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

Samuel, Omaji; Omojo, Akogwu Blessing; Mohsin, Syed Muhammad; Tiwari, Prayag; Gupta, Deepak; Band, Shahab S.

An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology

Published in:
IEEE Systems Journal

DOI:
[10.1109/JSYST.2022.3170406](https://doi.org/10.1109/JSYST.2022.3170406)






Published: 01/06/2023

Document Version
Peer reviewed version

Please cite the original version:
Samuel, O., Omojo, A. B., Mohsin, S. M., Tiwari, P., Gupta, D., & Band, S. S. (2023). An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology. *IEEE Systems Journal*, 17(2), 2422-2433.
<https://doi.org/10.1109/JSYST.2022.3170406>

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

An Anonymous IoT based e-Health Monitoring System using Blockchain Technology

Omaji Samuel , Akogwu Blessing Omojo, Syed Muhammad Mohsin , Prayag Tiwari , Deepak Gupta , and Shahab S. Band 

Abstract—The Internet of things (IoT) has made it possible for health institutions to have remote diagnosis, reliable, preventive and real-time decision making. However, the anonymity and privacy of patients are not considered in IoT. Therefore, this paper proposes a blockchain-based anonymous system, known as GarliMediChain, for providing anonymity and privacy during COVID-19 information sharing. In GarliMediChain, garlic routing and blockchain are integrated to provide low-latency communication, privacy, anonymity, trust and security. Also, COVID-19 information is encrypted multiple times before transmitting to a series of nodes in the network. To ensure that COVID-19 information is successfully shared, a blockchain-based coalition system is proposed. The coalition system enables health institutions to share information while maximizing their payoffs. In addition, each institution uses the proposed fictitious play to study the strategies of others in order to update its belief by selecting the best responses from them. Furthermore, simulation results show that the proposed system is resistant to security-related attacks and is robust, efficient, and adaptive. From the results, the proposed proof-of-epidemiology-of-interest (PoEoI) consensus protocol has 15.93% less computational cost than 26.30% of proof-of-work (PoW) and 57.77% proof-of-authority (PoA) consensus protocol, respectively. Nonetheless, the proposed GarliMediChain system promotes global collaborations by combining existing anonymity and trust solutions with the support of blockchain technology.

Index Terms—Blockchain, e-health, Fictitious Play, Healthcare, Internet of Things (IoT), IoT data

I. INTRODUCTION

Today, the Internet of things (IoT) is a new technological way to bring together different sensors via the Internet [1]. Besides, the concept of IoT was initiated in 1999 to connect all electronic items via the Internet using radio frequency identification (RFID) [2]. Also, IoT allows other information from sensors to be collected for management and intelligence

gathering. Nevertheless, IoT may connect other input-output devices, such as smart mobiles, medical sensors, fitness trackers, cameras, bluetooth devices, near field communication, etc., [2]. The technological advancement in IoT facilitates the emergence of the Internet of medical things (IoMT). The IoMT allows the remote management and monitoring of patients' data. It is also utilized to solve a variety of health information technology infrastructure problems [3]. In this study, the IoT devices are resource-constrained, which means that they cannot be used for activities that require large computations and memory storage. To resolve this challenge, the IoT devices are connected to edge nodes, which have more memory storage and high computational capabilities. Additionally, the privacy and anonymity of users are not fully explored in IoT, which are the main focus of this study.

A. Anonymity Protection of COVID-19 Patients using Garlic Routing

The invisible Internet project (I2P) provides an efficient network that enables users to communicate in an encrypted and anonymous manner [4]. I2P uses the onion routing concept for providing anonymity to users that deployed the network. Moreover, onion routing provides low-latency Internet connections that prevent traffic analysis and other network attacks. It also uses public-key encryption for encrypting messages in an onion-like structure to be decrypted by the intended recipients. For example, the work in [5] deployed onion routing for enabling users to anonymously access the Internet.

The improvement over the onion routing is the garlic routing. Garlic routing is a technique that establishes a path or tunnel through a series of peers. The sender in garlic routing continuously encrypts messages which are decrypted by every hop as they are transmitted via the tunnel. During the establishment phase, the path for routing messages is known to each peer. The peer formed intermediate nodes in the garlic routing technology. Unlike onion routing, garlic routing encapsulates all relayed messages from the intermediate nodes in encrypted form and sends the ciphertexts to the concerned nodes [4]. The authors in [6] developed a sidechain system, which is a hybrid of garlic routing and onion routing. The objective of the sidechain is to enhance the privacy of transactions within the network. However, the trust concerns among nodes in the blockchain are not considered. The authors in [7] designed an approach that is based on garlic routing for enhancing secure information sharing among users. The proposed approach provides anonymity in the context of information security. The

O. Samuel is with the Department of Computer Science, Confluence University of Science and Technology (CUSTECH), Osara, 264103, Kogi State, and Edo State University, Uzairue, 300281, Nigeria; Email: omajis@custech.edu.ng.

A. B. Omojo is with the Applied Mathematics and Simulation, Advanced Research Centre, SHESTCO, Kwali, Abuja 186 Nigeria; Email: omojo@shestco.gov.ng.

S. M. Mohsin is with the Department of Computer Science, COMSATS University Islamabad, 45550 Pakistan; Email: syedmmohsin9@yahoo.com; FA17-PCS-008@isbstudent.comsats.edu.pk

P. Tiwari is with the Department of Computer Science, Aalto University, 02150, Espoo, Finland; Email: prayag.tiwari@aalto.fi

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

S. S. Band is with Future Technology Research Center, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan; Email: shamshirbands@yuntech.edu.tw.

Corresponding authors: Prayag Tiwari, and Shahab S. Band

proposed approach, on the other hand, does not solve the issue of a single point of failure or user trust problems during the manufacturing process.

