An IoT-Based Secure Vaccine Distribution System through a Blockchain Network

Geetanjali Rathee, Sahil Garg, Georges Kaddoum, and Dushantha Nalin K. Jayakody

Abstract

COVID-19 is an extremely dangerous disease because of its highly infectious nature. In order to provide quick and immediate identification of infection, proper and immediate clinical support is needed. Researchers have proposed various machine learning and smart IoT-based schemes for categorizing COVID-19 patients. Artificial neural networks (ANNs), which are inspired by the biological concept of neurons, are generally used in various applications including healthcare systems. The ANN scheme provides a viable solution in the decision making process for managing healthcare information. The aim of this article is to provide secure COVID-19 vaccine distribution through IoT-based systems. The level-wise blockchain network is used to ensure security among IoT devices while distributing the vaccines. The proposed phenomenon is analyzed and verified over synthesized data where vaccine units are supplied by various distributors. The proposed approach is validated over accurate report generation and data alteration parameters against existing methods.

Introduction

The World Health Organization (WHO) has classified the novel coronavirus 2019 (COVID-19) as a pandemic due to its dangerously infectious situations in today's world. The virus has been identified as a severe acute respiratory syndrome coronavirus 2 (SARS-COV2) due to lack of oxygen supply to lungs [1]. COVID-19 is a highly contiguous disease that spreads in a contiguous way from one person to another [2]. In order to control this pandemic, the entire world is working hard with all its capacity and might. Since its first appearances, researchers are also highly motivated to understand, explore, and discover new devices and treatments to terminate it from present generation [3]. Currently, COVID-19 is severely affecting healthcare centers because of its unknown treatment and unlimited number of cases. Scientists, researchers, and authors need to do some severe quantification in a proper and immediate manner to treat infected patients. According to a recent study of WHO, approximately 10.5 million confirmed cases, 151,000 deaths, and 10.1 million recovered cases were registered at the time of writing [4, 5]. These cases have been registered in almost the entire world from the United Kingdom, Italy, India, Germany, the United States, Korea, China, Japan, and many other countries. The immediate symptoms to identify any COVID-19 patient at its first instance is eye redness, fatigue, fever, throat infection, chills, and respiratory issues [6]. However, these symptoms are consistently appearing within four to five or more days after a patient is positive. American labs have realized an antidote to cure COVID-19 patients, and remote monitoring vaccine distribution schemes are proposed where these vaccines are distributed to the entire world in order to recover from this pandemic [7]. However, a secure and transparent way to efficiently distribute the vaccines to the required centers still needs to be explored.

Motivation

The integration and immense contribution of automotive devices, online storage, and IoT devices have made it feasible to generate intelligent and smart IoT-based healthcare centers. Nowadays, a number of healthcare centers have shifted to automatic techniques by exploring the novel and smart services of the latest techniques to store and process recorded data. However, the huge amount of data generated by IoT devices makes it complex to handle and process the data in an efficient and secure manner. Further, the involvement of intruders during the communication process may further cause an organization to hesitate in fully adapting IoT-based systems. Researchers have proposed several cryptographic techniques to ensure security, generate, analyze, and distribute information among various entities. However, it may further lead to intermediate costs, time, and transparent overhead among the parties [8]. The intermediaries may sometimes steal the information for third party for their personal benefit. Along with several success stories in the clinical and distribution fields, blockchain technique can be considered as a secure medium to conduct transparent and efficient communication among parties. The distributed blockchain architecture known as DApp is the backbone of the blockchain mechanism in order to overcome the transparency, security, and privacy issues among decentralized networks for real-time applications. The blockchain architecture provides a reliable and transparent security mechanism having real-time communications among the nodes. The proposed framework ensures smart distribution of vaccines by a blockchain mechanism through an artificial neural network (ANN). The ANN scheme provides a viable solution in the decision making process for managing healthcare information.

Contributions

The contribution of this article is to propose a secure and efficient blockchain mechanism while distributing the vaccines to healthcare centers. The proposed mechanism uses a three-level distribution architecture by dividing the entities into certain layers for reducing the communication overhead and storage complexity. The potential contribution is illustrated as follows:

- A three-level distributed blockchain architecture is proposed to securely distribute the vaccines among centers.
- The proposed mechanism uses a permissioned blockchain network to further reduce the complexity and computational overhead.
- The system is analyzed, simulated, and experimented over data alteration and accurate report generation metrics against the conventional approach.

