Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.038335
Article

Blockchain and IIoT Enabled Solution for Social Distancing and Isolation Management to Prevent Pandemics

Muhammad Saad[1], Maaz Bin Ahmad[1,*], Muhammad Asif[2], Muhammad Khalid Khan[1], Toqeer Mahmood[3], Elsayed Tag Eldin[4,*] and Hala Abdel Hameed[5,6]

[1]College of Computing and Information Sciences, Karachi Institute of Economics & Technology, Karachi, Pakistan
[2]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan
[3]Department of Computer Science, National Textile University, Faisalabad, 37610, Pakistan
[4]Faculty of Engineering and Technology, Future University in Egypt New Cairo, 11835, Egypt
[5]Faculty of Computer and Information Systems, Fayoum University, Faiyum, Egypt
[6]Khaybar Applied College, Taibah University, Medina, Saudi Arabia
*Corresponding Authors: Maaz Bin Ahmad. Email: maaz@kiet.edu.pk; Elsayed Tag Eldin. Email: elsayed.tageldin@fue.edu.eg
Received: 08 December 2022; Accepted: 17 April 2023; Published: 09 June 2023

Abstract: Pandemics have always been a nightmare for humanity, especially in developing countries. Forced lockdowns are considered one of the effective ways to deal with spreading such pandemics. Still, developing countries cannot afford such solutions because these may severely damage the country's economy. Therefore, this study presents the proactive technological mechanisms for business organizations to run their standard business processes during pandemic-like situations smoothly. The novelty of this study is to provide a state-of-the-art solution to prevent pandemics using industrial internet of things (IIoT) and blockchain-enabled technologies. Compared to existing studies, the immutable and tamper-proof contact tracing and quarantine management solution is proposed. The use of advanced technologies and information security is a critical area for practitioners in the internet of things (IoT) and corresponding solutions. Therefore, this study also emphasizes information security, end-to-end solution, and experimental results. Firstly, a wearable wristband is proposed, incorporating 4G-enabled ultra-wideband (UWB) technology for smart contact tracing mechanisms in industries to comply with standard operating procedures outlined by the world health organization (WHO). Secondly, distributed ledger technology (DLT) omits the centralized dependency for transmitting contact tracing data. Thirdly, a privacy-preserving tracing mechanism is discussed using a public/private key cryptography-based authentication mechanism. Lastly, based on geofencing techniques, blockchain-enabled machine-to-machine (M2M) technology is proposed for quarantine management. The step-by-step methodology and test results are proposed to ensure contact tracing and quarantine management. Unlike existing research studies, the security aspect is also considered in the realm of blockchain. The practical implementation of the proposed solution also obtains the results. The results indicate the successful implementation

of blockchain-enabled contact tracing and isolation management using IoT and geo-fencing techniques, which could help battle pandemic situations. Researchers can also consider the 5G-enabled narrowband internet of things (NB-IoT) technologies to implement contact tracing solutions.

Keywords: Blockchain; contact tracing; distributed ledger technology; geo-fencing; internet of things; industrial internet of things; isolation management; social distancing; ultra-wideband

1 Introduction

A pandemic is spreading any disease over a large geographical area worldwide. The history of the pandemic is as old as the human. These occurred occasionally and caused severe damage to the human race. These damages ranged from disrupting daily activities, developing mental stress and fear, destroying the economy, and causing millions of deaths. The first declared pandemic of all time was influenza, which occurred in 1918 [1], and then the world faced its second and third waves in 1957 and 1968 consecutively. Later, severe acute respiratory syndrome (SARS) and swine flu emerged as the pandemics of the 21st century, which caused a large number of fatalities, followed by other epidemics, middle east respiratory syndrome (MERS), Ebola, and the avian flu [2]. COVID-19 is an ongoing pandemic that emerged in December 2019 in Wuhan City, China. The pandemic was declared by WHO on 11th March 2020.

By 2020, thousands of millions of people are facing a lockdown situation, affecting not only local economies but the global economy is also being affected [3]. COVID-19 has been spread over 226 countries, with over 506 million confirmed cases, including 6.2 million casualties (as of April 2021) [4]. The detailed analysis and statistics of COVID-19 cases until April 2022 are presented in Fig. 1.

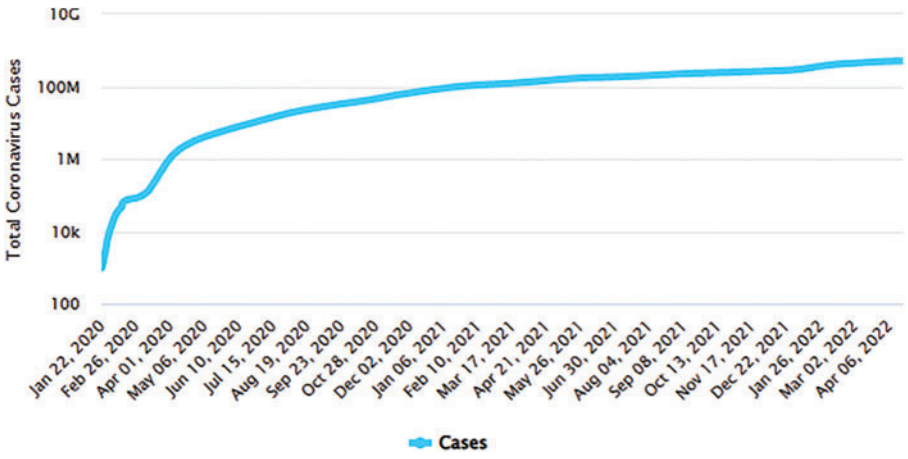

Figure 1: Statistics of COVID-19 cases

The researchers highlighted the significance of technologies in various studies to battle pandemic-like situations. The economies of developing countries are poorly affected, along with business processes and industries. Therefore, technological advancements are required in this era to battle such situations. Currently, the 5th wave of COVID-19 is brutally hampering the ordinary business operations of organizations and causing more deaths than the previous waves, especially in China. Unfortunately, it is not the end. History reflects that pandemics keep on occurring consistently. So, a

proactive mechanism should be available to organizations to run their business processes smoothly during the pandemic. This article aims to highlight the use of IoT-based technologies to handle pandemics. The existing studies emphasize handling situations using technologies instead of data management and security [5]. Therefore, implementing IoT and blockchain-enabled technologies not only brings advancement in the battleground of a pandemic but also helps to prevent pandemics. Contact tracing [6] and quarantine management are significant factors that can minimize pandemics. However, deploying the proposed solution can save millions of lives and the economies of developing countries.

Social distancing is a significant practice mentioned in standard operating procedures outlined by WHO. It highlights that individuals should maintain at least 3 meters from each other to avoid contacting the droplets released by mouth during talking, coughing, and sneezing, which can be infectious. Social distancing leads toward the smart contact tracing mechanism, which is the focal point of researchers nowadays, and several studies are being proposed in this dilemma. Similarly, unlike other studies on the concept, our proposed solution emphasizes its theoretical aspect and practical implementation using blockchain and IIoT technologies [7,8].

Isolation management is another crucial factor after social distancing violation. Therefore, this article also considers quarantine management to ensure smart prevention and handling of a pandemic using technologies. The components of the social distancing solution are extended to provide a foolproof mechanism for isolation using geofencing techniques. The smart contact tracing and isolation management of infected people are achieved in this article.

This article highlights the importance of advanced technologies in governing local and global economies in pandemic-like situations. The aim is to prevent and mitigate the effects of pandemics using technologies for developing countries. This study is highly stimulated by the recent COVID-19 pandemic, which has affected the global economy and swept the local economies of developing countries due to violations of social distancing and isolation management. Researchers around the globe present theories to manage COVID-19 using current technologies like IoT, IIoT, deep learning, and data sciences [9,10], but the security aspect is missing in most articles. Therefore, the proactive tamper-proof blockchain-enabled mechanism is proposed in this study for smart and secure contact tracing using IIoT for businesses and organizations to reduce the pandemic's impact on the economies of developing nations. The motivation of this study is to provide a comprehensive solution, especially for industries, to mitigate the effect of the pandemic using blockchain-enabled IoT solutions.

