AI and Blockchain-Based Cloud-Assisted Secure Vaccine Distribution and Tracking in IoMT-Enabled COVID-19 Environment

Ashok Kumar Das, Basudeb Bera, and Debasis Giri

Abstract

Coronavirus 2019, called COVID-19, is a transmissible disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). It earlier impacted the citizens of China alone. However, it has rapidly spread all over the world. The COVID-19 supply chain system aims to facilitate access to several critical items, such as personal protective equipment (PPE), biomedical equipment, diagnostics supplies, and vaccines. In this article, we discuss a robust security framework for vaccine distribution and tracking in an Internet of Medical Things (IoMT)-based cloud-assisted COVID-19 environment by considering both intra-country and inter-country scenarios. Various transactions related to vaccine requests, orders, distribution, and tracking are put into the blockchain in the form of blocks. Since blockchain technology offers immutability, transparency, and decentralization, the security of the proposed framework has been improved significantly. The proposed framework also supports artificial intelligence(AI)-based big data analytics on the information stored into the blocks in the blockchain. Furthermore, a practical demonstration of the proposed framework has been done through a blockchain simulation study.

Introduction

Wuhan City, in the Hubei province of China COVID-19, was the first reported source where COVID-19 affected the human life in December 2019. COVID-19 then rapidly spread throughout the world [1, 2]. Figure 1 shows the COVID-19 statistics [3] maintained by the World Health Organization (WHO) for the top 10 worst affected countries of the world based on COVID-19 affected persons and deaths as of 16 February, 2021.

The ongoing global COVID-19 pandemic caused an acute shortage of vital supplies. To solve this serious problem, a Supply Chain Task Force was setup to oversee establishment of the COVID-19 Supply Chain System based on the request of the United Nations Secretary-General and WHO Director-General and also in support of the UN Crisis Management Team [4]. The Supply Portal is presently used to facilitate access to roughly 50 critical items, such as personal protective equipment (PPE), biomedical equipment, and diagnostics supplies. However, in the current situation, vaccination of healthcare personals and other citizens has become extremely essential to stop the COVID-19 pandemic. Therefore, to build a secure vaccine distribution and tracking system is very important at the same time due to tracking of vaccinated persons with side effects if present.

To track a person with COVID-19 vaccine doses administered, the Internet of Medical Things (IoMT) plays a very important role [5–7]. In the IoMT environment, a person's body is deployed with various wearable/implantable smart devices which communicate with the nearby mobile device owned by that person. The information collected by the mobile device is then stored in the cloud server(s). Since storing the data in the cloud servers is a problem, particularly for sensitive data and also for several other attacks like data poisoning and noise insertion attacks, a block-based solution is a viable option. Blockchain acts as a decentralized, distributed ledger technology that keeps the records of digital assets (information). Once the data in the form of transactions in blocks are inserted into the blockchain, the blocks cannot be tampered with other fake information (immutability property). In recent years, researchers have discussed and designed security protocols in the cloud-based IoMT environment using blockchain technology [8–11]. To facilitate the advantages of blockchain, in this article we design a new blockchain-based cloud-assisted secure vaccine distribution and tracking framework, specifically for an IoMT-enabled COVID-19 environment.

The remainder of this article is ordered as follows. We first discuss the system models, containing both network and threat models. After that, a new cloud-assisted secure vaccine distribution and tracking framework in the IoMT environment for the COVID-19 scenario has been proposed. Next, we discuss the security of the proposed security framework. The blockchain implementation of the proposed framework is then provided. Finally, the concluding remarks and some future research directions have been put at the end of this article.

System Models

This section elaborates two important models, namely network and threat models, that are useful in discussion in the proposed framework.

Network Model

We consider a cloud-assisted blockchain-envisioned IoMT model for COVID-19 vaccine distribution/tracking in Fig. 2, in which intra-country and inter-country scenarios are taken into account. For vaccine distribution/tracking, we also consider the supply chain as proposed for COVID-19 [4].

In the *intra-country* case, the government drug control agency (GDAC), as a registration authority in a country, is responsible for registering all cloud servers (known as peer nodes) in a peer-to-peer (P2P) cloud server network (called a P2P CS network) and all the vaccine manufacturing companies (VMCs). Next, in each hospital in the country, the hospital authority (HA) will be responsible for registering all its entities (doctors, nurses, patients, staff, insurance companies, etc.). Under this case, after receiving the vaccine supply from the respective vaccine manufacturing company (VMC), instructed by the GDAC, the vaccines are given to the registered healthcare personnel in each hospital. The transactions in the form of information from the GDAC, VMC, and HA of each hospital are securely sent to the P2P CS network for private block creation, and verification and addition of the generated blocks through a voting-based consensus process. Later, artificial intelligence(AI)-based big

Ashok Kumar Das and Baudeb Bera are with the International Institute of Information Technology, Hyderabad.

Debasis Giri is with Maulana Abul Kalam Azad University of Technology , West Bengal.

