poverty line. Moreover, industries are also facing a shortage of human sources due to the restrictions on mobility and continuous lockdowns. Short-term mitigation efforts like lockdowns and restrictions on mobility are not sustainable solutions for COVID-19 circumstances. That compelled us to find suitable long-term methods to handle immense cases with limited medical facilities. The latest research outcomes highlight the importance of real-time data and its role in the pandemic mitigation process.

Even the real-time data is increasing abruptly, its consistency and accountability are still doubtful. For instance, data censorship by the local governing body creates barriers to understand and predict the actual pandemic behaviour. Moreover, pieces of small valuable

information from huge people groups play a vital role in pandemic detection and mitigation. Even though enormous mobile computing facilities are available on personal gadgets, active participation in information sharing among the people is surprisingly minimal in the pandemic.

We can reduce the time and efforts required for mitigation efforts by adopting the latest technologies and smart healthcare system models [1–3]. Certain combinations can simplify the mitigation efforts like tracing of infected persons and their contacts, test sample tracking, and result-based treatment [4]. Furthermore, the smart healthcare system applications can enhance the efficiency of the complete process of 3T's (Trace, Test, and Treat) [5]. The governments of different countries adopted various technological approaches to limit the COVID-19 pandemic effect on people and their economic condition. For example, the developing countries are using mobile computing technologies to trace the infected or suspected people using people personal gadgets [4, 6–8]. Though these approaches are simple and easy to implementable, they are still server-centric models. As there is a necessity for a user-centric decentralised community-controlled platform, many researchers focused on blockchain-based solutions. In this work, we have introduced one such architectural solution named iBlock. The basic overview of the proposed iBlock architecture is illustrated in Fig.1. Moreover, it also showcases how different stakeholders are interconnected.

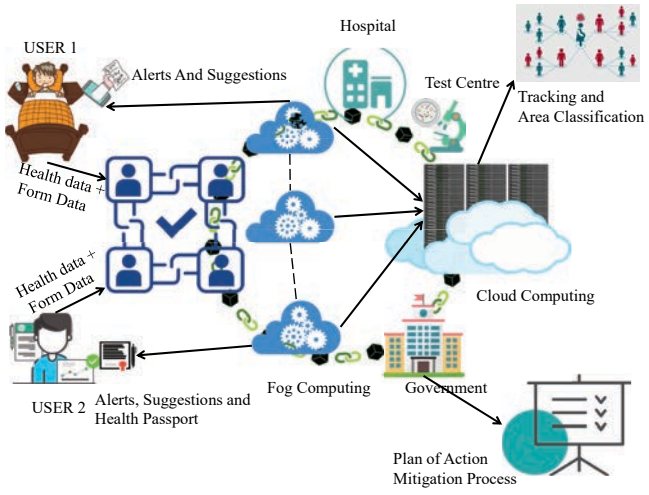


Fig. 1: The Overview of iBlock Architecture

Though 3T is considered as a thumb rule in the mitigation process still, it is infeasible in a real-time scenario without actual data [9]. Remarkably, developed and emerging countries are facing limitations in medical services due to the tremendous growth in infection rate and daily death rate [10–15]. Although the lock-down is mostly an adopted mechanism, but it creates lots of social and economic issues. Hence, most countries initiated the unlock process, which influenced the number of active cases respectively. Even post-pandemic people still live in the fears of new variants and infections. To overcome this situation a regular trusted information sharing and assistance is needed all the time [16,17]. In addition, real-time pandemic detection and alerting systems become fruitful when they implanted at the pre-pandemic stage or in the early stages. The timely preventive measures can eliminate the stress on the total healthcare system and similarly reduce the new infection. The major problem is the unavailability of timely ground-level data across the community and no proper preparations to mitigate the virus spreading. Due to this, there is a need for a detection and alerting system which runs in a collaborative environment where people can share the pandemic information transparently in real-time scenario. When an abnormality is identified at any point in any area, we can predict the outcome with the help of real-time ground data. The mitigation steps only become successful when transparent and tamper-proof data is available for all the stakeholders all the time.

Rest of the paper is organized ass follows: The contributions and challenges are discussed in Section II. Section III discuses the related works and real-time implementations of COVID-19 applying 3T process. We discussed the proposed system architecture and its working model in section IV. The core features of iBlock is discussed in Section V. The theoretical analysis is conducted in Section VI. The iBlock results are canvassed in Section VII and finally we discussed conclusion and future work.

II Contributions of the Current Paper

A. The Objectives in Current COVID-19 iBlock

i) Provides the data integrity and availability during the pandemic time to make the system more alert.
ii) Find out the areas where the existing systems or classical systems fail to detect the pandemic situation.
iii) Removes the drawbacks of the cloud-centric and third party controlled systems.
iv) Benefits smart health care systems with the help of edge and cloud computing fabrication.

B. Research Problems Addressed in the Current COVID-19 iBlock

i) The classical system drawbacks like centralized data processing, data immutability, and third party trust issues.
ii) The privacy and security issues in data sharing on decentralized healthcare systems.
iii) Scalability issues of blockchain in larger data storage and management.
iv) Integration of robust technologies like AI/ML with blockchain on Hybrid computing to provide defined services to users.

C. The Challenges in Solving Problem in the Current COVID-19 iBlock

i) The integration of blockchain with hybrid computing and AI/ML is a complex process.
ii) It provides CIA and privacy to data on the public distributed platform using blockchain and cryptography techniques which is an open challenge for researchers.
iii) Automate the basic alert and 3T operations using smart contracts is a simple process that lacks in dynamic processes.
iv) It leverages distributed data storage system and hybrid computing with blockchain and AI/ML demand knowledge in different domains like protocols, mechanisms, and standards.

D. Novel Contributions of the Current Paper

i) Proposed novel architecture model for pandemic detection and alerting using a blockchain called "iBlock". It supports sharing of real-time data utilization.
ii) The proposed system introduces suitable privacy and security mechanisms to cover system-level data privacy and security.
iii) Suggest a logical combination of blockchain and AI/ML on hybrid computing to support global level requirements in pandemic mitigation and alert the systems.

III Related Previous Works and Research Gaps

Present pandemic tracking and mitigation healthcare applications are fragmented in nature and limited to person, hospital, city, or at most one country level. Moreover, they are not suitable to detect and alert in real-time about pandemics like novel coronavirus (COVID-19), which requires human interference in data management and alert system. Few applications have shown very high accuracy in detecting infected people using identity information such as Aadhar cards information, phone number, and other personnel details. One of the successful applications in this category is the AI4COVID-19 app [18] which can detect the infection using patient cough patterns. The TraceTogether App [7] is used to track the patients whereas COCOVID [19] is developed to digitalize the mitigation efforts. MIT came up with PACT: Private Automated Contact Tracing [20] to automate the contact-tracing. Some of the other well known 3T supporting applications are Arogya Sethu [21] for contact tracing and treatment, ALHOSN [8] for sterilization of complete public utilities, etc. In addition to that, few other applications show their potentiality by using lung computed tomography (CT), scan reports, and facial images to determine the infection. Though these applications provide highly accurate results, despite that they lack people's trust and participation. However, more often people shared incorrect personal information for conducting tests and treatments to avoid contact tracing. Additionally, there is a fear of identity leakage, which affects mitigation efforts.

