Internet of Things Framework for Oxygen Saturation Monitoring in COVID-19 Environment

Rahul Saha, *Member, IEEE*, Gulshan Kumar, *Member, IEEE*, Neeraj Kumar, *Senior Member, IEEE*, Tai-Hoon Kim, *Member, IEEE*, Tannishtha Devgun, Reji Thomas, and Ahmed Barnawi

***Abstract*—The pandemic/epidemic of COVID-19 has affected people worldwide. A huge number of lives succumbed to death due to the sudden outbreak of this corona virus infection. The specified symptoms of COVID-19 detection are very common like normal flu; asymptomatic version of COVID-19 has become a critical issue. Therefore, as a precautionary measurement, the oxygen level needs to be monitored by every individual if no other critical condition is found. It is not the only parameter for COVID-19 detection but, as per the suggestions by different medical organizations such as the World Health Organization, it is better to use oximeter to monitor the oxygen level in probable patients as a precaution. People are using the oximeters personally; however, not having any clue or guidance regarding the measurements obtained. Therefore, in this article, we have shown a framework of oxygen level monitoring and severity calculation and probabilistic decision of being a COVID-19 patient. This framework is also able to maintain the privacy of patient information and uses probabilistic classification to measure the severity. Results are measured based on latency of blockchain creation and overall response, throughput, detection, and severity accuracy. The analysis finds the solution efficient and significant in the Internet of Things framework for the present health hazard in our world.**

***Index Terms*—Covid, fog, healthcare, Internet, Internet of Things (IoT), medical, monitoring, privacy.**

I. Introduction

THE PRESENT world is facing one of the most devastating pandemics of the years known as COVID-19. As per the World Health Organization (WHO) report, more than 150 million of people are infected by the deadly corona virus with a death toll of more than 3.2 million [1]. The second wave of this pandemic is also in existence. Almost all the countries of the world are suffering from this virus infection. The major symptoms researched for this infection include fever, sore throat, dry cough, and other respiratory trouble. Apart from these intense symptoms, the mutated viruses are also developing the mild symptoms with less oxygen saturation, tiredness, and others that are very common in daily lives due to other health issues. Furthermore, the asymptomatic patients are very crucial to be diagnosed or detected at the early stage leading to the failure of the required medical help [2]. Therefore, doctors are recommending every individual to monitor their oxygen saturation measurements on daily basis and any deviation from the standards can be reported for medical help even though other COVID-19 symptoms are not existing [3], [4]. It is true that oximeter reading is not the screening process for COVID-19 but, it helps for early detection and precaution measures. With this connection, people are having their oximeters; however, the obtained measurements are not properly analyzed, and sometimes they do not try to convey the measurements to the medical team out of fear and/or lack of awareness. This leads to the critical problem in the present situation to detect the COVID-19 patients in advance of time. As a result, countries are counting on the increased number of deaths.

The Internet of Things (IoT) has shown its potentials in healthcare systems [5]. However, in the present situation of the pandemic, the applicability of the IoT infrastructure is less identified due to the pandemic's sudden exploration. Though various wireless oximeters, fitness bands are available in market but, their significant usage for the pandemic situation is missing. Therefore, a system is urged to be developed so that the medical team can direct the asymptomatic patients or detect them properly. An observation of the oxygen level in blood is to be monitored and analyzed probabilistically to analyze the COVID-19 infection. Thus, the proper isolation or medical facilities can be provided to the patients on time. Along with this medical help, privacy issues are also important [6]. Many incidents have been observed during this COVID-19 pandemic that affects the social networking of the patients leading to depression and other psychological problems [7]–[9]. Therefore, in this present work, we address the above problems and provide a solution with an IoT and fog computing framework. The framework provides a probabilistic classification for patients' severity based on the oximeter values. The severity is calculated based on this probability to

Manuscript received January 5, 2021; revised March 26, 2021 and May 12, 2021; accepted July 14, 2021. Date of publication August 5, 2021; date of current version February 21, 2022. *(Corresponding authors: Gulshan Kumar; Tai-Hoon Kim.)*

Rahul Saha and Gulshan Kumar are with the School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India (e-mail: rsahaaot@gmail.com; gulshan3971@gmail.com).

Neeraj Kumar is with the Department of Computer Science and Engineering, Thapar University, Patiala 147004, India, also with the Department of Computer Science and Information Engineering, Asia University, Taichung City 413, Taiwan, and also with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India (e-mail: neeraj.kumar@thapar.edu).

Tai-Hoon Kim is with Konkuk University (Glocal Campus), Seoul 27478, South Korea (e-mail: taihoonn@daum.net).

Tannishtha Devgun is with Nokia Solutions and Networks Private Ltd., Karnal 132001, India (e-mail: jmd.tannishtha@gmail.com).

Reji Thomas is with the School of Chemical Engineering and Physical Sciences, Lovely Professional University, Phagwara 144411, India (e-mail: rthomas.eyyalil@gmail.com).

Ahmed Barnawi is with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: ambarnawi@kau.edu.sa).

Digital Object Identifier 10.1109/JIOT.2021.3098158

avoid fatal deaths. The novelty of the our presented solution are: 1) the framework monitors the oxygen saturation in blood as a critical factor of COVID-19 severity symptom; 2) it uses the IoT-fog framework and blockchain for transmission and analysis of the measurements; 3) probabilistic classification of severity is implemented; and 4) privacy of the patients are ensured, only the authorized health center can access patients' location for medical help.

We have organized the remainder of the article as follows. Section II discusses some developments for the COVID-19 environment. These developments majorly analyzes the e-healthcare perspectives and machine-deep learning-based image analysis for COVID-19 detection. Section III shows the proposed system, including the network model used for the solution, preliminaries used for the understanding of the system, and blockchain approach. Section IV analyzes the performance of the solution. We conclude this article in Section V.

II. Related Work

COVID-19 is also considered as a novel coronavirus infection and, therefore, it can be called zero-day vulnerability for human health. In this section, we review the existing literature in two halves. The first half deals with the existing e-healthcare developments and frameworks; the second half shows the existing computing research status on COVID-19.

A monitoring system in e-healthcare with geo-distribution clouds is shown in recent past [10]. It ensures minimum service delay and privacy preservation. Traffic analysis problem is reduced by transforming the health information data into nonhealth information data. A nonlinear dynamic model for interpreting the spatial and temporal dynamics of epidemics is researched significantly [11]. It is based on the susceptible-infected-removed (SIR) type. The problem is formulated with a Bayesian framework and is estimated using the probability hypothesis density (PHD) filter. Daily patient monitoring reports are available for prediction. Early prediction of the epidemic in terms of peak and duration can be predicted with the known model parameters. Facial surface electromyogram-based pain monitoring tool also has been proved significant in e-healthcare [12]. This is based on the IoT-cloud framework and depends on a face mask that works as a sensor node. The applicability of the IoT framework in healthcare and patient monitoring is researched significantly [13]. Some of the IoT-based solutions for the remote patient monitoring purpose are worth mentioning here [14]–[16]. In the same direction, the energy efficiency in IoT-based patient monitoring activity has been also triggered [17]. A recent study in this direction shows the application of artificial intelligence techniques in IoT for patient assistance and care [18]. It uses an iterative golden section-optimized deep belief neural network (IGDBN). A data mining-based monitoring system with the IoT framework for cardiac arrhythmia patients is well researched recently [19]. The observation that has been concluded for these literature is that the IoT-fog-cloud framework has been well utilized in e-healthcare but precisely emphasis has been provided for patient monitoring functions. However, the prediction model in IoT for e-healthcare is less researched. When we talk about the healthcare data or patient data, privacy is an important factor. An exhaustive survey for security and privacy issues in healthcare is discussed recently [20]. A blockchain-based security solution for e-healthcare records storage and maintenance shows the feasibility of blockchain implications in this direction [21]. Some other privacy-preserving developments are shown in [22] and [23]. The former uses a identity-based verifiable storage system for healthcare and the latter uses electrocardiogram-based authentication.