Digital Object Identifier: 10.1109/IOTM.0001.2100016

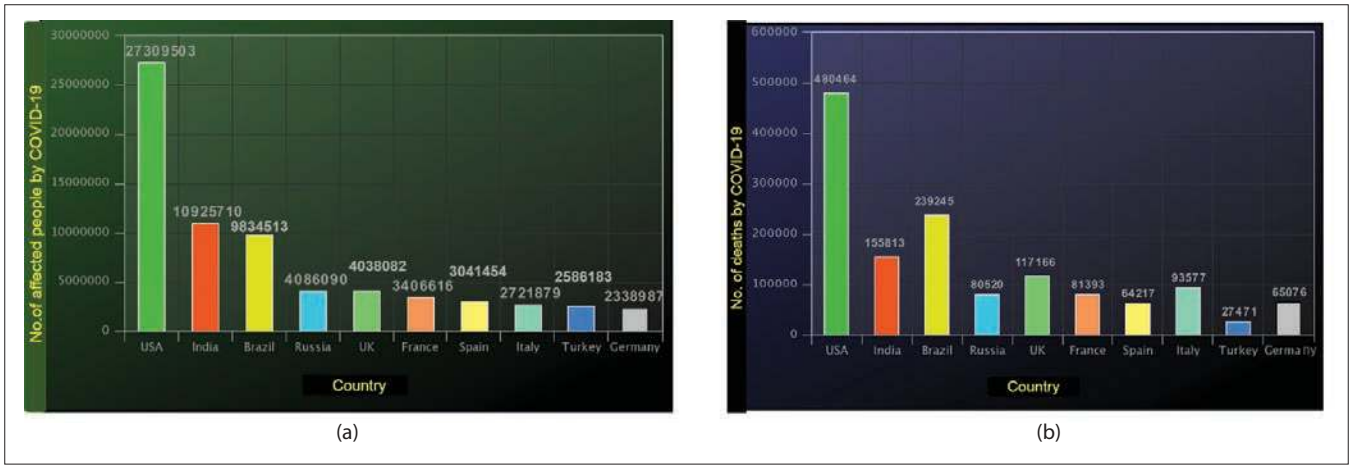

FIGURE 1. Statistics of COVID-19 affected persons and deaths as of 16 February, 2021 (Data Source: WHO Coronavirus Disease [COVID-19] Dashboard [3]: a) number of affected people by COVID-19 for the top 10 countries; b) number of deaths reported by COVID-19 for the top 10 countries.

data analysis on the information stored in blocks in the blockchain may be performed for better prediction of results and tracking of vaccines in a country.

We also consider the *inter-country* case, where supply request and delivery of vaccines from other countries are put in the form of transactions, and then sent to the P2P CS network maintained by the participating countries. In this case, we consider the public blockchain so that each country can track the vaccine distribution from other countries and vaccine tracking in other countries too. The GDAC in each country is responsible for registering the cloud server(s) in their country, which become peer node(s) as a part of the P2P CS network. Similar to the intra-country scenario, AI-based big data analysis on the information stored in blocks in the public blockchain may also be performed for better prediction of results and tracking of vaccines in the participating countries.

Threat Models

In the proposed cloud-assisted blockchain-envisioned IoMT model for COVID-19 vaccine distribution/tracking, the following threat models have been considered from internal and external adversaries. The contemporary Dolev-Yao threat model, known as the DY model [12], has been adopted, in which the communications happen between different entities in the network via an open channel. Therefore, there is not only threat of information interception (eavesdropping), but also of tampering with the information including modification, deletion, and inserting fake data in between the communication. Under the DY model, the endpoint entities (doctors, nurses, patients, staff, insurance companies, etc.) are not treated as trusted. We also incorporate the present de facto model, known as the Canetti and Krawczyk (CK)-adversary model [12], because it is more powerful threat model as compared to the DY model. Under the CK-adversary model, an adversary not only has the capabilities of the DY model, but can also compromise the session states, session keys, and temporal secret information (e.g., random secrets) through session-hijackng attacks. This certainly suggests generating the session keys among the entities in such a manner that the session keys should depend on both short- (temporal) and long-term secrets so that compromise of session keys by the CK-adversary will be very difficult. In addition, the GDAC, VMCs, and HA (in each hospital) are considered fully trusted, while the cloud servers are semi-trusted. Furthermore, a privileged insider of GDAC, VMCs, and HA, being an inside attacker, may misuse the confidential information. In order to protect the privileged insider attacker, we assume that the entities will not directly supply their sensitive confidential information to the registration authorities.

Proposed Cloud-Assisted Secure Vaccine Distribution and Tracking Framework

This section provides a novel cloud-assisted secure vaccine distribution and tracking framework in the IoMT environment for the COVID-19 scenario, called CSVDTF-IoMTCOVID-19. In the following, we discuss various related phases that are needed for CSVDTF-IoMTCOVID-19.

Registration Phase

For the *intra-country* scenario, this phase is executed by the trusted GDAC for registering various VMCs and cloud servers in the P2P CS network. In addition, the trusted HA in each hospital is responsible for enrolling various entities, including doctors, nurses, patients, staff, insurance companies, and so on. For the *inter-country* case, only the GDAC in a country is responsible for registering the cloud server(s) maintained in the P2P CS network.

