This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Samuel, O.; Omojo, A. B.; Onuja, A. M.; Sunday, Y.; Tiwari, Prayag; Gupta, Deepak; Hafeez, G.; Yahaya, A. S.; Fatoba, O. J.; Shamshirband, Shahab

IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain

Published in:
IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS

DOI:
[10.1109/JBHI.2022.3143576](https://doi.org/10.1109/JBHI.2022.3143576)

Published: 01/02/2023

Document Version
Peer reviewed version

Please cite the original version:
Samuel, O., Omojo, A. B., Onuja, A. M., Sunday, Y., Tiwari, P., Gupta, D., Hafeez, G., Yahaya, A. S., Fatoba, O. J., & Shamshirband, S. (2023). IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain. *IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS*, 27(2), 823-834.
<https://doi.org/10.1109/JBHI.2022.3143576>

IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain

Omaji Samuel , Akogwu Blessing Omojo, Abdulkarin Musa Onuja , Yunisa Sunday, Prayag Tiwari , Deepak Gupta , Ghulam Hafeez, Adamu Sani Yahaya, Oluwaseun Jumoke Fatoba, and Shahab Shamshirband

Abstract—Internet of medical things (IoMT) has made it possible to collect applications and medical devices to improve healthcare information technology. Since the advent of the pandemic of coronavirus (COVID-19) in 2019, public health information has become more sensitive than ever. Moreover, different news items incorporated have resulted in differing public perceptions of COVID-19, especially on the social media platform and infrastructure. In addition, the unprecedented virality and changing nature of COVID-19 makes call centres to be likely overstressed, which is due to a lack of authentic and unregulated public media information. Thus, people who are susceptible to the COVID-19 virus may not get authentic media information to manage and minimize both its risk and transmission. Furthermore, the lack of data privacy has restricted the sharing of COVID-19 information among health institutions. To resolve the above-mentioned limitations, this paper is proposing a privacy infrastructure based on federated learning and blockchain technology. The proposed infrastructure has the potentials to enhance the trust and authenticity of public media communication and deliver an authentic method to disseminate COVID-19 information. Also, the proposed infrastructure can effectively resolve the issue of large data silos and provide a shared model while preserving the privacy of data owners. Furthermore, information security and privacy analyses show that the proposed infrastructure is robust against information security-related attacks.

Index Terms—Blockchain, COVID-19, epidemiology, federated learning, information security, reinforcing addition

I. INTRODUCTION

Since the massive outbreak of the coronavirus (COVID-19) pandemic in 2019, social media has become paramount in the dissemination of public health information [1]. Besides, different news items integrated have produced variations of public opinions regarding COVID-19. For instance, disease infectious experts confirmed in 2020 that COVID-19 can be spread from person to person or community to community [1]. The proper understanding of the growth in the emerging topics of COVID-19 on the media to change public behavior is vital to designing effective communication strategies or technologies for achieving public health interventions. Today,

remote healthcare is a vital area of the Internet of medical things (IoMT) to detect COVID-19 patients [2]. Various devices enable the remote monitoring of patients. Data generated by these devices is processed using different machine learning and deep learning approaches for diagnosis. The movement of sensitive and personal healthcare data from individual devices to central servers for training leads to privacy and security concerns. To deal with the problem, federated learning (FL) has been proposed by the research community [3]. Instead of transferring the data generated by the individual device to a central server, the FL model is deployed on devices for local training of data. For global training of the data, locally processed data is forwarded towards the central server thereby protecting sensitive healthcare information.

The IoMT is the integration of medical devices and applications to improve health information technology. The IoMT has been used to solve different problems of health information technology infrastructures [4]. To our utmost knowledge, no infrastructure combines artificial intelligence (AI) [5] and blockchain technology to analyze and integrate different information produced during a major public health emergency. Moreover, the authors in [6] combined FL and blockchain, known as the BFL model, for IoMT. The model divides large clusters of IoMT into multiple sub-clusters to connect each BFL. Another work in [7] presented a lightweight hybrid FL framework that is based on blockchain for IoMT. The framework ensures trust management and security of the federated nodes. In [8], the authors presented a framework based on blockchain and FL for improving computed tomography image identification across several hospitals. A Capsule network is utilized in the framework to detect COVID-19 patients. However, their framework does not address the problem of unauthentic COVID-19 information propagation from different media sources. The work in [9] proposed a platform using blockchain, known as BlochIE. BlochIE consists of fairness based packing algorithms for ensuring fairness among users. However, the platform does not consider the impact of public media awareness of COVID-19 induced by blockchain. The authors in [10] designed an architecture for the security and privacy of health users using FL and blockchain. In the proposed architecture, the data of users is stored in a cloud. However, the architecture has no assurances on the information stored in the cloud by the users. Also, blockchain suffers efficiency issues by providing single-keyword over encrypted data. To that aim, the authors in [11] created a multi-keyword search protocol based on a bloom filter to help users maintain their privacy. However, because the protocol gives two outputs, “yes” and “false”, it may not convey information about items that are near to being searched correctly. Furthermore, the authors do not consider the waiting times to submit transactions into the blockchain, which create a high deviation of transaction response times, known as the lack of fairness problem. To resolve the problem, the authors in [12] provided a solution using the Fair-Pack algorithm for

O. Samuel; A. M. Onuja and Y. Sunday are with the Department of Computer Science, Confluence University of Science and Technology (CUSTECH), Osara, 1040, Kogi State, Nigeria; e-mail addresses: omajimani1@gmail.com, omajis@custech.edu.ng; onujaam@custech.edu.ng; yunisasunday1986@gmail.com

A. B. Omojo and O. J. Fatoba are with the Applied Mathematics and Simulation, Advanced Research Centre, SHESTCO, Kwali, Abuja Nigeria; e-mail address: lucyblex1@gmail.com; oluwaseunfatoba5@gmail.com

G. Hafeez is with the Open AI Lab, National Yunlin University of Science and Technology, Douliou 64002, Taiwan; e-mail address: ghulamhafeez393@gmail.com

A. S. Yahaya is with the Department of Information Technology, Bayero University, Kano Nigeria; e-mail address: asyahaya.it@buk.edu.ng

P. Tiwari is with the Department of Computer Science, Aalto University, Finland; email address: prayag.tiwari@aalto.fi

D. Gupta is with the Maharaja Agrasen Institute of Technology, Delhi, India; email address: deepakgupta@mait.ac.in

S. Shamshirband is with Department of Computer Science and Information Engineering, National Yunlin University of Science and Technology, Taiwan; e-mail address: shamshirbands@yuntech.edu.tw

Corresponding authors: Shahab S. Band, Prayag Tiwari, Deepak Gupta.

selecting transactions via theoretical analysis. The authors in [13] proposed an architecture that combines FL and blockchain technology for ensuring efficient data sharing between multiple parties while preserving data privacy. Other authors in [14] proposed an architecture that is based on blockchain and FL, known as BlockFL. The BlockFL architecture allows on-device machine learning. An autonomous FL based blockchain technology, known as BFL, is proposed by the authors in [15]. The BFL architecture provides coordinated data sharing for autonomous vehicles. However, none of the works in [6]–[15] considers the impact of public awareness induced by blockchain for controlling COVID-19. In order to prevent the pandemic, it is also critical to develop both theoretical and practical technologies that promote effective information communication. Furthermore, the proposed infrastructure must include information security features that protect patients' privacy and prevent rumour-mongering. It is also important to assess the influence of blockchain-driven public awareness on the COVID-19 pandemic. In addition, an efficient mathematical epidemiological model that depicts the impact of blockchain in the management and risk reduction of the novel coronavirus is essential.

Therefore, this study proposes an infrastructure based on a secure FL and blockchain technology as the available method to address the challenges. The proposed infrastructure effectively solves the problem of large data depository and provide a shared model without obtaining local data while preserving the privacy of data owners. By default, blockchain provides trust and security via the proposed consensus protocol; whereas, FL prevents the issues of insufficient data and privacy through collaborative data sharing and differential privacy (DP). In addition, the proposed blockchain-based disease epidemiological model addresses the problem of an inefficient disease model regarding public awareness. The contributions of this paper are given below.

- 1) To propose privacy and information security infrastructure, known as a federated blockchain-based medical system (FedMedChain) to solve the problems of privacy and insufficient data to detect COVID-19. The proposed infrastructure also minimizes the burden of call centres in terms of public communication.
- 2) To propose a blockchain-based mathematical model for analyzing the COVID-19 pandemic. This model will help medical experts to determine the impact, management of COVID-19 and its transmission.
- 3) A new blockchain consensus protocol is proposed for the creation of blocks and the selection of miners. The proposed protocol is based on two rounds of a reinforcing addition game.
- 4) Security and privacy analyses are performed, which show that the proposed system is robust against privacy and information security-related attacks.

The remaining part of this paper is organized as follows. Section II presents the literature review in three subsections while the proposed infrastructure is given in Section III. The proposed problem formulation is given in Section IV, and Section V provides the information security and privacy analyses. Section VI provides the simulation results of the proposed privacy infrastructure, and Section VII concludes the paper with future work.

II. LITERATURE REVIEW

The literature review section is discussed in three parts, which are applications of AI for COVID-19, integration of FL and blockchain, and mathematical models for analyzing the COVID-19 pandemic.