As COVID-19 pandemic has affected the global health, technological frameworks, and infrastructures are also in the continuous research mode to enhance the monitoring, detection, and other functionalities related to COVID-19. In this direction, comprehensive surveys and discussions are available that show the importance of IoT and blockchain applications in the COVID-19 situation [24], [25]. The efficiency of the SIR model in [11] has been enhanced by the application of the SIER model in [26]. This model is based on the ordinary differential equation. As the COVID-19 infection is related with respiratory syndromes, the chest X-rays are the important factor for detecting this disease. Taxonomical understanding, systematic survey, and applicability of artificial intelligence techniques help us about the knowledge base for the ongoing work in this domain [27]. Some of such applications are significantly contributory. For example, CoroNet [28], nCOVnet [29], and CovXNet [30]. Some other methods include the deep learning methods [31]–[35]. One method for disease spreading monitoring is researched using point-of-care diagnostics and the IoT framework [36]. A detection method for COVID-19 patients with the hybrid feature selection and enhanced KNN classifier is a significant contribution [37]. The other detection techniques are summarized in [38]. The discussion regarding IoT-based COVID-19 research clearly shows that the detection process with chest X-ray images are more operational, whereas the other factors, such as prediction models, predictive patient isolation, and the blockchain feasibilities are less studied. Moreover, apart from the chest X-rays the other symptoms are in concern for COVID-19. The shortness of breathing is another critical observation [39]. Therefore, oxygen-saturation is required to be monitored for early prediction of COVID-19 patients for rapid diagnosis, which is missing in the existing literature. Trouble in breathing can also occur for plenty of other reasons such as smoking, cough, asthma etc.; therefore, a proper analysis of oxygen-saturation trend can be helpful for the prediction process. To address this issue and enhance the COVID-19 analysis process, the present work shows a prediction model of oxygen-level monitoring through IoT infrastructure and blockchain-based implications. The major contributions are: 1) the present work considers the oxygen-saturation levels with oximeters available with individual for predicting COVID-19 suspicious cases; 2) the framework uses IoT as an infrastructure with fog computing and blockchain applications for analysis the recorded data for prediction with the assurance of required security and privacy of the patient data; and 3) the intuitive results promises and proves to be beneficial for detecting the COVID-19 cases in early prediction

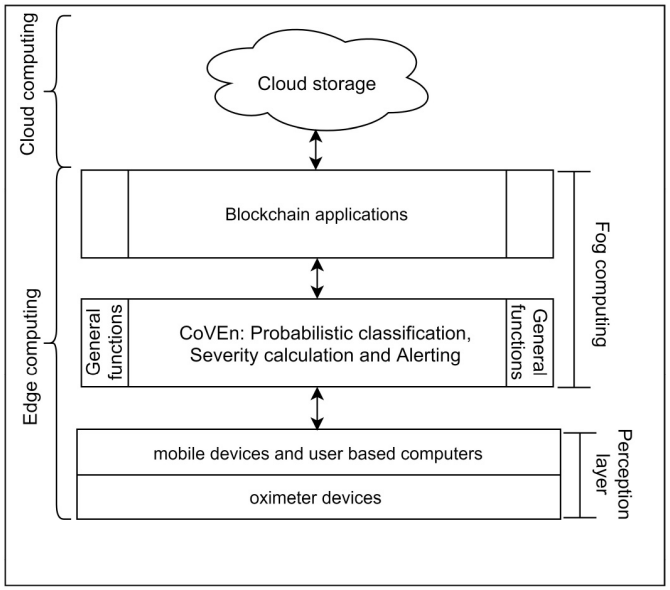

Fig. 1. Proposed framework of the solution.

and moving toward further medical assistance and isolation process.

III. Proposed System

The present work in this article is motivated from our previous works as mentioned in [40]. The framework uses oximeters and mobile devices in the perception layer. The oximeters read the oxygen saturation in the human body and passes the data to the mobile devices either manually (manual application for recording the oxygen parameter) or wirelessly (Bluetooth-based oximeters). After receiving the readings, the fog computing along with its general functions uses the COVID-engine. The main function of the engine, named CoVEn, uses the probabilistic classification of oximeter readings and calculate the severity levels. It also generates alert for severity levels accordingly for the users and the nearby healthcare officials. The later phase is beyond the scope of the present work and has been considered for future extension. One thing needs to be assumed here; the presented work considers that the health centers are connected in peer-to-peer (P2P) basis to utilize the blockchain provisions. More specifically, a consortium blockchain among the health centers are used here. We show the overall framework of the proposed solution in Fig. 1.

A. Network Model

The network model considered here is hybrid in nature. It means that both the client server (CS) architecture and the P2P architecture are used in the network model utilization. CS is responsible for oximeter reading and transmitting to the fog layer and receiving the alerts accordingly. P2P main functions in the consortium blockchain. We show the network model in Fig. 2.

To generalize the concept, we assume to have a network of n nodes (mobile devices having oximeter readings). The nodes transmit the data to CoVEn with the help of mobile communication and WiFi, i.e., the IoT infrastructure is used here. CoVEn works as an analysis engine, synonymous to the part of a distributed server helping in the blockchain data storage. The consortium blockchain shown in Fig. 2 is comprised of health centers H_1, H_2, H_3, H_4 connected with each other and forming a P2P network. In generalization, N number of health centers are to be considered as peers. Therefore, the total network size $\mathcal{N}$ is: $\mathcal{N} = n + N$.

B. Preliminaries

As the framework is related with medical data and patients' data privacy and security is important in such applications; cryptographic approaches are also required to be ensured. For all the cryptographic operations, we use the group constructs. Two groups G_1 and G_2 are considered to be the cyclic groups of same order q. G_1 is an additive group and G_2 is a multiplicative group. A bilinear map $e : G_1 \times G_2 \rightarrow G_e$ is used as a function. This function considers $\forall u \in G_1$ and $\forall v \in G_2; a, b \in \mathbb{Z}$, such that [41]

$$e\left(u^a, v^b\right) = e(u, v)^{ab}.$$

These mapping functions are also called as bilinear pairings. Let, g_1 and g_2 be the group generators of G_1 and G_2, respectively, the bilinear map is admissible if $e(g_1, g_2)$ is able to generate the elements of G_e and e is efficiently computable. Such admissible mapping should also possess the property of nondegeneracy and computability.

Nondegeneracy: A bilinear map $e : G_1 \times G_2 \rightarrow G_e$ is nondegenerate if it satisfies the conditions.

1) $Ker(e) = \{0\}; e(u, v) = 0\ \forall u \in G_1$ implies $v = 0$ and *vice versa*.
2) $dim\ G_1 = dim\ G_2$.

Computability: There exists an efficient algorithm to compute $e(g_1, g_2)$ for $g_1 \in G_1$ and $g_2 \in G_2$.