The remaining structure of the article is as follows. The recent literature using blockchain architecture in healthcare centers for ensuring secure communication is discussed. In addition, the article illustrates the proposed distributed architecture separated into three levels. Further, the metrics for verify-

Geetanjali Rathee is with Netaji Subhash University of Technology, India.
Sahil Garg is with the École de Technologie Supérieure, Montreal and National Research Tomsk Polytechnic University, Russia.
Georges Kaddoum is with École de Technologie Supérieure, Montreal, Canada.
Dushantha Nalin K. Jayakody is with the National Research Tomsk Polytechnic University, Russia, and Sri Lanka Technological Campus, Sri Lanka.

Digital Object Identifier: 10.1109/IOTM.0001.2100028

Author's name	Approach	Mechanism	Performance
Han *et al.* [9]	Self-healing secure recovery and communication system	The proposed system uses a trust-based scheme using single value distribution where the performance and security can be performed using efficient data transmission	The proposed approach is validated through simulation results using IoT-based networks
Huang *et al.* [10]	Efficient data distribution schemes	A Bayesian classification method is used to estimate the distribution metrics. The proposed mechanism is validated over empirical study analyzed over real datasets with online travel sites	The authors claim that their proposed approach performs better as compared to conventional classification schemes
Hao *et al.* [11]	Reliable data deletion scheme	The authors propose an outsourced policy method integrated with decryption and key schemes	Formal extensive results are demonstrated to examine the efficiency and reliability of the proposed approach
Hasanat *et al.* [12]	Real-time data-centric mechanism	The proposed system has provided a unique feature of managing and creating the supervision mechanism using humidity and temperature of the carrier	The proposed mechanism has efficiently enhanced the vaccine distribution supervision and monitoring in distributed scenarios
Nash *et al.* [13]	Web-based distributed model	The paper focuses on entropy modeling using data vaccine preventable diseases as an example of a modeling scheme	–.
Jiang *et al.* [14]	Community priority vaccine distribution system	The individuals are grouped into various communities by prioritizing according to their assigned vaccines	The proposed approach assist in the accurate distribution of vaccines using infected and uninfected people through various network types
McGhin *et al.* [15]	Research issues and challenges	The authors discuss several types of fraud, smart contracts, and identity verification systems by addressing the key management and mining overheads	A number of potential challenges available for research are discussed in this survey paper

TABLE 1. The security mechanisms.

ing the proposed phenomenon are detailed. Finally, the entire article is concluded including some future directions.

Related Work

Han *et al.* [9] proposed a self-healing secure recovery and communication system. The authors proposed two different layers where thectop layer deploys the access control and deterministic link through polynomial schemes. The proposed system used a trust-based scheme using single value distribution where the performance and security can be measured using efficient data transmission. The proposed approach is validated through simulation results using IoT-based networks. Huang *et al.* [10] proposed an efficient data distribution scheme for IoT-based systems using sample-based modeling. In addition, a Bayesian classification method is used to estimate the distribution metrics. The proposed mechanism is validated over empirical study, which is analyzed over real datasets from online travel sites. The authors claimed that the proposed approach performs better as compared to conventional classification schemes.

Hao *et al.* [11] proposed a reliable data deletion scheme using an attribute-based encryption method. The authors proposed an outsourced policy method integrated with decryption and key schemes. The efficiency of the proposed approach was shown through a comprehensive comparison with data deletion parameters in cloud servers. Formal extensive results were demonstrated to examine the efficiency and reliability of the proposed approach. Hasanat *et al.* [12] proposed a real-time data-centric mechanism for monitoring the transportation and distribution of vaccines. The proposed system provided a unique feature of managing and creating the supervision mechanism using humidity and temperature of the carrier. The proposed mechanism has efficiently enhanced vaccine distribution supervision and monitoring in distributed scenarios.

Nash *et al.* [13] developed a web-based distributed model for uploading, creating, and interacting with the information along with their test models. The article focused on entropy modeling using data on vaccination preventable diseases as an example of a modeling scheme. Jiang *et al.* [14] proposed a community priority vaccine distribution system in order to optimize vaccine resources. Individuals were grouped into various communities by prioritizing according to their assigned vaccines. The proposed approach benefited the accurate distribution of vaccines using infected and uninfected people through various network types. McGhin *et al.* [15] discussed the research issues and challenges of including blockchain technologies in various applications of healthcare systems. The authors discussed several fraud types, smart contracts, and identity verification systems by addressing the key management and mining overheads. A number of potential challenges available for research were also discussed in this survey article. Haghighi *et al.* [16] proposed a hierarchical key establishment and authentication mechanism for the IoT-based environment to ensure secure and reliable communication in the network. The authors proposed a lightweight authentication mechanism for distributing the computational load in the network. Polap *et al.* [17] proposed a neural network and blockchain-based Medical IoT (MIoT) network for ensuring reliable and secure data storage using a decentralized learning mechanism. A brief introduction of the related work is also detailed in Table 1.