In order to execute this phase, system parameters, like a non-singular elliptic curve over a finite field of a large prime order p and its base point G whose order is as bid as p, are selected. Note that $k*G$ will denote an elliptic curve point (scalar) multiplication, that is, point G is added to itself k times. In addition, elliptic curve encryption/decryption, and its signature generation and verification algorithms (ECDSA.Sig(.) and ECDSA.Ver(.)) [13] are chosen over the elliptic curve. Furthermore, a collision-resistant one-way cryptographic hash function, say $h(.)$, such Secure Hash Algorithm (SHA-256) that produces 256-bits hash output), is also chosen.

At first, the GDAC picks an elliptic-curve-based private-public key pair (Priv-GDAC, Pub-GDAC), where Pub-GDAC = Priv-GDAC *G, and publishes the public key Pub-GDAC and keeps its own private key Priv-GDAC secret. The GDAC then registers all the VMCs and provides the registration details to them. After receiving the registration details, each VMC creates its own private-public key pair (Priv-VMC, Pub-VMC), where Pub-VMC = Priv-VMC * G, and publishes the public key Pub-VMC and keeps its own private key Priv-VMC secret. In a similar way, each HA in a registered hospital generates its own private-public key pair (Priv-HA, Pub-HA), where Pub-HA = Priv-HA * G, and publishes the public key Pub-HA and keeps its own private key Priv-HA secret.

Next, various users, such as doctors, nurses, patients, staff, and insurance companies, send registration requests to the HA with their credentials. After credentials validation, the HA issues a smart card with essential credentials stored in it for authentication and key agreement purposes in the next section to each successfully registered user.

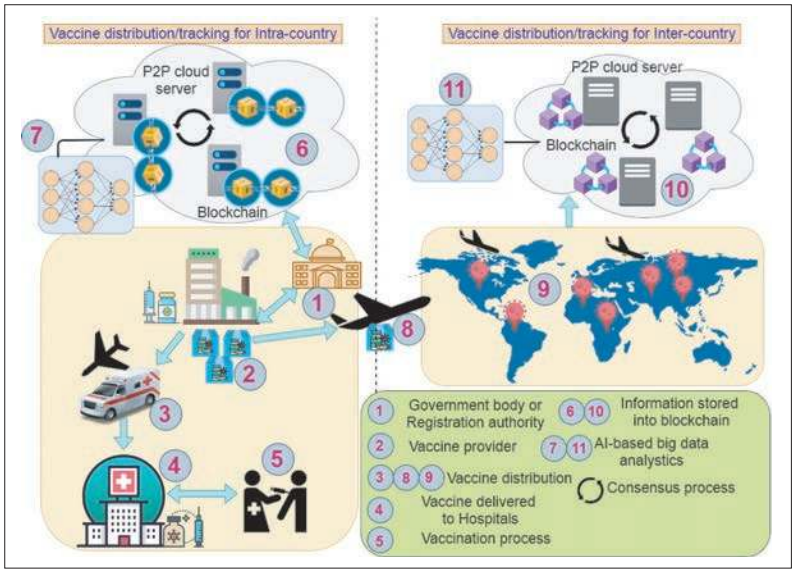

FIGURE 2. Cloud-assisted blockchain-envisioned IoMT model for COVID-19 vaccine distribution/tracking.

For *intra-country inter-country* cases, only the GDAC in a country first registers all the cloud servers in the P2P CS network and only the cloud server(s) residing in the country, respectively. After successful registration, each cloud server in the P2P CS network creates its own private-public key pair (Priv-CS, Pub-CS), where Pub-CS = Priv-CS*G, and publishes the public key Pub-CS and keeps its own private key Priv-CS secret.

Authentication and Key Agreement Phase

The sole purpose of this phase is to establish secure communications among the HA and its various associated users (doctors, nurses, patients, staff, insurance companies, etc.). In addition, the wearable IoT-enabled smart devices deployed in a patient's body need to make communication with the mobile device owned by that user (patient) secure and then establish secure communication among the user's mobile device and the HA.

To execute this phase, a robust authenticated key agreement protocol, such as the scheme proposed in [7], can be utilized for secure communications between the HA and its various users by means of establishing the session keys among them after a successful mutual authentication process. On the other side, the session key establishment among the wearable devices deployed in a patient's body and the mobile device owned by that patient can be executed by using a secure authentication scheme designed in [6]. Thus, using the established session keys, various entities can secure communication in a hospital. Moreover, the secure communication can be made between the mobile device and the HA using the polynomial-based key management scheme, as mentioned in [7].

Block Creation, Verification, and Addition Phase

In this section, we discuss the block generation and then validation followed by addition into the blockchain in the proposed CSVDTF-IoMTCOVID-19.

In the *intra-country* case, the GDAC first places the orders to the VMCs based on the requirements of hospitals securely. The information is encrypted using elliptic curve cryptography (ECC)-based encryption with the help of the public key Pub-VMC of the associated VMC. Later, this information is put in the form of transactions, and the transactions are securely sent to the associated cloud servers in the P2P CS network using ECC encryption with the help of the public key Pub-CS of the cloud servers (CSs). The respective VMC then decrypts the orders using its own private key Priv-VMC with the ECC decryption and prepares the vaccines to be delivered through the supply chain process to the respective HAs of the destination hospitals. The vaccines supply information forms transactions, which are then securely put to the cloud servers in the P2P CS networks from the VMCs. Once the vaccines are received by the respective HAs, they start vaccination to the registered healthcare personnel, and the information is then put in the form of transactions. Later, these transactions are securely sent to the CSs in the P2P network by the HAs. After vaccination, for tracking purposes, the information regarding healthcare personnel about the date vaccinated, vaccine band, any side effects, and number of vaccine doses is put in the form of transactions. These transactions are also sent by the HAs securely to the CSs in the P2P network.