A. Applications of Artificial Intelligence for COVID-19

The ongoing pandemic has drawn the attention of researchers, academia and medical experts into proffering ways to combat and minimize the spread of COVID-19. Besides, different strategies and technologies are deployed to tame COVID-19. The AI is not an exception to the enormous technologies used for the treatment, diagnosis and prediction of health-related diseases including COVID-19. However, AI becomes inefficient due to the following challenges: insufficient COVID-19 data, privacy concerns and the imbalanced nature of COVID-19 data. Thus, the challenges provide open research gaps for researchers and academia. To this end, this study proposes an infrastructure that combines FL and blockchain to resolve the challenges.

The author in [16] presented a review that evaluates AI to determine its role in fighting COVID-19. Also, the pitfalls, limitations and constraints of AI on COVID-19 were discussed. The authors in [17] discussed platforms and conceptual structures in the field of AI-based techniques that are useful for addressing issues of COVID-19. They also discussed different existing AI-based methods or techniques that are suitable as diagnosing models for COVID-19, such as recurrent neural network, long-term-short memory, generative adversary model, extreme learning method, etc. Also, the choices of selecting the appropriate parameters of nonclinical and clinical datasets were mentioned. The authors in [18] provided a review that analyzes the role of AI as a decisive technology to prevent and combat COVID-19. They also discussed AI applications in terms of early diagnosis and disease prevention. This helps medical experts and physicians to train AI-based models, design algorithms and, analyze and optimize data that deals with coronavirus with accuracy and precision. The authors in [19] proposed a diagnosis scheme that is based on deep learning for breast cancer analysis. The scheme uses the 5G to receive the breast pathology images, which are subjected to deep and transfer learning models to derive the diagnostic model. However, the scheme does not ensure trust and security as attackers can manipulate the images received through the 5G inception-v3 network. To ensure the trust of a scheme, the authors in [20] proposed a blockchain-based scheme that provides traceability and revocation of medical records of coronavirus. The scheme uses the decision Bilinear-Hellman assumption to provide security against attacks. However, the scheme does not consider the impact of public awareness driven by blockchain technology. For ensuring the security of a scheme, the authors in [21] proposed a method that is based on 0-1 coding technology for IoMT. The method is flexible and efficient because it uses fine-grained access control and ciphertext-policy weighted attribute-based encryption. However, the privacy of data owners is not considered. To ensure the privacy of a scheme, the authors in [22] designed a privacy preservation scheme that is based on Elgamal blind signature. The proposed scheme protects the records of patients from attacks. However, the problem of insufficient data for training deep learning methods is not considered. From the above discussions, in the existing reviews [16]–[22], none of the authors investigated the impact of public awareness driven by blockchain technology for COVID-19. This gap provides a new research area, which is one of the focuses of this study.

B. Integration of Federated Learning and Blockchain

Due to the emergence of the IoMT [7], health data have become beneficial and available for medical experts, researchers, etc. Nowadays, the improvement in AI-based applications has provided accurate health data that can be monitored without human interventions [7]. Health institutions can now deploy AI applications to perform triad: treatment, prognoses and

diagnosis; thereby, minimizing the waiting time for patients to consult medical doctors [23]. However, security and privacy concerns of health data are not fully explored in AI applications. To this end, the present AI applications enable health data to be trained locally using FL. The FL allows collaborative and distributive training where the trained data are not shared with cloud systems [7]. It prevents single points of failure and enables the security and privacy of the trained data under the control of the data owners. FL has salient features, such as parallelization of training, local training autonomy, minimizing the cost of data management, transfer learning and reduced cost of data labelling. In addition, FL enables all nodes to participate in the data training process; however, malicious nodes can compromise the training model, aggregation and decision processes. Therefore, an appropriate control mechanism is needed as a defensive measure [24]. Also, another limitation of FL is the problem of trust among nodes. Thus, blockchain is employed as one of the numerous technologies that enforce trust in a decentralized fashion [25].

Blockchain is a distributed and decentralized system with strong cryptographic strength that secures transactions among untrusted entities in the network. It is a distributed ledger technology that records transactions over the network. Also, it has consensus protocols, such as proof-of-work, proof-of-stake, proof-of-authority, etc., that ensure the correctness of transactions and provide a nonpartisan way of achieving agreement on the general state of the network [26]. Recent studies that combine FL and blockchain technology are given in [27]–[36]. However, these studies do not provide extensive solutions to the problems of information security and privacy, data insufficiency, and trust management. Also, the impact of public awareness driven blockchain technology on COVID-19 was not investigated.

C. Mathematical Models for Analyzing COVID-19 Pandemic

In recent times, different mathematical models are proposed for analyzing the COVID-19 pandemic. The authors in [1] proposed a multiple information susceptible discussing immune (M-SDI) model to understand the important key information pattern on the social network. In their proposed model, several microblogs' reports about COVID-19 were analyzed and the least square method was used for parameters estimation. The authors in [37] proposed a deterministic dynamic model to examine the interaction of disease propagation and investigate media reports on the spread of COVID-19. Also, a cross-correlation analysis was performed to demonstrate the correlation between media reports and infection case data. For parameters estimation, they have used next-generation matrix Latin hypercube sampling (LHS) and partial rank correlation coefficients. The authors in [38] proposed a mathematical model to investigate the current outbreak of coronavirus disease in Wuhan, China. They investigated the role of the environmental reservoir in the transmission and spread of the disease. Also, a non-constraint transmission rate, which changes with epidemiological status and environmental conditions that reflect the impact of the ongoing disease control measures was investigated. A standard least square method was used for parameters estimation.

The authors in [39] developed an optimal response strategy that evaluates and implements prevention, and control intervention (PCI) model for COVID-19 in Chongqing and Guizhou provinces. They also proposed an adaptive metropolis hastings algorithm to perform the Markov chain Monte Carlo (MCMC) procedure for estimating the undermined parameters. Also, a Geweke convergence diagnostic method was proposed to access convergence of the PCI model. The authors in [40] proposed a discrete-time stochastic epidemic model with

binomial distributions to study the transmission of COVID-19 disease. Whereas, the authors in [41], proposed a dynamic model that reflects the changes of medical resources on the transmission of COVID-19 in Wuhan. Other authors in [42] proposed a model that predicts the cumulative number of reported cases of a finalized size. The model key features are timing implementation of major public policies restricting social movement, identification and isolation of unreported cases, and impact of asymptomatic infectious cases. The authors in [43] proposed a model based on non-pharmaceutical intervention (NPI) on the transmission dynamics of the COVID-19 epidemic in Nigeria. From the existing mathematical models for COVID-19 proposed by the authors in [1], [37]–[43], none of the authors considers the impact of public awareness driven by blockchain technology. Also, a secure and decentralized disease model is not considered.

Table I shows the comparison of the proposed infrastructure with other existing schemes in terms of year, objectives, techniques, epidemiological model, blockchain, consensus protocol and limitations.

Fig. 1: The proposed IoMT privacy infrastructure

III. THE PROPOSED PRIVACY INFRASTRUCTURE

This study collects arbitrary epidemiological data from several centres for disease control (CDCs), as depicted in Fig. 1. In this paper, suppose we have data fragments $D \triangleq \{d = 1, 2, 3, \dots, D\}$ held by different CDCs, then the individual data in D is integrated into a single form by matching identifiers of the same instance. Note that CDCs and parties are used interchangeably in this paper. Both parties decide to release their integrated data in an anonymous manner via the blockchain to some medical experts for disease analysis. During the collaboration, parties do not wish to disclose any information more than what is needed by the collaboration. In Fig. 1, the terms “Test” and “Train” are the methods used to determine the accuracy of the proposed deep learning model. Whereas, the term “Release Data” is the data given to the medical expert for analysis and mining. In the proposed architecture, wireless radio frequency is used as the communication medium. Connectivity options for smart health devices include Wi-Fi, 2G/3G/4G, LTE, LoRaWAN, and others. All devices in this study are connected to a LoRaWAN gateway for the concerned CDC so that data can be collected. The gateway allows healthcare devices to send data to the CDC over longer distances and even when there is no Internet connection. This is advantageous for patients who do not have access to the Internet. The proposed architecture consists of four components, such as individuals, CDCs, consortium blockchain and FL. Each component of the proposed architecture is discussed as follows.

A. Individuals

Individuals are people that can either be susceptible, vaccinated, latently infected, asymptomatic or recovered. Fig. 2 shows the proposed flow diagram of the COVID-19 epidemic, which has eight compartments. The figure also presents the proposed blockchain-based mathematical epidemiological model, which is discussed in Section IV. Individuals in the infected class have fully developed disease symptoms and are capable of infecting others, as shown in Fig. 2. Individuals in the exposed group are in the incubation stage; they have no symptoms but can still infect others.

Fig. 2: The proposed flow diagram of COVID-19 epidemic. S : susceptible; S_q : susceptible quarantine; E_q : exposed quarantine; E : exposed; I_a : infectious asymptomatic; I_s : infectious symptomatic; H : hospitalized and R : recovery

B. CDCs

The CDC in this study can be health institutions, government establishments, etc., and they are responsible for controlling and preventing epidemics in a country. To avoid generalization, this study considers CDC as two-dimensional areas with different epidemiology of interests (EoIs), as the restriction that the CDCs may encounter. EoIs are defined as $EoI \triangleq \{eoi = 1, 2, 3, \dots, EoI\}$ and each of them finds and analyze the existence of an epidemic with a certain amount of disease information to be collected by the CDCs. Also, we define the restriction as $R \triangleq \{r = 1, 2, 3, \dots, R\}$ since CDCs may deploy smart devices with limited computational capabilities.