C. System Approach

CoVEn is basically a module working as the data aggregator (DG) with some security provisions. It is also configured in a way such that CoVEn must be connected with a key generator (KG), which is trusted and responsible for the generation of keys and verifying other cryptographic operations. In this section, we discuss the phases of the proposed system's functionalities. CoVEn's logical architecture is shown in Fig. 3. It shows that the data from devices come to the DG in a signcrypted format; DG verifies the authenticity of the message, unsigncrypts it, and processes it for the probabilistic classification. It also calculates the severity and generates the alerts to the users' devices.

1) Registration and Key Generation: The data of oximeters are passed on to the mobile devices and then sent to the CoVEn. Therefore, keeping in mind the security dynamics of mobile devices, the framework needs to utilize some cryptographic authentication services. For this purpose, we have used the bilinear pairings-based signcryption–unsigncryption for transferring the data from users to CoVEn. The process starts with a registration phase. In this phase, mobile devices send the integrated circuit metrics (ICMetrics) data to the

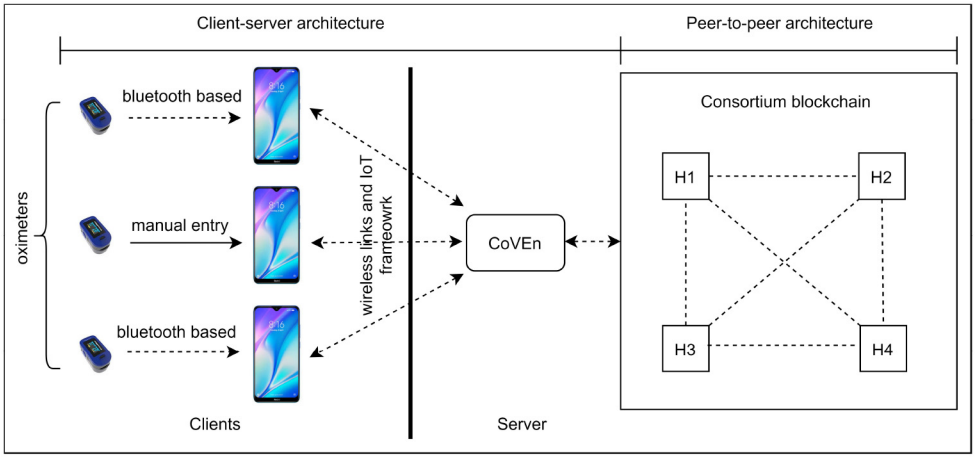

Fig. 2. Network model for the proposed architecture.

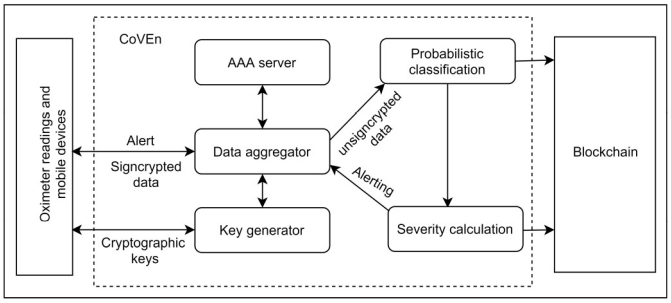

Fig. 3. CoVEn components.

CoVEn for generating the keys [42]. It uses system-level characteristics to provide identification of the devices. We then map the ICMetrics to provide a pseudo-identity to the devices and the mapping can be stored separately by the network operator(s). We assume here that the framework already has obtained the ICMetric data from the operator and then proceeds accordingly. These ICMetrics data are the initialization point in the registration phase. Receiving these data, KG computes hash of it. PHOTON-256 hash (PH) is used here [43]. This hash algorithm provides the benefits of lightweight and less complexity. KG generates the private-public key pair (K_{u+}, K_{u-}) for the respective user (device willing for registration). KG inputs a random point on an elliptic curve E over a finite field $\mathbb{Z}_q$ with an order $p = q^k$, where q is a random prime number and k, a, and b are the integer elements such that: $y^2 = x^3 + ax + b$, $(a, b) < q$.

It then computes a master secret key (msk) and system parameters *(param)*. These parameters further help the device in the signcryption process. Once this registration is completed and system parameters are set up, the hashed ICMetrics and timestamp t are processed along with the msk and param. The timestamp is of 64 bits. Timestamp helps for preventing stale or revocation of the keys. δt is used for synchronizing the system time error. The given ICMetrics identity (ICM) of the device is hashed with PHOTON-256 to output $\mathrm{ID}_{(u_i)}$ as: $\mathrm{ID}_{(u_i)} = PH(ICM)^{256}_{\{0,1\}}$. Using this hashed identity, KG's msk, and master public key, device-based key pairs are calculated

Algorithm 1 Registration and Key Generation

Input:$y^2 = x^3 + ax + b$
Output: (K_{u+}, K_{u-})
Obtain a cyclic additive group G_1 from $\mathbb{Z}_q$ of prime q order with generator g_1
Obtain the non-zero elements of $\mathbb{Z}_q$ to generate the cyclic multiplicative group G_2. The order of this group should be q and generator is g_2.
e:$G_1 \times G_1 \rightarrow G_2$
Select a random number $r \in \mathbb{Z}_q^* \rightarrow msk, G_1 \subseteq \mathbb{Z}_q^*$
Master public key $(mpk) = r.g_1.g_2$
KG public key $(K_{(v+)} = mpk.g_1.g_2$
Initialize the hash function PH
Publish param:$\{G_1, G_2, e, g_1, g_2, K_{v+}\}$
Compute $ID_{u_i} = \{PH(ICM)\}^{256}_{\{0,1\}}$
$K_{u-} = (msk.ID_{u_i}||(t + \delta t)$
$K_{u+} = (mpk.ID_{u_i} \parallel (t + \delta t)$
Return K_{u+}, K_{u-}

and sent to the users through a preassumed secure channel. The overall process is summarized in Algorithm 1.

2) Oximeter Signcrypted Transmission: Once the oximeter readings are obtained from the patients, either the smart healthcare network or the manual accounting through mobile devices is done. The mobile device (user) sends the reading data in a signcrypted way. These reading data contain the age, sex, address, location area (mobile device), and oxygen saturation measurements *osm*. In generalization, these data can be represented as a message $\mathscr{M}$ of variable size, which is given as

$$\mathscr{M} = \{\text{age, sex, address, locationarea, osm}\}.$$

Therefore, it means that the mobile device sends the signcrypted message over the transmission medium of the IoT framework. The reasons for using signcryption include to reducing network overhead, less complexity, and less time consuming, which are the inherent advantages of signcryption methods over generic confidentiality-authentication schemes. The keys generated in the registration phase are used for this signcryption. A registered mobile device or user u_i executes a

Algorithm 2 Signcryption for Data Request

Input:$param$, $\mathscr{M}_i$, K_{u-}, K_{v+}
Output: $\mathscr{M}$
Choose two random numbers $r_1, r_2 \in \mathbb{Z}_q^*$
Compute $Y_i = r_1.K_{v+}$
Compute $S_i = r_2^{-1}(K_{u-} + g_1.g_2)$
Compute $\mathscr{C}_i = E(\mathscr{M}_i||r_2)_{(K(v+))}$
Compute $H_i = PH(\mathscr{C}_i, Y_i, S_i)$
Compute $W_i = r_2(r_1 + H_i)modp$
Return C_i:$\mathscr{C}_i, Y_i, S_i, W_i$

Algorithm 3 Unsigncryption by DG

Input: $\mathscr{C}_i$
Output: $\mathscr{M}_i$
Compute $Dec(\mathscr{C}'_i)_{K_{v-}}$
Compute r'_2
Compute $r'_1 = Y^{-1}.K_{v+}$
Compute $H'_i = PH(\mathscr{C}'_i, Y'_i, S'_i)$
Compute $W'_i = r'_2(r'_1 + H'_i)modp$
If $W'_i = W_i$, then accept M'_i as M_i else abort

signcryption process. The signcryption process inputs *param*, message $\mathscr{M}$, private key K_{u-}, and KG's public key K_{v+}. The process outputs a signcrypted message $\mathscr{C}$. This message is then transmitted along with the ID_{u_i}. The process is shown in Algorithm 2. Here, $E()$ represents Hummingbird encryption function, which enhances the complexity reduction and provides standard security [44].