To improve the anonymity and privacy of users' transactions, blockchain has been combined with garlic routing. In [8], the authors presented an anonymous technique for ensuring users' privacy during energy trading that is built on blockchain and garlic routing. For the selection of miners and the construction of blocks, the proposed technique used a proof-of-authority (PoA) consensus process. However, the technique does not resolve the issues of trust concerns and miners' centralization problems. In [9], the authors developed a solution based on blockchain and garlic routing to protect the privacy and secrecy of bills of landing users. However, the system does not solve the problem of trust among users. In literature, none of the works done in [4]–[9] considered how to solve the problem with tracing of nodes when errors have been committed. Additionally, coalition among nodes for ensuring trustworthy data sharing is not considered.

B. Privacy and Anonymity of COVID-19 Patients using Blockchain Technology

Currently, different technologies and approaches have been deployed to reduce and minimize the danger and transmission of the pandemic coronavirus, known as COVID-19, since its outbreak in 2019. These technologies range from artificial intelligence [10]–[13], epidemiological models [14], [15], etc. Besides, different open research areas, such as integrative medicine, vaccine development, drug discovery and public communication are essential to finding lasting solutions to COVID-19 [16]. Interestingly, public communication is vital in the fight against COVID-19 through media propagation and public awareness. However, inappropriate COVID-19 information exchange among health institutions can result in excessive coronavirus transmission. Also, because of lack of trust and unauthentic media propagation of COVID-19 information from several unregulated news items, patients infected by COVID-19 cannot get proper guidance on the prevention and mitigation of the spread of the virus. Therefore, an efficient technology to track and minimize the spread of the COVID-19 virus is essential. Furthermore, researchers are not limited to just discovering a cure for the pandemic; they are also building theoretical and practical technologies to aid in the effective exchange of information in the fight against the pandemic. The proposed system helps in mitigating the spread of the COVID-19 virus through authentic public information dissemination. In this paper, before any information about COVID-19 is shared, it must be validated and authenticated by a trusted entity (see Section II-C4 for the credibility of the trusted entity). Furthermore, rumour mongering is eliminated while unnecessary news items are scrutinized before adopting them as a means of information dissemination.

Nowadays, unlike several emerging technologies, blockchain provides a secure and decentralized way of data storage where untrusted parties are allowed to participate in the global wellbeing of the system. The authors in [17] proposed a blockchain-based system to track critical COVID-19 data. During data sharing; however, the technology does

not ensure privacy or anonymity to the health institutions. The authors in [18] identified methods of blockchain that are addressing the problems, which may arise from the COVID-19 pandemic. These methods include disease control, supply chain control of medical items, treatment transparency control, tracking control of health instruments, etc. However, privacy concerns and scalability issues of blockchain are not considered. Similar work in [19] presented the roles of blockchain in detecting COVID-19, such as contact tracing, e-government, online education, supply chain management, automated surveillance, manufacturing management, etc. However, salient features of blockchain such as security, scalability, throughput, resource management require further improvement. The authors in [20] presented a system, known as Beeprace, which is based on blockchain for providing an efficient contact tracing. However, the Beeprace solution does not consider the anonymity of users. The authors in [21] proposed a framework that is based on blockchain to preserve the privacy of patients using their smartphones. However, anonymity depends on pseudonyms, which make it difficult to trace defaulter during a record auditing. The authors in [22] presented a k-anonymity method along with hyper-ledger system to preserve the privacy of patients. However, k-anonymity method is prone to temporal attack, complementary release attack and unsorted matching attack. The authors in [23] proposed a system that is based on blockchain for preserving the privacy of COVID-19 patients. In the proposed system, an identity-based broadcast group signcryption was used. However, they do not address the elucidation key escrow problem.

Moreover, there is a similar work with our proposed system. The work in [8] considers anonymity and privacy preservation of energy users. However, the system in [8] incurs high computation costs since the energy users are resource-constrained, i.e., energy users are smart meters. In addition, no information regarding the robustness, efficiency and adaptability of the system were discussed. To solve the problems, this study introduces edge computing to solve the problem of resource constraints of medical devices. Furthermore, the efficiency, robustness and adaptability of the system are presented. Table I compares the proposed GarliMediChain system with existing systems in terms of year, techniques, limitations, consensus protocol, robustness, efficiency and adaptability.

C. Motivation

Motivated by the drawbacks of existing schemes [17], [18], [20], [21] regarding the lack of anonymity and privacy concerns of patients' health information, our proposed research is conceived. For example, because of the societal stigmatization of those who are infected by the COVID-19 virus, there is a need to develop a system that provides both anonymity and privacy for the patient during data sharing. The concerns of privacy and anonymity for COVID-19 data sharing in public health scenarios are addressed in this study. It is important to note that anonymity refers to the concealment of patients' identities; whereas, privacy refers to the protection of patients' private information from other patients. As the risk of infections and transmission of ongoing pandemics increases, the

TABLE I: The proposed system is compared to other systems

Ref.	1	2	3	4	5	6	7
[4]	2019	I2P	Communication link falsification and fault-tolerance issue	X	X	X	X
[5]	2018	I2P	Communication link falsification and fault-tolerance issue	X	X	X	X
[6]	2019	Sidechain	Trust concern	X	X	X	X
[7]	2019	Garlic routing	Trust concern	X	X	X	X
[8]	2021	Garlic routing and blockchain	Problem with tracing of nodes when errors have been committed	✓	X	X	X
[9]	2021	Garlic routing and blockchain	Trust concern	X	X	X	X
[17]	2020	Blockchain	System does not provide users' privacy and anonymity	X	X	X	X
[18]	2020	Blockchain	Privacy concern and scalability issue	X	X	X	X
[19]	2020	Blockchain	Privacy concern and scalability issue	X	X	X	X
[20]	2020	Blockchain	Anonymity issue	X	X	X	X
[21]	2021	Blockchain	Anonymity issue	X	X	X	X
[22]	2021	k -anonymity system	Prone to temporal, complementary release and unsorted matching attacks	X	X	X	X
[23]	2021	Blockchain	Elucidation key escrow problem	X	X	X	X
Our	2022	GaliMediChain	The overall computational cost of the proposed system model is not considered	✓	✓	✓	✓