Since CDCs are restricted by the amount of epidemiological data stored on the smart devices because of battery power and security, we propose a federated blockchain-based medical system, known as FedMedChain, that pools epidemiological data from different CDCs across the country. Besides, CDCs collect data in variable time slots; hence, we define the total amount of data collection periods, denoted as P where $P \triangleq \{p = 1, 2, 3, \dots, P\}$ and each period p contains time slots T where $T \triangleq \{t = 1, 2, 3, \dots, T\}$. If EoI is needed by CDCs, then the data is collected. The acquired data is securely distributed across the proposed blockchain network before performing data mining and analysis.

C. The Consortium Blockchain System

This study employs a distributed ledger as the storage service and builds a consortium blockchain, which has $N \triangleq \{n = 1, 2, 3, \dots, N\}$ number of nodes for storing and sharing data. The nodes are categorized as follows.

1) *Mining Nodes*: These are nodes employed for verifying data sharing transactions and encapsulating them into blocks. Mining nodes constantly use the method of a reinforcing addition game to become miners for adding blocks to the blockchain network.

2) *Non-mining Nodes*: These nodes are responsible for receiving and broadcasting data sharing requests over the network. Although they do not require the same level of computational resources as the mining nodes, they relay data sharing requests over the network. In this study, consortium blockchain maintains valid transactions using smart contracts. It is assumed that CDCs have smart contracts for each collection of EoI. Also, CDCs upload their collated data from the FL system to the blockchain network. For each period of update, the total amount of data storage request V made by the CDCs is formulated as

$$V = P \times C, \quad (1)$$

where C is the unit cost of data storage. Inspired by [45], the number of blocks on the blockchain is denoted as ξ , which is also the depth of the blockchain. The meta-data of the proposed blockchain is constructed as follows

$$blockchain = \{block_1 || block_2 || \dots || block_\xi\}, \quad (2)$$

where “||” means concatenation. The arrangement of transactions in ascending order on the blockchain follows a Merkle hash tree. By computing the hash value of a block, a new structure of the block is designed, which is defined as follows

$$newBlock = \{mt, ntxt, stxt, preHash, currentHash\}. \quad (3)$$

In the blockchain, $preHash$ denotes the previous hash of the block, mt is the Merkle tree of the current block, and hash of the current block is described as

$$currentHash = H(mt, ntxt, stxt, preHash, ctimestamp), \quad (4)$$

where $H(\cdot)$ is a hash function, $ctimestamp$ is the current timestamp, $ntxt$ is the number of transactions and $stxt$ is a series of transactions. After reaching consensus, a new block is added at the end of the blockchain with longest chain, as described below

$$blockchain = \{block_1 || \dots || block_\xi || newBlock\}. \quad (5)$$

D. The Proposed Federated Learning System

The proposed FL system consists of the following phases: data collection, data preprocessing, and FL, as depicted in Fig. 3. The details of each phase are discussed as follows.

1) *Data Collection Phase*: Data in the form of EoI about patients stored by several CDCs are collected in this phase. These records may contain the same parameters of two or more CDCs that are used for matching and integration. Furthermore, constructing a data bank is a vital challenge when training deep learning models. As a result, in order to properly train a deep learning model, it is critical to collect data from many sources.

2) *Data Preprocessing Phase*: Once the data is collected, it is sent to the data preprocessing phase. In the data preprocessing phase, missing and erroneous data are recovered and removed using the method of interpolation. In this study, the three-sigma rule of thumb method is used for interpolating data [47]. In addition, the data imbalance problem is solved in the preprocessing phase by generating synthetic data, which are the instances of the actual data. The aim of generating synthetic data is because of the irregularity in the presentation of data by CDCs in terms of daily, weekly or monthly rhythms. In the literature, a generative adversary network has been employed to generate synthetic data for solving a data imbalanced problem [48].

TABLE I: Comparison of the proposed infrastructure with existing infrastructures.

Ref.	Year	1	2	3	4	5	6
[1]	2020	Understanding the key information pattern on social media	M-SDI and least square method	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[27]	2019	Create valuable shared resources	Incremental learning and incentive mechanism	✗	✓	✗	Lack of epidemiological model
[28]	2020	Improve service quality delivery and optimize functionalities of home appliances	Hierarchical FL system, normalized technique, incentive method and DP	✗	✓	✗	The proposed system is vulnerable to linking and double spending attacks
[29]	2020	Trustworthy distributed system for unmanned aerial vehicles	FL	✗	✓	✗	Lack of epidemiological model
[30]	2020	Prevent single point of failure in cloud system	FL, hybrid identity generation method and poison attack mechanism	✗	✓	✗	Tradeoff between efficiency and privacy protection is not considered. Also, real-time optimization of computation cost is not considered
[31]	2020	Implement asynchronous collaborative machine learning for heavy haul trains	Support vector machine, FL and punishment factor method	✗	✓	✗	Real-time computation cost for block mining is not considered
[32]	2020	Prevent single point of failure for on-device machine learning	FL and end-to-end latency model	✗	✓	✗	Privacy and security are not analyzed
[33]	2020	Enhancing quality of service via data sharing	DP and FL	✗	✓	✗	Tradeoff between accuracy and data utility is not considered
[34]	2020	Resource management in crowd computing	FL and re-encryption algorithm	✗	✓	✓	The impact of the re-encryption algorithm on computational cost of crowd computing is not considered
[35]	2020	Provenance and auditability for multi access edge computing (MEC)	FL and modified version of practical Byzantine fault tolerant	✗	✓	✓	Resource management for MEC is not considered
[36]	2020	An accurate traffic flow prediction	FL, gated recurrent neural network and secure aggregated mechanism	✗	✓	✓	Trust management is not considered
[37]	2020	Examine and investigate media report for COVID-19	Deterministic dynamic model and next generation matrix LHS	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[38]	2020	Investigate the role of environmental reservoir in transmission and spread of disease	Mathematical model and standard least square method	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[39]	2020	Provide optimal response strategy for COVID-19	An adaptive metropolis hashings algorithm and Geweke convergence method	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[40]	2020	Study the transmission of COVID-19	Discrete time stochastic epidemic model and binomial distribution	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[41]	2020	Analyze the change of medical resources on transmission of COVID-19 in Wuhan	A dynamic model	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[42]	2020	Predict cumulative number of reported cases of finalized size	Mathematical model	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
[43]	2020	Evaluate the transmission of COVID-19 in Nigeria	Non pharmaceutical intervention model	✓	✗	✗	Impact of public awareness driven by blockchain is not considered
Ours	2021	A secure and blockchain based COVID-19 epidemiological model	FL, DP and two rounds reinforcing addition game	✓	✓	✓	Scalability and real-time computation cost are not considered

✗: no; ✓: yes; 1: Objectives; 2: Techniques; 3: Epidemiological Model; 4: Blockchain; 5: Consensus Protocol; 6: Limitations.

3) *Federated Learning Phase*: This phase is divided into two parts, federated client and server. The former is responsible for receiving the global model from the server, computing the local gradient and returning the local model to the server. The latter is responsible for the receiving model from the client, aggregating local models, and computing and broadcasting the global model to the client. The details of other components of the federated system are discussed as follows.

- A. *Local Party*: It is comparable to the traditional deep learning approach, in which the demand for a party is not met due to a lack of data and processing resources.
- B. *Training*: A new smart contract is initiated for each local gradient by the party. Besides, the gradient can be further processed by the server.
- C. *Model Local Training*: Every party independently trains its local model and at each iteration, the party generates its local gradient to the smart contract.
- D. *Global Model Training*: The model is jointly trained using aggregated models and gradient parameters. The model is trained iteratively and for each iteration process, all parties share their gradients. Then, a transaction is initiated for that process in the blockchain. The current gradients that train the model are used to update the parameters of the FL model by the leader of the blockchain network. Afterwards, each party updates its local model, and a new iteration of model training can begin.

The proposed FedMedChain uses blockchain that implements cryptographic primitives to ensure data security and privacy of the system and data owners, respectively. The FL system's basic parameters are agreed upon and signed by all parties. At each round of model training, the model's local gradients are wrapped as transactions in the blockchain. The local gradient parameters, represented as $\Delta w_{i,j}$, are local weights. When all of the transactions have been completed, the smart contract uploads them to the blockchain. The new gradient is then transmitted across the network. The network's leader calculates the weight and updates it using Eq. (6).

$$E_k(w_{i+1}) = \frac{1}{N} + E_k(w_i) + \sum_{j=1}^N E_k(\Delta w_{i,j}), \quad (6)$$

where $E_k(w_i)$ is the encrypted weight at round i , $E_k(w_{i+1})$ is the encrypted weight for training the model at round $i+1$, $j = 1, 2, \dots, N$ is the index of party and k is the shared key.

EoI distribution and block production are the two primary processes in the proposed FedMedChain. When CDCs sign up for FedMedChain, they are granted *CovidCoin* accounts, which keep track of all token transactions, and wallet accounts, which hold all *CovidCoin* account addresses. In the first stage, all CDCs are allocated the same amount of *CovidCoin* for EoI distribution; in the second stage, at round 0, an initial block called the genesis block is constructed, which contains the first transaction that shows ownership for each *CovidCoin*. After the genesis block is established, the randomized seed is generated using a pseudo-random number generator (PRNG), which is publically available for all CDCs. The randomized seed is employed in the reinforcing addition game, which aims to determine the game's leader for each round of the game in order to create a new block. In addition, the leader receives *CovidCoin* as a reward.