For the *intra-country* scenario, we consider the following types of transactions in a private blockchain:

Tx-intra-Type1: This type of transaction is needed when the GDAC wants to make requests to a VMC to deliver the required number of vaccines to hospitals residing in a state of a country. The fields containing this kind of transaction are *Tx-intra-Type1* = {Request-number, GDAC-name, VMC-name, Request-date, Expected-delivery-date, Destination-hospitals, Vaccine-name, Number-of-vaccines-ordered}, where Request-number, GDAC-name, VMC-name, Request-date, Expected-delivery-date, Vaccine-name, and Number-of-vaccines-ordered signify the request number, name of GDAC, VMC name, vaccine request date, expected vaccine supply date, name of the vaccine brand to be delivered, amount of vaccines to be supplied, and a list of hospitals in a state of a country where the vaccines are to be supplied, respectively.

Tx-intra-Type2: The purpose of this transaction is to keep records of vaccine delivery from a particular VMC to destination hospitals in a country. It has the format of *Tx-intra-Type2* = {Request-number, GDAC-name, Source-VMC-address, Destination-hospital-address, Invoice-number, Vaccine-name, Number-of-vaccines-delivered, Vaccines-tracking-numbers}. The request number, name of GDAC, originated VMC address, destination hospital address where the vaccines will be delivered, invoice number, name of vaccine brand, amount of vaccines to be delivered, and tracking numbers of vaccines (batch numbers with manufactoring and expiry dates) are denoted by Request-number, GDAC-name, Source-VMC-address, Destination-hospital-address, Invoice-number, Vaccine-name, Number-of-vaccines-delivered, and Vaccines-tracking-numbers, respectively.

Tx-intra-Type3: This transaction is formed by the HA of each hospital when the healthcare personnel receive vaccines. The format of this kind of transaction is *Tx-intra-Type3* = {HeathcarePersonal-ID, HeathcarePersonal-address, HeathcarePersonal-medicalhistory, Date-vaccinated, Source-hospital-ID, Source-hospital-address, Vaccine-name, Vaccine-batchnumber, Number-of-vaccinedoses}. The identity, address, and medical history of a healthcare worker are denoted by HeathcarePersonal-ID, HeathcarePersonal-address and HeathcarePersonal-medicalhistory, respectively. Other fields, such as Date-vaccinated, Source-hospital-ID, Source-hospital-address, Vaccine-name, Vaccine-batchnumber, and Number-of-vaccinedoses signify the date when the vaccine was given, the name of the hospital and its address from where the vaccine was given, the brand name of the given vaccine, its batch number, and the number of doses given to a healthcare personal, respectively.

Tx-intra-Type4: This transaction is mainly needed for tracking the information of already administered vaccine doses to the healthcare personnel. The various fields involved in this transaction are *Tx-intra-Type4* = {HeathcarePersonal-ID, Date-vaccinated, Source-hospital-ID, Source-hospital-address, Vaccine-name,

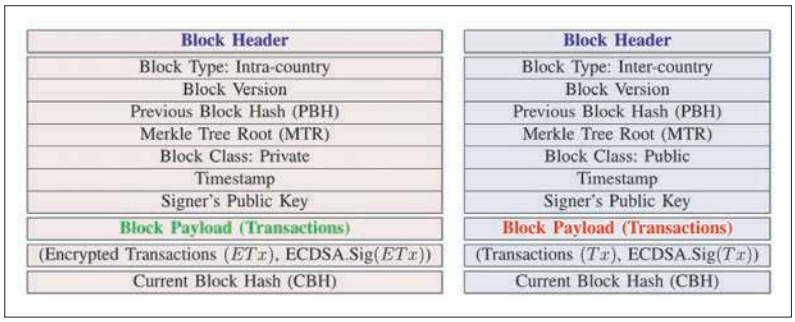

FIGURE 3. A block structure (private or public).

Vaccine-batchnumber, Number-of-vaccinedoses, Date-tracking, Side-effects}, where Date-tracking and Side-effects denote the date when a healthcare worker was tracked and the side effects of administered vaccine doses, if any.

On the other side, for the *inter-country* scenario, after vaccine orders are requested from other countries, the GDAC securely sends the vaccine supply requests to the respective VMCs. After analyzing the requests from the GDAC, the VMC securely sends the information regarding the vaccine doses to the countries that have been requested by encrypting the information using the public key of other countries' GDACs. Next, the VMC supplies the vaccines through the supply chain process to the demanded countries. The receiving countries then keep track of the vaccines with the number of doses administered in that country and side effects. We consider the following types of transactions in a public blockchain for the *inter-country* scenario:

Tx-inter-Type1: This transaction involves the information regarding the order information from the requested countries, which has the format *Tx-inter-Type1* = {Request-number, country-GDAC-name, VMC-name, Request-date, Expected-delivery-date, Destination-country, Vaccine-name, Number-of-vaccines-ordered}.