A number of secure mechanisms have been proposed by various scientists/researchers to ensure a reliable and trusted blockchain mechanism in a variety of healthcare applications. However, very few of them have focused on a secure distribution mechanism (vaccines, reports, medicine distribution) using blockchain. In addition, the existing approaches address computational, storage, and communication overhead while distributing the products and maintaining the blockchain among various vendors. The aim of this article is to provide reliable transparency and security using blockchain while distributing the vaccines without increasing the delay and cost of communication among vendors.

Proposed Approach

The system model of the designed mechanism, represented in Fig. 1, consists of a vaccine supplier company whose headquarters is situated at location A, and the vaccine supply units are placed at location B. Afterward, the suppliers will supply the vaccines to various locations including hospitals, business organizations, and others. Secure and efficient vaccine distribution

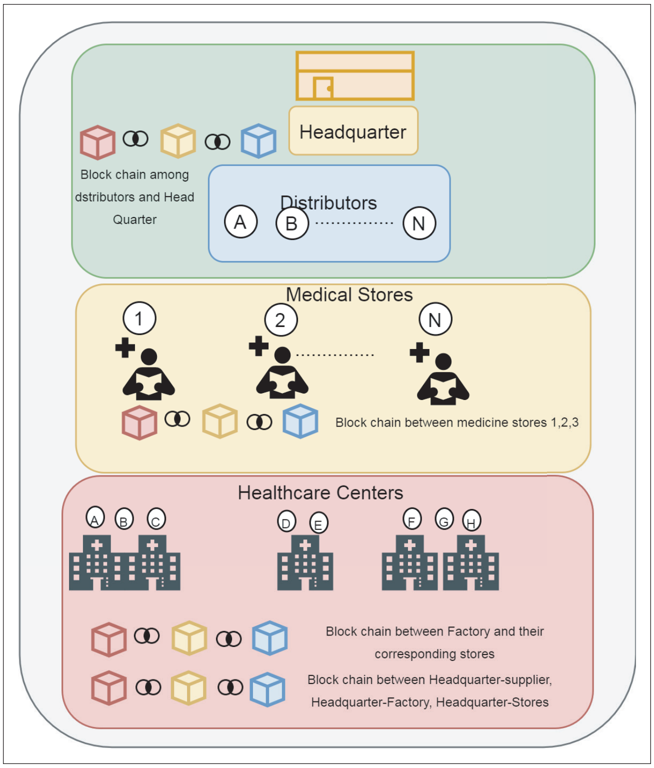
Headquarter
Block chain among dstributors and Head Quarter
Distributors
A
B
N
Medical Stores
1
2
N
Block chain between medicine stores 1,2,3
Healthcare Centers
A
B
C
D
E
F
G
H
Block chain between Factory and their corresponding stores
Block chain between Headquarter-supplier, Headquarter-Factory, Headquarter-Stores

FIGURE 1. Proposed blockchain mechanism.

is done through a level-wise blockchain network. The level-wise distributed blockchain ensures less complexity, storage, and size of validating each data unit.

In addition, in order to trace each and every activity of all participating entities, suppliers have used a permissioned blockchain as depicted in Fig. 1. The initial implementation is started at the headquarters, which has rights to trace every activity and progress at each level. Further, healthcare, business and organization firms, distributors, and medical stores have independent blockchain networks in order to maintain and trace the progress among various entities. The working progress of each entity at various levels is presented below.

Working Process of the Proposed Approach

The efficient organization and management of the proposed blockchain system is divided into three stages. Stage 1 constitutes the headquarters and distributor's blockchain, where medical stores along with distributors and headquarters combine to form the stage 2 blockchain. In addition, healthcare systems with patients' details along with headquarters form the stage 3 blockchain. In the proposed mechanism, the headquarters is the main entity, which is connected to all the levels in order to trace each activity by ensuring a secure and transparent system. The blockchain architecture including the three stages is represented in Fig. 2.

Stage 1: The genesis block of the network is set up by the headquarters between distributors and headquarters. The distributors start the supply process right after getting an order from various organizations or medical stores in accordance with the finished notification and product requirements. The transparency is provided by maintaining a stage 1 blockchain among headquarters and distributors upon adding all the supply requests in the ledger.