The proposed research target two main areas, i.e., social distancing and isolation management based on DLT. The implementation of blockchain will not only provide legitimate data logs of contact tracing but will also provide legitimate data logs of contact tracing and enable secure communication across IoT components. The blockchain-enabled solution would not only facilitate organizations to maintain tamper-proof tracing logs but to run their standard business processes while reducing the transfer of viruses from one individual to another. Public/private key authentication techniques and state-of-the-art communication technologies are also used to achieve a comprehensive mechanism for organizations to preserve privacy. The proposed mechanism will not only be useful in the current situation but will also be helpful for future pandemics.

This study proposed a detailed overview and methodology for privacy-preserving contact tracing and quarantine management using blockchain-enabled IIoT and M2M communication models. The novelty of this study is to provide end-to-end solutions for organizations to run their businesses in pandemic-like situations and to use inherent characteristics of blockchain towards information security for contact tracing to prevent record tampering and to provide legitimate information. The

proposed solution also contributes towards the security of advanced technologies like M2M, IoT, IIoT, and DLT. The proposed geo-fencing mechanism also extends the horizon of this study for other practitioners to use in different sectors. The proposed blockchain and IIoT-enabled framework reduces the spread of the pandemic and helps preserve local and global economies. The IoT band with embedded UWB technology is proposed for the contact tracing mechanism, followed by blockchain implementation to omit centralized dependency by storing tracing logs in a distributed manner. A blockchain-based system enables organizations to permit a specific count of employees in a particular location or area to manage social distancing. The public/private key architecture is also proposed to keep information in the blockchain consisting of employees. The cryptography-based mechanism also plays a vital role in facilitating employees with the necessary information by using the key-matching mechanism for authentication. The implementation details are described briefly in the methodology section.

The later sections of this study are classified as follows: Section 2 elaborates on the background, including related technologies. Section 3 presents a literature review and comparison of existing studies. Section 4 demonstrates the methodology and implementation details. Section 5 comprises experimental analysis and discussion, and lastly, Section 6 concludes the framework and highlights future directions.

2 Background and Related Technologies

2.1 Contact Tracing

The concept of contact tracing is not advanced. It has been practised since the first pandemic of influenza. The digital contact tracing mechanism has evolved using mobile applications [11]. The Bluetooth signals of smartphones detect the tracing logs; this phenomenon is known as Bluetooth-based-contact tracing [12,13]. The centralized and decentralized variants are available and proposed by several practitioners. Still, BLE technology cannot be considered state of the art to serve the purpose of contact tracing as it drains the user battery and leads to other attacks by which information can be misused. Therefore, DLT-based architectures are being used by organizations like Apple, Google, and IBM to achieve transparency, immutability, and security in different sectors.

2.2 Distributed Ledger Technology (DLT)

DLT has gained popularity among researchers since 2008. It is being deployed in various sectors, for example, financial services, energy, supply chain, IoT, IIoT, and identity management. Blockchain is based on DLT, which helps to decentralize instead of having a single point or centralized dependency. Satoshi Nakamoto is considered the founder of digital currency. In [14], Nakamoto proposed a decentralized platform for well-known digital currencies like Bitcoin and Ethereum. The proposed decentralized architecture enables peer-to-peer communication without relying on centralized authority. Therefore, bitcoin is considered as state of the art example of digital currency. The bitcoin architecture consists of connected blocks. Each block holds the information of the transaction, known as a record, and the link to the next connected block. This consecutive connectivity of blocks forms the chain called the chain of blocks or blockchain. The individual block holds the information as a hash, making it immutable as irreversible. The participating nodes in this network hold the network's complete information, known as the ledger. A shared ledger is like a shared database that enables nodes to exchange ledgers for validation and to preserve trust [15].

Blockchain offers various security and distributed architecture features that can be used for contact tracing. Proof of work (POW) and proof of stake (POS) are two common mechanisms

blockchain uses to prompt nodes to prove the worth of publishing blocks over the network. The nodes in the network make decisions based on the consensus mechanism to prove integrity and transparency. The consensus is achieved based on the competition over computing resources in POW and POS [16].

2.3 Industrial Internet of Things (IIOT)

The IIoT is the wireless network of industrial devices to exchange information with the infrastructure and among each other. IIoT-based devices consist of sensors, actuators, gateways, and objects connected over a wireless network. These devices are designed to collect data from the environment to share over the server to transform raw data into meaningful information. For example, sensors sense the environment and perceive environmental information. The perceived information is transmitted to the servers to process the data into meaningful information, such as weather conditions and predictions of storms, etc., based on raw data from the sensors. The composition of IIOT and machine-to-machine communication techniques helps to achieve a state-of-the-art communication model to store transactions over the network using inherent characteristics of blockchain and other storage schemes.

There are many applications of IoT or IIoT, for example, home automation, the internet of vehicles, fleet telematics, fuel telematics, digital card-based healthcare system, smart car parking, etc.

IIoT is gaining the research community's attention to solve the problems of particular domains like healthcare, finance, businesses, and industrial operations [17]. The overview of IIoT and its application is further demonstrated in Fig. 2, along with the transition toward industry 4.0.

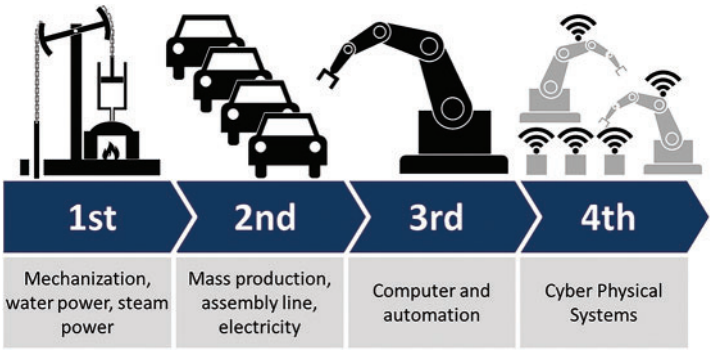

Figure 2: IIoT and industry 4.0

The IIoT infrastructure [18] is designed in such a way that the actuators, sensors, and edge nodes collect information from the deployed environment and transmit it to IoT or edge gateway to transfer the raw data to the IoT platform or cloud, which further performs data processing activities and drive meaningful information from the data as illustrated in Fig. 3.

2.4 Ultra-Wide Band Technology (UWB)

The UWB is one of the most powerful wireless technology in IoT [19]. It is widely used for indoor positioning systems due to its inherent characteristics of distance measurement. The transmitter and responder are two significant components of the UWB mechanism. The travelling time of the signal across these components is used to measure distance in indoor environments, as illustrated in Fig. 4.

The detailed working of UWB is demonstrated in Fig. 5, and the steps are as follows

- Each Fixed UWB Device sends signals to the nearby mobile device.
- Mobile UWB devices immediately respond with the acknowledgement signal.
- Fixed UWB device measures the time the signal travels, known as the Time of Flight.
- The system calculates the location by using the Time of Flight.