Few applications require continuous Bluetooth or WiFi connection to trace the contacts as well as for alerting. In our work, we suggest a pseudo digital identity that protects the user's personal information from leakage. In addition, it helps directly in conducting test, trace, treatment operations without revealing the personal identity. Moreover, with iBlock, we can provide free of cost assistance and alerting services without considering peoples detail like address, gender, status respectively. Some of the most essential features for a novel pandemic detection and alert system are privacy management, early detection, monitoring, alerting, area labelling, prediction and assistance [22] respectively. The main goal of these applications is to reduce the burden on the healthcare system and preventing the disease from spreading of infection. Another major issue affect the success of present Personal Digital Assistant (PDA) applications is the lack of transparency and privacy issues in personal health data utilization. Present applications are mostly cloud-centric, that introduce data privacy and data availability issues [23–25]. Also, applications require personal identity information for registration which has a high chance of leaking confidential personal information. The highlighted issues can be addressed with the help of blockchain and access control mechanism. The Blockchain guarantees data integrity using public ledgers and data availability. Research works like CoviChain [26], GlobeChain [27] showcased how to incorporate blockchain technology in

the pandemic mitigation process. Moreover, blockchain eliminates the central server or controlling authority role in information sharing. However, like any other technology, blockchain has its own limitations like low storage capability, high processing cost and time. The leveraging of blockchain and InterPlanetary File System (IPFS) eliminates the mentioned limitations [28].

IV Architecture of the Proposed iBlock

A. Overview of iBlock

The proposed architecture collects the information from multiple personal health cyber-physical systems (H-CPS) and gadgets. Also, iBlock provides a simple web-based API to interact with the blockchain-based CMD networks. The collected user health data is validated before publishing to the local CMD repository. Simultaneously, hybrid computing performs data preprocessing, analytics, and AI/ML operations. The collected user data is identified and aggregated using a pseudo digital identity generated from a random number generator. The iBlock prevents accidental and forced modifications once its added to CMD with the help of public ledger. Due to this, the system guarantees data usage transparency. As shown in Fig.2 Blockchain creates a public ledger for every transaction with the help of the hash tree (Merkle tree). Likewise, IPFS store files and create its URL using the hash tree. Therefore, the fabrication of Blockchain and IPFS becomes easy and forms a CMD network. In Blockchain, every block contains a unique set of transactions, whereas, in iBlock, every file URL on CMD is considered as transaction data for block creation. IPFS file system divides the larger file into smaller chunks and stores it on the distributed peer-to-peer (P-2-P) network on hybrid computing. Subsequently, it creates a file hash and returns it as a file accessing address on the P-2-P storage network. Comparatively storage capacity of blockchain is limited concerning IPFS for that reason we have only considered file hash values and their address in the ledger to make the queries faster and simple.

The iBlock architecture logically divided into three layers: such as data collection layer, AI/ML layer, and alert or suggestion making layer. Fig. 3 illustrates iBlock elements and their flow of operations. The first layer consists of different healthcare sensors, H-CPS, and other personal gadgets. The gateways receives the data and validates its integrity and authenticity before considering it for AI/ML modules. The second layer receives raw data and performs preprocessing and analysis. After that, iBlock can able to count newly infected cases, and death cases in a particular area. Besides this,

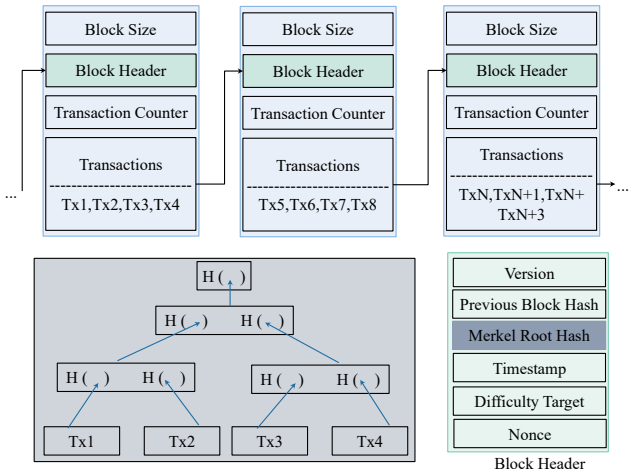


Fig. 2: Overview of Blockchain Ledger Creation or Blocks Creation Process

the processed data-set is handed over to AI/ML module for prediction and alert generation process. Subsequently, area-labelling is performed based on two factors: one is for confirmed events and another one is for prediction events. Afterwords, the data is divided into two sub-datasets to cope with data privacy. The first data sub-dataset contains confidential information with all necessary medical data for services. While the second data sub-dataset contains pseudo-identity with the non-personal information. In addition, both sub-datasets are encrypted with different keys before storing on CMD. The sub-dataset with personal information is encrypted with the user's public key followed by the hybrid computing system's private key. The non-personal information is published to global CMD in an encrypted format using a system's private key.

We combined random forest (RF) and support vector machine (SVM) to achieve distributed machine learning classifier. The outcomes from this classifier are used to generate alerts and suggestions. Moreover, iBlock allows only known organizations to share its information and and allow to hybrid computing along with its AI/ML modules. Hybrid computing combines both fog and cloud computing paradigms to achieve higher scalability and lower latency. The AI/ML module is distributed among all nodes in hybrid computing over the blockchain CMD networks. We have chosen IPFS technology to eliminate the storage limits of blockchain.

The various steps required for generating a health passport for users is illustrated in Fig. 4. Additionally, it showcases the iBlock internal modules fabrication in an abstract form. The overall process starts with AI/ML user risk group calculation. It undergoes various steps