Stage 2: The extended blockchain is maintained at stage 2 among distributor, headquarters, and organizations upon supplying the requested vaccines to the medical stores. An automatic notification will be received by the headquarters. For example, notification A of supplying *x* vaccine units will be received by headquarters upon departure to corresponding stores. Likewise , stores 1, 2, and 3 will send a B notification upon receiving the vaccine units. The total vaccines produced, ordered, and delivered by the distributors and firms will be reflected in the stage 2 blockchain network.

Stage 3: The edge level of a blockchain such as stage 3 includes patients' and healthcare systems. Whenever the vaccines are received by a healthcare system, a notification will be sent to the headquarters. As represented in Fig. 4, when healthcare systems have eceived the vaccines, a notification C will be sent to the headquarters. The addressing of blockchain to several associations is illustrated as follows.

Suppose there are four entities: the headquarters as the first that creates the genesis and a lock over the remaining progress, and distributors d1 and d2, which are responsible for delivering vaccine upon receiving order requests from various stores. Further, medical stores determine the third entity, which accepts the vaccines and distributes it to remaining healthcare firms, which finally receive the vaccines to vaccinate patients according to their demand. The tabular representation of all four entities is depicted in Fig. 3.

Transparency Among Entities

Suppose that upon receiving the delivery of 100 units of vaccine from healthcare firms, the headquarters will set up a generic block and orders distributors d1 and d2 to supply the vaccines. Let d1 have to transfer 60 vaccines and d2 40 vaccines; cheating while altering the units would be very difficult as each and every activity can easily be traced by the headquarters. No distributor can increase or decrease the delivering units without administrator permission.

- Headquarters HR generates the genesis block of transmission as the first block among H-D1 and H-D2 by broadcasting to available ledgers. HR contains the details of all distributors, medical stores and healthcare systems.
- After that d1 and d2, upon accepting HR's request, will start delivering the ordered vaccine units by adding another blockchain in the existing network. D1 and d2 further include medical stores in their blockchain to ensure each other's transparency.
- Medical stores may further add the healthcare systems by generating a new hash and adding with previous ones. The generated blockchain makes certain that all stores and healthcare systems are placed where stores may see each other.
- Finally, healthcare systems x, y, and z will receive the vaccines. Here, the blockchain is maintained among healthcare systems that may check each other's delivery details.

Performance Analysis

The analysis of the proposed blockchain mechanism is done in [9, 10], where vaccines are distributed through a blockchain network to the concerned patients. For verifying the systems, an IoT-based network is considered over 3600 epochs having 5.1234, 6.341, and 8.678 s at different levels. Synthesized data is generated having 1000 vaccines units that are ordered and requested by various entities in the blockchain network. Table 2 represents the obtained results over existing schemes. The data analysis is done over true generated reports (accurate results) and altered data. Further, in order to analyze the comparative results in comparison to the baseline mechanism, a malicious environment is created in order to measure the data alteration in the network. The proposed approach is simulated and analyzed over various metrics for identifying the accurate and altered reports from the environment.

- True generated reports: It is defined as the total number of vaccine orders placed by healthcare systems and actual orders delivered by distributors.
- Alteration in data: It is known as the number of reports generated and altered by intermediate entities while placing the order among distributors and healthcare systems.