1: Years, 2: Techniques, 3: Limitations, 4: Consensus Protocols, 5: Robustness, 6: Efficiency, 7: Adaptability, ✓: Considered, X: Not considered

technology for implementing medical public communication is also improving. As more researchers, academia and health practitioners are expected to be involved, these problems are more vital to the development of such technology in order to alleviate the risk of transmission via public health awareness. In this regard, we offer solutions to the issues mentioned, as well as the following contributions to this work:

- 1) To propose a privacy and anonymity health system for COVID-19 data sharing using a garlic routing and blockchain technology, known as GaliMediChain.
- 2) Trust among coalition group is enforced using fictitious play. Fictitious play enables users to update their beliefs by selecting from the best responses of the opponents' play.
- 3) A consensus mechanism is proposed for the generation of blocks and the selection of miners. The proposed mechanism is based on proof of epidemiology of interest (PoEoI).
- 4) The proposed system's performance is analyzed, which reveals that it is robust, efficient, and adaptive in the presence of security-related threats.

The remaining part of the paper is organized as follows. Section II presents the proposed system model while Section III provides the security analysis of the system. Finally, Section IV presents the conclusion with future work.

II. THE PROPOSED SYSTEM MODEL

In centralized solutions [2]–[5], control and utilization of resources are possible. However, the problem of a single point of failure and the high cost of computation may make the centralized solutions impractical in a real-world scenario especially when the number of IoMT devices increases. Also, the solutions that are based on centralization does not solve the problem of decision making especially when the patients involved have divergent opinions. Furthermore, the centralized system manages each patient's transaction records in consolidated solutions. Patients are also subjected to additional judicial oversight. Each patient has a copy and control over their transactions with our proposed solution, which is not achievable with a centralized system. Therefore, the scenario considers in this study solves the above-mentioned problems of

centralized solutions. The proposed system model is depicted in Fig. 1. From the figure, the proposed system model consists of five important components, such as edge devices, garlic routing, consortium blockchain system and coalition group. These components are discussed as follows.

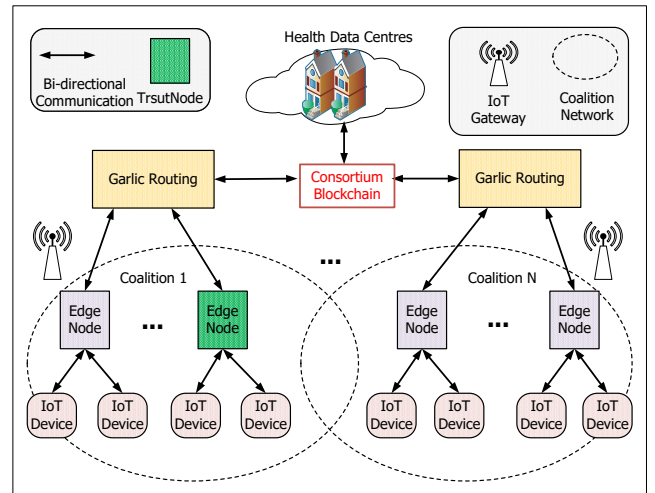


Fig. 1: The anonymous IoT based e-health monitoring system

A. Edge Nodes

Edge computing was introduced to intelligently connect several IoT devices and remote servers including data centres [24]. It allows the efficient management and processing of load, and data storage that are handled by edge nodes. This makes the edge nodes to be increasingly sophisticated and smart. In existing literature [24], cloud system plays a central role in data analysis and management of edge nodes. Besides, edge nodes are just meant to relay and filter remote data to the cloud system, not to undertake in-depth data analysis. Furthermore, edge nodes provide content caching, persistent storage and service delivery. However, distributing edge nodes to different networks bring the problems of security, privacy, anonymity and single point of failures. To address these problems, we introduce blockchain technology, which will be discussed in Section II-C.

B. Garlic Routing

The proposed anonymous IoT healthcare system layer encryption process in Fig. 2, is comprised of a set of source nodes (senders), a set of intermediate nodes and a set of destination nodes (receivers). Any node in the source nodes can communicate with a node in the destination nodes via the intermediate nodes. Before communication is established, a trusted node, known as *TrustNode*, is selected based on its credibility among other nodes. *TrustNode* is responsible for setting up the system credentials, which include a pair of keys (i.e., private and public keys), blind certificates, pseudonyms and path selection model. The system credentials are initialized before any node can communicate with each other for mitigating fraudulent dealings in the proposed system. The pair of keys are used for encrypting and decrypting multiple messages before and after transmission, the blind certificates are used to ensure the authenticity of transmitted messages, and the pseudonyms are used to provide anonymity of entities during communication. A path selection is randomly chosen to prevent the same path from being used repeatedly. It prevents network traffic analysis attacks [25] and also ensures the anonymity of entities involved during data sharing.