A set of incentives is given to CDCs to encourage them to submit their data with FedMedChain. Furthermore, CDCs do not provide an equal quantity of data, implying that they are compensated based on how much data they share. In addition, all CDCs must agree on the fees that will be charged to train the model. Before FL, the data from each CDC is checked for

integrity and legitimacy. If a CDC submits inaccurate data, it will be penalized by paying fines. If FL is completed, each party can benefit from the trained model, which can generate revenue for them by charging medical specialists who wish to utilize the trained model for a fee.

To train an FL model, parties must agree on the training deep neural network, method, and network configuration parameters, such as the number of network layers, size of mini-batch, number of neurons, number of iterations, and so on, as shown in Fig. 3. Also, the model's initial weight, which can be modified after the i th training iteration.

E. The Proposed Two Rounds Reinforcing Addition Game

In this study, the goal of the game is to allow each CDC to participate in the proposed system model. Each CDC is a player in the game, and a miner will be chosen from among them, which depends on their overall score. The players are $X \triangleq \{x = 1, 2, 3, \dots, X\}$, and each player has two rounds to play the game. The following are the guidelines for playing the game. (1) A PRNG is employed to generate the necessary score values for the game. The initial seed is generated randomly by the proposed model. (2) A pseudo-random number is rolled 9 times and on each roll, one player displays the number, which is broadcasted to all players in the blockchain network.

1) *Method of Scoring*: The proposed two rounds reinforcing addition game is shown in Fig. 4. To determine the total score for each round (a total of two rounds), eight computations are used, as shown in the figure. Let $Ro1$, $Ro2$, and $Ro3$ represent the sum of the values in rows 1, 2, and 3, respectively. Also, the total of the values in columns 1, 2, and 3 is $Co1$, $Co2$, and $Co3$, respectively. The sum of the values in the two diagonals is $Do1$ and $Do2$, respectively. We define their sums as follows:

$$\begin{aligned} Ro1 &= \sum_{j=1}^N C_{1,j}; Ro2 = \sum_{j=1}^N C_{2,j}; Ro3 = \sum_{j=1}^N C_{3,j}; \\ Co1 &= \sum_{i=1}^N C_{i,1}; Co2 = \sum_{i=1}^N C_{i,2}; Co3 = \sum_{i=1}^N C_{i,3}; \\ Do1 &= \sum_{i=1}^N \sum_{j=1}^N C_{i,j}, \forall i = j; Do2 = \sum_{i=1}^N \sum_{j=N}^1 C_{i,j}, \forall i \neq j. \end{aligned} \quad (7)$$

The total score for each round is defined as:

$$\begin{aligned} ts &= \sum_{j=1}^N C_{1,j} + \sum_{j=1}^N C_{2,j} + \sum_{j=1}^N C_{3,j} + \sum_{i=1}^N C_{i,1} + \sum_{i=1}^N C_{i,2} \\ &\quad + \sum_{i=1}^N C_{i,3} + \sum_{i=1}^N \sum_{j=1}^N C_{i,j} + \sum_{i=1}^N \sum_{j=N}^1 C_{i,j}. \end{aligned} \quad (8)$$

(1) The total sums of scores are not cancelled in each player's first-round score. (2) After 2 rounds, the totals are added and the player with the highest sum is the winner.

2) *Strategy of the Game*: All players start the game at the same time. It means that all players are given equal chances of participating in the mining and consensus processes.

Assumption 3.1: Let $TS \triangleq \{ts = 1, 2, 3, \dots, TS\}$ be the set of total scores in the game, and it is assumed that two players do not have the same total score.

Definition 3.1: Let $x_i(t)$ and $x_j(t)$ be two players at time t who have total scores $ts_i \neq ts_j$ where i and j are indices of the players and ts_i and ts_j are total scores of players $x_i(t)$

Fig. 3: The proposed IoMT architecture based on federated learning system

Fig. 4: The proposed two rounds reinforcing addition game

and $x_j(t)$, respectively. Then, the following condition holds to choose a winner of the game.

- a If $ts_i > ts_j$, then x_i is the winner; otherwise, x_j is the winner at time t .

Theorem 3.1: If $ts_i = ts_j$, then a winner cannot be selected among the players.

Proof 3.1: The proof of Theorem 3.1 is given as follows. In this study, proof by contradiction is provided. Suppose that Definition 3.1 holds, then a winner is selected among players with the highest totals. Besides, the PRNG ensures randomness in the generation of values before the scores are calculated. Besides, a different number of rounds are allowed so that $ts_i = ts_j$ does not hold. Hence, $ts_i \neq ts_j$ holds for the final round of play. Thus, $ts_i \neq ts_j$ contradicts Theorem 3.1.

Theorem 3.2: There is no mining centralization problem in the proposed consensus protocol.

Proof 3.2: The proof of Theorem 3.2 is given as follows. In the mining centralization problem, the same player is always selected as the winner for each round of play. To solve the problem, this study ensures that Definition 3.1 holds. Besides, Definition 3.1 may not be sufficient alone; thus, we introduce a computational factor (CF), which is defined as [44]

$$CF_i = \begin{cases} \frac{\theta_i}{\sum_{i=1}^N \theta_i}, & \text{if } \rho > \Phi, \\ 0, & \text{otherwise,} \end{cases} \quad (9)$$

where $CF_i \in [0, 1]$, the number of computational resource of each player is θ_i , which is obtained by the hash rate and $\rho \in [0, 1]$ is the defined threshold that controls player's malicious activities. $\sum_{i=1}^N \theta_i$ is the overall computational resources of proposed blockchain network and $\Phi \in [0, 1]$ is the defined consensus threshold. If $CF > 0$, then it means that $\rho > \Phi$. Hence, TS is written as follows.

$$TS = \begin{cases} ts_i + CF_i, & \text{if } \rho > \Phi, \\ ts_i, & \text{otherwise,} \end{cases} \quad (10)$$

where $i \in N$. Since θ_i is not the same for each player, then the mining centralization problem is solved. Thus, Theorem 3.2 is proven.

IV. PROBLEM FORMULATION

The problem formulation is discussed as follows.

Definition 4.1 (Federated learning): Define N CDC data owners $\{x_1, x_2, \dots, x_N\}$ who all want to train a machine learning model by combining their own data $\{D_1, D_2, \dots, D_N\}$. To train a model M_{sum} , a common way is to collect all data and use $D = D_1 \cup D_2 \cup \dots \cup D_N$. A FL system is a learning method M_{fed} that allows data owners to collaborate on training a model without exposing their data to one another. Additionally, the accuracy of M_{fed} , also known as AC_{fed} , should be very near to that of M_{sum} and AC_{sum} . Let $\bar{\delta}$ be a non-negative real number if and only if

$$|AC_{fed} - AC_{sum}| < \bar{\delta}, \quad (11)$$

where AC_{sum} is the accuracy of M_{sum} and we say that FL algorithm has $\bar{\delta}$ -accuracy loss.

A. Security and System Parameters

The security parameters used to calculate the computational logarithm in the finite field problem are defined in this section. In the proposed system model, a tripartite protocol based on bilinear maps is used to secure the identification of CDC. The proposed system security architecture was built in accordance with the work of [46].

Definition 4.2: Let $\mathbb{G}$ be an addition group of point on an elliptic curve. $z \in \mathbb{G}$ be an order of $\mathbb{G}$ and Q is the generator of $\mathbb{G}$. Let $E_k(y)$ be a symmetric encryption protocol using the secret key k to decrypt y and let H be the hash function. We represent $x \xleftarrow{R} X$ to mean that the element x is randomly selected from the set X .

1) Trusted Authority: In this study, the trusted authority (TA) is any trusted node in the network, but not necessarily a trusted third party. Each CDC registers with TA and obtains the key pairs (i.e., private key sk_n and public key pk_n where $n \in N$) to become a legitimate member of the proposed network. The keys are used during the processes of encryption and digital signature. During the encryption and signature processes, CDC encrypts and signs the data with sk_n and forwards them to TA, which then verify with pk_n whether the data come from the legitimate CDC or not, and if they are genuine. In this paper, CDCs are assumed to be honest-but-curious, which means that they behave honestly at times by

sharing their data and dishonestly at other times by not sharing their data. In each round of the gradient parameter update, CDCs launches a particular level of denial of service attack if they act dishonestly. we establish two levels of attacks, level-1 and level-2, with level-2 being more severe than level-1.

- Generates $(y_1, y_2, \dots, y_n) \xleftarrow{R} \mathbb{Z}_z^*$ and calculates $\omega_i = y_i Q$ where $y_i \in (y_1, y_2, \dots, y_n)$.
- Chooses $H_0 : \{0, 1\} \rightarrow \{0, 1\}^n, H_1 : \mathbb{G} \rightarrow \mathbb{Z}_z^*, H_2 H_3 : \{0, 1\}^* \rightarrow \{0, 1\}^l$.
- Selects $M \leftarrow GF(2^l)$.
- Defines the master private key vector to be $(y_1, y_2, \dots, y_n)$.
- Defines the master public key vector to be $\omega = (\omega_1, \omega_2, \dots, \omega_n)$.
- Defines the system parameters to be $(\mathbb{G}, z, \omega, H, E_k(\cdot))$ and make them public.