Tx-inter-Type2: This transaction particularly involves the information about the vaccine delivery by the VMC of the source country, and it is prepared by the source country's GDAC. This transaction is of the form: *Tx-inter-Type2* = {Request-number, source-GDAC-name, Source-VMC-address, Destination-GDAC-number, Invoice-number, Vaccine-name, Number-of-vaccines-delivered, Vaccines-tracking-numbers}.

Tx-inter-Type3: This transaction is prepared by the destination country's GDAC to track the vaccines that are administered to their healthcare personnel with side effects of the vaccines, if any. This transaction has the form: {*Tx-inter-Type3*} = {Date-vaccinated, Source-GDAC-name, Vaccine-name, Vaccine-batchnumbers, Number-of-vaccinedoses, Date-tracking, Side-effects}.

In the P2P CS network, the nodes communicate with each other by applying the message passing mechanism. The transactions are sent by the different parties (e.g., healthcare personnel in a hospital, vaccine manufacturing providers, and drug controller authority) to the P2P CS network securely. It is worth noting that the above discussed authentication and key agreement phase helps to establish the session (secret) keys among various entities in the network. Thus, the established session keys can be applied for secure communication of different transactions among various entities. After reaching a transactions threshold, a block is created by a newly elected leader or proposer who has responsibility to start the block addition process. A block verification and addition process into the blockchain is then executed by a voting based distributed algorithm, namely Practical Byzantine Fault Tolerance (PBFT) [14]. The block structures that are put into the blockchain are considered to be of two types (intra-country and inter-country), and they are elaborated in Fig. 3. For the *intra-country* scenario, each transaction in a block is encrypted using ECC encryption with the help of the public key Pub-GDAC of the GDAC, and then its digital signature is generated using the ECDSA-Sig(.) algorithm using the private key Priv-CS of a signer (a cloud server). A block contains the Merkle tree root, which is the hash of all the transactions involved in that block along with previous block hash, signer's public key, and other information. Finally, the current block hash is computed as the hash of all the fields present in the block. Similarly, for the *inter-country* scenario, a block is formed, except the transactions are not encrypted because the blocks are put in the public blockchain.

There is a transactions pool maintained by each peer node in the P2P CS network. The detailed process for executing the consensus mechanism is as follows:

- Once a transaction is received by the P2P CS network, it is stored in every peer node's transactions pool.
- Once the transactions pool reaches a pre-defined transaction threshold value, the peer nodes (cloud servers) start a new round, and a proposer is elected in a round-robin fashion. The remaining nodes, which are then treated as the followers, agree on it.
- The proposer now sends a PRE-PREPARE message to the followers. The nodes then enter the PRE-PREPARED state.
- Next, the proposer broadcasts a PRE-PREPARE message with the proposed block, and the followers broadcast this message to other nodes at the same time.
- The follower nodes verify the proposed block by having the same transactions with their own transaction pools. After successfully verifying and agreeing on the proposed block, the followers send a PREPARE message.
- After receiving $2f+1$ such messages (where f is the number of faulty nodes in the network), the nodes change their state to the PREPARED state.
- The prepared nodes then send a COMMIT message to other follower nodes.
- After receiving $2f+1$ COMMIT messages from others nodes, the follower nodes move to COMMIT state and add the block to the chain.
- After successfully adding the proposed block, the nodes move to the FINAL COMMITTED state.
- This consensus process is repeated by electing another proposer with new proposed blocks.

Vaccine Tracking Phase in Blockchain

For vaccine tracking, in both the intra- and inter-country cases in the proposed CSVDTF-IoMTCOVID-19, a block is validated using the following:

- The Merkle tree root *MTR'* is computed based on all the transactions present in the block. After that, if the re-computed *MTR'* matches the stored *MTR* in the block, the next step is executed.
- The signature attached with a required transaction is then verified using the ECDSA.Ver(.) signature verification algorithm with the help of the public key of the signer that is stored in the block. If the signature is valid, the next step is then performed.
- Finally, the hash of all the fields excluding the current block hash (CBH) is re-computed and then verified against the stored CBH. If there is a match, the block is treated as authentic.

Once the block is validated successfully, the GDAC of a country can track the administered vaccines, their side effects, if any, and also other statistics.

AI-Based Big Data Analytics Phase

Combination of blockchain and AI helps big data analysis on the information stored on blocks in the blockchain for better prediction of results and tracking of vaccines in a country in