3) CoVEn Unsigncryption: DG receives the signcrypted messages C_i and unsigncrypts them. After unsigncryption, it sends the data for analysis with the probabilistic classification phase. The unsigncrypted data are sent further by DG only if they are found secure, else the received C_i is aborted. To verify the security parameters, DG takes the help of KG for security service verification. As signcryption–unsigncryption is used here, the framework ensures the security services of confidentiality, integrity, digital signature, and nonrepudiation and privacy in addition. DG accumulates all signcrypted messages C_i with corresponding ID_{u_i} so that the consecutive readings of a user can be correlated and processed for probabilistic classification. Consider that DG has received a version of C_i as $C'_i : \mathscr{C}'_i, Y'_i, S'_i, W'_i$. DG decrypts $\mathscr{C}'_i$ using its preconfigured private key K_{v-}. It then obtains $(M'_i||r'_2)$. It computes r'_1. Then, the hash value of $\mathscr{C}'_i$, Y'_i, and S'_i is calculated using PHOTON-256. This hashed output is then used for the calculation of W'_i and is compared to W_i. If the matching result is true, $\mathscr{M}'_i$ is accepted. The process is summarized in Algorithm 3.

Once CoVEn receives the measurements of oximeters in $\mathscr{M}'_i$, it maps the data with ID_{u_i} and stores in the database. The decreasing oxygen saturation level is having the pivot role in the presented solution. However, the decreasing oxygen saturation level needs to be monitored multiple time. Therefore, CoVEn stores the values of oxygen saturation corresponding to ID_{u_i}. Whenever a message is unsigncrypted, DG searches ID_{u_i} in the database, if found, then it appends the values in a time-based function; else, it adds the new ID_{u_i} and maps the saturation value for further processing. Fig. 4 shows this data aggregation process in CoVEn.

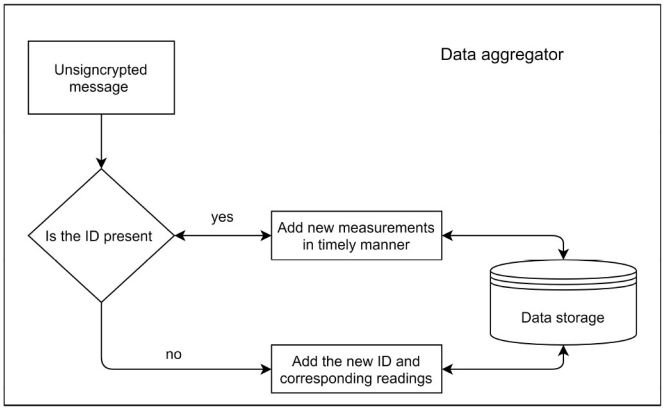

Fig. 4. Data aggregation process.

4) Probabilistic Analysis: The data stored by the DG are processed for probabilistic classification. The probabilistic classifier is used to predict for a given input of observation sets and a probability distribution over a set of classes. As a categorization of this classifier, the presented framework uses binary classification [45]. Binary classification is used to classify the elements of a given set into two groups; hence, the name is "binary." It predicts the belongingness of the elements in a group on the basis of a classification rule [46]. In the literature, we observe that binary classification is already in use for COVID-19 detection [31]; however, medical images (chest X-rays) are used for this. Therefore, it is a novelty of the presented framework that analyzes the probability based on oxygen saturation using an IoT framework.

Binary classification using the Probit Model [47] is advantageous in the presented framework as it uses two classes: 1) suspicious and 2) nonsuspicious. These two classes are considered to be the elements of a response Y. This model also uses a vector of regressors X which are assumed to influence the outcome Y . The relationship between X and Y is given as

$$P(Y = 1|X) = \varphi\left(X^T\beta\right)$$

where P is the probability, φ is the cumulative distribution function (CDF) of the standard normal distribution, and β is calculated by maximum likelihood estimate (MLE). Consider the system works on a data set $\{x_i, y_i\}_{i=1}^n$, where x_i is an oximeter data and y_i is the classification response. For the single oximeter reading observation, conditional probability on the vector of inputs of that observation, CoVEn calculates the following:

$$P(y_i = 1|x_i) = \varphi\left(x_i^T\beta\right), \text{ and}$$
$$P(y_i = 0|x_i) = 1 - \varphi\left(x_i^T\beta\right)$$

where x_i is calculated as $k\times 1$ vector, i.e., oximeter readings for a single user and β is calculated as the vector of coefficients. Following this, the likelihood is estimated for a single user observation as

$$\mathscr{L}(\beta; x_i, y_i) = \varphi\left(x_i^T\beta\right)^{(y_i)}\left[1 - \varphi\left(x_i^T\beta\right)\right]^{(1-y_i)}.$$

Algorithm 4 Probabilistic Classification

Input: x_i
Output: $P(y_i)$
Initialize threshold of saturation *th*
Initialize binary class: suspicious=1, non-suspicious=0
If ($osm < th$)
$P(y_i) = 1$
Else
{
For (m successive osm)
If ($x_i > x_(i+1)$)
Compute $ln\mathscr{L}(\beta; x_i, y_i)$
Severity alert ( )
Return $P(y_i)$
}

Algorithm 5 Severity Alert ()

Input: osm_i
Output: alert
If ($osm_1 < th$)
alert = high
Else
{
for i=1 to m
{
Calculate $\delta_i = osm_i - osm_{(i+1)}$
If (δ_i is in decreasing mode)
alert = high
Else
alert = low
Return alert

Since the observations are independent and identically distributed, the likelihood of the entire sample (n users), or the joint likelihood is calculated as the product of the likelihoods of the single observations as

$$L(\beta; x_i, y_i) = \Pi_{(i=1)}^{n} \varphi\left(x_i^T \beta\right)^{(y_i)} \left[1 - \varphi\left(x_i^T \beta\right)\right]^{(1-y_i)}.$$

Following the joint likelihood, the joint log-likelihood function is calculated for all the observations as:

$$\ln\mathscr{L}(\beta; x_i, y_i) = \sum_{(i=1)}^{n} y_i \ln\left(\varphi\left(x_i^T \beta\right) + (1 - y_i)\ln\left(1 - \varphi\left(x_i^T \beta\right)\right)\right).$$

The estimator $\hat{\beta}$ maximizes the function if $E[XX^T]$ is nonsingular. This log-likelihood function is globally concave in β and converges fast to the unique maximum. $\hat{\beta}$ is given by the following.

$$\sqrt{n}\left(\hat{\beta}, \beta\right) \rightarrow \mathscr{N}\left(0, \Omega^{(-1)}\right) \text{ where}$$

$$\Omega = \frac{E\left[\left(\Phi^2\left(X^T\beta\right)\right)\right]}{\left(\varphi\left(X^T\beta\right)\left(1 - \varphi\left(X^T\beta\right)\right)XX^T\right.} \text{ and}$$

$$\hat{\Omega} = \frac{1}{n}\sum_{(i=1)}^{n} \frac{\left(\Phi^2\left(x_i^{(}T)\hat{\beta}\right)\right)}{\left(\varphi\left(X^T\hat{\beta}\right)\left(1 - \varphi\left(X^T\hat{\beta}\right)\right)\right)} x_i x_i^{(T)}.$$

$\Phi = \varphi^T$ denotes the probability distribution function of the standard normal distribution.