The private keys of CDCs are also managed by the TA. The identities (IDs) of the CDCs are the disease identification numbers (DINs) of the epidemic for individual CDC with ID and let the key be

- $sk_{ID} = \sum_{i=1}^n b_i y_i \mod z$,
- $pk_{ID} = \sum_{i=1}^n b_i \omega_i \mod z$,

where b_i is the i th bit of $H_0(ID)$, $i = 1, 2, \dots, n$.

2) *CDC as an Initiator*: Any CDC that initiates an EoI request is considered an initiator. The initiator creates the epidemiological data description message in accordance with a world health organization (WHO) defined context. The following are the responsibilities of an initiator.

- Defines values γ and v , and their values play an important role in the proposed protocol.
- Selects $(ID_1, ID_2, \dots, ID_{v-\gamma}) \xleftarrow{R} ID$ list sets, $\overline{ID} = \{ID_1, ID_2, \dots, ID_{v-1}\}$.
- For each $ID_i \in \overline{ID}$, calculates $pk_i = \sum_{i=1}^n b_i \omega_i$ where b_i is the i th bit of $H_0(ID)$ and ω_i is the i th value in the master public key vector, $i = 1, 2, \dots, n$.
- For each $ID_i \in \overline{ID}$, computes a random number μ_i as the index number of individual CDC.
- For each $ID_i \in \overline{ID}$, defines pseudo-identities with public key pk_i , selects $g_i, h_i \xleftarrow{R} \mathbb{Z}_z^*$ arbitrarily and calculates
 - $g_i = g_i Q + h_i pk_i$.
 - $\theta_i = -h_i H_1(\phi_i)$.
 - $S_i = g_i \theta_i$.

Where (θ_i, ϕ_i) is a valid EC-Elgamal signature of S_i since $S_i Q = H_1(\phi_i) + pk_i \phi_i$.

- Defines Π together with disease description message msg , threshold value γ , ring size v as initiator request (IQR),

$$\Pi = \left(\{ID_1, ID_2, \dots, ID_i\}, \{\mu_1, \mu_2, \dots, \mu_i\} \right). \quad (12)$$

- Broadcasts IQR over the blockchain network to invite other CDCs.

3) *CDC as a Replier*: The initiator must send IQR to the CDC, which serves as a replier. This indicates that the CDC has accepted an initiator's invitation. Repliers have the following responsibilities.

- Obtains (msg, γ, v, Π) from the IQR.
- Calculates $k = H_2(msg)$ where k is a symmetric key and the size of the key is l .
- Defines a polynomial f over $GF(2^l)$ that fulfills the followings
 - $deg(f) = v - \gamma$.
 - $f(0) = H_3(v||\gamma)$.

- $f(\mu_i) = E_k(S_i)$, $i = 1, 2, \dots, v - 1$.

- Selects random index $\mu \xleftarrow{R} \mathbb{Z}_z^*$ where $(\mu_1, \mu_2, \dots, \mu_{v-\gamma})$ and $S_i = E_k(\mu)$.
- Generates $\varpi \xleftarrow{R} \mathbb{Z}_z$ and calculates the EC-Elgamal signature (θ_i, ϕ_i) of S_i where $\theta_i = \varpi Q$, $\phi_i = (S_i - sk H_1(\phi_i)) \varpi^{-1}$.
- Wraps $(\varpi, S_i, (\theta_i, \phi_i), ID)$ as CDC's request (CQR). Finally, the replier forwards CQR to the initiator.

4) *CDC as a Verifier*: The CQR received from the replier must be verified by the CDC as a verifier. The following tasks are carried out by the Verifier.

- Sets the verifier's response (VQR) $(< ID_1, \mu_1, S_1, (\theta_1, \phi_1) > \dots < ID_i, \mu_i, S_i, (\theta_i, \phi_i) >, msg, \gamma)$
- Calculates $k = H_2(msg)$ where k is a symmetric key.
- For each ID_i calculate $pk_i = \sum_{i=1}^n b_i \omega_i$ where $i = 1, 2, \dots, v$ and b_i is the i th bit of $H_0(ID)$ and ω_i is the i th value of the master public key vector, $i = 1, 2, \dots, n$.
- For each ID_i , verifies equations $S_i Q = H_1(\phi_i) \cdot pk_i + \theta_i \phi_i$. If any one of the tuples $< S_i, \theta_i, \phi_i >$ does not fulfill the equation, then verifier declines the signature.
- Selects $< (0, H_3(v||\gamma)) >$ and $v - \gamma$ pairs of $< \mu_i, E_k(S_i) >$ randomly in VQR and reconstructs the polynomial f as
 - $deg(f) = v - \gamma$.
 - $f(0) = H_3(v||\gamma)$.
 - $f(\mu_i) = E_k(S_i)$, $i = 1, 2, \dots, v - \gamma$.
- Verifies the rest of pair $< \mu_i, E_k(S_i) >$ in the VQR if any of them does not fulfill $f(\mu) = E_k(S_i)$, then verifier declines the signature. Else, verifier accepts the signature that the VQR is valid.

B. The Proposed Blockchain based Epidemiological Model

According to the proposed flow diagram of the COVID-19 epidemic in Fig. 2, we formulate the proposed mathematical model for the COVID-19 pandemic. Eight compartments are considered in the proposed mathematical model, which are susceptible (S), exposure (E), susceptible infectious (I_s), asymptomatic infectious (I_a), susceptible quarantine (S_q), expose quarantine (E_q), hospitalized (H), recovery (R) and blockchain impact (B). The derivative functions of the proposed blockchain-based epidemiological model are given as

$$\dot{S} = C_s \phi_B (1 - C_q) \frac{I_s}{N} S - C_a \phi_B (1 - C_q) \frac{I_q}{N} S - \lambda_B S B + R_q S_q, \quad (13)$$

$$\dot{E} = C_s \phi_B (1 - C_m) P_T \frac{I_s}{S} - C_a \phi_B (1 - C_m) P_T \frac{I_a}{N} S - (\sigma + \lambda_B B) E, \quad (14)$$

$$\dot{I}_s = (1 - r) \sigma E - (\phi_s + \tau_s + \delta_s) I_s, \quad (15)$$

$$\dot{I}_a = r \sigma E - \tau_a I_a, \quad (16)$$

$$\dot{S}_q = C_s \phi_B (1 - C_m) P_T + \lambda_B S B - R_q S_q, \quad (17)$$

$$\dot{E}_q = C_s \phi_B P_T C_m + \lambda_B E B - \delta_q E_q, \quad (18)$$

$$\dot{H} = \phi_s I_s + \delta_q E_q - (\tau_h + \delta_h) H, \quad (19)$$

$$\dot{R} = \tau_s I_s + \tau_a I_a + \tau_h I_h, \quad (20)$$

$$\dot{B} = \eta_B (\delta_1 I_s + \delta_2 I_a + \delta_q E_q) - \mu_B B, \quad (21)$$

where P_T is the transmission probability of effective infected individuals, σ is the rate of progression from exposed compartment to infected compartment; besides, $(\frac{1}{\sigma})$ is the incubation period. $(1 - C_m)$ is the proportion of individuals missed during