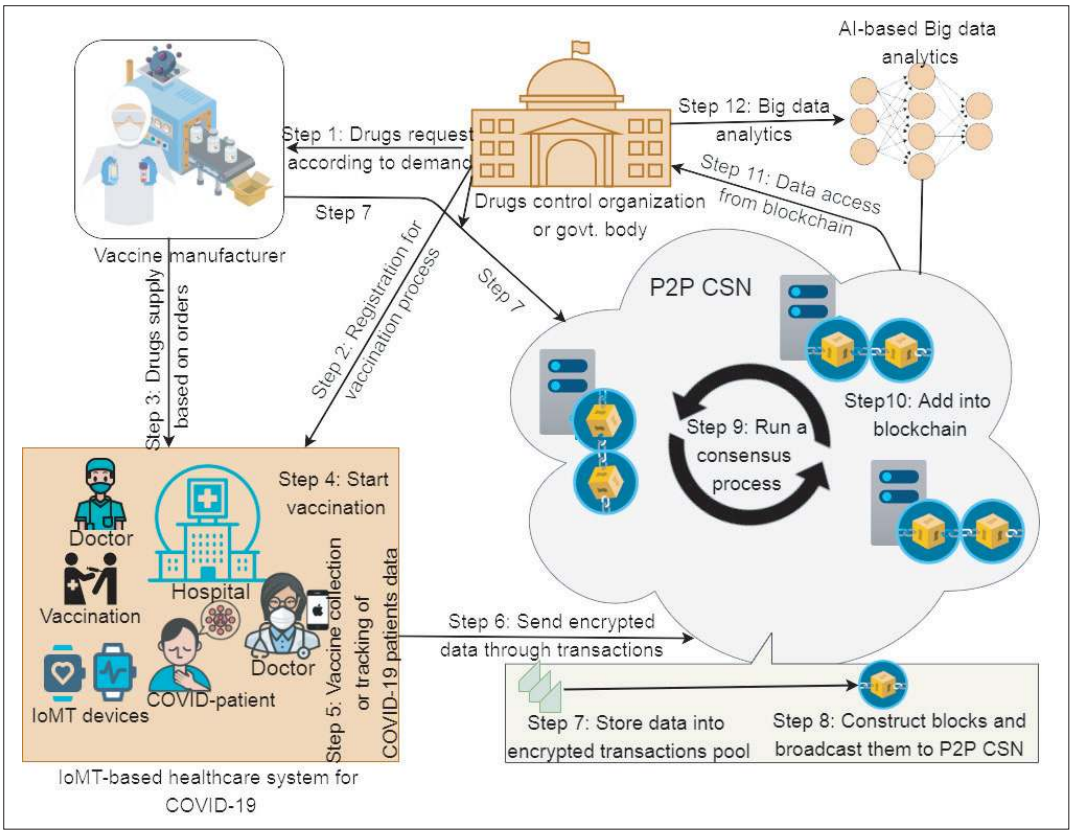

FIGURE 4. Overall process in the proposed framework for COVID-19 vaccine distribution/tracking (intra-country).

CSVDTF-IoMTCOVID-19. For instance, if the transactions are not stored in blockchain, several attacks can be performed by an attacker, such as Poisson noise insertion attack (PNIA) and data poisoning attack (DPA). In PNIA, an attacker may insert noise into the dataset. Poisson noise is considered as a statistical noise that can be modeled by a group of Poisson processes. On the other side, DPA allows an attacker to launch an attack by either injecting some noise on the data stored on the server or changing the label of the data. Since the blockchain provides immutability, transparency, and decentralization, once the blocks are validated successfully, the information stored in the blocks is taken as genuine. Thus, if we apply the AI and machine learning(ML)-based approaches on the authenticated datasets stored in the blockchain, we arrive at correct predictions. It then helps the GDACs in the countries to have better big data analytics for COVID-19 data including vaccine distribution and tracking.

The overall processes in the proposed framework for COVID-19 vaccine distribution/tracking for the intra-country and inter-country scenarios are demonstrated in Figs. 4 and 5, respectively.

Security Analysis

The proposed framework can resist various well-known attacks against passive and active adversaries. Discussion of some prominent attacks with regard to the proposed framework (CSVDTF-IoMTCOVID-19) is given below.

In replay attack, an adversary may attempt to mislead another legal entity by means of reusing the information during communication. Thus, this attack is treated as an attempt by an illegal third party entity who records the transmitted messages. In man-in-the-middle (MiTM) attack, an attacker may intentionally intercept the communicated messages and then try to delete, modify, or even insert fake contents into the messages that are intended to be delivered to the recipients. In privileged-insider attack, a trusted authorized user within an organization may sometimes act as a privileged-insider attacker. During the registration phase, no entity should supply their secret credentials directly to the trusted authority. In impersonation attacks, an attacker may try to falsify a counterfeit message in order to cheat other recipients in the network on behalf of a sending/receiving entity. Based on the threat model discussed in this article, in the proposed framework, the registration process and authentication mechanism are executed in such a way that replay, MITM, privileged-insider, and impersonation attacks are resisted.

In an ephemeral secret leakage (ESL) attack scenario, if the ephemeral secrets are known, an attacker can have the private keys of entities, and it may lead to compromising the session key to be known to the attacker from the intercepted messages. In the proposed framework, the session keys depend on both short- (temporal) and long-term secrets. Therefore, compromise of session keys by an CK-adversary is difficult as the adversary needs to compromise both temporal and long-term secrets. As a result, the ESL attack is protected against in the proposed framework.

Blockchain Implementation

In this section, we elaborate on the implementation of blockchain in the proposed framework by creating a virtual distributed system with the help of node.js scripts.

We first create P2Ps distributed nodes (here, a P2P CS network) with 11 peer nodes as CSs. The system configuration is Ubuntu 18.04.3 LTS, Intel® Core™ i5-8400 CPU @ 2.80vGHz×6, 7.6 GB memory, OS type 64-bit, disk size 152.6 GB, which is considered as a server setup.