Note that this probabilistic classification is applicable for a span of multiple readings for each user, if any user's reading is found less than the oxygen saturation threshold *th*, the probability can be fixed as 1 and severity can be calculated accordingly. In the present experimentation process, 95% oxygen saturation is considered as *th*. The summarization of this phase is shown in Algorithm 4.

5) Severity Detection and Alerting: The above phase classifies the user readings as suspicious or nonsuspicious for COVID-19 infection. Along with this classification, the present solution also uses severity detection depending upon how rapid decrease of oxygen saturation needs medical help; thus, to generate an alarm to the user to visit near by medical center. The severity is alarmed to the users in either of the three levels: 1) low; 2) mild; and 3) high. We use the Severity alert ( ) with the following conditions as shown in Algorithm 5 to generate the alarm back to the users. Note that this is a user-specific calculation.

The alerts are then responded back to the user by CoVEn using the application alerts. These responses also use the same IoT infrastructure for obtaining the alert responses.

6) Data Block Generation: Once the CoVEn calculates classification probability and severity alert, the same data are also transmitted in the blockchain. To create the blockchain, the DG bundles the transactions of messages (oximeter messages and alerts) in a single block. Being the consortium blockchain, the proof of blockchain member authenticity is not important. However, some special issues like compromised peers or 51% handling problem can be researched as future work on this present framework. The use of the blockchain in the present solution is having the objectives such that using the severity and classification results, the medical help can be properly provided to the required patients of COVID suspects. Along with this, every stakeholder involved in the process; for example, medical officers, medicine suppliers, and resource managers can also be beneficial using the information of the this blockchain. Moreover, an overall monitoring process by the government can be issued. The block generation is shown in Fig. 5. Blocks B_i are generated periodically by the CoVEn

7) Consensus and Chaining of Blocks: Reputation-based Byzantine fault tolerant (RBFT) is used in the framework as it is suitable for a consortium network. It provides the required benefits of decentralization, transaction finality, security and reliability, increased throughput, and reduced delay [48]. In the presented framework, a customization of RBFT is executed to reach the consensus decision. After the creation of the block B_i , the validator broadcast it in the blockchain network. The members of the blockchain validate the information of the block individually and sign the header of the block initiated. The signatures from the entities are working as votes. The use of the consortium blockchain and this vote-based consensus help in advantageous factors of low latency, high speed and prevention of 51% attacks. For signature, lightweight identity-based signature is used [49]. However, any other signature schemes can also be used here. Algorithm 6 shows

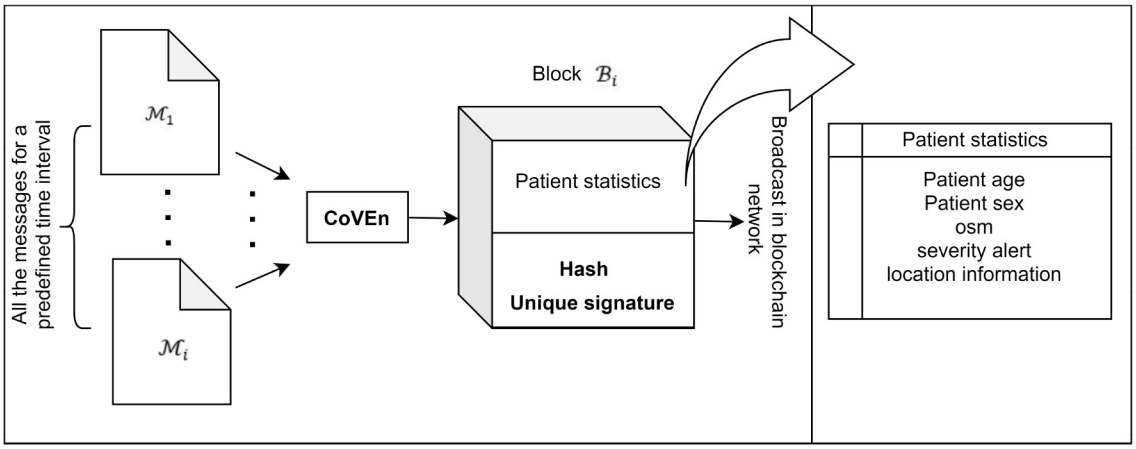

Fig. 5. Single block generation by CoVEn.

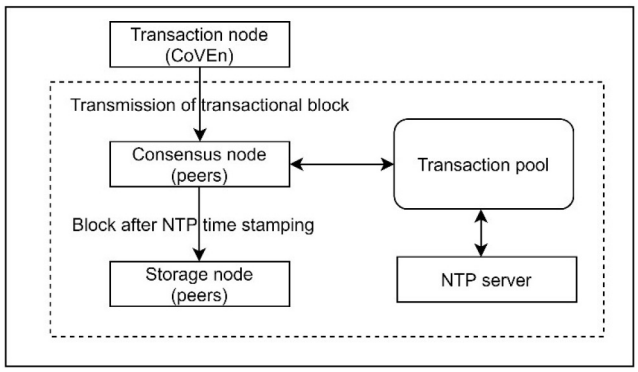

Fig. 6. Customized RBFT in the system.

the consensus approach. We assume N number of members in the consortium and μ unique signatures to be executed on the block B_i for the block to be verified. Here, verification only needs to be checked for the integrity of the block information and data availability in distributed orientation. RBFT functioning is shown in Fig. 6.

Algorithm 6 Customized RBFT and Block Chaining

Input: B_i
Output: Consensus decision
CoVEn: Broadcast B_i
Verify the transactions and write into local transaction pool
for (member=i to N)
{ calculate Sig(B_i:header);
$j++;$}
If ($j \geq \mu$)
{
NTP server invoke
Compute timestamp and hash
Consensus = true
Update the blockchain
}
Else
Wait for next time period T
Return consensus

IV. Performance Analysis

The presented framework has been experimented with system configuration and specifications as shown in Table I. It classifies the specifications in two parts: 1) prerequisite for hyperledger fabric and 2) framework specification for hardware. Reputation-based Byzantine Fault Tolerance is coded in C++ and integrated with the Python framework. The blockchain feasibility in COVID-19 prediction with oxygen saturation is a novel exploration in the direction of disease detection and therefore, direct comparative study is insignificant. The experimental specifications, performance metrics, and results are discussed in the following sections.

A. Experimental Environment

The technical specification maintained for executing the Hyperledger Fabric is shown in Table I as experimental parameters and specifications. The implementation of hyperledger fabric is followed from the guide [50]. Hyperledger caliper is also installed and implemented as per the solution requirement to monitor the system performance [51].

B. Evaluation Metrics

As per the Caliper framework of the benchmark test, latency and throughput are measured for the present system. Besides, the detection percentage and severity accuracy are also evaluated based on 100 probable candidates as samples. The candidates are aged from 25 to 55 years.