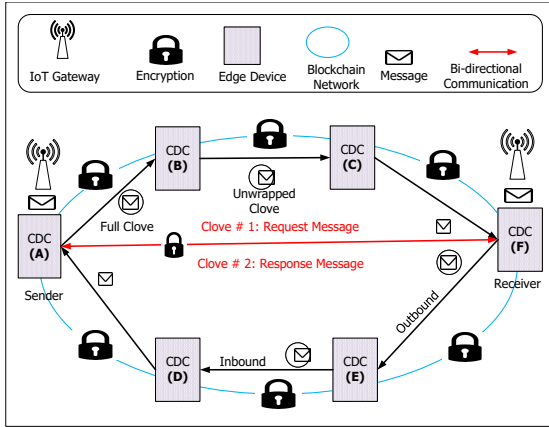


Fig. 2: The anonymous IoT based e-health system layer encryption process

A method called garlic routing, as defined by I2P [26], is used in the proposed GarliMediChain system. Garlic routing is a private network that hides senders' and recipients' identities. Within a garlic routing network, numerous messages are encased in layers of encryption structure. The GarliMediChain system employs the onion routing concept, allowing the recipient to decode a packet by unfolding one layer of the encryption structure across a one-way tunnel [8]. Each sender encodes the packets in the garlic routing, referred to as "cloves." Before being sent between nodes, the encoded cloves are encased in a predetermined size termed "garlic." The destination node is the only node that decodes each clove, making it undetectable to the other nodes, which re-translate the clove to the next hop in the network. In this paper, nodes and centre for disease controls (CDCs) are used interchangeably.

In Fig. 2, the CDC A can select multiple paths: CDC B \rightarrow CDC C and CDC D \rightarrow CDC E, for forwarding packets to CDC F. Identity-based encryption is used to safeguard the

identities of nodes in the paper, and it was inspired by the work in [8]. Let the set of source nodes be defined as $SN \triangleq \{sn = 1, 2, 3, \dots, SN\}$, the set of intermediate nodes be $IMN \triangleq \{imn = 1, 2, 3, \dots, IMN\}$ and the set of destination nodes be $DN \triangleq \{dn = 1, 2, 3, \dots, DN\}$. To avoid verbosity, the proposed GarliMediChain system has a similar architecture with the work presented in [8]. Fig. 3 shows the processes and relationships between protocols and analyses. From the figure, it is shown that each IoT device requested a login credential from *TrustNode* through the registration protocol at step (1). In step (2), *TrustNode* requested session, private and public keys of all nodes from the layered encryption protocol. The keys generated by layered encryption protocol are sent to IoT users via *TrustNode* at steps (3) and (4). The IoT user gets a list of path sets from the path selection protocol in steps (5) and (6). Steps (6), (8) and (9) enable IoT users to encrypt the message and route via intermediate nodes to the destination node while the destination node decrypts the message using its private key.

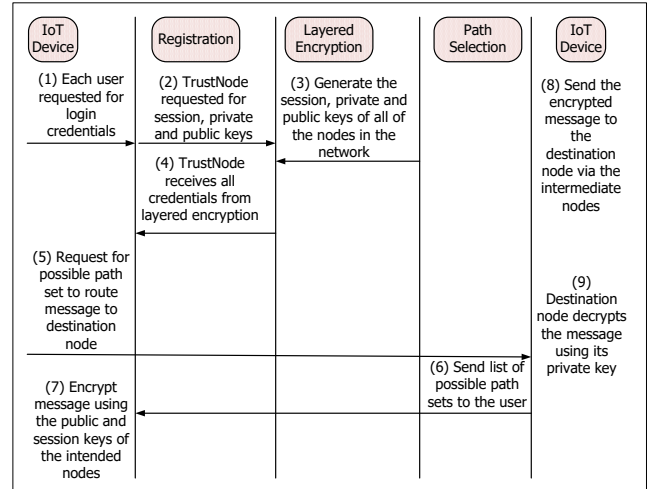


Fig. 3: A sequence diagram showing the processes and relationship between the different protocols of the proposed system model

C. Consortium Blockchain System

In medical edge computing, data sharing from controllers to patients may cause problems like insecurity, lack of both privacy and trust. Blockchain is one of the plausible solutions to efficiently address the above-mentioned problems. In the blockchain, all messages are broadcasted and communicated in a distributed and decentralized fashion. These messages are written onto the blockchain in an immutable manner and can be audited and verified by entities in the network. In this study, we aim to combine the advantages of edge computing, garlic routing and fictitious play with blockchain. Also, all calculations are performed within the proposed network and off-chain. It means that the computations are performed distributively by using edge computing, which minimizes the overall computing cost of the proposed system model. Note that the validation of transactions, selection of miners and consensus protocol are discussed as follows.

1) *Validator Selection Process*: Inspired by [27], two types of blockchain nodes are considered in this paper: evaluator and validator. Hospitals who take and transmit ledger data are represented by evaluator nodes, and every CDC in the blockchain network is a node. All nodes have a greater probability of becoming validator nodes, allowing them to be part of the consensus process. Validators are nodes on the blockchain that send block confirmation messages to the rest of the nodes in the network. They are chosen from a list of high credible nodes. Any validator with a high credibility is qualified to write a block onto the blockchain, and is referred to as a *TrustNode*. *TrustNode* digitally signs and hashes a hospital's record before submitting it to the blockchain. The signed record is stored in the blockchain as a candidate block transaction. Hospitals rate CDCs based on their current performance, and each *TrustNode* saves a copy of its network's credibility scores. A node becomes a validator node in the PoEoI consensus protocol only when its credibility score exceeds the defined credibility threshold value, which lies between "0" and "1". The defined threshold value in this paper is assumed to be 0.6. Although, we are not constrained by the defined threshold value, it can be chosen dynamically. The validator nodes do not include nodes with credibility scores less than the defined threshold value.

2) *Processes for Creating and Validating Blocks*: With the assistance of some validators, the *TrustNode* validates the candidate block. As soon as the candidate block arrives from the *TrustNode*, each validator compares its signature to the signature of the preceding block that was remotely stored. After successful verification, validators on the blockchain network broadcast confirmation messages. The *TrustNode* then provides the necessary epidemiological data sharing service to the hospitals and opens a new transaction for it. When the *TrustNode* receives the $(N - NCN)$ amount of confirmation messages with all validators signatures attached, a new block is created. The number of malicious node is denoted by NCN . If $(N - NCN)$ confirmation messages are received, the block is published; otherwise, it is not. In chronological order, a new block is added to the blockchain. The system is considered attacked if the *TrustNode* does not properly store the data.