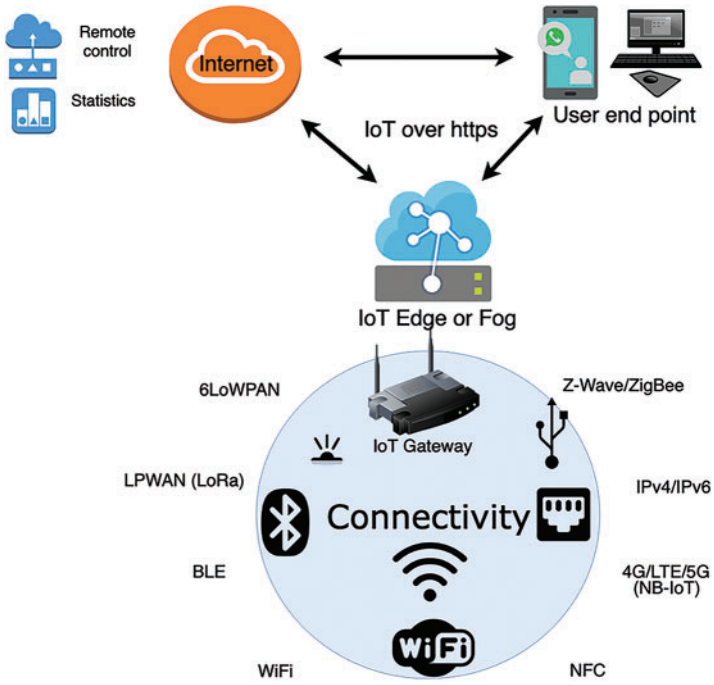

Figure 3: IIoT infrastructure and data transmission

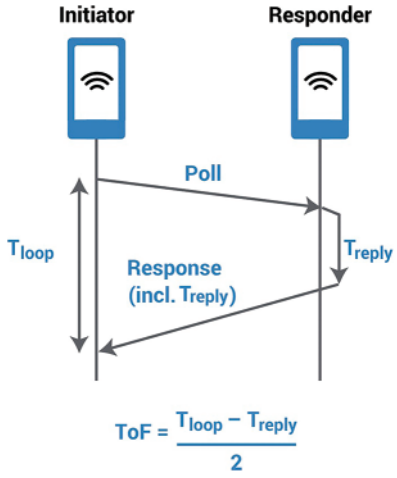

Figure 4: UWB components and communication mechanism

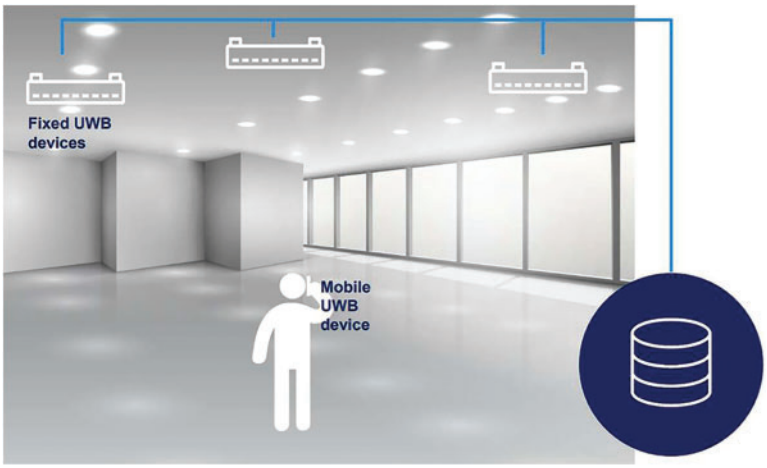

Figure 5: UWB positioning and working mechanism

The principle of UWB positioning uses the Time Difference of Arrival (TDOA) algorithm for positioning. UWB positioning requires three base stations; otherwise, the accuracy will be affected [20]. The precise identification of real-time indoor positioning is one of the significant characteristics of UWB compared to other indoor positioning techniques, such as BLE or WIFI positioning systems. The precision can reach about 10 cm, and it is the first choice of researchers for high precision at indoor locations.

2.5 Geo-Fencing

The Geo location-based fencing techniques enable users to create virtual boundaries over google or open street map (OSM) for the entry and exit alert notifications [21]. Similarly, this technique is used for employees, departments, activity areas, and other locations within the organization to restrict them to prevent fence violations using the proposed methodology, as discussed later in this article. Circular and polygonal fences are used in this study to create virtual boundaries over the map. The following Fig. 6 represents the layout of the fence and virtual boundaries.

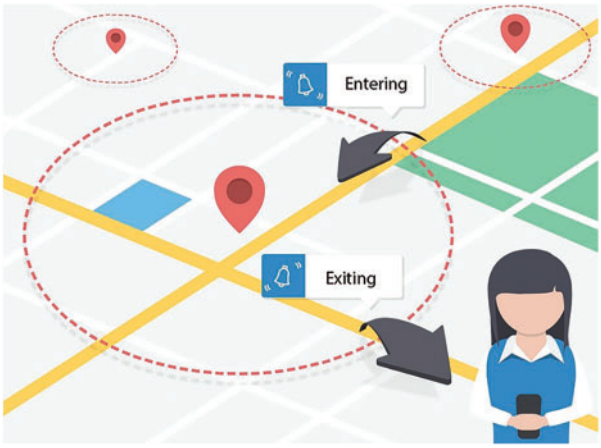

Figure 6: Geo-fencing and the creation of virtual boundaries

2.6 Machine-To-Machine (M2M) Communication

M2M communication is a significant component of IoT and IIoT [22]. M2M enables things to communicate with each other based on standard parameters. Implementing M2M promotes the communication model's state and eliminates human intervention in the IoT environment. The primary example of M2M communication is the mobility of static IP over global system for mobile communication (GSM) supported nodes. For example, GSM and long term evolution (LTE) based routers with static IP are being used to achieve advanced wireless networks with the inherent characteristic of mobility.

Machine-to-Machine (M2M) is a broad term. It encompasses any technology that allows devices to interact and share data autonomously. M2M communication is a crucial sanctioning technology for long-running industrial IoT applications, as no human intervention is required. The blockchain-enabled network allows M2M devices to store data in the form of ledgers and blocks over the network to achieve immutable and tamper-proof records for further use.

M2M communication comprises Artificial Intelligence (AI) and Machine Learning (ML) that facilitates IoT devices to communicate automatically and provides an ultra-modern architecture for the smart communication of IoT devices [22]. It also contributes to the accurate connectivity and integration of computerized processing machines like sensors, actuators, controllers, and robots. The M2M architecture is shown in Fig. 7.

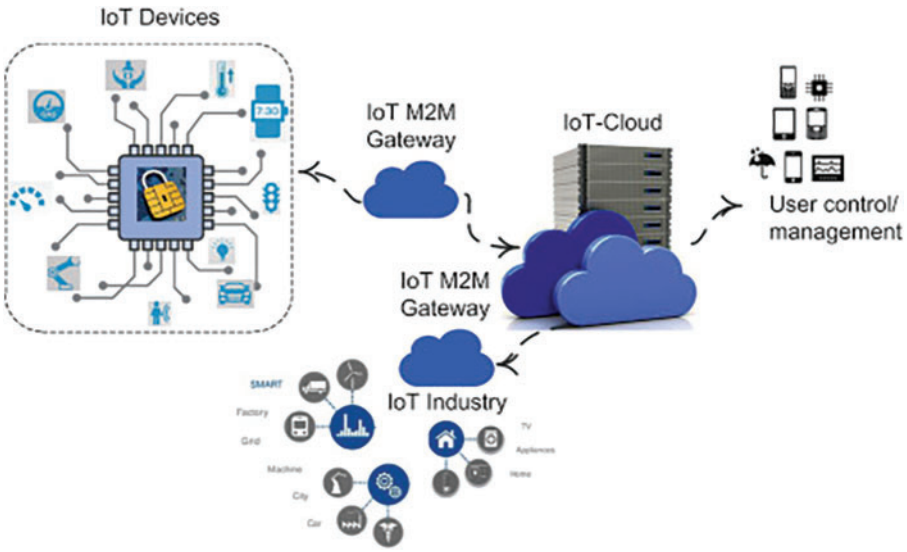

Figure 7: M2M layered architecture

3 Literature Review

COVID-19 has changed the era and our lives completely. It has become the most prominent area of study for practitioners. Through their studies and experiments, the practitioners continuously try to propose solutions to prevent pandemics. Several research studies emphasize target diagnosis and tracking of the disease, which evolved around artificial intelligence (AI) and deep learning-based techniques for early disease prediction. The existing research also highlights the significance and awareness of contact tracing techniques. In particular, contact tracing is a significant area that requires

the research community's attention. The detection of contact tracing is practised using composite emerging technologies such as computer vision, data science, AI, Bluetooth, UWB, and IoT have a significant impact on achieving social distancing and tracking [23]. In this study, we proposed enabling wireless technologies to enforce proper social distancing mechanisms.