Algorithm 1 The proposed protocol algorithm

```

1: Initialization: Generate  $(y_1, y_2, \dots, y_i) \xleftarrow{R} \mathbb{Z}_z^*$  and select  $H_0 : \{0, 1\}^n \rightarrow \{0, 1\}^n, H_1 : \mathbb{G} \rightarrow \mathbb{Z}_z^*, H_2, H_3 : \{0, 1\}^l \rightarrow \{0, 1\}^l$ 
2: Define  $(y_1, y_2, \dots, y_n)$  and  $\omega = (\omega_1, \omega_2, \dots, \omega_n)$  to be the master private and public key vectors, respectively
3: Define  $(G, z, \omega, H, E_k(\cdot))$  to be the system parameters.
4: Set  $\gamma$  and  $v$  to be threshold value and ring size, respectively
5: Select  $(ID_1, ID_2, \dots, ID_{r-\gamma}) \xleftarrow{R} ID$  and set  $\overline{ID} = \{ID_1, ID_2, \dots, ID_{v-1}\}$ 
6: Set  $\mu_i$  to be index number of each CDC
7: for each  $ID_i \in \overline{ID}$  do
8:   Solve  $pk_i = \sum_{i=1}^n b_i \omega_i$  ▷ initiated by the initiator
9:   Select  $g_i, h_i \xleftarrow{R} \mathbb{Z}_z^*$ 
10:  Calculate the EC-Elgamal signature  $(\theta_i, \phi_i)$ 
    •  $g_i = g_i Q + h_i pk_i$ 
    •  $\theta_i = -h_i H_1(\phi_i)$ 
    •  $S_i = g_i \theta_i$ 
11:  Generate initiator's request  $\Pi$  as IQR
12:   $\Pi = \left( \{ID_1, ID_2, \dots, ID_i\}, \{\mu_1, \mu_2, \dots, \mu_i\} \right)$ 
     $(S_1, S_2, \dots, S_i), \{\theta_1, \theta_2, \dots, \theta_i\}, msg$ 
13:  Forward IQR to the replier
14:  if  $(msg, \gamma, v, \Pi)$  is received then ▷ (IQR is received by replier from initiator)
15:    Generate  $k = H_2(msg)$ 
16:    Solve a polynomial  $f$  over  $GF(2^l)$  such that
    •  $deg(f) = v - \gamma$ 
    •  $f(0) = H_3(v || \gamma)$ 
    •  $f(\mu_i) = E_k(S_i), i = 1, 2, \dots, v - 1$ .
17:    Generate signature
18:     $\theta_i = \varpi Q$  ▷ where  $\varpi \xleftarrow{R} \mathbb{Z}_z$ 
19:     $\phi_i = (S_i - sk H_1(\phi_i)) \varpi^{-1}$ 
20:    Wrap  $(\varpi, S_i, (\theta_i, \phi_i), ID)$  as CQR to verifier
21:  end if
22:  if CQR is received then ▷ Verifier receives CQR from replier
23:    Generate verifier's response as  $(\langle ID_1, \mu_1, S_1, (\theta_1, \phi_1) \rangle \dots \langle ID_i, \mu_i, S_i, (\theta_i, \phi_i) \rangle, msg, \gamma)$ 
24:    Goto line 15 to generate the shared key  $k$ 
25:    Goto line 8 to generate the public key  $pk_i$ 
26:    Verify the equation  $S_i Q = H_1(\phi_i), pk_i + \theta_i \phi_i$ 
27:    if  $\langle S_i, \theta_i, \phi_i \rangle$  satisfies the equation then
28:      Verifier accepts
29:    else
30:      Verifier rejects
31:    end if
32:  end if
33:  Select  $\langle (0), H_3(v || \gamma) \rangle$  and  $v - \gamma$  pairs of  $\langle \mu_i, E_k(S_i) \rangle$  randomly in VQR and reconstructs the polynomial  $f$  as
    •  $deg(f) = v - \gamma$ 
    •  $f(0) = H_3(v || \gamma)$ 
    •  $f(\mu_i) = E_k(S_i), i = 1, 2, \dots, v - \gamma$ .
34:  Verify the pair  $\langle \mu_i, E_k(S_i) \rangle$  in the VQR
35:  if  $f(\mu) = E_k(S_i)$  is fulfilled then
36:    Verifier accepts the signature as valid
37:  else
38:    Verifier rejects signature as invalid
39:  end if
40: end for

```

contact tracing, $(1 - C_q)$ is the proportion of individuals willing to stay quarantined, λ_B is the quarantined rate induced by awareness driven by blockchain technology, C_a, C_s are effective contact rates for asymptomatic and symptomatic individuals, respectively. B is the cumulative density of awareness program driven by blockchain technology, $(1-r)$ is the fraction of exposed individuals who show symptoms at the end of the incubation period, ϕ_s is the hospitalized rate of infected individuals, τ_s, τ_a, τ_h are the recovery rates of individuals in I_s, I_a and H compartments. $\delta_1, \delta_2, \delta_q$ are hospitalized rates of individuals in I_s, I_q and E_q , C_m is the proportion of individuals exposed to COVID-19 virus during contact tracing, δ_h is the disease-induced death rate, μ_B is the reduction rate of public awareness due to limitations of blockchain technology and η_B is the response intensity of blockchain technology on newly confirmed cases.

$$\phi_B = B_a \exp^{B_c(H_r - j)}, \quad (22)$$

where B_c is the rate of block creation by the leader, B_a is the number of awareness driven by blockchain technology, H_r is the relative hash of CDC for block creation, j is the index of CDC and ϕ_B is the blockchain function.

In this paper, the next-generation matrix is employed to derive the reproduction number R_0 , which is the expected number of secondary cases caused by a single typical case at the onset of an epidemic. The next-generation matrix is a square matrix G in which (ii, jj) th element of G , $g_{ii, jj}$ is the expected number of secondary infections of type ii caused by a single infected individual of type jj assuming the population of type ii is entirely susceptible. In G , there is one eigenvalue that is real, positive and strictly greater than all others. The eigenvalue is known as dominant of matrix G . Besides, R_0 is always simple of the dominant eigenvalue of G .

$$S_{ii, jj} = \frac{\delta R_0}{\delta g_{i, j}}, \quad (23)$$

R_0 is the clear exponential decay of an epidemic disease.

Theorem 4.1: It is theorized that the disease will invade a susceptible population when R_0 is greater than a threshold value. However, if R_0 is less than a threshold value, the disease will die out.

The next-generation matrix is derived from the Jacobian matrix, i.e., getting the partial derivative of a given system of equations. In this study, the large domain next-generation matrix method is used, which is defined as

$$J(E, I_s, I_a, S_q, E_q, H) = -\Gamma \Delta^{-1}, \quad (24)$$

where Γ is the transmission matrix that accounts for new infections, Δ is the transmission matrix that categorizes transition from one compartment to another and the Jacobian form of the system is given as $J(E, I_s, I_a, S_q, E_q, H)$.

$$\Gamma = \begin{pmatrix} (\sigma + \lambda_B B) & 0 & 0 & 0 & 0 & 0 \\ -(1-r)\sigma & (\phi_s + \tau_s + \delta_s) & 0 & 0 & 0 & 0 \\ -r\sigma & 0 & \tau_a & 0 & 0 & 0 \\ 0 & 0 & 0 & R_q & 0 & 0 \\ -\lambda_B B & 0 & 0 & 0 & \delta_q & 0 \\ 0 & -\phi_s & 0 & 0 & -\delta_q & (\tau_s + \delta_h) \end{pmatrix} \quad (25)$$

$$\Delta = \begin{pmatrix} 0 & -C_s \phi_B (1 - C_q) & C_a \phi_B (1 - C_q) & -R_q & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (26)$$

V. INFORMATION SECURITY AND PRIVACY ANALYSES

This section presents the information security and privacy analyses of the proposed infrastructure.

A. Threat Model

We can model the actions of parties in the proposed privacy infrastructure using the threat model. Furthermore, there are no established principles for developing threat models, according to [49]. A threat model is capable of predicting an impending information security threat. The threat model makes risk assessment and security system design for information system infrastructures much easier. In this study, it is considered that one or more parties may use the proposed infrastructure to intentionally attack others by secretly adding hidden backdoors. In addition, inference attacks may be possible with the proposed infrastructure. As a result, adversarial parties can deduce membership as well as other features associated with the training dataset. By generalization, this paper assumes that the parties can be honest, which means they share data honestly; honest-but-curious, which means they share data honestly at one point but dishonestly at another; and malicious,

which means they engage in malicious activities to exploit the proposed infrastructure's vulnerability. In order to mitigate or discourage dishonest behavior of CDCs, the proposed privacy infrastructure provides incentives to CDCs who share their data and enforces fines on the CDCs who behave dishonestly. The analyses in this work are based on three information security goals: confidentiality, integrity, and availability.

Theorem 5.1: The proposed privacy infrastructure is robust against information confidentiality related attacks.

The following is the proof of Theorem 5.1. Let $sif = \{x_i, EC_k, x_j\}$ represents the secure information flow, with x_i and x_j representing permitted information carriers and EC_k representing the encrypted communication channel. Assume that x_w is a carrier with illegal access to sensitive data. Then x_w has the ability to violate, destroy, leak, forge, and block information access. It may also carry out malicious attacks on x_i and x_j . x_w may be a new element in the proposed architecture. By allowing x_i and x_j to have access rights, it implies that they will get key pairs from TA. If one of the elements in sif is substituted, the confidentiality of the information is jeopardized. The state of information being compromised is 2^3 in binary notation (we examine the "AND" logic scenario) since sif is made up of three elements. Where "1" denotes data that has not been compromised and "0" denotes data that has been compromised. Furthermore, eavesdropping is only possible if all three elements are compromised. Also, the proposed architecture prevents both passive and active attacks.

Even if x_w intercepts the communication channel in a passive attack, it is unable to obtain significant plaintext information from the public key and ciphertext. If x_w uses a different pseudo-random number for each decryption, the plaintext will be different. As a result, the proposed privacy infrastructure is not vulnerable to passive attacks. If x_w receives both the ciphertext and the public key, it generates a new ciphertext that differs from the original plaintext. As a result, the proposed infrastructure is robust against an active attack. The proposed infrastructure is resistant to information confidentiality attacks based on the above-mentioned techniques.

Theorem 5.2: The proposed privacy infrastructure is robust against information integrity related attacks.

The following is the proof of Theorem 5.2. The term "information integrity" refers to the fact that the intended data is not altered while in transit. Information integrity has been achieved using hashing and signed messaging. The procedures of message hashing and signing can be performed by CDC as an initiator, replier, or verifier in the proposed privacy infrastructure. Furthermore, each CDC is assigned a unique ID, and the private key is generated using the public key received from the set of master keys. Each message must be digitally signed and hashed by the message's owner in order to be authenticated. This means that forgery is easily detectable. The hash function accepts a variable-length input and returns a fixed-length output. It indicates that a modification in the original message can be easily discovered since the original message's hashed result differs from the modified message's hashed result. Assume that x_w is familiar with the proposed infrastructure's digital signature process and hash function. With this information, x_w may be able to take advantage of the proposed infrastructure's weakness. Furthermore, with the public key, x_w is unable to alter the communication without the agreement of all participants. As a result, the proposed infrastructure is robust to data integrity attacks.

Theorem 5.3: The proposed privacy infrastructure provides data availability at all times.