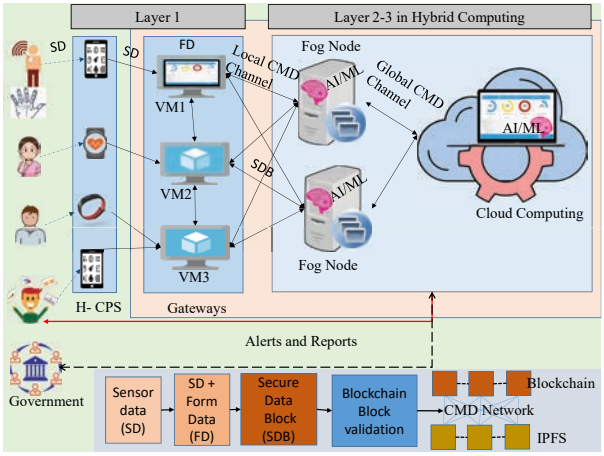


Fig. 3: Overview of iBlock in Layered Architecture

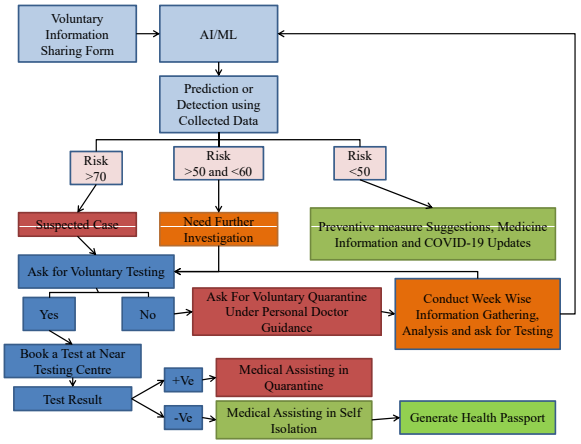


Fig. 4: Overview of the Proposed System Internal Flow

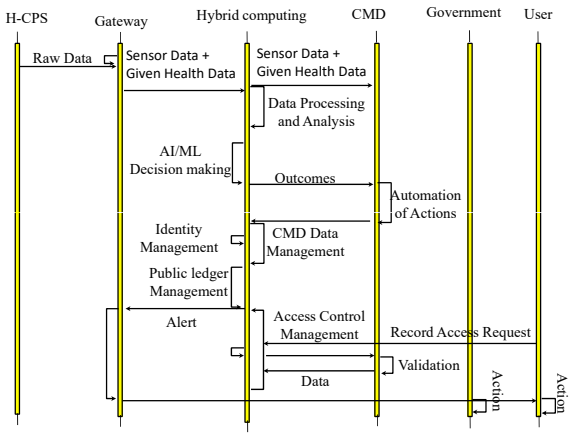


Fig. 5: Overview of iBlock Logical Operational Flow

to divide users into the suspected group and risk-free group. Thereafter, it initiates group-specific services like health passport generation for the risk-free group. Further, a simplified iBlock operational flow is depicted in the Fig. 5. The logical operational flow of iBlock showcases how events of the proposed system trigged. The raw data generated by H-CPS transferred with signature to nearest gateways or personal health devices. Thereafter, the gateway validates the signature of the sender for data aggregation. Afterwards, receiver validates data integrity before considering it for the system usage. In addition, it appends additional health data which is received from users to the sensor data. The appended data further handed over to the nearest fog node for data processing and analysis in an encrypted format. Concurrently, the data is written to the local CMD network. The outcomes from AI/ML from the data is used to generate alerts using blockchain smart contracts (chain code). In hybrid computing, AI/ML decision-making system generates the outcomes from the user data. The AI/ML modules are trained and optimised with early limited pandemic datasets in a supervised learning environment.

Hybrid computing performs critical operations such as identity management, CMD data management and public ledger management, respectively. The iBlock access control records are distributed on the CMD network with the help of blockchain and IPFS. The access rules are updated regularly on the CMD for data transparency. Proposed iBlock either allows or denies the request based on the access credentials provided by the actors and devices. If an unauthorised access request is identified then the user is alerted about the event and a threshold value is incremented by one. The access control system blocks the device from accessing the data when a threshold value is four. The user can attempt 4 times within 5 minutes, if it is failed then the device is blocked. If the blocked device tries again the system adds another 5 minutes every time. Even after trials, if the requester failed another time then the system will blacklist the device for the next 24 hours. The iBlock provides access for authorised user to CMD network followed by the required data in an encrypted format. Moreover, it shares decryption key along with file address as a response. The prediction from AI/ML modules is broadcast to all the gateways in that area for planning mitigation activities.

The local CMD layer contains a complete dataset whereas the global CMD contains selected non-personal sub-set in a secure format. The AI/ML modules in hybrid computing perform infection detection, alerts generation, and assistance operations. Blockchain technology takes care of ledger maintenance. Based on the area

classification, the proposed approach suggests preventive measures to the users. Cloud computing performs global level operations required for mitigation efforts and provides a health passport to the user without revealing the user personal identity.

B. Operational Model

To avail the services, the user needs to install and register the iBlock mobile application on their gadgets. The application creates a unique pseudo digital identity using device configuration and environmental information for uniqueness. Later, iBlock uses this pseudo identity for user identification and system activity. Fig. 6 illustrates iBlock working flow, where the H-CPS generates and passes the data to the nearest gateway. The gateway or user device adds additional metadata required for prediction and area labelling. Thereafter, the encrypted data is handed over to the fog computing device for data processing and prediction. The sub-dataset of non-personal information is pushed to the cloud for data analytics and area labelling.

The AI/ML intelligent module receives the data and generates predictions. User risk group classification is done based on user age, living style, symptoms and severity. Besides this, user also includes the duration of suffering, number of days passed from primary symptoms and their area details. The iBlock categorises users into three groups a low-risk group, moderate-risk group, and high-risk group using AI/ML module. A person falls into a high-risk group when the prediction value is 70% and above. In such cases, iBlock changes the user profile status to a highly suspected group and encouraged for volunteer testing. If the person accepts the request, iBlock automatically registers and reserves a test slot using the user pseudo digital identity.

C. Cryptographic Methods for iBlock

The proposed cryptographic methods use a robust encryption algorithm known as Elliptical Curve Cryptography (ECC) with a key size of 256 bit. The following subsection gives an overview of iBlock security and privacy methods. We introduced a lighter mutual authentication and validation mechanism to eliminate third-party servers interference. The overall crypto-process is divided into two stages: known as registration and validation. Every element in the architecture generates individual public and private key pairs using the system-level ECC curve parameters suggested by the iBlock application. The registration sub-process generates a service identity (SID_{node}) and a mutual authentication token (MAT_{node}) for every participating device.

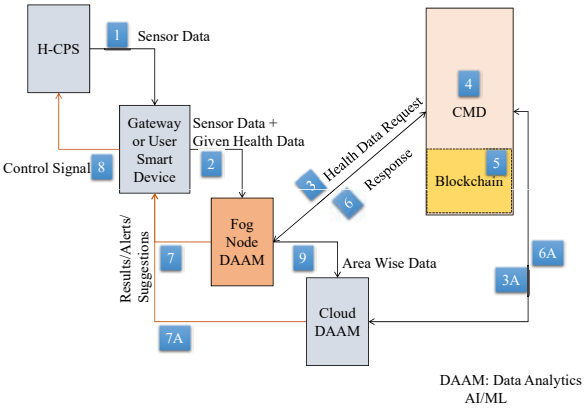


Fig. 6: Overview of the Proposed Systems Working Flow

Whereas, in the validation sub-process, all registered devices can use individual mutual authentication tokens (MAT) to prove their identity on the iBlock without any interference of third party.

The registration sub-process starts with a simple registration request from the participating user device. In the initial phase user device (node) sends a registration request by adding its node identity (N_{type}) and its public key (Pub_N) to the hybrid computing. The nearest fog node receives the request and acknowledges the communication. In the next stage, hybrid computing provides the registration identity (R_{ID}) and register node public key (Pub_{fog}) for the device in an encrypted form. The fog computer also generates H(R_{ID}), R_{ID} and group identity (G_{ID}) for each device and maintains a registration record on local CMD network. A service identity (SID) is allotted for easy device-service management. In the next stage, the H-CPS transmits sensor data with SID, MAT and public key in an encrypted format to the nearest fog node. The user devices validate before allowing them to participate in iBlock with the help of the device validation sub-process. Simultaneously, the iBlock data privacy and confidentiality is managed by the data access control and privacy management module. The data access rules are generated by the hybrid computing under the supervision of data owners. The above mentioned cryptography mechanisms are explained in the following subsections.

a. Unique Pseudo Digital Identity Generation

Pseudo digital identity generation function $f()$ takes two set of parameters. One set of values represent H-

CPS device type, public key, and user non-personal data. The other set of parameters consist of environment variables like humidity, temperature, sound, light, etc. to add randomness to the function. The first set of values are static values whereas the other set values are dynamic in nature. The function $f()$ is an one-way function so that the relation between the inputs (x,y) and outputs (z) are eliminated so that the intruder may not get knowledge about input. Fig. 7 depict the total process of unique digital identity generation.