The following sub-sections of the literature review consist of a fundamental understating of the concepts and technologies used in the proposed methodology. Therefore, terminologies are discussed in light of existing research in corresponding sub-sections.

In Table 1, there are nine existing projects mentioned, namely, Trace Together [24], Google/Apple [25], national health service (NHS) and China Project [26,27], mHealth, Baidu Big Data (BDD), Block-HPCT, blockchain-based contact tracing and privacy-preserving architecture including our proposed solution. The comparative analysis is based on attributes such as used technology, contact tracing functionality, power management, security, and privacy and isolation management. Trace Together application is based on BLE technology, which only keeps track of clients nearby in broadcasting mode, resulting in battery drainage issues. Bluetooth technology is criticized due to open security loopholes and the high risk of replay attacks. It is not endorsed by practitioners anymore for contact tracing. Therefore there is a need for advanced technology, as proposed in this study named UWB technology. Google contact tracing projects are also based on Bluetooth technology, but it does not record the real identity of the users, which makes them different from other projects. Regardless of this attribute, the same issues and concerns are discussed regarding Bluetooth technology. This application uses a centralized mechanism for contact matching and notification but makes it vulnerable to trajectory attacks for the misuse of user information.

Table 1: Comparison of proposed and existing solutions

Reference	Technology	Contact tracing	Power management	Security	Privacy-preserving	Isolation management
[24] Trace together	BLE	✓	×	×	×	×
[25] Google/Apple contact tracing project	BLE	✓	×	✓	✓	×
[26] NHS contact tracing project	BLE	✓	×	×	✓	×
[27] China health code project	GNSS and QR	✓	✓	✓	×	×
[28] Tele-health	Mobile technology	✓	×	×	✓	✓
[29] Baidu big data (BDD)	Big data and GPS	✓	×	×	×	✓
[30] Block-HPCT	Smart contracts	✓	×	✓	×	×
[31] Blockchain-driven contact tracing	Blockchain, BLE and sound	✓	×	×	×	×
[32] ABAFOR	Blockchain	✓	×	✓	✓	×
Proposed solution	Blockchain, IoT and UWB	✓	✓	✓	✓	✓

Similarly, the NHS application faced severe concerns regarding its implementation due to BLE technology. The health code system is based on QR instead of Bluetooth and proximity technology. It is only used upon passing through checkpoints. It is reliable to some extent but limited to a specific location and does not serve the need for a smart contact tracing mechanism to cover large areas.

Mobile health (mHealth) is one of the advanced concepts of remote patient monitoring, which helps to detect, track and diagnose infections [28]. This technology has also emerged with COVID-19 for smartly managing infected people.

On the other hand, BDD technology has also emerged during the pandemic to locate the zones of infected patients and track their movements to identify high-risk zones and enforce lockdown decisions [29]. The recent research on blockchain-enabled digital health passports and contact tracing (Block-HPCT) is also explored in this article, emphasizing the use of smart contracts for trust management, transparency, and security of the records [30]. Practitioners are also proposing blockchain-driven contact tracing solutions to ensure privacy and trust among entities. The sound-based technology is proposed by one researcher in his recent article along with BLE for proximity detection in contact tracing [31]. Lastly, a blockchain enables privacy-preserving architecture (ABAFOR) is also explored for efficient contact tracing and analysis [32].

Several distancing studies are also based on Unmanned Aerial Vehicles (UAVs), which can also be used to reduce human intervention. However, current research emphasizes UAVs for outdoor navigation based on global navigation satellite system (GNSS) [33]. The UAV technology is unsuitable for indoor environments due to its low accuracy. Therefore, such methods cannot be applied for indoor contact tracing and quarantine management. Several other methodologies are also employed to resolve open issues [34,35] by practitioners to deal with such pandemic-like situations.

The existing research revolves around BLE, barcode, mobile, and big data technologies having several open issues related to security and privacy preservation. Therefore, the proposed solution considers all the open issues related to security by providing a state-of-the-art blockchain-enabled mechanism for tamper-proof and immutable data management. The accuracy and ease of implementation are some of the most critical that are missing in existing research researchers have not touched on its practical implementation, making our proposed solution more unique, secure, and easy to implement.

4 Proposed System and Implementation

Pandemic prevention and quarantine management are among developing countries' highest pandemic priorities. The prevention of pandemics is only achieved using WHO standards and mechanisms consisting of contact tracing and isolation management. The need for blockchain is considered to preserve privacy during solution implementation for contact tracing as per standards. The 5G-enabled wearable using UWB technology is proposed to enable a smart indoor positioning system that supports bi-directional M2M communication for tracing. This section comprises two major sub-sections to answer the following:

- How to achieve blockchain-enabled contact tracing for organizations?
- How do geo-fencing techniques for isolation or quarantine management restrict employees to specific areas?

4.1 Blockchain-Enabled Contact Tracing

Blockchain-enabled contact tracing can be achieved by following the steps.

Step 1 is key distribution, in which public key infrastructure-certified authorities distribute keys to the users with wearable wristbands.

The first step is the distribution of keys. PKI/CA distributes keys to the wristband users, as shown in Fig. 8.

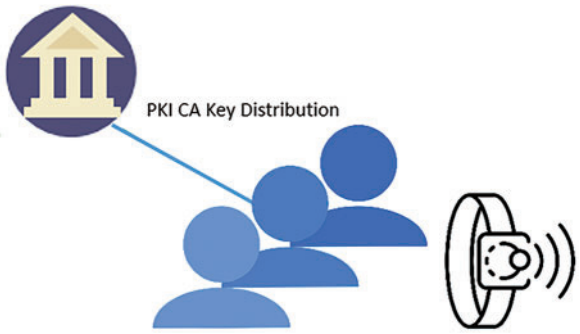

Figure 8: Distribution of keys

In the second step, the wearable device generates a private key once daily to couple addressing. The specified private key will be saved in the local storage of the wearable device in an encrypted format to ensure the user's privacy from threats, as highlighted in Fig. 9. The pseudonym relies on the generated private key to be coupled with the irreversible blockchain address. The device also collects positioning data to hold meaningful information.

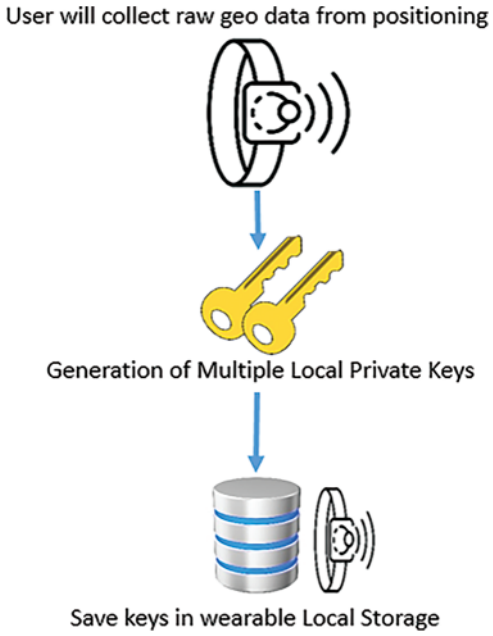

Figure 9: Generation and storage of private keys

In the third step, the wristband generates hashed data using a CA-recognized public key to encrypt its current UWB positioning information and date time. The hashed data is used as a suffix of the address or user code, as shown in Fig. 10.

In the fourth step, the pseudo-identity of the user is established using the above steps and coupling the user's private key. The coupling of positioning data enhanced its security to form a highly secured blockchain address, as shown in Fig. 11. The block's declaration over the network will take place in this step after having a secured address.