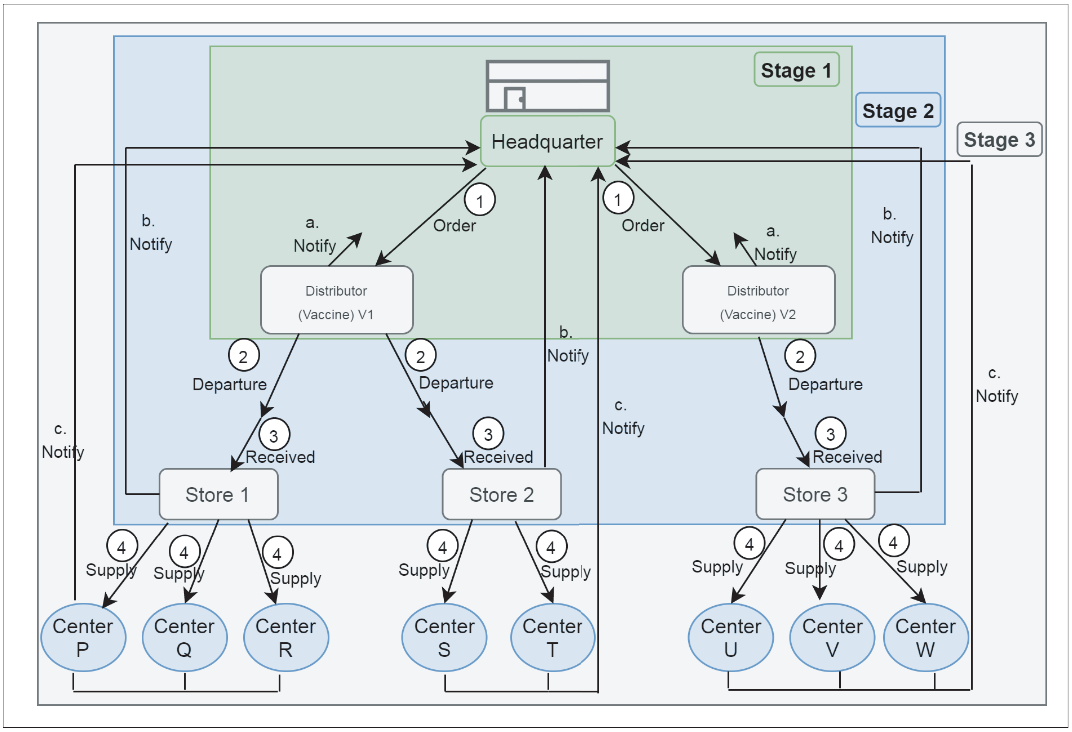

FIGURE 2. Architecure of the blockchain network.

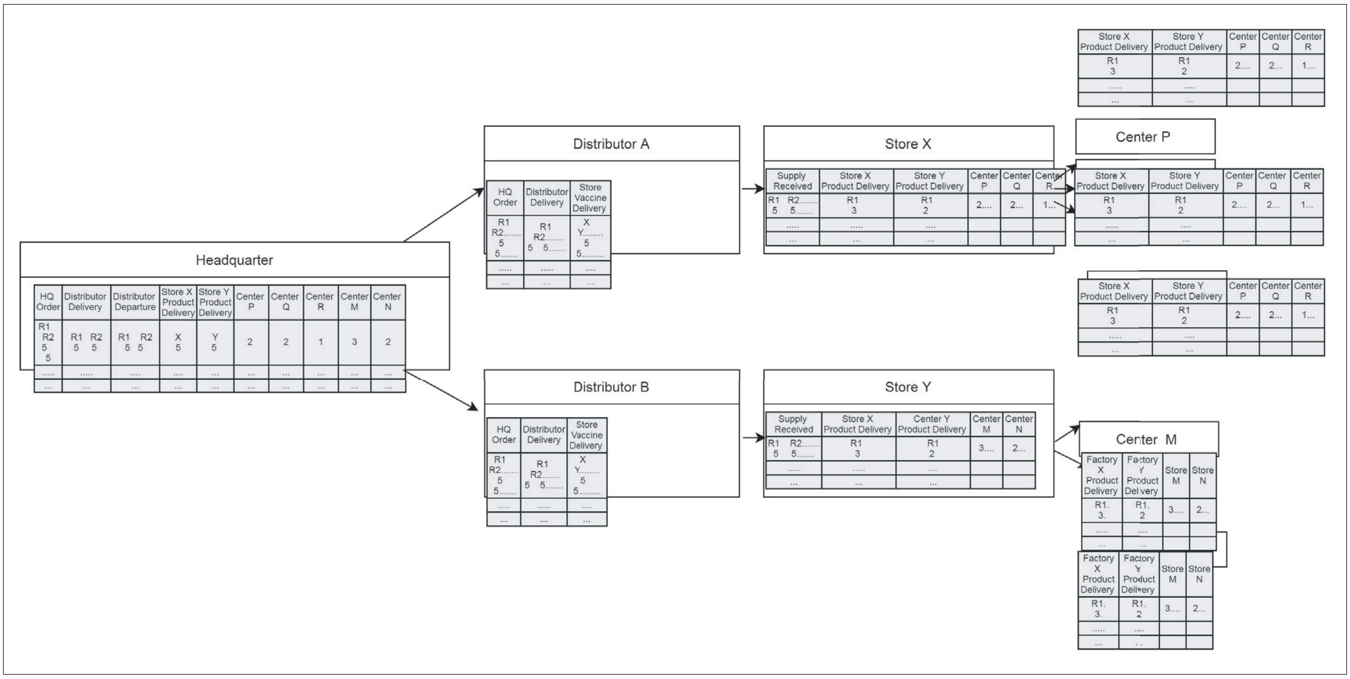

FIGURE 3. Vaccine distribution mechanism using blockchain.