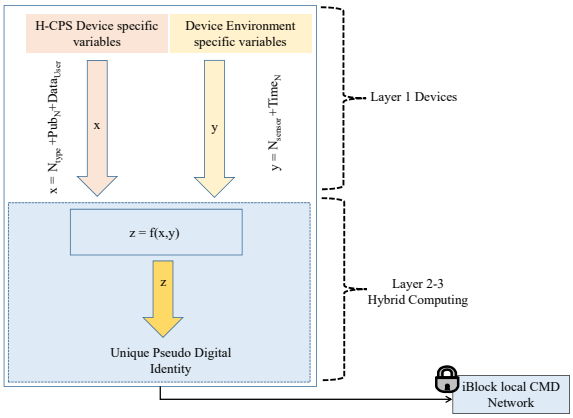


Fig. 7: Unique Pseudo Digital Identity Generation Function

b. The Device Validation and Data Uploading

i) The user H-CPS or personal smart device approaches the hybrid computing for its authenticity validation process. The overall process starts with simple unique identification values exchange between layer two and layer one devices as described previously. When the SID, R_{ID}, and MAT are valid then hybrid computing allows the device to participate in iBlock network otherwise it does not allow the devices to participate. In the next stage, layer one devices generate health data and converts it into an encrypted form like $E(Pub_{fog}, [R_{ID}, SID, Data, MAT_A])$. Here, the "$Data$" represents combination of two datasets and service information. The "$Data$" is represented as $[[U_{ID} \oplus SID] \oplus Token]$. For Initial step the token value is set to 1 and for every communicating sequential processes the value is increased by 1.

ii) The nearest fog node receives and decrypts data with its private key and also validates sender's MAT before considering for AI/ML module. Simultaneously, it stores the data on respective CMD networks ones the sender identity and data integrity is validated.

iii) For an authorised sender, hybrid computing responds with a acknowledgement (ACK) as "$E(SID, Token + 1 \oplus U_{ID}, AccessRuleTable_{ID})$". The ACK contains communication token value, and $AccessRuleTable_{ID}$ which are required for data access control management. The communication tokens are generated with the help of a random number generator. In order to upload the data, a secret message decryption key $Secret\_Key$ is generated and shared with the sender.

iv) Device uploads the data in an encrypted format as "$E(Pub_{fog}, E(SID_{device}, Data) \; ||SID_{device}, Hash(Data), Timestamp, Token)$" and terminates the communication to save energy.

v) Hybrid computing validates the data integrity and also preforms system specific data analytics to provide service to the users.

c. Access Control and Privacy Management

i) The hybrid computing stores the personal sub-dataset with pseudo identity on local user centric CMD network. Where as, the non-personal sub-dataset pushed to global CMD network, where the personal sub-dataset is isolated from public access.

ii) The local CMD data is encrypted with the help of two different encryption keys. Only users with $Secret\_Key$ and access rights are allowed to view or download the data from CMD networks.

iii) The "$AccessRuleTable_{ID}$" accessing key $Secret\_Key$ is generated with the help of a true random number generation module and shared only with an authorised devices.

d. Access Rule Generation Process

i) The access rules are generated and represented in the form of "$AccessruleGenerate(actor, AccessRuleTable, U_{ID})$". Here, it generate new rule by user pseudo identity, targeted audiences identity and access rights. In a situation when data access is questioned the access control mechanism verify the requester rights in $AccessRuleTable$. If the requester identity is not equal to data creator identity ($actor_{ID} \neq U_{ID}$) then it sets new permissions for requester $SetPermissions(AccessRuleTable)$ and adds them to access rule table using $Add(G_{ID}, actor_{ID}, Permissions, U_{ID}, Data)$.

ii) Every request is validated using local cache of $AccessRuleTable$ for faster response. If the cache

is not available in local CMD, then it searches in the global CMD network for access rules. The initial process takes more time as compared to later processes because of cache unavailability.

iii) The hybrid computing takes care of *AccessRuleTable* update management on blockchain-based IPFS CMD network.

V The Core Features of iBlock

A. Early Detection

The proposed system encourages people to use their health data anonymously in the pandemic detection and mitigation process. The detection module identifies the specific pattern to classify whether it is positive or negative based on the symptoms. Further, the collective area wise information is considered for AI/ML pandemic detection engine as testing data. The iBlock AI/ML engine predictions are validated manually by the medical specialist's group before broadcasting to local people as an alert. The overall data collection and analytics are conducted automatically without any delay. Therefore mitigation teams can prepare with mandatory steps to control the infection. Proposed system shares real-time pandemic information to the people as a reward for their contribution. In addition to that, it provides suggestions to limit the virus from spreading in their locality.

B. Monitoring People's Health to Design Sustainable Healthcare Solutions

The majority of pandemic detection and alerting systems are limited to prediction and alert, meanwhile iBlock further simplifies the area-labelling to prepare area wise mitigation mechanisms. Moreover, iBlock maintains all crucial data on the blockchain for future sustainable healthcare solutions. The area-wise information used to speed up the mitigation process with suitable methods in a shorter span. It also provides different views of local people health and living style.

C. Area Classification and Contact Tracing

The classification of areas helps the government and healthcare organizations to plan sustainable preventive measures in a real-time scenario. Our proposed system classifies the locations as green, brown and red zones based on the number of confirmed cases and prediction cases in real-time scenario. The iBlock uses pseudo-identity in tracing the suspected or infected people and contacts. However, the true identity of the respective persons not revealed throughout the process. The number of confirmed cases and suspected cases considered to mark areas as a low-risk zone or medium risk zone or else a high-risk zone.

Algorithm 1 Dataset Preparation and Area Classification

Input: dataset,features, and labels
Output: area classification, accuracy

```
Function inputFile():
    Read input csv file using pandas.read_csv()
      Jumble dataset order
      Divide dataset into features and class labels
      Convert the scale of the feature vectors between 0 and 1
      return Features, Class Labels
Function labelArea():
    Define K, X, C and Type of SVM_kernel.
      Define Labelling_Accuracy = []; i = 0;
      while i<K do
        Randomly select 'C' cluster centers
          Split dataset into two sets A,B for training and validation
          Define parameters = [C, X]
          Instantiate Clustring for [pipeline=SVM_kernel, parameters]
          Train model on A
          Test model on B
          Store result in Labelling_Accuracy.
          i = i + 1;
    Compute average clustering accuracy of all vector files.
      return avg_Labelling_Accuracy
```

The Algorithm 1 showcases the pseudo algorithm system use in area classification. The function $inputFile()$ takes the complete dataset from local CMD in .csv format using "pandas" python library function. It divides the dataset into features and classes for system training and testing. Whereas, $labelArea()$ function performs the feature and class mapping in a recursive manner using SVM_kernal. Finally, it returns the algorithm accuracy for the given test dataset.