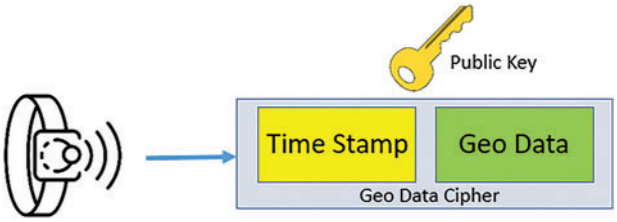

Figure 10: Generation of hash consists of geo data

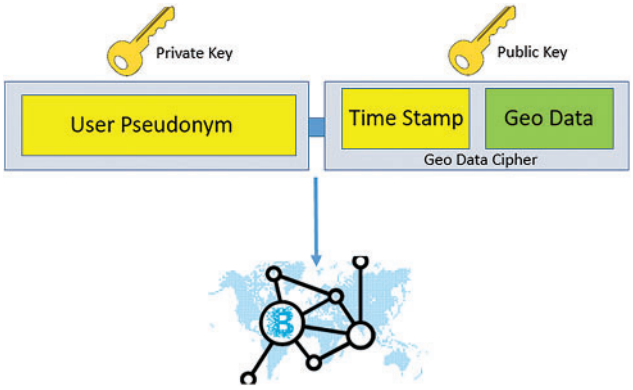

Figure 11: Coupling of user identity with hashed geo data along with publication on the blockchain network

In the fifth step, contact tracing is achieved by decoupling using the prefix of address as it is indexable by any trusted party having a key issued by CA as of victim's signed pseudonym because it is bounded with geo data cypher in case of violation of contact tracing and published over the blockchain network. On the other hand, privacy is also preserved due to anonymity achieved using a pseudo-identity mechanism. The updated block is also published on the network after recoupling.

The trusted parties with authorized keys can now perform contact tracing using their reserved keys over the blockchain network.

Cryptographic techniques are applied to generate pseudonyms using symmetric encryption in the proposed methodology. Fig. 12 elaborates on the address composition consisting of the pseudonym of the user or victim as a prefix and positioning as the suffix. The user uses the private key to create a hash or prefix, and the public key encrypts, positioning information as suffixes. The coupling of generated prefixes and suffix enables the user to generate an address and share it over the blockchain network. The only trusted nodes will be able to separate suffixes and prefixes. However, only trusted nodes will have a certified key to identify the signed pseudonym without knowing their identity using this model. The trusted chain is developed using the proposed methodology to expose only relevant information and to make contact tracing more secure and reliable.

The proposed blockchain network is completely isolated from the internet. Therefore IP and routing access information are concealed in the proposed methodology. The proposed chain is the only coupling of pseudonyms and positioning information. Tracing for the other users is also tricky to continuously changing positioning data, making our methodology more secure.

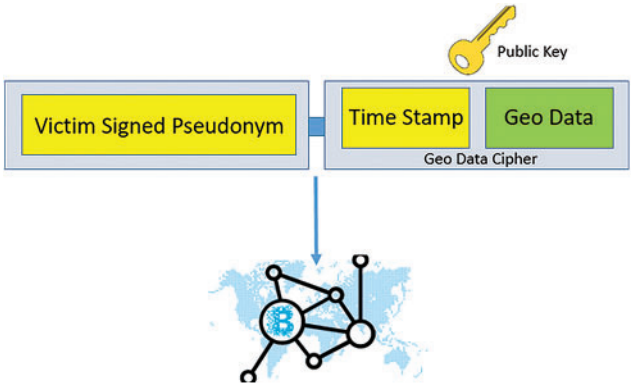

Figure 12: Coupling of victim signed pseudonym and hashed geo data along with republication of address over the blockchain network

4.2 Hardware Components for Contact Tracing

This section comprises proposed hardware technical specifications followed by network configuration for blockchain-enabled contact tracing.

The following components are used to propose a contact tracing solution:

- M2M Mobile Node (Wearable IoT device)
- M2M Locator Node

4.2.1 M2M Mobile Node (Wearable Wristband)

The proposed wristband is an 'out of the box' social distancing solution. It needs to power up, and its state-of-the-art technology does the rest. A red light and vibration alert activate if another device is less than 6 ft away. Suppose proximity decreases to 3 ft or less. In that case, the band' LED will flash red with a stronger vibration and an audible alarm-notifying both wearers that action should be taken immediately. The proposed mobile device communicates with fixed devices to identify UWB positioning to collect data for transmission. This wearable is also based on android OS and general packet radio services (GPRS)/GSM connectivity, which helps to manage the communication with the servers and to perform cryptographic operations to ensure pseudo-identity. It is reusable and rechargeable. The applications of this device are as follows

The proposed device can also be conFig.d using a smart application. The application can set parameters like connection type and data transmission interval easily.

Furthermore, UWB technology makes it more robust for indoor positioning. Internal details of the wristband are highlighted in Fig. 13.

The proposed device helps achieve blockchain-enabled contact tracing to maintain social distancing. The usage of the device not only helps reduce the impact but also avoids the spread of virulent disease.

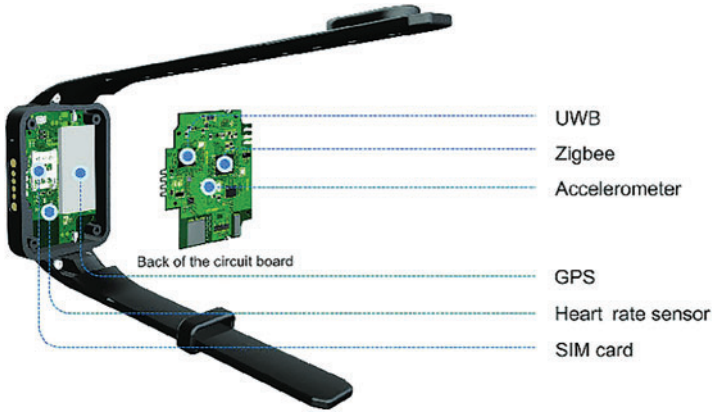

Figure 13: Wearable chipset information

4.2.2 M2M Locator Node

The wireless M2M locator device is widely used for IoT-based applications. The locator device is exhibited in Fig. 14, which helps to detect nodes transmitting UWB packets over the wireless network. The high accuracy is achieved using the locator node in the proposed methodology for indoor positioning to calculate distance across multiple wristbands.

Figure 14: Locator node

4.2.3 Network Connectivity

The blockchain-enabled network is achieved using UWB-enabled wristbands for contact tracing. The wearable devices acted as transmitters, and the locator acted as a responder. The positioning data is calculated based on the communication between the locator and wristband. The wristband is also equipped with LTE technology to transmit data over the server using the internet. Therefore, positioning information is also obtained in local networks and the internet. Subsequently, the positioning data is processed by the firmware of the wristband and generates violation alerts based on data perceived via locator nodes.

4.2.4 Application and Use Cases

The proposed wristband helps organizations keep their production going to boost the economy and protect their workforce by violating standard operating procedures of social distancing.

The proposed social distancing wristband can also help owners to get fans back in the stadium supporting their favourite teams regardless of pandemic-like situations. They can issue wristbands at the gate to help them maintain proper social distancing practices as they use concessions and other stadium facilities.

4.3 Implementation Strategy of Contact Tracing

The proposed methodology can be deployed using the hardware mentioned above and the following steps:

- The activity of deployment of the locator device is carried out at the organization's premises to detect the transmitters to identify violations.
- The wearable devices are configured in this step to act as transmitters. The settings, like transmission interval, connection type, etc., are managed accordingly.
- The end users or employees of the organization are prompted to wear the wristbands in the area where the locator is installed to make contact. The data is also transmitted over the server using an LTE connection.
- Contact tracing logs are generated by the wristband and transmitted to the server for the user to monitor and control the activities.