The proof of Theorem 5.3 is given as follows. Let us assume that x_w has high computational resources to compromise the proposed blockchain system by exploring distributed denial of service attacks. To avoid verbosity, each block in the

blockchain has the same copy of the ledger. It means that the compromise of a block does not affect the other blocks in the blockchain. Besides, the proposed consensus protocol ensures that the validator (i.e., party with the highest TS) can mine blocks in the blockchain. Therefore, it becomes difficult for x_w to compromise the proposed infrastructure by exploring distributed denial of service attack that overwhelms the blockchain and FL system. Thus the proposed privacy infrastructure ensures data availability at all times.

VI. SIMULATION RESULTS

Due to the unavailability of data on public awareness driven by blockchain, this study provides an empirical analysis of the expected outcomes of the proposed privacy infrastructure. The data used in this study to evaluate the proposed infrastructure is taken from CDC [43]. Besides, parameters of the blockchain-based epidemiological model are estimated using the least square method. The initial susceptible case $S(0)$ is equal to the number of inhabitants' population. Individuals that are quarantined will stay isolated for at least 14 days [37]. The period of incubation is 3-7 days and the average period to transit from hospitalized to recovery is 7-8 days. The implementation of the proposed architecture are found in Github¹. In Fig. 5, the accuracy of the FedMedChain is compared with

TABLE II: The values of parameters used in this paper [38]

Parameters	Description	Values
ϕ_B	Weight of blockchain effect on contact rate	0.8
R_q	Releasing rate of quarantined individuals per day	0.071
P_T	Transmission probability of effective infected individuals per contact	0.800
σ	Progression from exposed compartment to infected compartment per day	0.200
λ_B	Quarantined rate induced by awareness driven by blockchain technology	0.500
C_a	Effective contact rates for asymptomatic individual per day	0.200
C_s	Effective contact rates for symptomatic individual per day	0.100
ϕ_s	Hospitalized rate of infected individual per day	0.300
τ_s	Recovery rates of individuals in I_s compartment per day	0.330
τ_a	Recovery rates of individuals in I_a compartment per day	0.201
τ_h	Recovery rates of individuals in H compartment per day	0.130
δ_s	Hospitalized rates of individuals in I_s	0.110
δ_a	Hospitalized rates of individuals in I_a	0.102
δ_q	Hospitalized rates of individuals in E_q	0.200
C_m	Proportion of individuals exposed to COVID-19 virus during contact tracing	0.200
δ_h	Disease-induced death rate	0.003
μ_B	Reduction rate of public awareness due to limitations of blockchain technology	2.951
η_B	Response intensity of blockchain technology on newly confirmed cases	0.735
$(1-r)$	Fraction of exposed individuals who show symptoms at the end of the incubation period	0.130
$(1-C_m)$	Proportion of individuals missed during contact tracing	0.500
$(1-C_q)$	Proportion of individuals willing to stay quarantined	0.300
B_c	Rate of block creation by the leader per minutes	10
B_a	Number of awareness driven by blockchain technology	100
H_r	Relative hash power of CDC for block creation per second	1414

local learning using mean square error (MSE). In this study, 100 CDCs are used for the analysis. It is observed from the

¹Github implementation of the proposed architecture.

figure that the accuracy of each CDC varies, which means that the gradient from the best MSE value will be considered for training the model. The elapsed time for creating a block is

Fig. 5: Accuracy of the proposed FedMedChain

0.3910 seconds, while the cost of block creating is 1263 per second. The cost of block creation is computed based on the hash power, which is the ratio of the number of nonces to the number of elapsed time. Moreover, based on the proposed two rounds reinforcing addition, the leader among CDCs has a total cost of 137.

A. Impact of Public Awareness driven by Blockchain

The number of confirmed cases, which are linked to the number of EoIs collected by CDCs, is used to assess public awareness driven by blockchain technology. The analysis is done using a cross-correlation approach. The degree of linkage between the number of confirmed cases and the number of EoIs is determined via cross-correlation. Based on Eqs. (25) and (26), Eq. (27) is generated. From the equation, it is observed that the exposed class is 0.0016, which means that the COVID-19 has a negligible impact on the population as public media awareness induced by blockchain is adopted.

$$J(E, I_s, I_a, S_q, E_q, H) = \{0.0016, -0.0324, 0, -0.999, 0, 0\}. \quad (27)$$

To provide parameter estimation of the proposed model, the initial stage of the epidemic is evaluated using R_0 , which measures the mean of the newly infected individuals during the time of the infection. The next-generation matrix is employed to get R_0 . Besides, the total number of confirmed individuals, the total number of individuals that died and the total number of public awareness induced by blockchain technology are used to fit the model. If R_0 is greater than what WHO estimated, then the epidemic will be minimized and vice versa. In this study, the rate of contact, probability of disease transmission, period of incubation are the sensitivity parameters for evaluation. If the rate of contact and probability of transmission is minimized, then the disease peak time is delayed. This will eventually minimize the number of individuals hospitalized, infected and reduce the period of incubation. On the other hand, increasing the rate of infectious individuals that are hospitalized, the progressive rate of infectious individuals can minimize the peak size of both infected and hospitalized individuals. Improving the adoption of public awareness driven by blockchain technology on the number of confirmed individuals and quarantine rate of individuals can greatly reduce the peak size of individuals that are infectious and hospitalized. On the other hand, increasing blockchain awareness rate, blockchain induced quarantine rate, and blockchain impact on contact rate will reduce outbreak rate and increase the response rate to public awareness driven by blockchain technology.

B. Comparison with a Similar Framework in the Literature

Existing work in [50] develops a framework that is based on blockchain technology and FL for COVID-19. The framework takes a minimum amount of data from several sources to train the deep learning model. Besides, the framework is similar to our proposed privacy infrastructure; but there are differences between the two systems as described in Table III.

VII. CONCLUSION

This paper proposes an infrastructure based on FL and blockchain technology for IoMT scenarios. Firstly, an FL system is proposed to solve the problem of data privacy and inefficient prediction of COVID-19. Secondly, the blockchain is employed to ensure trust among entities, data immutability, availability and information security. In the blockchain system, a new consensus protocol is proposed based on the method of a reinforcing addition game. The proposed consensus protocol is used for the creation of blocks and the selection of miners. Thirdly, an epidemiological model is proposed, which includes the impact of blockchain technology on the control and prevention of COVID-19. Lastly, security and privacy analyses show that the proposed privacy infrastructure is robust against information security related attacks.

To the best of our knowledge, the proposed infrastructure is the first of its kind to fill the gap between blockchain technology and the COVID-19 pandemic. Moreover, the proposed infrastructural model addresses the limitations in technology for public communication and alleviates the stress for COVID-19 hotline centres. Also, this study aims that the proposed infrastructure will serve as a potential tool to forecast the evolution of public opinions. Furthermore, it will provide an idea on how to communicate public health strategies during global health crises, such as the present COVID-19 pandemic.

In future, we aim at implementing the proposed architecture to determine its real-time applicability and scalability. Besides, different assumptions regarding public behaviour will be considered in the formulation of the epidemiological model. In conclusion, we hope to collaborate with health institutions, practitioners and the government concerning the development of the prototype system of our proposed infrastructure.

REFERENCES

- [1] Fulian, Y., Jiahui, L., Xiaojian, Z., Xinyu, X., & Jainlong, W. (2020). COVID-19 Information Propagation Dynamics in the Chinese Sina-microblog. *Mathematical Biosciences and Engineering*, 17(3), 2676-2692.
- [2] Hemanth J. D., Anitha, J., & George A. T. (2021). *Internet of Medical Things: Remote Healthcare Systems and Applications*. Springer Nature.
- [3] Dayan, I., Roth, H. R., Zhong, A., Harouni, A., Gentili, A., Abidin, A. Z., & Li, Q. (2021). Federated learning for predicting clinical outcomes in patients with COVID-19. *Nature medicine*, 27(10), 1735-1743.
- [4] Qian, Y., Shen, J., Vijayakumar, P., & Sharma, P. K. (2021). Profile Matching for IoMT: A Verifiable Private Set Intersection Scheme. *IEEE Journal of Biomedical and Health Informatics*, 25(10), 3794-3803.
- [5] Jelodar, H., Wang, Y., Orji, R., & Huang, S. (2020). Deep sentiment classification and topic discovery on novel coronavirus or covid-19 online discussions: Nlp using lstm recurrent neural network approach. *IEEE Journal of Biomedical and Health Informatics*, 24(10), 2733-2742.
- [6] Jin, H., Dai, X., Xiao, J., Li, B., Li, H., & Zhang, Y. (2021). Cross-Cluster Federated Learning and Blockchain for Internet of Medical Things. *IEEE Internet of Things Journal*, 21(8), 15776-15784.
- [7] Mohamed, A. R., Shamim, M. H., Mohammad, S. I., Nabil, A. A., & Ghulam, M. (2020). Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access*, 8, 205071-205087.
- [8] Kumar, R., Khan, A. A., Kumar, J., Zakria, A., Golilarz, N. A., Zhang, S., & Wang, W. (2021). Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging. *IEEE Sensors Journal*, 1-14.
- [9] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a blockchain-based platform for healthcare information exchange. In *2018 IEEE international conference on smart computing (smartcomp)*, Taormina, Italy, 49-56.