Results and Discussion

Figure 4 represents the comparison of two security measures, true generated reports and altered data, in the proposed and existing phenomena. Figure 4a represents the graph that determines the number of true reports generated by the proposed approach. The generated reports in the case of the proposed phenomenon are always true and accurate as compared to existing mechanisms because of maintaining a blockchain architecture among several entities. The blockchain maintains the transparency by ensuring accurate and correct reports by the IoT devices during communication. In addition, the generation of blockchain data requires less delay and complexity as compared to existing phenomena. This is due to level-wise block generation, which reduces the storage maintenance in the system.

Further, the proposed phenomenon is analyzed against the data alteration process. As depicted in Fig. 5, the alteration in number of generated units done by any malicious intermediate entity can be immediately and easily recognized by the proposed scenario. The altered data generation is quite critical for maintaining the blockchain database during the communication process. The proposed phenomenon generates significant improvement as compared to conventional approaches because of blockchain.

Multi-layered algorithm	Optimized hidden nodes
BP	8
BR	4
Viterbi	4

TABLE 2. Optimized structure results using BP, BR, and Viterbi algorithms.

Research Challenges

A number of researchers have proposed various cryptographic and blockchain-based security mechanisms in a variety of smart applications, but it is further needed to focus on various blockchain issues before integrating with any technique. Following are a number of blockchain-based challenges and issues that need to be focused on before further integrating with any smart-based application:

- Verification delay: The time required to validate any new block before adding it into the existing blockchain is considered as one significant parameter that needs to be addressed. Nodes taking more time to verify the blocks may invite various wireless security threats such as authentication, man-in-the-middle, and handoff attacks, among others.
- Special node selection: The number of nodes selected to validate or verify the incoming data is considered as another major issue. A number of trusted mechanisms are needed to identify the legitimacy of each node that may further participate as a special node for validating the incoming blocks.
- Network scalability: The number of entities participating in the communication or distribution mechanism can be increased or decreased depending on its application. A network with a large number of entities may further increase the verification and validation delay as well as the storage and complexity of the network.
- Double spending threat: Sometimes, distributors may try to earn money from both parties by promising the delivery of the same package to different places. Therefore, it is necessary to introduce a secure and accurate mechanism to check this issue.

Conclusion

This article has proposed an IoT-based blockchain-enabled vaccine distribution system. The proposed phenomenon maintains a level-wise blockchain architecture where each and every activity is performed by the IoT system maintaining a blockchain network. The proposed phenomenon efficiently maintains security by improving the efficiency of vaccine distribution with less delay and complexity. In addition, the IoT-based blockchain architecture is significantly analyzed over true generated and altered data graphs against an existing security mechanism with improved results. The proposed phenomenon can be further enhanced by maintaining the ledger's time required to verify each block in future communications.

Acknowledgments

This work was supported in part by the Fonds de recherche du Québec – Nature et technologies (FRQNT) through PBEEE via File No. 287201; in part by the Tomsk Polytechnic University, Russia, through the Competitive Enhancement Program; and in part by the Sri Lanka Technological Campus, Sri Lanka, Seed Grant RRSG/20/A7.

References

[1] L. H. Schwamm, A. Erskine, and A. Licurse, "A Digital Embrace to Blunt the Curve of Covid19 Pandemic," *NPJ Digital Medicine*, vol. 3, no. 1, 2020, pp. 1–3.

[2] D. Zhang *et al.*, "Design and Implementation of 5G Ehealth Systems, Technologies, Use Cases and Future Challenges," arXiv preprint arXiv:2106.05086, 2021.

[3] S. Verma and A. Gustafsson, "Investigating the Emerging Covid-19 Research Trends in the Field of Business and Management: A Bibliometric Analysis Approach," *J. Business Research*, vol. 118, 2020, pp. 253–61.

[4] L. Catarinucci *et al.*, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet of Things J.*, vol. 2, no. 6, 2015, pp. 515–26.

[5] G. Rathee *et al.*, "A Hybrid Framework for Multimedia Data Processing in IoT-Healthcare Using Blockchain Technology," *Multimedia Tools and Applications*, 2019, pp. 1–23.

[6] J. R. Larsen *et al.*, "Modeling the Onset of Symptoms of Covid-19," *Frontiers in Public Health*, vol. 8, 2020, p. 473.