D. Prediction of Future Cases

The prediction of new cases and death rates computed with the help of a dedicated AI/ML detection engine module. In the iBlock, the computation of rates depends on local CMD data that helps the government to make proper mitigation plans with limited healthcare infrastructure. Besides, it also helps the drug and vaccination manufacturing and supply chain to scale up its capabilities for future purposes.

E. Reward and Fake Data Detection Mechanism

To motivate the people to share legitimate data, the proposed model suggests a reward mechanism to influence the number of participants. The reward con-

tains two types of benefits. Firstly, the user will get real-time pandemic information on time with no additional charge. Secondly, the users are rewarded with some health tokens for every accurate information. In due course of time, the patients can use these health tokens to get discounts for clinical testing, purchase of medicines and any other treatment.

The fake data is excluded before publishing new data to local CMD using AI/ML. The proposed system compares and clusters the incoming data based on the local CMD data. The clustering mechanism is associated with specific area information and its risk zone. The new data is flagged as false if it deviates more than 50% from the CMD data and trained dataset. If any user continuously sends contradictory information for earning health tokens such users are prohibited for the next 24 hours. Finally, user will get remaining services such as safety tips and medical facility details in the nearest location with a warning message.

In iBlock, we proposed a novel blockchain-based intelligent framework to cope with pandemics like COVID-19 data management. The additional features of iBlock are outlined as follows: identifying high-risk zones, creating awareness about preventive measures. The classification of highly affected areas helps the mitigation teams to simplify the national disinfection program also simplify test reports and assigning temporary medical facility management.

F. Development and Deployment of Drugs and Vaccines

Transparent drug manufacturing and distribution is possible only with the help of global CMD and blockchain ledger. The iBlock with blockchain prevents data forgery and accidental modifications to bring transparency in the drug and vaccines development process and distribution. It also gives confidence to the people about the drug or vaccination effectiveness which can encourage the voluntary vaccination process.

G. Providing Health Passport

The proposed model provides a global level health passport by verifying vaccination information on local CMD. A unique pseudo digital identification is embedded into the digital health passport to avoid personal information leakage. A health passport assures people vaccination status, which provides various benefits like self-certification of no COVID-19 history, allow people into public places, and also work from offices. The process overview of getting a health passport illustrated in Fig. 5. A blockchain-based zero-knowledge protocol is used to verify the health passport validity using user pseudo-identity.

VI Analysis of the iBlock

We have deployed our test-bed on a local virtual system network on VMware Workstation with five ubuntu systems. All virtual systems are configured and connected through a blockchain-based IPFS network. Three high-end systems are configured as hybrid computing (layer 2-3) and reaming two systems with lower configuration is assigned for user-end devices and gateways (layer 1).

A. Threat Analysis

Data security and privacy are the major concerns for a decentralised smart healthcare system where a patient's medical data resides on an untrusted network. We demonstrated the security capabilities of our system with the following theorems.

Theorem 1 *Assume that intruder got access to local CMD network without the fog computing access permission, such intruder fails in retrieving original data from the network.*

Proof : Our proposed system encrypts the data before storing it into the CMD network. Moreover, the encryption keys nowhere stored on a hybrid computing network. Further, the data don't have any direct relation with individual personal identity. Hence, the attacker does not know the data belongs to whom. Therefore, the intruder left with only a brute-force attack which requires high computational capability and time. The access control system blocks the requester device from accessing the plain data from the CMD network upon a threshold value of four continuous failed attempts in 5 minutes. If the blocked device tries again within the time then it adds another 5 minutes for every unsuccessful attempt. Even if the requester has failed once again after a specified time interval then the system will blacklist the user device for the next 24 hours. Also, blockchain-based ledger modification attacks are infeasible in a limited time. Therefore, an intruder can't guess the data on CMD as well as the decryption keys.

Theorem 2 *Even though the intruder is successful in getting SID, U_{ID} over a communication channel, then also it is difficult to compromise the access control system to retrieve the user data.*

Proof : The iBlock uses two different methods to prevent man-in-the-middle attacks. Firstly, sensors use the token number in every communication to detect duplicate communication which is known only to the partic-

ular sender and receiver. Moreover, the token mechanism varies from communication to communication in the same network to create confusion to intruders about the tokens. Secondly, an intruder has to guess the secret device identity and its key to upload the forgery data or fabricated data which are only known to the respective device. In that case, if the device is compromised then only it is possible to know the device-specific details. Therefore, our system is secure from man-in-the-middle attacks.

B. Discussion

i) Security: iBlock protects all its communications over transmission with the support of Datagram Transport Layer Security (DTLS) and ECC data encryption algorithm [29] to provide data confidentiality in the transport layer. At the same time, it prevents man-in-the-middle attacks. Hyperledger fabric insists only on authorized organizations which can participate in blockchain operations.
ii) Privacy: iBlock guarantees data privacy with a system-specific access control mechanism called "*AccessRuleTable*" and public-key cryptosystem. Hybrid computing can only store the data on the CMD network but does not have adequate control over its access rules. This mechanism helps the system in maintaining transparency in privacy management. In addition to that, the sensitive data is detached from the cloud-based CMD.
iii) Immutability: The data on the CMD network is tampered-proof and immutable against accidental or malicious modifications. The traditional systems are vulnerable to data modification attacks like accidental or malicious changes in the transmission and storage. The blockchain-based ledger system protects the data integrity on CMD network. Moreover, every data is signed before it is transmitted to the other device to give additional protection against the data modification attacks.
iv) Availability: As our proposed system uses a decentralised distributed blockchain-based CMD mechanism on hybrid computing, which guarantees the data availability all time at multiple levels with integrity. In traditional models, the data is stored in a central location that may affect the data availability.

VII Experimental Results

We have created an iBlock testbed with five virtual systems as illustrated in Fig. 3. The system configurations suggested for the testbed are specified in Table 1. Concurrently a simplified web user interface is provided for easy access to the smart contracts (chain code) on the Blockchain. The symbols and notations used in iBlock are given in the Table. 2. The complex AI/ML and hybrid computing operations are relocated to high-end systems whereas the remaining low-end systems are dedicated for layer one. All devices are interconnected through a virtual local area network (VLAN). The hybrid computing nodes cluster combinedly take the iBlock operational load such as CMD network management, access control management, and AI/ML decision making. The data hash is committed to the Blockchain ledger once it is written to IPFS in order to maintain data integrity and transparency. The Algorithm 1 labels every area either a green zone (safe) or orange zone (moderate risk) else a red zone (high risk) based on the new cases and death rate. We have considered a publicly available COVID-19 dataset [30] for system evaluation. Also, we assumed few parameter values as shown in the Table. 4 based on the theoretical calculations from the data. Based on the above parameters and their values we built a distributed AI/ML classifier using a random forest (RF) and support vector machine (SVM). We have showcased our AI/ML classifier accuracy with respect to the considered dataset in Table. 3. The testbed execution contains two logical operations one for Hyperledger fabric execution to form a CMD network and another one for hybrid computing. Fig. 9 and Fig. 10 represents hyperledger fabric execution followed by Blockchain ledger creation process. The first experimental screenshot (i.e Fig. 9) shows how the organizations are enrolled on blockchain and how chain codes are deployed in iBlock. The next figure (i.e Fig. 10) illustrates the overview of the Blockchain network of iBlock at that time. It provides details such as the number of blocks in the chain, transactions, nodes, smart contracts. Whereas, Fig. 11 presents details of a newly created block such as block-hash, timestamp, previous-hash, data-hash, number of transactions.