Nodes can provide puzzle solutions, which are a random number of nonces that resolve the cryptographic hash issues of the proof of work (PoW) consensus protocol [28], on the blockchain. The difficulty of PoW is unrelated to the network nodes' credibility. By resolving the puzzling issue [28], a node on the blockchain can create a new block.

$$H(\text{nonce} || H(bh)) \leq f(CS(n)).\text{target}, \quad (1)$$

where $||$ denotes "append," $H(\cdot)$ signifies a function of cryptographic hash, bh denotes a block header, and $f(\cdot)$ denotes a function that produces the puzzle difficulty. During each consensus process, *target* is the system's difficulty target for all validators. The *TrustNode* becomes the quickest validator on the blockchain that answers cryptographic puzzles by broadcasting the candidate block across the network. While the other validators evaluate the correctness of the nonce that generates the candidate block. If the validation procedure went well, it means the validators were in agreement. In a

linear order, the recently produced block in the blockchain is linked to the preceding block. After that, each blockchain node updates its record in order to keep track of the information of the newly created block [28].

3) *Properties of the Proposed System*: In this study, the computational power of the proposed system is measured based on its hash rate. The hash rate of the system is calculated as the ratio of the successful nonce to the total number of elapsed time. Other salient properties of the proposed system are discussed as follows.

- 1) *Security*: The security of the proposed system is determined based on blockchain and garlic routing. The blockchain used in this study is a consortium system where access control is used to limit the number of unauthorized users. Here, only users with valid credentials can authenticate and have access to the system. In addition, identity-based encryption mechanism is adopted for the encryption of session keys and messages before they are transmitted over the network. Note that only the intended users can decrypt the messages even if they are sent to the intermediate nodes for routing to the next hop.
- 2) *Scalability*: The scalability of the proposed system is determined by the number of coalitions created. It means that more nodes are added to the system without necessarily increasing the computing cost of the system.
- 3) *Throughput*: The throughput of the system depends on the system's efficiency and to avoid verbosity, see discussion in Section II-C5.
- 4) *Resource Management*: The proposed system uses application intensive consensus mechanism, which requires minimum energy resources as compared to the PoW consensus mechanism, which is CPU intensive [18]. This means that the proposed system does not required high computational power for mining and adding of blocks to the blockchain. Moreover, in future, we intend to consider the overall computational cost by proposing an efficient optimization method.

The benefit of employing blockchain for the anonymity and privacy of patients' information is discussed as follows. The traditional anonymity method [22] does not guarantee trust in information. Also, it may violate the privacy of the data owners. Furthermore, it may lead to homogeneity and background knowledge attacks. Whereas, the traditional privacy method may create the problem of data accuracy. Therefore, to solve these problems, blockchain is employed in this study to ensure the trust of information and privacy while garlic routing provides anonymity to patients.

4) *Credibility of the Trusted Node*: In this paper, it is assumed that *TrustNode* can either behave honestly or maliciously. To prevent the malicious behavior of *TrustNode*, a credibility method is adopted. Here, every node in the network is allowed to participate in the evaluation process of *TrustNode*. The evaluation process considered in this work includes direct and indirect evaluations. In the direct evaluation process, a rating score between $[0, 1]$ is awarded to *TrustNode* while for the indirect evaluation process, the historical honest behavior of *TrustNode* is used for assessing

its credibility. Although, direct evaluation is prone to feedback sparseness and misjudgment [29]. However, in this study, time relevance is incorporated in the evaluation process to prevent misjudgment. If *TrustNode* receives a rating score between 0 – 5, it means that *TrustNode* is involved in malicious activity; otherwise, a rating score between 5 – 10 is awarded to *TrustNode*, which means that it has an honest behavior. For the indirect evaluation, trust recommendation from other nodes is used to determine the honest behavior of *TrustNode*. The historical honest behavior of *TrustNode* is measured on the basis of two consecutive high rating scores that are above 5.

5) *The Proposed Protocol for Proof of Epidemiology of Interest*: The proposed PoEoI protocol is based on the addition number game, as shown in Fig. 4. The steps for playing the

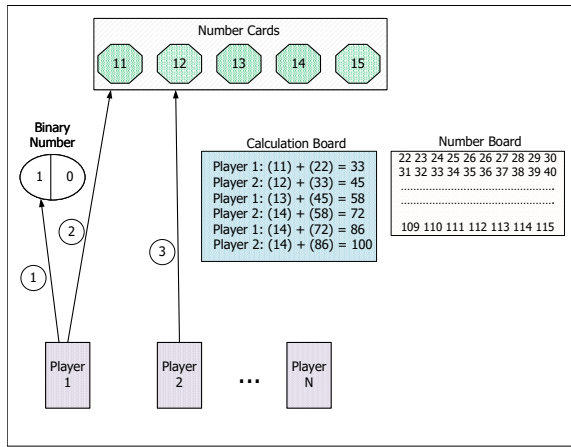


Fig. 4: The proposed addition number game

game are described as follows.

- Step ①: To start the game, a binary number “1” or “0”, is generated by the system. If any player selects “1”, it means that the player can start the game. On the other hand, if “0” is selected, it means that the player cannot start the game.
- Step ②: A winner begins the game by choosing $x \xleftarrow{R} X$. This indicates that a number x is chosen at random from the set of numbers X contained in the number cards. Where $X = \{11, 12, 13, 14, 15\}$. The player adds the number x to any number in the number board and then returns x to the other four numbers in the number cards.
- Step ③: The second player picks $x \xleftarrow{R} X$ and adds to the sum obtained by the first player.
- Step ④: The players continue to add $x \xleftarrow{R} X$ alternately to the sum obtained by the opponent.
- Step ⑤: The game continues until one player obtains an overall total of 100 and beyond. It means that the player is declared the winner of the game.