Latency: The time between a submission of a request and the receipt of a response. The blockchain-based latency is measured as

$$\text{Blockchain Latency} = (\text{Confirmation time @ decision threshold}) - \text{submit time}.$$

Latency is also measured from the networks perspectives. It is measured as

$$\text{Network Latency} = \text{Alert receiving time} - \text{submit time of oximeter readings}.$$

TABLE I
TECHNICAL REQUIREMENTS AND SPECIFICATION

Pre-requisite specification used for Hyperledger Fabric	CPU	Core i7, 7th Generation
	RAM	16 GB
	ROM	1 TB
	Operating system	Ubuntu Linux 14.04 LTS (both 64-bit)
	Docker Engine	Version 17.03
	Docker-Compose	Version 1.8
	Nodejs/ node-gyp	Version 8.9
	Node Package Manager	Version v5.x
	Git	Version 2.9.x or higher
	Python	Version 2.7.x
Proposed framework specification	Consensus protocol	Customized RBFT
	Geographic distribution of nodes	Ethereum network
	Hardware environment of all peers	3.6 GHz, 16 GB RAM, Octa-core, 2 TB HDD
	Blockchain environment	1 server as CoVEn, 20 peers, P2P network
	Perception nodes category 1	Oximeter (Hesley, PC-60F) – 15 nos
	Perception nodes category 2	Smartphones (Samsung, Redmi, Apple) – 35 nos
	Test tools and framework	Hyperledger Caliper
	Type of data store used	CouchDB

Throughput: It measures the flow rate of all the block transactions through the system in transactions per second (tps), during a cycle T. It is measured as

$$\text{Blockchain Throughput} = \text{Total committed transactions}/\text{total time in seconds}\ \#\text{committed nodes}.$$

Detection Accuracy: As the sample size is 100 in the experimented solution, detection accuracy is the ratio of total number of candidates detected accurately for COVID-19 suspects. We also follow up from those candidates and have validated the results.

Severity Accuracy: If a candidate is detected to be positive for COVID-19, the severity is also validated. It is measured as

$$\text{Severity accuracy} = (\text{suspects of a severity class})/(\text{Number of samples of suspects}).$$

We consider three severity classes, the validation is measured for all the three classes: 1) low; 2) mild; and 3) high.

Cost measurement: The cost measurement is also important for a system. Two types of costs are measured for the presented framework: 1) computational cost and 2) transaction cost. Computational cost refers to the complexity of the computation for generating the blocks. Transaction cost refers to the complexity of communicating the blocks in the network and its successful commitment.

C. Results and Discussion

First, the blockchain latency metrics are measured in maximum, minimum, and average. Maximum and minimum are calculated for all the peers and all the blocks for a time period T and the average of all maximum and the average of all the minimum are calculated. The results are also compared to the increasing number of peers and shown in Table II.

Table III shows that the maximum latency increases with the number of peers with an average increasing factor of $+1.53$. The minimum latency also increases with the average increasing factor of $+1.30$. The use of signcryption and lightweight cryptographic processes induces these latency values, which is stable and can be used significantly in blockchain applications in the IoT paradigm. Furthermore, network latency is also measured by increasing the number of users from 5 to 100. The result is shown in Fig. 7. It infers that the latency in the presented solution is linearly dependent on the number of users as the blockchain processes and its internal calculations are not generating any overhead. Besides, it also infers the linear stability of the system and avoids drastic fluctuation of jitter. Thus, it becomes suitable for network applications. The statistical relationship between network latency and the number of users can be generalized as

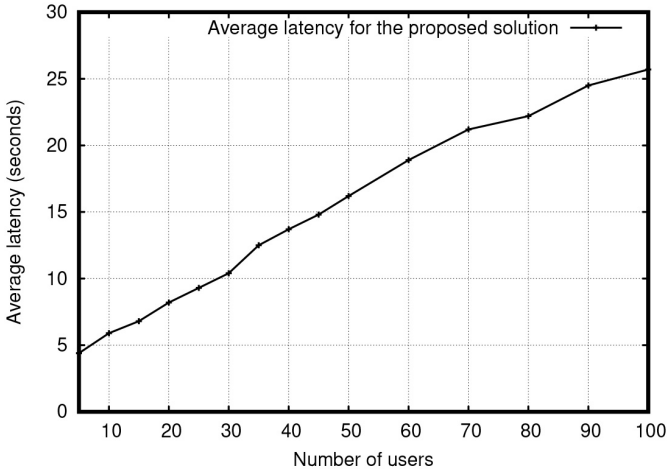

Fig. 7. Latency with the increasing number of users.

$$\text{Network latency} = \delta + O\delta(\log n).$$

where δ is the initialized latency factor and n is the number of users.

Next, the observation is made on throughput. It is measured in two ways. First, with the increasing number of peers, the send rate varies; however, the average send rate is listed in Table III. The outputs measure throughput at successful commits of the blocks in the network. It shows that the average throughput for the proposed solution increases; however, the overall stability is observed with an approximated factor of 0.8 of the send rates. Here, throughput is measured for all the

TABLE II
BLOCKCHAIN-BASED TRANSACTIONAL LATENCY

No. of peers	Success	Fail	Maximum latency (average) in seconds	Minimum latency (average) in seconds	Average latency in seconds
5	100 %	0	0.90	0.32	0.66
10	100%	0	2.67	0.94	1.80
15	100%	0	5.33	2.77	4.01
20	100%	0	10.23	4.50	7.36

TABLE III
BLOCKCHAIN-BASED THROUGHPUT MEASUREMENT

No. of peers	Success	Fail	Average Send rate (tps)	Average throughput (tps)
5	100 %	0	200.8	196.7
10	100%	0	189.5	180.6
15	100%	0	170.5	162.7
20	100%	0	165.3	159.5

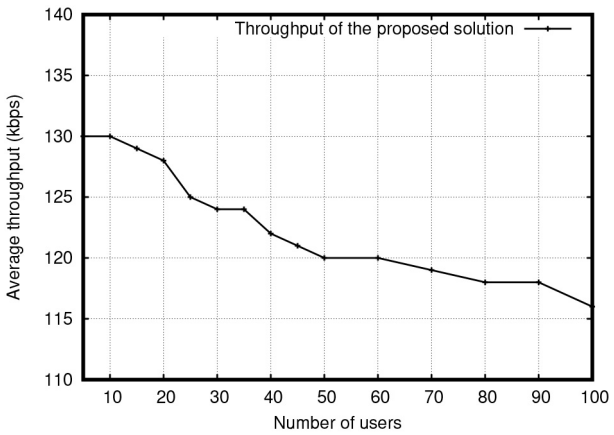

Fig. 8. Throughput with the increasing number of users.

TABLE IV
COST MEASUREMENT

Computational cost	Transactional cost
O(Nlogn)	O(N-1)logn
N is the number of peers and n is the number of users	

peers and then average values are shown. Second, the overall solution's throughput stability is measured with the increasing number of blocks and shown in Fig. 8. It shows that the system is having no overhead with the increasing number of users. Thus, this less complex signcryption computation with lightweight functional modules helps in reduction of overhead and it gets an approximately stable output form. Hence, it is suitable for IoT and Internet of Medical Things (IoMT) too.

Finally, we measure the cost of the solution. The comparison of the complexities is shown in Table IV. It shows computational cost and transaction cost. Computational cost consists of the cryptographic computation including key generation, signcryption, unsigncryption, hashing and signature. Transactional cost consists of the key transmission, signcrypted message transmission and cost of consensus.