A blockchain-based system enables organizations to permit a specific count of employees in a particular location or area to manage social distancing. DLT omits the centralized dependency by transferring data among employees without depending on the centralized node. Privacy preservation was essential in facilitating employees with the necessary information using private and public key-matching mechanisms. The public and private key pairs are generated when an employee provides a wearable. Authentication is achieved when the wearable uses its private key to generate the address on the organizational chain. Similarly, the private key is linked to an employee's wearable. This contact tracing system has become more secure, fast, and versatile.

Future work can include developing a mobile application for employees to use as the blockchain wallet. The wallet will represent employees' number of tokens used to spend as movement tokens several times before expiry. Organizations can verify the tokens to restrict the presence of employees who only have active tokens to carry out operational activities at a particular time at a specific location or department. It will help control the employees department-wise within an organization. Blockchain technology's implementation emphasizes scalability and promotes an efficient way to manage many employees or populations as an extended use case for social distancing. A mobile application will make this system user-friendly in multiple situations, such as event management, restricting entries with a movement token, managing roadside units, etc.

4.4 Implementation Strategy of Quarantine

Quarantine management is another significant measure adopted as a reactive method to prevent the spread of the pandemic. Smart quarantine management aims to restrict infected people in a specific location and to monitor them using technological advancement.

The research is further extended to UWB and LTE technology to provide an implementation strategy for quarantine management using the above-proposed hardware. The proposed wristbands

have the feature to transmit positioning data over the server using LTE. This communication model transmits positioning data to the servers where data processing occurs. The objective was to receive UWB positioning data and process it to generate meaningful information on fence violations. Therefore, the Haversian algorithm provides the positioning data to identify if the received data lies in the fence's boundary. This way, fence in and out logs are obtained on the server.

The following steps are used to generate fence logs using UWB-based wearables.

- Quarantine centres are marked on the maps using circular fences having a radius of 500 meters to have an eye on entry and exit logs. The logs are obtained using the Euclidean mathematical distance calculation model as illustrated in the proposed algorithm.
- The positioning data is transmitted by the bands to the server using LTE and processed accordingly in the realm of implemented geo-fencing technique. The logs are obtained and transmitted to the wristbands and the concerned authority for management and control.

Algorithm I is proposed for circular fence checking. It receives three inputs comprising a list of fences, point or current geo-location, and radius assigned to detect a violation. The input point is compared to each coordinate available in the list of fences to get the distances across them. If any distance exceeds the radius, it is considered a violation and continues for other iterations accordingly.

4.4.1 Algorithm I—Circular Fence Checking

Algorithm I: Circular Fence Checking

Input: P: x, y; Q: q1, q2; R: 500 (Given a point as P, list of fences as Q and radius as R)
Output: S (Boolean variable true or false)
Where q1 → (q1x, q1y)
Initialize Boolean Variable
1: S ←false
2: Foreach Q:
Start
/∗Iteration 1 Illustrated∗/
3: $A \leftarrow q1x - Px$
4: $B \leftarrow q1y - Py$
5: $C \leftarrow A^2 + B^2$
6: D ← Square root (C)
Where D: represents the distance
7: If Distance < R
Start
8: S ← true
End
Else
Start
9: S ← false
End
End
10: Return S;

Algorithm II is proposed for polygonal fence checking. It receives two inputs comprising a point or current geo-location and a list of polygonal fences to detect violations. The input point is compared

to each polygon available in the list of fences to get the slope value across them. If the point-slope is less than the edge slope, it is considered a violation and continues for other iterations accordingly.

4.4.2 Algorithm II—Polygonal Fence Checking

Algorithm II: Polygonal Fence Checking

Input: P: x, y; Q: e1, e2; (Given a point P, list of polygonal edges with coordinates x and y Q)
Output: T (Boolean variable true or false)
Where e1 → (A1, B2) → (A1x, A1y), (B1x, B1y)
Initialize Boolean Variable
1: T ←false
2: Foreach Q: Iteration 1
Start
3: If ((Py > B1y) or (Py < A1y) or (Px > max (A1x, B1x)))
Start
4: T ← true
End
5: Else if (Px < min (A1x, B1x)
Start
6: T ← false
End
Try
Start
7: EdgeSlope ← (B1y – A1y)/(B1x – A1x)
8: Except InfinityError:
End
Try
Start
9: PointSlope← (Py – A1y)/(Px – A1x)
10: Except InfinityError
End
11: If pointSlope >= edgeSlope
Start
12: T ← false
End
End
13: Return T;

5 Analysis and Discussion

We installed the M2M locator node at different locations of an organization as a demo project. The main gate, help desk, cafeteria, and ballroom are targeted to achieve the desired results of distance violations within the organization's premises. The wearable device is provided to 10 employees to monitor their activities in targeted locations. The results are obtained after deploying the proposed solution in an indoor environment. The further detailed analysis and generated results are discussed in later sub-sections.

5.1 Descriptive Analysis of the Corpus and Generated Results in the Form of Logs

Different techniques are proposed and implemented to provide organizations with a single-window solution. The proposed solution would not only prevent the pandemic spread but also helps in implementing standard operating procedures (SOPs) inside the organizations. Ultimately, it would help prevent the country's economic crash during the pandemic. Using this, organizations could run their standard business processes during any pandemic. Another benefit of the proposed solution is that the organizations should invest only once to adopt it. It would remain available to them for current and future pandemics.

Firstly, several available communication technologies are investigated, and the most appropriate one is selected based on UWB technology. UWB and BLE 5.0 technology is used to enhance the scalability of the network. Secondly, network infrastructure is created using a locator node to validate the concept, and communication is tested between the wristband and the servers. Wristbands worked as the active devices connected with the locator node to establish the connection. Further, the node was connected to the server, and contact tracing logs were transmitted to the server using this network scheme.

The results obtained from the implementation of contact tracing are mentioned in Table 2, which represents the logs

Table 2: Generated logs and blockchain address mapping for contact tracing

Employee ID	Victim ID	User identity	Geo location cipher	Blockchain address	Location	Signal strength	Event
111	679	/nU/ESHWMHwm S8q40ZMaLQ==	oKqWHdHctBEHQL+ 2DM3jEdtETfcW3+5 p535hCHj+fEK3CnoJ YYQmx6qZkpNGPS UTrs5E2byFZJI=	/nU/ESHWMHwmS8q40ZMaLQ ==oKqWHdHctBEHQL+2DM3j EdtETfcW3+5p535hCHj+fEK3C noJYYQmx6qZkpNGPSUTrs5E2 byFZJI=	Helpdesk	7	Distance violation
679	111	eq1q2nBQt2jDSkAH T8YpZQ==	jkVZC7agp8CheaVEsl 2I8+WKHb4fGWCa5 35hCHj+fEK3CnoJYY Qmx6qZkpNGPSUTrs 5E2byFZJI=	eq1q2nBQt2jDSkAHT8YpZQ== jkVZC7agp8CheaVEsl2I8+WKH b4fGWCa535hCHj+fEK3CnoJY YQmx6qZkpNGPSUTrs5E2byFZJI=	Helpdesk	7	Distance violation
1247	457	Qb++ZgWxjnvcbi nAYSxAOA==	5kcA1c26Ykjq0M5f +mc8QfSwjuc6Yy1lQ Vn3lMsho+t1QhC0+ LsdTCa0jt2AK7bYD kuA6g6PrUE=	Qb++ZgWxjnvcbinAYSxAOA= =5kcA1c26Ykjq0M5f+mc8QfSw juc6Yy1lQVn3lMsho+t1QhC0+ LsdTCa0jt2AK7bYDkuA6g6PrUE=	Ball room	8	Distance violation
1815	1025	9AkAR8dLJkJkIpi8 KldlBQ==	MaKmNWv1pQ81Gd JcOZG9K7bvf7+KiR4 TFZ/3MVwolt1ZB8s z9b3njSjEmNZMzc8J	9AkAR8dLJkJkIpi8KldlBQ==Ma KmNWv1pQ81GdJcOZG9K7bv f7+KiR4TFZ/3MVwolt1ZB8sz 9b3njSjEmNZMzc8J	Cafeteria	7	Distance violation
457	1247	mirsqKCV+nBzbL PNi6ghTg==	cXLwyG+ySoN8GhZ qfa+r9ViVJVrPZfa/Q Vn3lMsho+t1QhC0+ LsdTCa0jt2AK7bYD kuA6g6PrUE=	mirsqKCV+nBzbLPNi6ghTg==c XLwyG+ySoN8GhZqfa+r9ViVJ VrPZfa/QVn3lMsho+t1QhC0+Ls dTCa0jt2AK7bYDkuA6g6PrUE=	Ball room	7	Distance violation
1025	1815	xTFCfpYYkewmue udCqpkKA==	5GYA0NsgdQumpJT 1bVoj3Qd1DCLm0Sb XFZ/3MVwolt1ZB8s z9b3njSjEmNZMzc8J	xTFCfpYYkewmueudCqpkKA= =5GYA0NsgdQumpJT1bVoj3Q d1DCLm0SbXFZ/3MVwolt1ZB 8sz9b3njSjEmNZMzc8J	Cafeteria	9	Distance violation