The strategies of this game are (1) every player is given an equal opportunity to pick a random binary number, which was generated by the system at the start of the game and (2) a winner is declared if it has a total of 100 and above against its opponent. In this study, the proposed GarliMediChain system is resilient because any faulty in CDCs does not affect the

total operations of the network. Algorithm of the proposed GarliMediChain system is given in Algorithm 1. Moreover, the properties of the proposed PoEoI consensus protocol are given as follows.

Efficiency: The efficiency of the proposed GarliMediChain system is evaluated in this research based on the time it takes each CDC to respond to or request EoI either in the same coalition group or different coalition groups (see Section II-D). We consider the communication time C_T , delivery time D_T and the total cost for requesting EoI, which is defined as

$$EoI_C = C_T + D_T. \quad (2)$$

Let the system’s throughput be represented as R_p and suppose that the request of EoI from any CDC is greater than R_p , then the system is said to be overloaded with requests (i.e., $R_p < \frac{D_T}{N}$). The actual time taken AC_T , also known as the elapsed time, for any CDC to provide an authentic EoI is defined as

$$AC_T = D_T + F_T, \quad (3)$$

where F_T is the function of CDC request for EoI and the total number of CDCs.

$$F_T = \frac{N}{D_T}, \quad (4)$$

where N is the number of CDCs. If $R_p < F_T$, the system is saturated and AC_T will grow infinitely.

Robustness: The estimated cost that the proposed GarliMediChain system will fail multiplied by the probability of the failure is referred to robustness of GarliMediChain system. Let Pr_{CDC} denotes the probability that a CDC may fail to respond or supply EoI, C_{CDC} represents the cost of reassigning the request of EoI from another CDC and C_L is the cost of losing the request for EoI from a single CDC. Thus, the weakness of the system, denoted as W_{sys} , is defined as

$$W_{sys} = Pr_{CDC}C_{CDC} + Pr_{CDC}C_L. \quad (5)$$

Adaptability: In GarliMediChain system, the ability to keep records of transactions upto date in a way that any fault can be detected easily in real-time, is referred to as adaptability. Besides, the capacity C_{cap} of the proposed GarliMediChain system to keep records is defined as

$$C_{cap} = \frac{N}{D_T} + \frac{1}{R_p}. \quad (6)$$

In this paper, the proposed PoEoI consensus protocol is explained in the following phases, as shown in Fig. 5.

Request Phase: Each hospital initially requests EoI to the winner CDC. The winner CDC checks the authenticity of the request before processing it. Afterwards, it sends the prepare EoI message to other CDCs for validation.

Prepare Phase: The CDCs broadcast a prepared EoI message to each other while checking for its validity. When a CDC receives $2n$ valid EoI from different CDCs, the “prepare phase” is completed. Where $n \in N$.

Commit Phase: Each CDC broadcasts a commit EoI message to one another for validation. Once the number of commit EoI messages is greater than $2n + 1$, the EoI message is added to the blockchain.

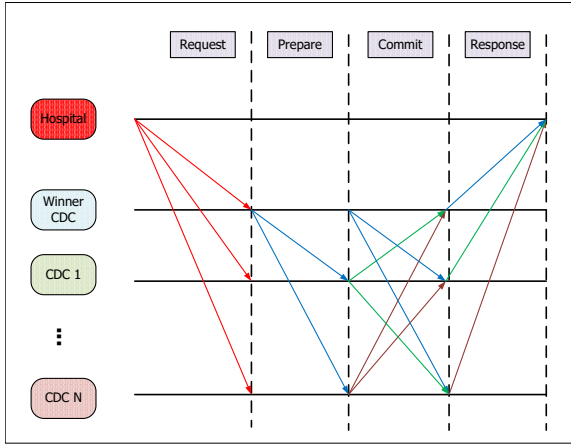


Fig. 5: Phases of proposed PoEoI consensus protocol

Response Phase: In this phase, when the hospital receives $2n + 1$ of the same reply of the EoI messages, the consensus is completed.

D. The Coalition Group

In this paper, each CDC can accumulate more quantity of epidemiological information EI that comprises of a set of actions, represented by A_{CDC} , which means the information sharing action that a CDC is willing to perform. Moreover, $A_{CDC} = \{P, ED_{avail}\}$, defines the available epidemiological data ED_{avail} at negotiation prices P . The values of P depend on the total amount of epidemiological data collected by each CDC after calculating $Rev = F(EI)$. Where $F(EI)$ is the function of the shared data and $EI = \sum_{i \in N} e_i$ such that $e_i \in EI$ is the i th shared information. Moreover, Rev is the revenue of CDC. At any given time slot t , the utility of CDC as a function of e_i is calculated as:

$$U_i(e_i) = q \ln(e_i), \quad (7)$$

where q is the payment negotiation parameter. When the requester CDC's maximum quantity of epidemiological information EI is not met, it receives EI from other CDCs who are ready to contribute. When the requester CDC receives EI , he or she is satisfied.

Note that $U_i(e_i)$ is the utility of CDC, which is expected to be a concave non-decreasing function of e_i , i.e., $\frac{\delta U_i(e_i)}{\delta e_i} \geq 0$ and $\frac{\delta^2 U_i(e_i)}{\delta e_i^2} < 0$.

Definition 2.1: Each CDC depends on the EoI that is equivalent to its negotiation power.