The detection accuracy and severity accuracy are shown in Table V. It shows that detection accuracy is stable with the increasing number of users; however, the severity accuracy is less in the system. This can be extended as a future research problem to optimize this factor.

TABLE V
ACCURACY MEASUREMENT

No. of users	Detection accuracy	Severity accuracy
10	98%	70%
20	98%	70%
30	98%	68%
40	98%	65%
50	98%	65%
60	98%	68%
70	98%	68%
80	98%	65%
90	98%	65%
100	98%	68%

The above discussion on the solution provides the following advantages.

1) The solution is a novel exposure in the direction of COVID-19 research.
2) The blockchain-based solution can provide a transparent decision making for the locationwise stakeholders related to medical assistance
3) As COVID-19 is spreading fast, the solution can provide an associative detection measure along with cough, cold, and fever symptoms.
4) The probabilistic alerts can help the patient candidates aware and to take necessary medical help.

V. CONCLUSION

In this article, we have shown a probabilistic model with oxygen saturation measurements based on the IoT framework and blockchain implications. The solution is novel in its kind as no other research in present has considered the oxygen saturation with the IoT framework for COVID-19 detection. Oximeter readings are aggregated and probabilistic classification is executed to obtain a certain alert. It also provides a severity calculation to check the seriousness. As an intermodular operation, the humming bird algorithm and photon hash are used to make the solution less computationally complex. The network-based parameters were evaluated and have been found satisfactory for IoT-based healthcare. However, the adaptability has not been experimented yet. The false-positive cases can be improved further and kept as a future scope of study.

REFERENCES

[1] *COVID-19 Coronavirus Pandemic*. Accessed: Jul. 25, 2020. [Online]. Available: https://www.worldometers.info/coronavirus/

[2] (Apr. 2020). *World Health Organization, Coronavirus Disease 2019 (COVID-19), Situation Report—73*. Accessed: May 17, 2020. [Online]. Available: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200402-sitrep-73-covid-19.pdf

[3] K. McCallum. *Can an Oximeter Help Detect COVID-19 at Home?* Accessed: Oct. 2020. [Online]. Available: https://www.houstonmethodist.org/blog/articles/2020/aug/can-an-oximeter-help-detect-covid-19-at-home/

[4] Apollo. *Importance of at-home Pulse Oximeter in Times of COVID-19*. Accessed: Aug. 2020. [Online]. Available: https://www.apollo247.com/blog/article/importance-home-pulse-oximeter-times-covid-19

[5] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, Apr. 2019, pp. 113–131.

[6] *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Accessed: Jan. 20, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK9579/

[7] J. He, L. He, W. Zhou, X. Nie, and M. He, "Discrimination and social exclusion in the outbreak of COVID-19," *Int. J. Environ. Res. Public Health*, vol. 17, no. 8, p. 2933, 2020.

[8] *The Social Impact of COVID-19*. Accessed: May 22, 2020. [Online]. Available: https://www.un.org/development/desa/dspd/2020/04/social-impact-of-covid-19/

[9] V. Muralidharan. *COVID-19: Exclusion, Isolation Nothing New for the Differently Abled*. Accessed: Jul. 20, 2020. [Online]. Available: https://www.downtoearth.org.in/blog/health/covid-19-exclusion-isolation-nothing-new-for-the-differently-abled-71507

[10] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo, "Exploiting geo-distributed clouds for a E-health monitoring system with minimum service delay and privacy preservation," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 2, pp. 430–439, Mar. 2014.

[11] A. Zamiri, H. S. Yazdi, and S. A. Goli, "Temporal and spatial monitoring and prediction of epidemic outbreaks," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 2, pp. 735–744, Mar. 2015.

[12] G. Yang *et al.*, "IoT-based remote pain monitoring system: From device to cloud platform," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 6, pp. 1711–1719, Nov. 2018.

[13] M. A. Akkaş, R. Sokullu, and H. E. Çetin, "Healthcare and patient monitoring using IoT, Internet of Things," *Internet Things* vol. 11, Sep. 2020, Art. no. 100173.

[14] P. Verma and S. K. Sood, "Fog assisted-IoT enabled patient health monitoring in smart homes," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1789–1796, Jun. 2018.

[15] R. K. Pathinarupothi, P. Durga, and E. S. Rangan, "IoT-based smart edge for global health: Remote monitoring with severity detection and alerts transmission," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2449–2462, Apr. 2019.

[16] T. N. Gia *et al.*, "Energy efficient fog-assisted IoT system for monitoring diabetic patients with cardiovascular disease," *Future Gener. Comput. Syst.*, vol. 93, pp. 198–211, Apr. 2019.

[17] A. Ghosh, A. Raha, and A. Mukherjee, "Energy-efficient IoT-health monitoring system using approximate computing," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100166.

[18] H. Fouad, A. S. Hassanein, A. M. Soliman, and H. Al-Feel, "Analyzing patient health information based on IoT sensor with AI for improving patient assistance in the future direction," *Measurement*, vol. 159, Jul. 2020, Art. no. 107757.

[19] E. Moghadas, J. Rezazadeh, and R. Farahbakhsh, "An IoT patient monitoring based on fog computing and data mining: Cardiac arrhythmia usecase," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100251.

[20] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[21] J. Vora *et al.*, "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, 2018, pp. 1–6.

[22] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight privacy-preserving identity-based verifiable IoT-based health storage system," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8393–8405, Oct. 2019

[23] P. Huang, L. Guo, M. Li, and Y. Fang, "Practical privacy-preserving ECG-based authentication for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9200–9210, Oct. 2019.

[24] R. P. Singh, M. Javaid, A. Haleem, and R. Suman, "Internet of Things (IoT) applications to fight against COVID-19 pandemic," *Diabetes Metab. Synd. Clin. Res. Rev.*, vol. 14, no. 4, pp. 521–524, 2020.

[25] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, 2020.

[26] P. D. Giamberardino, D. Iacoviello, F. Papa, and C. Sinisgalli, "Dynamical evolution of COVID-19 in Italy with an evaluation of the size of the asymptomatic infective population," *IEEE J. Biomed. Health Inform.*, vol. 25, no. 4, pp. 1326–1332, Apr. 2021.

[27] O. S. Albahri *et al.*, "Systematic review of artificial intelligence techniques in the detection and classification of COVID-19 medical images in terms of evaluation and benchmarking: Taxonomy analysis, challenges, future solutions and methodological aspects," *J. Infect. Public Health*, vol. 13, no. 10, pp. 1381–1396, 2020.

[28] A. I. Khan, J. L. Shah, and M. M. Bhat, "CoroNet: A deep neural network for detection and diagnosis of COVID-19 from chest X-ray images," *Comput. Methods Programs Biomed.*, vol. 196, Nov. 2020, Art. no. 105581.

[29] H. Panwar, P. K. Gupta, M. K. Siddiqui, R. Morales-Menendez, and V. Singh, "Application of deep learning for fast detection of COVID-19 in X-Rays using nCOVnet," *Chaos Solitons Fractals*, vol. 138, Sep. 2020, Art. no. 109944.

[30] T. Mahmud, M. A. Rahman, and S. A. Fattah, "CovXNet: A multi-dilation convolutional neural network for automatic COVID-19 and other pneumonia detection from chest X-ray images with transferable multi-receptive feature optimization," *Comput. Biol. Med.*, vol. 122, Jul. 2020, Art. no. 103869.