From the experimental analysis and mathematical calculations we came up with as simplified results as presented in Fig. 8. We have also calculated the worst-case values when 0.1% of infected people have survived from the infection as shown in Table. 5. From the theoretical analysis, we understand that at least 1500 infected people per million cases can be saved with the help of iBlock. The projected values are determined based on the available data till December 2020 using

the following expressions:

$$TDC = \sum_{n=1}^{N} \frac{No.of\ Fatality}{No.of\ Cases} * 100 \quad (1)$$

$$LSDC = \sum_{n=1}^{N} \frac{TDILS}{NCILS} * 100 \quad (2)$$

$$LTC = \sum_{n=1}^{N} \frac{TDILT}{NCILT} * 100 \quad (3)$$

$$\frac{dD(t)}{dt} = \imath\,\gamma\, I(t) + f\,\varepsilon\, C(t) \quad (4)$$

$$R_t(t) = \frac{(1 - SD(t))\beta}{\delta} \left(1 - \frac{\int_t^0 \alpha(t) S(t)}{N_{pm}}\right) \quad (5)$$

Table 1: Basic Configuration Details for iBlock Test Environment Setup.

System Details	Cloud	Fog nodes	VM nodes
System Hardware Configuration	12 GB RAM, 90 GB HDS, 2 Core CPU	12 GB RAM, 90 GB HDS, 2 Core CPU	8GB RAM, 50GB HDS, 1 Core CPU
Fabric Images	1.4+	1.4+	1.4+
Docker Swarm Identity Composer Version	1 1.13+	2 1.13+	3 1.13+
Node Version	8.6+	10.5+	10.5+
Operating System (Ubuntu)	16.04 LTS	18.04 LTS	18.04 LTS

Table 2: Symbols and Notations.

SYMBOL	ABBREVIATION	SYMBOL	ABBREVIATION
TDC	Cumulative Death Conversion	TCD	Total Cumulative Deaths
TCC	Cumulative Cases	LSDC	Last Seven days Death Conversion
TDILS	Total Deaths in Last 7 days	NCILS	New Cases in Last 7 Days
LTC	Last 24 hour Conversion	TDILT	Total Deaths in Last 24 hours
NCILT	New Cases in Last 24 Hours	CCPOM	Cumulative Cases Per One Million
CDPOM	Cumulative Deaths Per One Million	U_{ID}	User identity
$\frac{dD(t)}{dt}$	Death Rate	$R_t(t)$	Reproduction Number
N_{pm}	Events Per Million	$SD(t)$	Social Distancing Parameter
α	Protective Rate	β	Mean Infectious Rate
$\imath$	Died With No Treatment	C	Critical state
γ	Latent Mean	ε	Critical Cases Mean
$I(t)$	People with Infection at Time t	$f(t)$	Fraction of Critical Patients will Die
δ	Contagious	$S(t)$	Susceptible

We have calculated the survival rate and our AI/ML model accuracy using the data published from December 2019 to the 2020 year-end. We observed that total cumulative deaths are proportional to new cases in the last 24 hours. We have provided calculated mortality rates for a chosen set of countries and presented them in the table. 4. A SUEIHCDR mathematical model [31] is used to design an AI/ML prediction model to find out the respective survival rates for each county. We have considered various parameters like total death conversion rate, last seven days death rate, and last 24 hours death rate in our prediction model. Fig. 8 illustrates the relationship between parameters and their respective countries for the COVID-19 first wave period. Our experimental and theoretical analysis highlighted the necessity of a system like iBlock in the COVID-19 mitigation process by digitalising complex 3T processes in real-time. The input data undergoes feature extraction and scaling before clustering, based on the feature labels. We have combined random forest (RF) and SVM (Hybrid Classifier)to implement distributed prediction capabilities. The hybrid showed us it is more accurate than individual classifiers.

Table 3: Comparison of Hybrid classifier with SVM for 2-class.

Model	**Accuracy**
MLP	77.50
SVM(RBF kernel)	82.93
SVM(RBF kernel) with noise	83.74
Hybrid Classifier(RBF kernel)	82.95
Hybrid Classifier(RBF kernel)	84.89

Table 4: World Health Organization (WHO) Public COVID-19 Data [30].

	CCPOM	NCILS	NCILT	TCD	CDPOM
USA	56340.91	1334155	145489	328014	990.97
India	7382.48	156627	18732	147622	106.97
Brazil	35042.25	285582	22967	190488	896.16
Russian	20901.49	201871	28284	54778	375.36
France	38415.77	89093	2458	62197	952.87
UK	33232.31	251786	34693	70405	1037.11
South Africa	16775.13	82434	11552	26521	447.17

Table 5: Predicted Survival Rate Based on Available Data.

	LSDC	LTC	CDPOM	0.001%	0.01%
USA	0.01264	0.011629	0.000175	328.014	3280.14
India	0.01369	0.014894	0.000144	147.622	1476.22
Brazil	0.01694	0.020986	0.000255	190.488	1904.88
Russian	0.01941	0.019516	0.000179	54.778	547.78
France	0.02417	0.059397	0.000248	62.197	621.97
UK	0.01322	0.006053	0.000312	70.405	704.05
South Africa	0.02404	0.021208	0.000266	26.521	265.21

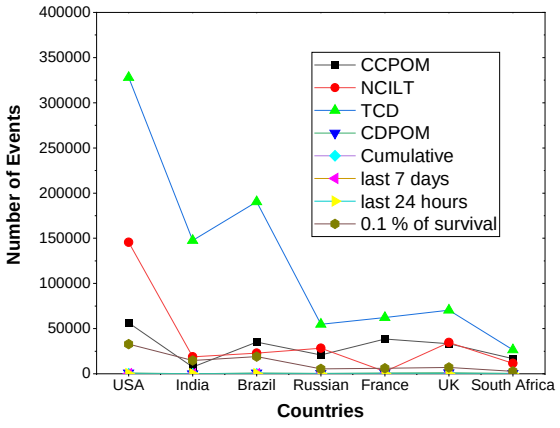


Fig. 8: The Most Affected Countries with Predicted and Survival Values.