[7] I. Ahmed *et al.*, "A Deep Learning-Based Social Distance Monitoring Framework for Covid-19," *Sustainable Cities and Society*, vol. 65, 2021.

[8] Y. Yang, H. Bidkhori, and J. Rajgopal, "Optimizing Vaccine Distribution Networks in Low and Middle-Income Countries," *Omega*, 2020.

[9] S. Han *et al.*, "A Secure Trust-Based Key Distribution with Self-Healing for Internet of Things," *IEEE Access*, vol. 7, 2019, pp. 114,060–76.

[10] J. Huang *et al.*, "Efficient Classification of Distribution-Based Data for Internet of Things," *IEEE Access*, vol. 6, 2018, pp. 69,279–87.

[11] J. Hao *et al.*, "Secure and Finegrained Self-Controlled Outsourced Data Deletion in Cloud-Based IoT," *IEEE Internet of Things J.*, vol. 7, no. 2, 2019, pp. 1140–53.

[12] R. T. Hasanat *et al.*, "An IoT Based Real-Time Datacentric Monitoring System for Vaccine Cold Chain," *2020 IEEE East-West Design & Test Symp.*, 2020, pp. 1–5.

[13] T. Nash and A. Olmsted, "shinysdm: Point and Click Species Distribution Modeling," *2017 12th Int'l. Conf. Internet Technology and Secured Transactions*, 2017, pp. 450–51.

[14] M. Jiang *et al.*, "Cps: A Community Priority Based Vaccine Distribution Strategy in Different Networks," *2018 IEEE 16th Int'l. Conf. Dependable, Autonomic and Secure Computing, 16th Int'l. Conf. Pervasive Intelligence and Computing, 4th Int'l. Conf. Big Data Intelligence and Computing, and Cyber Science and Technology Congress*, 2018, pp. 334–37.

[15] T. McGhin *et al.*, "Blockchain in Healthcare Applications: Research Challenges and Opportunities," *J. Network and Computer Applications*, vol. 135, 2019, pp. 62–75.

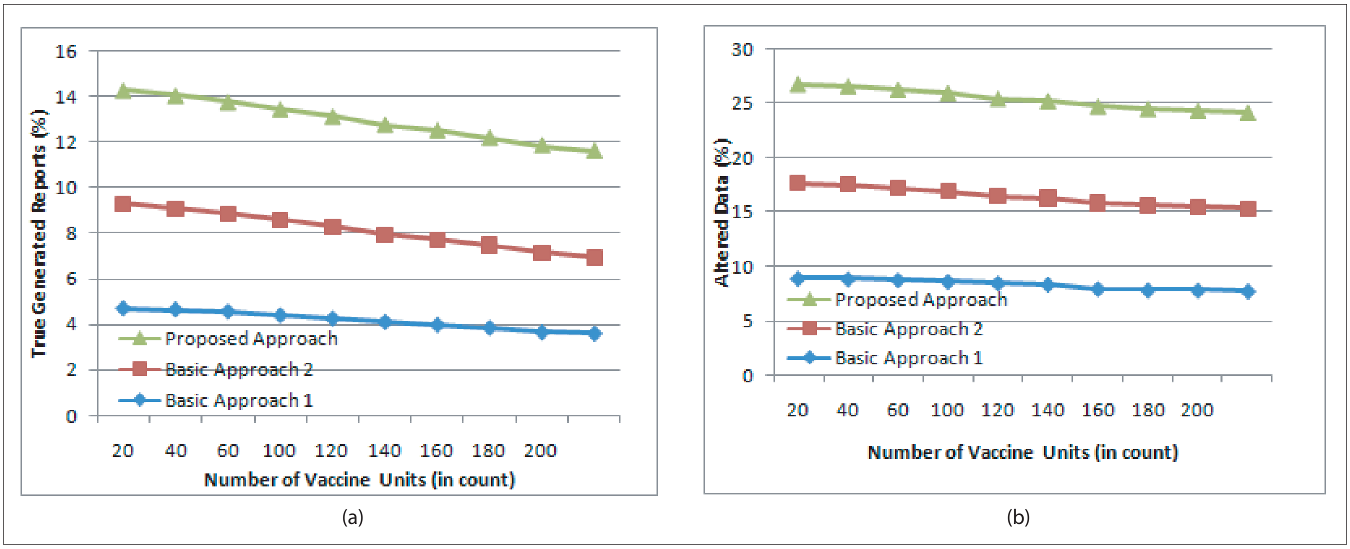

FIGURE 4. Security measures while distributing the vaccines a) true generated (accurate) reports, b) altered data.