The entire process of the blockchain addition into the blockchain is simulated in the following two different ways:

- **Case 1:** This case considers a fixed number of transactions that are stored into each block for each blockchain, which is

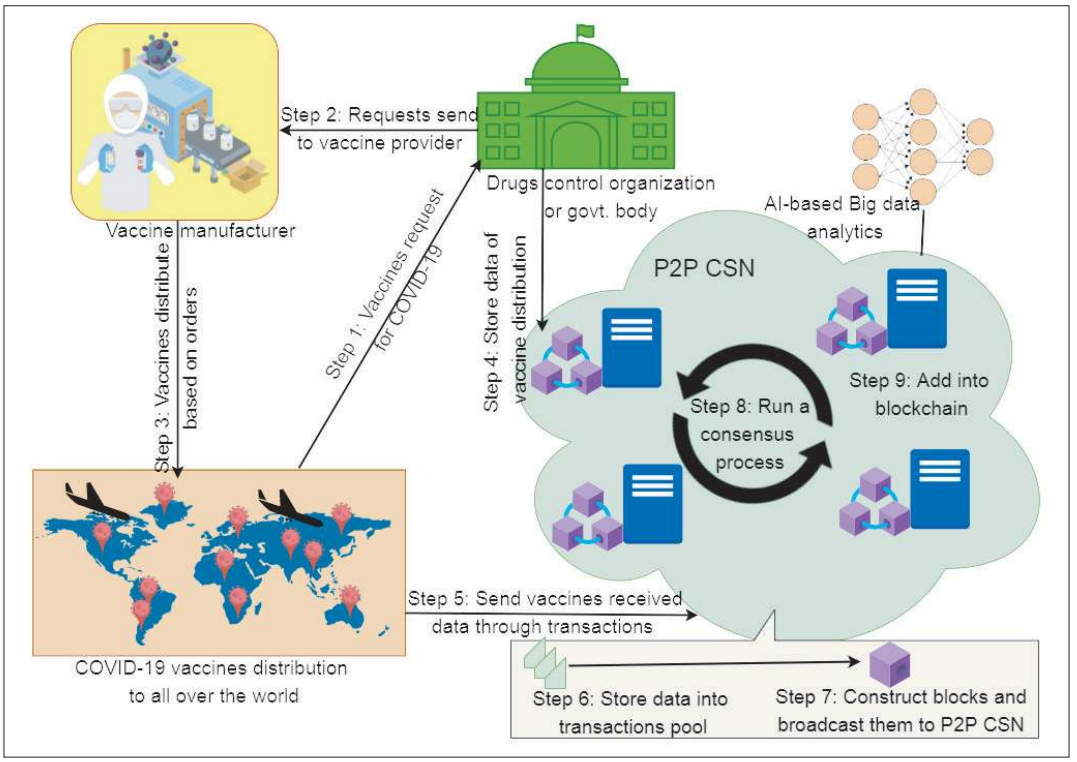

FIGURE 5. Overall process in proposed framework for COVID-19 vaccine distribution/tracking (inter-country)

taken as 41, and we vary only the block size for each chain. The simulation results are provided in Fig. 6a, and signify that the number of blocks mined into the blockchain differs from the total computational time (in seconds) linearly.

- **Case 2:** We suppose the fixed number of blocks for each chain and only vary the number of transactions with a fixed block size as 37. The simulation outputs presented in Fig. 6b demonstrate "the number of transactions loaded in a block varies linearly with the total computational time (in seconds) to add the transaction into block."

Conclusion and Future Research

In this article, we discuss the importance of vaccine distribution and tracking in both the intra-country and inter-country situations for ongoing COVID-19 with the help of a cloud-assisted IoMT-enabled blockchain solution. We first discuss the network and threat models that are associated with the proposed framework. Next, we discuss various phases including registration, authentication, blockchain formation, and AI-based big data analytics. We discuss the AI-based big data analytics phase by mentioning how the blockchain and AI/ML algorithms can play an important role for accurate prediction on the data stored into the blockchain. The proposed framework not only maintains the transactions related to vaccine order requests and distribution through the supply chain, but also tracks healthcare personnel about their vaccination with side effects, if any, by applying the genuine and authentic information stored in the blocks residing in the blockchain. A blockchain-based simulation study has been conducted to show the practical demonstration of the proposed framework.

In future, we would like to build a detailed AI-based big data analytics scheme by considering more prominent attacks that can be mounted by an adversary. Furthermore, for the intra-country case, it would be interesting to apply the search