[31] T. Ozturk, M. Talo, E. A. Yildirim, U. B. Baloglu, O. Yildirim, and U. R. Acharya, "Automated detection of COVID-19 cases using deep neural networks with X-ray images," *Comput. Biol. Med.*, vol. 121, Jun. 2020, Art. no. 103792.

[32] M. Toğaçar, B. Ergen, and Z. Cömert, "COVID-19 detection using deep learning models to exploit social mimic optimization and structured chest X-ray images using fuzzy color and stacking approaches," *Comput. Biol. Med.*, vol. 121, Jun. 2020, Art. no. 103805.

[33] L. Brunese, F. Mercaldo, A. Reginelli, and A. Santone, "Explainable deep learning for pulmonary disease and coronavirus COVID-19 detection from X-rays," *Comput. Methods Programs Biomed.*, vol. 196, Nov. 2020, Art. no. 105608.

[34] T. Tuncer, S. Dogan, and F. Ozyurt, "An automated Residual Exemplar Local Binary Pattern and iterative ReliefF based COVID-19 detection method using chest X-ray image," *Chemometr. Intell. Lab. Syst.*, vol. 203, Aug. 2020, Art. no. 104054.

[35] N. N. Das, N. Kumar, M. Kaur, V. Kumar, and D. Singh, "Automated deep transfer learning-based approach for detection of COVID-19 infection in chest X-rays," *IRBM*, to be published.

[36] H. Zhu *et al.*, "IoT PCR for pandemic disease detection and its spread monitoring," *Sens. Actuators B, Chem.*, vol. 303, Jan. 2020, Art. no. 127098.

[37] W. M. Shaban, A. H. Rabie, A. I. Saleh, and M. A. Abo-Elsoud, "A new COVID-19 Patients Detection Strategy (CPDS) based on hybrid feature selection and enhanced KNN classifier," *Knowl. Based Syst.*, vol. 205, Oct. 2020, Art. no. 106270.

[38] T. Ji *et al.*, "Detection of COVID-19: A review of the current literature and future perspectives," *Biosens. Bioelectron.*, vol. 166, Oct. 2020, Art. no. 112455.

[39] *Symptoms of Coronavirus*. Accessed: Jul. 10, 2020. [Online]. Available: https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html

[40] R. Saha, G. Kumar, M. K. Rai, and H.-J. Kim, "A security provisioned blockchain architecture for multi-purpose health information," *Int. J. Adv. Sci. Technol.*, vol. 116, pp. 141–150, May 2018.

[41] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692.

[42] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Integrating feature values for key generation in an ICmetric system," in *Proc. IEEE NASA/ESA Conf. Adapt. Hardw. Syst. (AHS)*, San Francisco, CA, USA, 2009, pp. 82–88.

[43] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Proc. Annu. Cryptol. Conf.*, 2011, pp. 222–239.

[44] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm," in *RFID. Security and Privacy* (Lecture Notes in Computer Science 7055), A. Juels and C. Paar, Eds. Heidelberg, Germany: Springer, 2012.
[45] N. Naik and S. Purohit, "Comparative study of binary classification methods to analyze a massive dataset on virtual machine," *Procedia Comput. Sci.*, vol. 112, pp. 1863–1870, Dec. 2017.
[46] M. Ala'raj, M. Majdalawieh, and M. F. Abbod, "Improving binary classification using filtering based on k-NN proximity graphs," *J. Big Data*, vol. 7, no. 1, p. 15, 2020.
[47] C. I. Bliss, "The method of probits," *Science*, vol. 79, no. 2037, pp. 38–39, 1934.
[48] K. Li *et al.*, "PoV: An efficient voting-based consensus algorithm for consortium blockchains," *Front. Blockchain*, vol. 3, pp. 1–11, Mar. 2020.
[49] D. Galindo and F. D. Garcia, "A Schnorr-like lightweight identity-based signature scheme," in *Progress in Cryptology (AFRICACRYPT)* (Lecture Notes in Computer Science 5580), B. Preneel, Ed. Heidelberg, Germany: Springer, 2009.
[50] B. Yang and D. Enyeart. *Hyperledger Fabric*. Accessed: Jun. 16, 2020. [Online]. Available: https://www.hyperledger.org/blog/2020/01/30/welcome-hyperledger-fabric-2-0-enterprise-dlt-for-production
[51] *Installing and Running Caliper*. Accessed: Jun. 28, 2020. [Online]. Available: https://hyperledger.github.io/caliper/vNext/installing-caliper/

Rahul Saha (Member, IEEE) received the Ph.D. degree from Lovely Professional University, Phagwara, India, in 2018, with area of specialization in cryptography, position and location computation in wireless sensor networks.

He is currently an Associate Professor with Lovely Professional University. He has many publications in well-renowned international journals and conferences.

Gulshan Kumar (Member, IEEE) received the Ph.D. degree from Lovely Professional University, Phagwara, India, in 2017, with area of specialization in position and location computation in wireless sensor networks.

He is working as an Associate Professor with Lovely Professional University. He has many publications in well-renowned international journals and conferences.

Neeraj Kumar (Senior Member, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra, India, in 2009.

He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is currently a Visiting Professor with Coventry University. He is also a Full Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has published more than 300 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, and John Wiley. Some of his research findings are published in top-cited journals, such as the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE NETWORK, *IEEE Communications Magazine*, IEEE WIRELESS COMMUNICATIONS, IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, *Future Generation Computer Systems*, *Journal of Network and Computer Applications*, and ComCom. He has guided many Ph.D. and M.E./M.Tech. students. His research was supported by fundings from Tata Consultancy Service, Council of Scientific and Industrial Research, and the Department of Science and Technology.

Prof. Kumar has awarded the Best Research Paper awards from IEEE ICC 2018 and IEEE SYSTEMS JOURNAL 2018 and 2020. He is also leading the Research Group Sustainable Practices for the Internet of Energy and Security, where group members are working on the latest cutting edge technologies. He is a TPC member and a reviewer of many international conferences across the globe.

Tai-Hoon Kim (Member, IEEE) received the B.E. and M.E. degrees from Sungkyunkwan University, Seoul, South Korea, and the Ph.D. degrees from the University of Bristol, Bristol, U.K., and the University of Tasmania, Hobart, TAS, Australia, in 2011.

He is currently with Konkuk University (Glocal Campus), Seoul. His main research interests include security engineering for IT products, IT systems, development processes, and operational environments.

Tannishtha Devgun received the M.Tech. degree from Punjab Technical University, Kapurthala, India, in 2016, with area of specialization in wireless networks.

Her area of interest includes wireless communication and network security and cryptography.

Reji Thomas received the Ph.D. degree from Indian Institute of Technology Delhi, New Delhi, India, in 1999.

He is currently a Professor with Lovely Professional University, Phagwara, India. His research interests include logic, memory, and energy storage devices.

Ahmed Barnawi received the M.Sc. degree from the University of Manchester Institute of Science and Technology, Manchester, U.K., in 2001, and the Ph.D. degree from the University of Bradford, Bradford, U.K., in 2005.

He is currently a Professor with the Faculty of Computing and IT, King Abdulaziz University, Jeddah, Saudi Arabia. He is also the Managing Director of the KAU Cloud Computing and Big Data Research Group. He has published more than 100 articles in peer reviewed journals. His research interests include big data, cloud computing, and advanced mobile robotic applications.