[16] M. S. Haghighi, O. Nader, and A. Jolfaei, "A Computationally Intelligent Hierarchical Authentication and Key Establishment Framework for the Internet of Things," *IEEE Internet of Things Mag.*, vol. 3, no. 4, Dec. 2020, pp. 36–39.

[17] D. Połap *et al.*, "Blockchain Technology and Neural Networks for the Internet of Medical Things," *IEEE INFOCOM 2020 Wksps.*, 2020, pp. 508–13.

Biographies

Geetanjali Rathee (geetanjali.rathee123@gmail.com) received her Ph.D. in computer science engineering from Jaypee University of Information Technology (JUIT), Waknaghat, Himachal Pradesh, India, in 2017. She is currently working as an assistant professor in the Department of Computer Science Engineering and Information Technology at JUIT. Her research interests include handoff security, cognitive networks, blockchain technology, resilience in wireless mesh networking, routing protocols and networking, and Industry 4.0. She has approximately 25 publications in peer-reviewed journals and more than 15 publications in international and national conferences. She is also a reviewer for various journals such as *IEEE Transactions on Vehicular Technology*, *Wireless Networks*, *Cluster Computing*, *Ambience Computing*, *Transactions on Emerging Telecommunications Engineering*, and the *International Journal of Communication Systems*.

Sahil Garg [S'15, M'18] (sahil.garg@ieee.org) received his Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently a research associate at the Resilient Machine Learning Institute (ReMI) in correlation with École de technologie supérieure (ÉTS), Montréal, Canada. Prior to this, he worked as a postdoctoral research fellow at ÉTS and a MITACS researcher at Ericsson, Montréal. He has many research contributions in the area of machine learning, big data analytics, security and privacy, the Internet of Things, and cloud computing. He has over 80 publications in high ranked journals and conferences, including 50+ top-tier journal papers and 30+ reputed conference articles. He has been awarded the 2021 *IEEE Systems Journal* Best Paper Award, the 2020 IEEE TCSC Award for Excellence in Scalable Computing (Early Career Researcher), and the IEEE ICC best paper award in 2018 at Kansas City, Missouri. He is currently a Managing Editor of Springer's *Human-Centric Computing and Information Sciences* journal. He is also an Associate Editor of *IEEE Network*, *IEEE Transactions on Intelligent Transportation Systems*, Elsevier's *Applied Soft Computing*, and Wiley's *International Journal of Communication Systems*. In addition, he also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications.

Georges Kaddoum [M'11] (georges.kaddoum@etsmtl.ca) received his Bachelor's degree in electrical engineering from the École Nationale Supérieure de Techniques Avancés (ENSTA), France, his M.Sc. degree in telecommunications and signal processing from Telecom Bretagne (ENSTB), Brest, in 2005, and his Ph.D. degree in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), Toulouse, France, in 2009. He is currently an associate professor and Tier 2 Canada Research Chair with the École de Technologie Supérieure, University of Quebec, Montréal, Canada. His recent research activities cover wireless communication networks, resource allocations, security and space communications, and navigation. He was awarded the ÉTS Research Chair in physical-layer security for wireless networks in 2014, and the prestigious Tier 2 Canada Research Chair in wireless IoT networks in 2019. He has published over 150+ journal and conference papers and has two pending patents. In addition, he received the research excellence award of the Université du Québec in 2018. In 2019, he received the research excellence award from ÉTS in recognition of his outstanding research outcomes.

Dushantha Nalin K. Jayakody [S'09, M'14, SM'18] (nalin.jayakody@ieee.org) received his Ph.D. degree in electronics, electrical, and communications engineering, from University College Dublin, Ireland, in 2014. He received his M.Sc. degree in electronics and communications engineering from the Department of Electrical and Electronics Engineering, Eastern Mediterranean University, Turkey, in 2010 (under a university full graduate scholarship). From 2014 to 2016, he was a postdoctoral research fellow at the Institute of Computer Science, University of Tartu, Estonia, and the Department of Informatics, University of Bergen, Norway. Since 2016, he has been a professor in the School of Computer Science & Robotics, National Research Tomsk Polytechnic University (TPU), Russia. He also serves as the Head of the Research and Educational Center on Automation and Information Technologies and founder of the Tomsk infocom Lab at TPU. In addition, since 2019, he also serves as the head of thr School of Postgraduate Research, Sri Lanka Technological Campus (SLTC), Padukka, and founding director of the Centre of Telecommunication Research, SLTC.