(Continued)

Table 2: Continued

Employee ID	Victim ID	User identity	Geo location cipher	Blockchain address	Location	Signal strength	Event
3519	2729	X5pEHVmEXfJ85nen Ssejvg==	KHjGhUVrs2l5tQZq3 DiChpgOlPCwmfOItkl 4kbsLAjr2hypgLNRz plPzn9K93Fxo	X5pEHVmEXfJ85nenSsejvg==K HjGhUVrs2l5tQZq3DiChpgOlP CwmfOItkl4kbsLAjr2hypgLNRz plPzn9K93Fxo	Helpdesk	6	Distance violation
2729	3519	yKgx57Io5mob7KN dWj/Rbw==	zYY/hRW4E4nYfBp TyElAZeS6uhbubSeV tkl4kbsLAjr2hypgLN RzplPzn9K93Fxo	yKgx57Io5mob7KNdWj/Rbw==z YY/hRW4E4nYfBpTyElAZeS6u hbubSeVtkl4kbsLAjr2hypgLNRz plPzn9K93Fxo	Helpdesk	8	Distance violation

Date Time: The specified date time field represents the global positioning system (GPS) time of the violation. Further, this field gets converted into a cypher along with geo coordinates in the column of the geo-location cypher.

Employee ID: This is the employee's assigned code mapped with the wearable.

Victim ID: This is also the assigned code of the employee mapped with the wearable but represents the employee found violating the distance.

User Identity: This field represents the employee's pseudo-identity, which is used as a key for contact tracing. It is used as the prefix of blockchain address.

Geo-location Cipher: This is the cypher text generated from the real-time GPS location and date and time received from the wearable. It is used as the suffix for the generation of blockchain addresses.

Blockchain Address: This field represents the block address published on the blockchain network. The specified address is constructed from the user identity and geo data cypher as prefixes and suffixes.

Location: This field represents the location based on the geo data where locator nodes are installed.

Signal Strength: This field represents the number of contacts or visible satellites to identify the strength of the signal.

Event: This event field helps the authority identify the alert type, whether it is related to distance or geo-fence violation

The proposed solution is primarily for the organizations to control the activities of the employees. The first part of the solution is to restrict the employee from wearing a wristband for social distancing. Secondly, as soon as an employee enters the premises, the second level of monitoring of contact tracing occurs. The contact tracing mechanism helps detect social distancing violations and trace the contacts. The proposed solution is easy to implement, significantly preventing pandemics, and boosting the economy in pandemic-like situations.

The results of implementing the geo-fencing technique for quarantine management are also mentioned in Table 3. The transmitted geo location of an employee found in the radius of the virtual boundary is processed by the server and logged by the system accordingly in case of an intimation. The logs are generated based on the fence in and out intimations. The date time represents the log time. Fence ID represents the fence code of the virtual boundary, which can be polygonal and circular, as highlighted in the attribute of fence type. The coordinates and fence radius are also shown in Table 3 to depict the exact violation location. Similarly, the status field 'ISIN" is used to determine the employee's current status, where 1 represents in and 0 represents out.

Table 3: Generated logs of geo-fencing based initimations

Date time	Fence ID	Fence type	Fence coordinates	Radius	Employee ID	Is in	Event
4/22/22 10:16 AM	1	Circular	24.8607835, 67.0595445	500	111	1	Help desk in
4/24/22 9:31 AM	2	Circular	24.872223, 67.063024	500	457	1	Main gate in
4/22/22 11:40 AM	1	Circular	24.8607835, 67.0595445	500	111	0	Help desk out
4/24/22 5:43 PM	2	Circular	24.872223, 67.063024	500	457	0	Main gate out

The design of the proposed solution is modular. Different modules can also be used at desired places as a stand-alone application. For example, the isolation management module can be deployed at quarantine centres, cells of high-profile jail criminals, house-arrest cases, etc. In a nutshell, the proposed project has a wide range of applications in addition to its use as a preventive measure against the pandemic's spread.

5.2 Economy and Quality of the Solution

This study aims to make some efforts to safely carry on the organization's regular business operations in pandemic scenarios. It would help in preventing the crash of the economy of the country. By adopting such products, the developing countries would gain confidence regarding preventing pandemics inside the organizations, thus allowing them not to enforce strict actions like forced lockdowns. Due to the modular nature of the solution, its modules can be deployed to several other places as a stand-alone application, as stated above. M2M and IIoT concepts are the project's core, which would minimize workforce use. The proposed solution is cost-effective as it is only a one-time expenditure to the organization and would be available in future pandemic scenarios. The fewer infected people in the organizations, the more workforce would be available, resulting in a more overall profit.

5.3 Limitations of the Proposed Solution

The proposed solution is tested on 3G/4G technology due to the limitations and restrictions of 5G technology in Pakistan. The proposed solution is based on GPS-enabled wearable devices, and the standard GPS inaccuracy is 3 to 4 meters, t. Therefore, the limitations of GPS should be considered before the implementation ofimplementing a geo-fence fence-enabled quarantine management solution. On the other hand, there is also a limitation of wearable device battery usage, which needs to get charged within 3 to 4 days, t. Soherefore, this study can be further extended towards NB-IoT technology to save battery consumption to avoid the issue of regular charging.

6 Conclusion and Future Directions

This paper comprises multi-disciplinary research which addresses networks and communication domains. The end-to-end solution is obtained in this study to prevent pandemics using industrial internet of things (IIoT) and blockchain-enabled technologies. The information security of the proposed solution is also preserved in this study by obtaining an immutable and tamper-proof contact tracing and quarantine management mechanism. The contact tracing mechanism is achieved using DLT and UWB technology that can be enhanced further by using 5G and NB-IoT technology as future prospect. The quarantine management mechanism is achieved using geofencing and M2M techniques. The experimental results indicate the successful implementation of blockchain-enabled