The explanation of Definition 2.1 is that CDC must collect more EoIs from infectious disease experts or world health organization (WHO). The cost for collecting EoI depends on P and the investment cost. Each CDC wishes to maximize its profit by learning or imitating other CDCs with the best strategies. Moreover, every CDC is expected to acquire the requisite knowledge on how to collect EoI through drug discovery, integrative medicine and vaccine development [16]. Otherwise, it has to get the required EoI alone or through negotiation with other CDCs.

Proposition 2.1 (Optimal Response): Every CDC maximizes its utility by adopting and improving on the optimal strategies of other CDCs.

Proof 2.1: The proof of Proposition 2.1 is given as follows. Each CDC initially believed that other CDCs have the best strategies. It means that CDC will fulfill its EoI by learning the opponent's play and strategy. Besides, it may deviate from existing strategies in order to optimize its payoff.

Definition 2.2: Let $P(S) = \{a, S\}$ be the joint policy that assigns all CDCs' joint state $S = [s_1, s_2, \dots, s_i]$ to the i actions $A = [a_1, a_2, \dots, a_i]$.

E. Fictitious Play

In a game theory, fictitious play is a type of learning paradigm in which CDCs are confronted with an uncertain distribution of their opponents' strategy. For example, even when a CDC is fully engaged in coalition activities, it is conceivable for the CDC to depart from those activities to maximize its utility. As a result, each CDC monitors the opponents' play techniques to update its belief by selecting the optimum response to their play. In terms of action a , the total utility of CDCs for engaging in coalition S is expressed as TU .

$$TU(S) = \max \left[\sum_{i \leq N} \left(\sum_{a_i \in a_S} U_i(a_i) \right) \right]. \quad (8)$$

$TC = \sum_{a \in S} TU(S)$ is used to calculate the total coalition value.

Using the fictitious play, a CDC can monitor the behavior of other CDCs by learning the collection of random probability distributions $pr_1, pr_2, pr_3, \dots, pr_i$. The probability law for random variables is defined by each distribution $pr_i \stackrel{R}{\leftarrow} [0, 1]$. As a result, $\sum_{i=1}^N pr_i = 1$. According to the fictitious play, CDC must calculate pr_i by taking into account a count c_i for each action that corresponds to EI . As a result, it is defined as

$$F_p = \frac{c_i}{\sum_{i=1}^N c_i}. \quad (9)$$

Note that the demand for EoI by any CDC is uncertain, which must conform to the supply EoI of other CDCs. Similarly, a requester CDC may negotiate with other CDCs by developing a probability pr_i for each negotiation. Thus, Eq. (8) is redefined as:

$$TU(S) = \max \left[\sum_{i \leq N} \left(\sum_{a_i \in a_S} pr_i U_i(a_i) \right) \right]. \quad (10)$$

III. SECURITY ANALYSIS

The proposed GarliMediChain system is subjected to a security assessment in this section. The analysis is based on threats to information system, which include Sybil attacks and double spending attacks. Besides, there are other attacks, such as distributed denial-of-service (DDoS) and man-in-the-middle attacks. These attacks are prevented by the proposed system model. The DDoS attack occurs when the network is overwhelmed with bogus traffic (e.g., a centralized system is

Algorithm 1: The proposed GarliMediChain Algorithm

Input: Number of CDCs
Output: CDC's strategies

```

1 set  $i = 1$ 
2 if  $\exists(n_i \in N == 0)$  then
3   Return  $CDC_i$ 
4 else
5   Return CDC such that
6    $TU(S) = \max \left[ \sum_{i \leq N} \left( \sum_{a_i \in a_S} U_i(a_i) \right) \right]$ ,
7   when fictitious ends;
8   foreach Coalition group do
9     Set the negotiation price;
10    Create a list of CDCs who are willing to share EoI;
11    Get a list of CDCs that require EoI;
12    Get the leader of the coalition group using the proposed addition number game;
13    Implement PoEoI consensus protocol to add a block to blockchain;
14    Evaluate the system's performance based on robustness, adaptability and efficiency;
15  Update  $TU(S)$  as
     $TU(S) = \max \left[ \sum_{i \leq N} \left( \sum_{a_i \in a_S} pr_i U_i(a_i) \right) \right]$ .
```

most vulnerable to this type of attack); thereby, making the system malfunction [31]. The proposed model is a distributed system, which means that the failure of any node does not affect the system. The advantage of the proposed system is that every node has the same copy of the ledger. The man-in-the-middle attack happens when an intruder intercepts the communication for the purpose of exploiting the vulnerability of the system [32]. This type of attack occurs when the intruder has knowledge of the proposed system. In this study, it is impossible for an intruder to intercept the network because of the architectural design of the system. Also, the consensus mechanism makes it difficult for an intruder to modify the information because all information in the form of the transaction must be validated and authenticated by the majority in the network.

Before performing the security analysis, a threat model is designed for the proposed system.

A. Threat Model

A threat model enables us to assess the security design and makes it easier to perform risk assessment on the system. However, there are no universal established principles for designing a threat model [30]. In this research, we assume that the proposed GarliMediChain system is vulnerable to identity-based attacks and honest-but-curious adversaries. Furthermore, some CDCs in the proposed system may be honest; in the sense that they provide EoI voluntarily, while others may be malicious; in the sense that they purposefully exploit the

system's vulnerability to create harm. Moreover, some CDCs may intentionally fail to respond or provide an incorrect EoI. The proposed PoEoI consensus protocol aims to safeguard against system's failure by using coalition decision making (i.e., it involves data of both correct and incorrect CDCs) that reduces the number of defaulter CDCs. Note that the GarliMediChain system is resilient to both Sybil and double-spending attacks because of the PoEoI consensus protocol. The protocol ensures that the identity of each CDC is verified, which prevents the creation of fake identities. Besides, before any transaction is written onto the blockchain, it must be verified and authenticated by validators, which prevent double-spending related attacks.