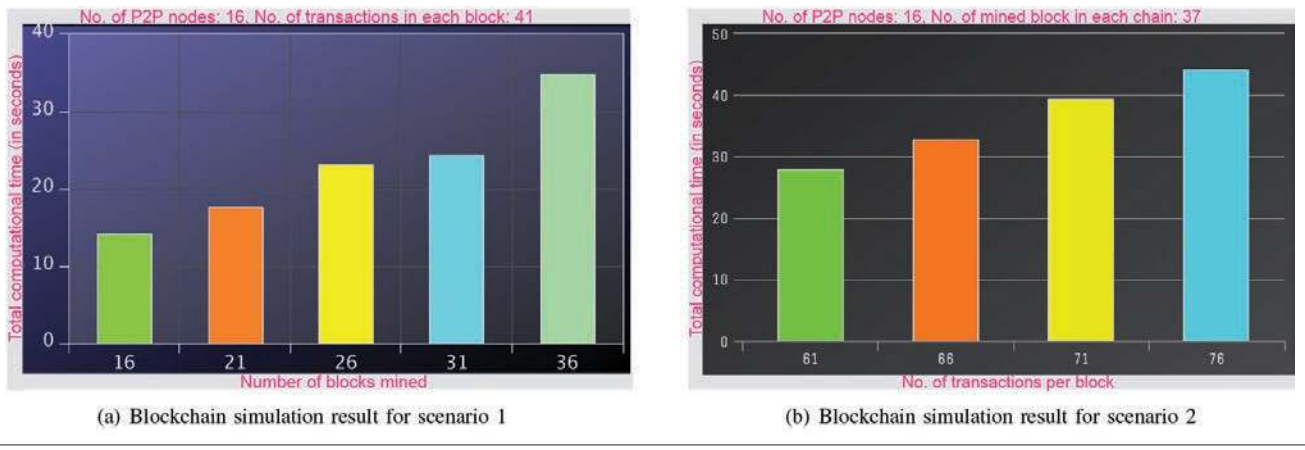

FIGURE 6. Blockchain simulation result for various cases: a) blockchain simulation result for scenario 1; b) blockchain simulation result for scenario 2.

on the encrypted data (transactions) that are present in the blocks in encrypted formats. Thus, it is desirable to know which encrypted transactions could be more useful before decrypting every encrypted transaction in the blocks. We can apply various techniques, like privacy-preserving searchable encryption, attribute-based symmetric searchable encryption, and keyword-based search, to achieve such a purpose.

References

[1] V. Chamola *et al.*, "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, 2020, pp. 90,225–965.

[2] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and Mass Surveillance System-Based Healthcare Framework to Combat COVID-I9 Like Pandemics," *IEEE Network*, vol. 34, no. 4, 2020, pp. 126–32.

[3] "WHO Coronavirus Disease (COVID-19) Dashboard," 2021;, https://covid19.who.int/table, accessed 16 Feb., 2021.

[4] N. Korin, "Using Blockchain to Monitor the COVID-19 Vaccine Supply Chain," 2020; https://www.weforum.org/agenda/2020/11/using-blockchain-to-monitor-covid-19-vaccine-supply-chain/, accessed Jan. 2021.

[5] R. Guo *et al.*, "O-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System," *IEEE Internet of Things J.*, 2021. DOI: 10.1109/JIOT.2021.3055541.

[6] A. K. Das *et al.*, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," *IEEE J. Biomedical and Health Informatics*, vol. 22, no. 4, 2018., pp. 1310–22

[7] N. Garg *et al.*, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, 2020., pp. 95,956–77

[8] M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the Internet of Medical Things," *IEEE BlackSeaCom*, Sochi, Russia, 2019, pp. 1–4.

[9] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, "A Mobile Cloud Based IoMT Framework for Automated Health Assessment and Management," *41st Annual Int'l. Conf. IEEE Engineering in Medicine and Biology Society*, Berlin, Germany, 2019, pp. 6517–20.

[10] B. S. Egala *et al.*, "Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things with Effective Access Control," *IEEE Internet of Things J*, 2021. DOI: 10.1109/JIOT.2021.3058946.

[11] D. C. Nguyen *et al.*, "BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," *IEEE Internet of Things J.*, 2021. DOI: 10.1109/JIOT.2021.3058953.

[12] D. Dolev and A. Yao, "On the Security of Public Key Protocols," *IEEE Trans. Info. Theory*, vol. 29, no. 2, 1983, pp. 198–208.

[13] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Int'l. J. Info. Security*, vol. 1, no. 1, 2001, pp. 36–63.

[14] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," *ACM Trans. Computer Systems*, vol. 20, no. 4, 2002, pp. 398–461.

Biographies

Ashok Kumar Das [M'17, SM'18] (iitkgp.akdas@gmail.com) received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He currently is working as an associate professor with the Center for Security, Theory and Algorithmic Research, IIIT Hyderabad, India. His current research interests include cryptography and network security, blockchain, and AI/ML security. He has authored over 265 papers in international journals and conferences in the above areas, including over 225 reputed journal papers. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Boards of the *IEEE Systems Journal*, the *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *IET Communications*, and *KSII Transactions on Internet and Information Systems*.

Basudeb Bera (basudeb.bera@research.iiit.ac.in) received his M.Sc. degree in mathematics and computing in 2014 from IIT (ISM) Dhanbad and his M.Tech. degree in computer science and data processing in 2017 from IIT Kharagpur. He is currently pursuing a Ph.D. degree in computer science and engineering from IIIT Hyderabad. His research interests are cryptography, network security, and blockchain technology. He has published 15 papers in international journals and conferences in his research areas.

Debasis Giri [M'17] (debasis_giri@hotmail.com) received his M.Sc., M.Tech, and Ph.D. degrees from the Indian Institute of Technology, Kharagpur, in 1998, 2001, and 2009, respectively. He is currently an associate professor with the Department of Information Technology, Maulana Abul Kalam Azad University of Technology (formerly known as the West Bengal University of Technology), Haringhata, India. His current research interests include cryptography, information security, e-commerce security, and blockchain. He has authored more than 80 research papers in reputed international journals and conference proceedings.