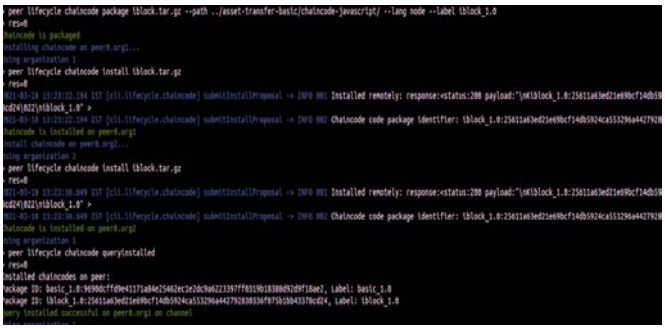
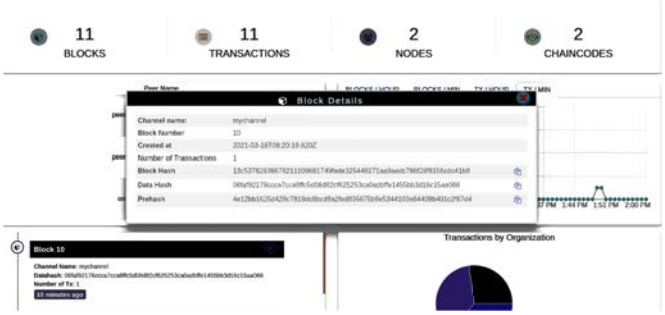


Fig. 9: iBlock execution process on VM1 Command-line Interface.



1

Fig. 10: iBlock ledger information in Hyperledger Explorer

Fig. 11: Block information of iBlock on Test-bed

VIII Conclusion and Future Directions

A decentralised iBlock model helps the pandemic mitigation teams by eliminating the stress on the medical infrastructure by providing real-time pandemic information with future predictions. The iBlock guarantees data immutability and its CI on CMD with the help of Blockchain and system-specific cryptography mechanisms. The data availability is guaranteed by hybrid computing and robust Blockchain IPFS fabrication distribute storage process. AI/ML on hybrid computing performs area wise labelling that helps the mitigation teams to focus on high-risk zones with required medical resources. Also, iBlock protects personal identity from leakage by replacing it with pseudo-identity when sharing health data over CMD. Moreover, iBlock helps in predicting the survival rate and death rate that directly affects the ongoing mitigation process and drafting plans. The disubstituted nature of this system eliminates the single point of failure and third party control on user data. This mechanism helps the system to achieve a good response from the people. In addition to that, it minimizes the dependency on third-party cloud computing services. In future work, we are planning to improve the system capabilities to predict future infections by combining two waves data and unsupervised prediction mechanisms.

Compliance with Ethical Standards

The authors declare that they have no conflict of interest and there was no human or animal testing or participation involved in this research. All data were obtained from public domain sources.

Acknowledgment

The Authors would like to thank the Science and Engineering Research Board (SERB) for supporting this work, Grant number TAR/2019/000286.

References

1. B. S. Egala, S. Priyanka, and A. K. Pradhan, “Shpi: Smart healthcare system for patients in icu using iot,” in *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2019, pp. 1–6. [Online]. Available: doi:10.1109/ANTS47819.2019.9118084
2. A. M. Joshi, U. P. Shukla, and S. P. Mohanty, “Smart healthcare for diabetes: A COVID-19 perspective,” 2020. [Online]. Available: arXiv:2008.11153 [q-bio.OT]
3. B. S. Egala, A. K. Pradhan, V. R. Badarla, and S. P. Mohanty, “Fortified-chain: A blockchain based framework for security and privacy assured internet of medical things with effective access control,” *IEEE Internet of Things Journal*, vol. Online first, pp. 1–1, 2021. [Online]. Available: doi:10.1109/JIOT.2021.3058946
4. R. Ranisch, N. Nijsingh, A. Ballantyne, A. van Bergen, A. Buyx, O. Friedrich, T. Hendl, G. Marckmann, C. Munthe, and V. Wild, “Digital contact tracing and exposure notification: ethical guidance for trustworthy pandemic management,” *Ethics and Information Technology*, vol. Online first, pp. 1–1, Oct. 2020.
5. M. A. Qamar, “COVID-19: a look into the modern age pandemic,” *Journal of Public Health*, vol. 4, pp. 1–6, May 2020.
6. A. K. Tripathy, A. G. Mohapatra, S. P. Mohanty, E. Kougianos, A. M. Joshi, and G. Das, “EasyBand: A Wearable for Safety-Aware Mobility During Pandemic Outbreak,” *IEEE Consumer Electronics Magazine*, vol. 9, no. 5, pp. 57–61, Sep. 2020.
7. H. Stevens and M. B. Haines, “TraceTogether: Pandemic Response, Democracy, and Technology,” *East Asian Science, Technology and Society: An International Journal*, vol. 14, no. 3, pp. 523–532, Sep. 2020.