contact tracing and quarantine management using advanced technologies, which could help battle pandemic situations. This study also extends the research towards blockchain-enabled technologies to identify infected individuals, track their cases and medication, contact tracing, isolation management, and smart quarantining. In blockchain profiles geo-positioning of the individual, travelling history and contact tracing with other known COVID-19-infected individuals, vaccination, and medical information will be added to the data pool to implement machine learning techniques employed with blockchain for scalability as a research direction. DLT will also be applied to the smart vaccination process. The government can issue vaccination certificates using DLT technology for smart tracing of cases and linked information such as personal information, especially an individual's age and medical history.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Palese, "Influenza: Old and new threats," *Nature Medicine*, vol. 10, no. 12, pp. S82–S87, 2004.
[2] K. K. C. Hung, C. K. M. Mark, M. P. S. Yeung, E. Y. Y. Chan and C. A. Graham, "The role of the hotel industry in the response to emerging epidemics: A case study of SARS in 2003 and H1N1 swine flu in 2009 in Hong Kong," *Globalization and Health*, vol. 14, no. 117, pp. 1–7, 2018.
[3] S. Platto, T. Xue and E. Carafoli, "COVID19: An announced pandemic," *Cell Death & Disease*, vol. 11, no. 9, pp. 799, 2020.
[4] Worldometers, "COVID-19 coronavirus pandemic," USA, 2004. [Online]. Available: https://www.worldometers.info/coronavirus/
[5] W. He, Z. Zhang and W. Li, "Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic," *International Journal of Information Management*, vol. 57, pp. 102287, 2021.
[6] A. Anglemyer, T. H. M. Moore, L. Parker, T. Chambers and A. Grady, "Digital contact tracing technologies in epidemics: A rapid review," *Cochrane Database of Systematic Reviews*, vol. 8, pp. 1–42, 2020.
[7] M. Saad, M. B. Ahmad, M. Asif, K. Masoof and M. Al-Ghamdi, "Social distancing and isolation management using machine-to-machine technologies to prevent pandemics," *Computers, Materials, & Continua*, vol. 67, no. 3, pp. 3545–3562, 2021.
[8] Z. Qingyi, S. W. Loke, R. Trujillo-Rasua, F. Jiang and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM Computing Surveys*, vol. 52, no. 6, pp. 1–34, 2019.
[9] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan *et al.,* "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3915–3929, 2020.
[10] A. Asraf, M. Z. Islam, M. R. Haque and M. M. Islam, "Deep learning applications to combat novel coronavirus (COVID-19) pandemic," *SN Computer Science*, vol. 1, no. 363, pp. 1–7, 2020.
[11] Y. Sahraoui, L. D. Lucia, A. M. Vegni, C. A. Kerrache, M. Amadeo *et al.,* "TraceMe: Real-time contact tracing and early prevention of COVID-19 based on online social networks," in *IEEE 19th Annual Consumer Communications & Networking Conf. (CCNC)*, Las Vegas, NV, USA, pp. 893–896, 2022.
[12] M. Condoluci, G. Araniti, T. Mahmoodi and M. Dohler, "Enabling the IoT machine age with 5G: Machine-type multicast services for innovative real-time applications," *IEEE Access*, vol. 4, pp. 5555–5569, 2016.
[13] V. Jahmunah, V. K. Sudarshan, S. L. Oh, R. Gururajan, X. Zhou *et al.,* "Future IoT tools for COVID-19 contact tracing and prediction: A review of the state-of-the-science," *International Journal of Imaging Systems and Technology*, vol. 31, no. 2, pp. 455–471, 2021.
[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, pp. 1–9, 2008. https://bitcoin.org/bitcoin.pdf

[15] H. Natarajan, S. Krause and H. Gradstein, "Distributed ledger technology and blockchain," in *World Bank*, 2017. [Online]. Available: https://elibrary.worldbank.org/doi/abs/10.1596/29053
[16] B. Sriman, S. G. Kumar and P. Shamili, "Blockchain technology: Consensus protocol proof of work and proof of stake," in *8th Int. Conf. on Intelligent Computing and Applications (ICICA)*, Melbourne, Australia, pp. 395–406, 2019.
[17] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 2018.
[18] S. Vitturi, C. Zunino and T. Sauter, "The industrial communication systems and their future challenges: Next-generation ethernet, IIoT, and 5G," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 944–961, 2019.
[19] D. Minoli and B. Occhiogrosso, "Ultrawideband (UWB) technology for smart cities IoT applications," in *IEEE Int. Smart Cities Conf.*, Kansas City, MO, USA, pp. 1–8, 2018.
[20] R. Yamasaki, A. Ogino, T. Tamaki, T. Uta, N. Matsuzawa *et al.,* "TDOA location system for IEEE 802.11b WLAN," in *IEEE Wireless Communications and Networking Conf.*, New Orleans, LA, USA, vol. 4, pp. 2338–2343, 2005.
[21] S. Ismail, M. A. M. Hanfi, R. Ismail, A. S. Khalid and F. S. Ismail, "Geo-fencing technique for internship placement-use cases deliverables," in *16th Int. Conf. on Ubiquitous Information Management and Communication (IMCOM)*, Seoul, South Korea, pp. 1–4, 2022.
[22] M. Kumar and S. Kumar, "Communication Technologies for M2M and IoT Domain," in *Internet of Things*, 1st ed., UK: Taylor & Francis, pp. 1–29, 2022.
[23] M. Hofmann, "COVID-19 tracking apps: Privacy and accuracy," *The ACM Magazine for Students*, vol. 28, no. 2, pp. 30–32, 2022.
[24] H. Stevens and M. B. Haines, "Tracetogether: Pandemic response, democracy, and technology," *East Asian Science, Technology and Society: An International Journal*, vol. 14, no. 3, pp. 523–532, 2020.
[25] Y. Gvili, "Security analysis of the COVID-19 contact tracing specifications by Apple Inc. and Google Inc.," *Cryptology ePrint Archive*, pp. 1–17, 2020. [Online]. Available: https://eprint.iacr.org/2020/428
[26] M. Hotopf, E. Bullmore, R. C. O'Connor and E. A. Holmes, "The scope of mental health research during the COVID-19 pandemic and its aftrmath," *The British Journal of Psychiatry*, vol. 217, no. 4, pp. 540–542, 2020.
[27] C. Swain, M. N. Sahoo, A. Satpathy, K. Muhammad, S. Bakshi *et al.,* "METO: Matching-theory-based efficient task offloading in IoT-fog interconnection networks," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12705–12715, 2020.
[28] X. Ding, D. Clifton, N. Ji, N. H. Lovell, P. Bonato *et al.,* "Wearable sensing and telehealth technology with potential applications in the coronavirus pandemic," *IEEE Reviews in Biomedical Engineering*, vol. 14, pp. 48–70, 2020.
[29] R. Shaw, Y. K. Kim and J. Hua, "Governance, technology and citizen behavior in pandemic: Lessons from COVID-19 in East Asia," *Progress in Disaster Science*, vol. 6, pp. 100090, 2020.
[30] M. M. Rashid, P. Choi, S. H. Lee and K. R. Kwon, "Block-HPCT: Blockchain enabled digital health passports and contact tracing of infectious diseases like COVID-19," *Sensors*, vol. 22, no. 11, pp. 1–23, 2022.
[31] Z. Hee and I. Salam, "Blockchain based contact tracing: A solution using bluetooth and sound waves for proximity detection," *Cryptology ePrint Archive*, pp. 1–21, 2022. [Online]. Available: https://eprint.iacr.org/2022/209.pdf
[32] S. I. Tauhidi, A. Abubakar, A. Ishola, A. I. Babate, Z. Umar *et al.,* "ABAFOR: A blockchain-based privacy-preserving architecture for efficient contact tracing and GIS analysis," *European Journal of Electrical Engineering and Computer Science*, vol. 6, no. 2, pp. 88–102, 2022.
[33] Z. Shao, G. Cheng, J. Ma, Z. Wang, J. Wang *et al.,* "Real-time and accurate UAV pedestrian detection for social distancing monitoring in COVID-19 pandemic," *IEEE Transactions on Multimedia*, vol. 24, pp. 2069–2083, 2021.

[34] P. C. Ng, P. Spachos, S. Gregori and K. N. Plataniotis, "Epidemic exposure tracking with wearables: A machine learning approach to contact tracing," *IEEE Access*, vol. 10, pp. 14134–14148, 2022.
[35] M. F. Mokbel, L. Xiong and D. Zeinalipour-Yazti, "Introduction to the special issue on contact tracing," *ACM Transactions on Spatial Algorithms and Systems (TSAS)*, vol. 8, no. 2, pp. 1–2, 2022.