TABLE III: Comparison with the proposed work with an existing work in literature. ✓: Yes, ✗: No

Ref.	Objectives	Techniques	Epidemiological Model	Threat Analysis
[50]	An efficient deep learning model for real-time detection of patients with COVID-19	Blockchain, FL, Lanczos interpolation and capsule network	✗	✗
Our scheme	A secure and decentralized COVID-19 epidemiological model that resolves issues of trust, privacy and data silos	FL, blockchain based epidemic model, DP and two rounds reinforcing addition game	✓	✓

- [10] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2021). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, 380-388.
- [11] Jiang, S., Cao, J., McCann, J. A., Yang, Y., Liu, Y., Wang, X., & Deng, Y. (2019, July). Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In *2019 IEEE International Conference on Blockchain, Atlanta, GA, USA*, 405-410.
- [12] Jiang, S., Cao, J., Wu, H., & Yang, Y. (2020). Fairness-based packing of industrial IoT data in permissioned blockchains. *IEEE Transactions on Industrial Informatics*, 17(11), 7639-7649.
- [13] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, 16(6), 4177-4186.
- [14] Kim, H., Park, J., Bennis, M., & Kim, S. L. (2019). Blockchain on-device federated learning. *IEEE Communications Letters*, 24(6), 1279-1283.
- [15] Pokhrel, S. R., & Choi, J. (2020). Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Transactions on Communications*, 68(8), 4734-4746.
- [16] Wim, N. (2020). Artificial intelligence vs COVID-19: limitations, constraints and pitfalls. *AI & Society*, 35, 761-765.
- [17] Jamshidi, M., Lalbaksh, A., Talla, J., Peroutka, Z., Farimah, H., Pedram, L., Morteza, J., Luigi, L. S., Mirhamed, M., Mojgan, D., Asal, S., Saeed, R., Sabhan, R., Nima, B., Bahare, M., Zahra, M., Alireza, J., Sarah, K., Hamed, H., & Wahab, M. (2020). Artificial Intelligence and COVID-19: Deep Learning Approaches for Diagnosis and Treatment. *IEEE Access*, 8, 109581-109595.
- [18] Raju, V., Mohd, J., Ibrahim, H. K., & Abid, H. (2020). Artificial Intelligence (AI) applications for COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 14 (2020) 337-339.
- [19] Yu, K., Tan, L., Lin, L., Cheng, X., Yi, Z., & Sato, T. (2021). Deep learning-empowered breast cancer auxiliary diagnosis for 5GB remote E-health. *IEEE Wireless Communications*, 28(3), 54-61.
- [20] Tan, L., Yu, K., Shi, N., Yang, C., Wei, W., & Lu, H. (2021). Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach. *IEEE Transactions on Network Science and Engineering*, 1-12.
- [21] Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., & Srivastava, G. (2021). An efficient ciphertext-policy weighted attribute-based encryption for the Internet of health things. *IEEE Journal of Biomedical and Health Informatics*, 1-12.
- [22] Sun, Y., Liu, J., Yu, K., Alazab, M., & Lin, K. (2021). PMRSS: Privacy-preserving Medical Record Searching Scheme for Intelligent Diagnosis in IoT Healthcare. *IEEE Transactions on Industrial Informatics*, 1-13.
- [23] Liu, Y., Yuan, X., Xiong, Z., Kang, J., Wang, X., & Niyato, D. (2020). Federated learning for 6G communications: Challenges, methods, and future directions. *China Communication*, 17(9), 105-118.
- [24] Aivodji, U. M., Gams, S., & Martin, A. (2019). IOTFLA : A secured and privacy-preserving smart home architecture implementing federated learning. In *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2019, pp. 175-180.
- [25] Wang, Y., Su, Z., & Zhang, N. (2019). BSIS: Blockchain based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network. *IEEE Transactions on Industrial Informatics*, 15(6), 3620-3631.
- [26] Samuel, O., & Javaid, N. (2021). GarliChain: A privacy preserving system for smart grid consumers using blockchain. *International Journal of Energy Research*, 1-17.
- [27] Harris, J. D., & Waggoner, B. (2019). Decentralized & collaborative AI on blockchain. In *Proc. IEEE Int. Conf. Blockchain*, Dec. 2019, pp. 1-9.
- [28] Zhao, Y. (2020). Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet Things*, 1-12.
- [29] Pokhrel, S. R. (2020). Federated learning meets blockchain at 6G edge: Adrone assisted networking for disaster response. In *Proc. 2nd ACM Mobi-Com Workshop Drone Assist. Wireless Commun. 5G Beyond*, Sep. 2020, pp. 49-54.
- [30] Qu, Y., Gao, L., Luan, T. H., Xiang, Y., S. Y., Li, B., & Zheng, G. (2020). Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet Things Journal*, 7(6), 5171-5183.
- [31] Hua, G., Zhu, L., Wu, J., Shen, C., Zhou, L., & Lin, Q. (2020). Blockchain based federated learning for intelligent control in heavy haul railway. *IEEE Access*, 8, 176830-176839.
- [32] Kim, H., Park, J., Bennis, M., & Kim, S. L. (2020). Blockchain on-device federated learning. *IEEE Communication Letter*, 24(6), 1279-1283.
- [33] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transaction on Industrial Informatics*, 16(6), 4177-4186.
- [34] Li, Z., Liu, J., Hao, J., Wang, H., & Xian, M. (2020). CrowdSFL: A secure crowd computing framework based on blockchain and federated learning. *Electronics*, 9(773), 1-21.
- [35] Majeed, U., & Hong, C. S. (2019). FLchain: Federated learning via MEC enabled blockchain network. In *Proc. 20th Asia-Pacific Netw. Oper. Manage. Symp.*, Sep. 2019, pp. 1-4.
- [36] Liu, Y., Member, S., Yu, J. J. Q., Kang, J., Niyato, D., & Zhang, S. (2020). Privacy-preserving traffic flow prediction: A federated learning approach. *IEEE Internet Things Journal*, 1(1), 7751-7763.
- [37] Weike, Z., Aili, W., Fan, X., Yanni, X., & Sanyi, T. (2020). Effects of Media Reporting on Mitigating Spread of COVID-19 in the Early Phase of Outbreak. *Mathematical Biosciences and Engineering*, 17(3), 2693-2707.
- [38] Chayu, Y., & Jin, W. (2020). A Mathematical Model for the Novel Coronavirus Epidemic in Wuhan, China. *Mathematical Biosciences and Engineering*, 17(3), 2708-2724.
- [39] Chenxi, D., Jing, Y., & Kaifa, W. (2020). Evaluation of Prevention and Control Interventions and its Impact on Epidemic of Coronavirus Disease 2019 in Chongqing and Guizhou. *Mathematical Biosciences and Engineering*, 17(4), 2781-2791.
- [40] She, H., Sanyi, T., & Libin, R. (2020). A Discrete Stochastic Model of the COVID-19 Outbreak: Forecast and Control. *Mathematical Biosciences and Engineering*, 17(4), 2792-2804.
- [41] Linping, W., Jing, W., Hongyong, Z., Yangyang, S., Kai, W., Peng, W., & Lei, S. (2020). Modelling and Assessing the Effects of Medical Resources on Transmission of Novel Coronavirus (COVID-19) in Wuhan, China, 17(4), 2792-2804.
- [42] Zhihua, L., Pierre, M., Ousmane, S., & Glenn, W. (2020). Predicting the Commutative Number of Cases for the COVID-19 Epidemic in China from Early Data. *Mathematical Biosciences and Engineering*, 17(4), 3040-3051.
- [43] Enahoro, A. I., Oluwaseun S., Calistus N. N., & Abba, B. G. (2020). Mathematical Modelling and Analysis of COVID-19 Pandemic in Nigeria, 17(6), 7192-7220.
- [44] Rabiya, K., Muhammad, W. M., Turki, A. A., & Nadeem, J. (2021). A Consortium Blockchain based Energy Trading Scheme for Electric Vehicles in Smart Cities. *Journal of Information Security and Applications*, 1(1), 2214-2126.
- [45] Chi, H. L., Qiuxia, L., & Shilin, W. (2019). Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning. *IEEE Transactions on Industrial Informatics*, 15(6), 1-11.
- [46] Lun, L., Jiqiang, L., Lichen, C., Shuo, Q., Wei, W., Xiangliang, Z., & Zonghua, Z. (2018). CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Transactions on Intelligence Transportation Systems*, 19(7), 1-17.
- [47] Zeeshan, A., Fahad, A., Ahmad, A., Muhammad, S., Mansour, Z., & Nadeem, J. (2020). An Attention Guided Semi-supervised Learning Mechanism to Detect Electricity Frauds in the Distribution Systems. *IEEE Access*, 8, 221767-221782.
- [48] Javaid, N., Hira, G., Sobia, B., Faisal, S., Chengjun, X., Lin, G., & Tanzeela, S. (2021). Using GANCNN and ERNET for Detection of Non-technical Losses to Secure Smart Grids. *IEEE Access*, 9, 98679-98700.
- [49] Egoshin, N. S., Konev, A. A., & Shelupanov, A. A. (2020). A Model of Threats to Confidentiality of Information Processed in Cyberspace based on Information Flows Model. *Symmetry*, 1-18.
- [50] Rajesh, K., Abdullah, A. K., Jay K., Zakria, N. A. G., Simin Z., Yang T., Chengyu Z., & Wenyong W. (2021). Blockchain-Federated-Learning and Deep Learning Models for COVID-19 detection using CT Imaging. *IEEE Sensor journal*, 1-14.