8. R. Abbas and K. Michael, "COVID-19 contact trace app deployments: Learnings from australia and singapore," *IEEE Consumer Electronics Magazine*, vol. 9, no. 5, pp. 65–70, 2020.
9. Y. Ji, Z. Ma, M. P. Peppelenbosch, and Q. Pan, "Potential association between COVID-19 mortality and healthcare resource availability," *The Lancet Global Health*, vol. 8, no. 4, p. e480, Apr. 2020.
10. A. Remuzzi and G. Remuzzi, "COVID-19 and Italy: what next?" *The Lancet*, vol. 395, no. 10231, pp. 1225–1228, Apr. 2020.
11. K. Dhama, S. Khan, R. Tiwari, S. Sircar, S. Bhat, Y. S. Malik, K. P. Singh, W. Chaicumpa, D. K. Bonilla-Aldana, and A. J. Rodriguez-Morales, "Coronavirus Disease 2019-COVID-19," *Clinical Microbiology Reviews*, vol. 33, no. 4, Sep. 2020.
12. R. Singh and R. Adhikari, "Age-structured impact of social distancing on the COVID-19 epidemic in India," *arXiv:2003.12055 [cond-mat, q-bio]*, Mar. 2020, arXiv: 2003.12055. [Online]. Available: http://arxiv.org/abs/2003.12055
13. A. Hoseinpour Dehkordi, M. Alizadeh, P. Derakhshan, P. Babazadeh, and A. Jahandideh, "Understanding epidemic data and statistics: A case study of covid-19," *Journal of Medical Virology*, vol. 92, no. 7, pp. 868–882, 2020.
14. A. Banerjee, M. Katsoulis, A. G. Lai, L. Pasea, T. A. Treibel, C. Manisty, S. Denaxas, G. Quarta, H. Hemingway, J. L. Cavalcante, M. Noursadeghi, and J. C. Moon, "Clinical academic research in the time of Corona: A simulation study in England and a call for action," *PLOS ONE*, vol. 15, no. 8, p. e0237298, Aug. 2020.
15. M. T. Nivedita Prasad, Anil Kumar, "Novel coronavirus disease (covid-19) pandemic in india: A review," *Eurasian Journal of Medical Investigation*, vol. 4, no. 3, pp. 279–283, 2020, doi: 10.14744/ejmi.2020.38479.
16. C. Sohrabi, Z. Alsafi, N. O'Neill, M. Khan, A. Kerwan, A. Al-Jabir, C. Iosifidis, and R. Agha, "World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19)," *International Journal of Surgery (London, England)*, vol. 76, pp. 71–76, Apr. 2020.
17. S. X. Zhang, Y. Wang, A. Rauch, and F. Wei, "Unprecedented disruption of lives and work: Health, distress and life satisfaction of working adults in china one month into the covid-19 outbreak," *Psychiatry Research*, vol. 288, p. 112958, 2020.
18. A. Imran, I. Posokhova, H. N. Qureshi, U. Masood, M. S. Riaz, K. Ali, C. N. John, M. I. Hussain, and M. Nabeel, "Ai4covid-19: Ai enabled preliminary diagnosis for covid-19 from cough samples via an app," *Informatics in Medicine Unlocked*, vol. 20, p. 100378, 2020.
19. S. Ahmad, P. Chitkara, F. N. Khan, A. Kishan, V. Alok, A. Ramlal, and S. Mehta, "Mobile Technology Solution for COVID-19: Surveillance and Prevention," in *Computational Intelligence Methods in COVID-19: Surveillance, Prevention, Prediction and Diagnosis*, ser. Studies in Computational Intelligence, K. Raza, Ed. Singapore: Springer, 2021, pp. 79–108.
20. J. Chan, L. Cox, D. Foster, S. Gollakota, E. Horvitz, J. Jaeger, S. Kakade, T. Kohno, J. Langford, J. Larson, P. Sharma, S. Singanamalla, J. Sunshine, and S. Tessaro, "Pact: Privacy-sensitive protocols and mechanisms for mobile contact tracing." *IEEE Data Engineering Bulletin*, vol. 43, no. 2, pp. 15–35, July 2020.
21. A. Jhunjhunwala, "Role of Telecom Network to Manage COVID-19 in India: Aarogya Setu," *Transactions of the Indian National Academy of Engineering*, vol. 5, no. 2, pp. 157–161, Jun. 2020.
22. Z. Wu and J. M. McGoogan, "Characteristics of and Important Lessons From the Coronavirus Disease 2019 (COVID-19) Outbreak in China: Summary of a Report of 72314 Cases From the Chinese Center for Disease Control and Prevention," *JAMA*, vol. 323, no. 13, pp. 1239–1242, 04 2020.
23. S. Mohanty, "COVID-19: A crisis or a springboard," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 100–102, 2020.
24. L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "Sayopillow: Blockchain-integrated privacy-assured iomt framework for stress management considering sleeping habits," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 1, pp. 20–29, 2021.
25. M. Azad, J. Arshad, S. Kamal, F. Riaz, S. Abdullah, M. Imran, and F. Ahmad, "A first look at privacy analysis of covid-19 contact tracing mobile applications," *IEEE Internet of Things Journal*, vol. PP, 09 2020.
26. S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, "Covichain: A blockchain based framework for nonrepudiable contact tracing in healthcare cyber-physical systems during pandemic outbreaks," *SN Computer Science*, vol. 2, no. 5, 2021.
27. S. Biswas, F. Li, Z. Latif, K. Sharif, A. K. Bairagi, and S. P. Mohanty, "Globechain: An interoperable blockchain for global sharing of healthcare data - a covid-19 perspective," *IEEE Consumer Electronics Magazine*, pp. 1–1, 2021.
28. Q. Zheng, Y. Li, P. Chen, and X. Dong, "An innovative ipfs-based storage model for blockchain," in *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, 2018, pp. 704–708.
29. A. H. Mohd Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "Iomt amid covid-19 pandemic: Application, architecture, technology, and security," *Journal of Network and Computer Applications*, vol. 174, p. 102886, 2021.
30. W. E. Taskforce, 2020. [Online]. Available: https://worldhealthorg.shinyapps.io/covid/
31. O. Pinto Neto, J. C. Reis, A. C. B. Brizzi, G. J. Zambrano, J. M. de Souza, W. Pedroso, R. C. de Mello Pedreiro, B. de Matos Brizzi, E. O. Abinader, and R. A. Zângaro, "Compartmentalized mathematical model to predict future number of active cases and deaths of COVID-19," *Research on Biomedical Engineering*, Aug. 2020. [Online]. Available: http://link.springer.com/10.1007/s42600-020-00084-6

Bhaskara S. Egala received his bachelor's degree in Information Technology from JNTU-K University, in 2011. He has received Post Graduation Diploma in IT Infrastructure, Systems and Security (PG-DITISS) from Centre for Development of Advanced Computing, Pune, 2013. He then commenced his master's in Cyber Security from JNTU-K University, in 2016. Now, he is pursuing Ph.D. degree in SRM University, Amaravati, AP. His current research interest covers security and privacy concerns in the context of the Internet of Things (IoT) and Smart Healthcare systems.

Ashok K. Pradhan is currently working as an Assistant Professor in the Department of Computer Science & Engineering, School of Engineering and Applied Science at SRM University, Amaravati, AP. He has received his M. Tech degree in the Department of Computer Science and Engineering from the National Institute of Technology (NIT), Rourkela, India, 2010. He has received his Ph.D. degree in the Department of Computer Science and Engineering NIT Durgapur, India, 2015. His areas of interest and research includes Optical Communication and Networks, Internet of Things (IoT), Blockchain Technology, Network Security & Privacy, Cloud Computing, Edge Computing, Fog Computing, and Computer Algorithms.

Venkataramana Badarla is currently working as an Associate Professor in the Department of Computer Science & Engineering at Indian Institute of Technology, Tirupati, AP. He has received his M.E degree in the Department of Information Systems from the Birla Institute of Technology and Science, Pilani, India, 1997. He has received his Ph.D. degree in the Department of Computer Science and Engineering, from Indian Institute of Technology, Madras, India, 2007. His areas of interest and research includes Wireless Networks, Cloud Computing, and Internet of Things (IoT). He has published more than 20 research papers in reputed peer-reviewed journals/conferences with high impact factors.

Saraju P. Mohanty received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the master's degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 400 research articles, 4 books, and 7 granted and pending patents. His Google Scholar h-index is 43 and i10-index is 164 with 7800 citations. He is widely credited as the designer for the first digital watermarking chip in 2004 and first the low-power digital watermarking chip in 2006. He is a recipient of 13 best paper awards, Fulbright Specialist Award in 2020, IEEE Consumer Technology Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 11 keynotes and served on 12 panels at various International Conferences. He has been serving on the editorial board of several peer-reviewed international transactions/journals, including IEEE Transactions on Big Data (TBD), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), IEEE Transactions on Consumer Electronics (TCE), and ACM Journal on Emerging Technologies in Computing Systems (JETC). He has been the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (MCE) during 2016-2021. He served as the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) during 2014-2018 and on the Board of Governors of the IEEE Consumer Technology Society during 2019-2021. He serves on the steering, organizing, and program committees of several international conferences. He is the founding steering committee chair for the IEEE International Symposium on Smart Electronic Systems (IEEE-iSES), steering committee vice-chair of the IEEE-CS Symposium on VLSI (ISVLSI), and steering committee chair of the OITS International Conference on Information Technology (OCIT). He has mentored 2 post-doctoral researchers, and supervised 13 Ph.D. dissertations, 26 M.S. theses, and 11 undergraduate projects.