In this study, we categorize the security assessment of the proposed system based on authentication attack, availability attack, confidentiality attack, and controllability of the system, as shown in Table II. Motivated by [33], the security assessment of the proposed GarliMediChain system is performed. To prevent certain attacks on the proposed system, it is paramount to give the security features of the blockchain nodes. Two cases of attacks can be possible in this scenario: internal and external attacks. The latter has no significant impact on the system since blockchain and garlic routing is secured. Moreover, our focus is on the former case, which occurs when a malicious user gains entry into the system. The impact of the attack may be degradation of patients' information or complete interruption of the system. Blockchain nodes' authentication is a vital part of the security architecture as CDCs formed the nodes in the blockchain. Furthermore, because they are real network users, CDCs may intentionally attack the system by compromising its security. The availability attack occurs when the blockchain nodes are not available for negotiation and interaction (i.e., coalition formation). The availability attack affects the performance and process of the system, such as delays in communication. Typically, DDoS is a kind of availability attack. To address this type of attack, a request threshold, denoted as *Request_Threshold*, is defined along with the maximum number of requests, *Max_Request* as given in Algorithm 2. Confidentiality attack enables the

Algorithm 2: DDoS mechanism

```

1 if  $Max\_Request > Request\_Threshold$  then
2   Alert the system for possible DDoS attack
3 else
4   Allow communication to happen
```

malicious user to gain access to both patients and system information when access right is not granted.

Definition 3.1: Considering that the malicious user gains access to the proposed system; then, it can exploit the system to determine its security, which is defined as follows.

$$\frac{1}{N} - \frac{1}{\Psi} \leq \theta, \quad (11)$$

where Ψ is the number of unavailable nodes and θ is the degree of availability attack.

TABLE II: Security assessment of the proposed system model

Attack Strength	Authentication	Availability	Confidentiality	Degree of Attack	Impacts
Low	Escrow key problem	Honest-but-curious	Non-repudiation	-	Short term
Medium	Sybil, DDoS, feather forking	DDoS	-	Partial	Efficiency degradation
High	Replay, timestamp dependence, re-entrancy	-	Eavesdropping	Full	Forgery of data

Theorem 3.1: The proposed system prevents availability attacks.

Proof 3.1: The proof of Theorem 3.1 is presented as follows. Suppose that Eq. 11 is not true. Then, the malicious user can conveniently exploit the vulnerability of the proposed system. However, because a single point of failure is not possible with the proposed system, which means failure in any node does not affect the entire system. Therefore, Theorem 3.1 is proven, which implies the proposed system prevent availability attacks.

Theorem 3.2: The proposed system prevents confidentiality attacks.

Proof 3.2: The proof of Theorem 3.2 is presented as follows. Suppose that Eq. 11 is true. Then, the malicious user has access to the proposed system. Besides, it is difficult for the malicious user to modify the private information of a patient because it requires the login credential of that patient. Therefore, the proposed system prevents confidentiality attacks.

IV. SIMULATION RESULTS

We implement the proposed system using Python 3.6.1. To create keys for the identity-based encryption, a Charm library is utilized, as well as a Crypto library for encryption and hashing [34]. The performance parameters considered in this paper to evaluate the proposed system are efficiency, robustness and adaptability. Besides, this paper is not limited to the above-mentioned performance parameters. The simulation results of the proposed GarliMediChain are provided in this section. The parameters used for performing simulation are given in Table III while the implementation can be found in Github ¹.

TABLE III: The parameter values utilized in this paper

Parameters	Meaning	Values
C_T	Communication time per second	10
D_T	Delivery time per second	3
R_p	System's throughput per second	3.4
N	Number of CDCs	1000
Pr_{CDC}	Probability that a CDC may fail to respond of supply EoI	0.6
C_{CDC}	Cost of reassigning the request of EoI from another CDC per second	30
C_L	Cost of losing the request for EoI from a single CDC per second	60
q	Payment negotiation parameter	0.6
P	Negotiation price	10
ED_{avail}	Available epidemiological data	100
e_i	The number of i th shared information	100
c_i	The i th count for each action that corresponds to EI	20
$iter$	The Number of iteration	1000

¹Github implementation of the proposed system model.

A. Evaluation of the proposed GarliMediChain System

In Fig. 6, we consider 1000 CDCs for the analysis. The efficiency of the proposed system is the amount of time (in seconds) needed by a CDC to request for EoI. From the figure, as the number of CDCs grows, the total cost of the system grows as well. It means that C_T and D_T are inversely proportional to each other, which have an impact on the total cost. Here, efficiency means that suppose 1000 CDCs decide to request for EoI, their total cost is 103 seconds.

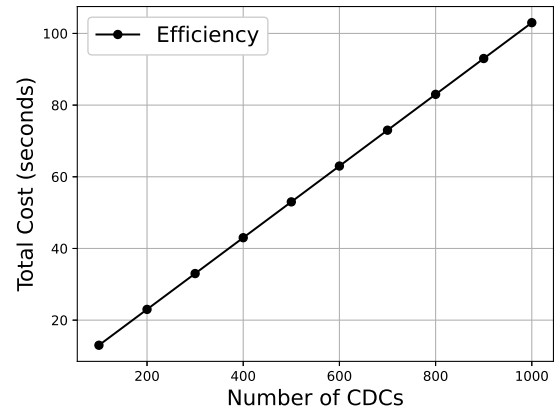


Fig. 6: Efficiency of the proposed GarliMediChain

In Fig. 7, the proposed system's adaptability is analyzed. Adaptability means that the system in real-time can store records up-to-date in a manner that any fault is detected. From the results in Fig. 7, it is observed that as the number of CDCs increases, the total cost reduces, which means that the system can store more records and keep them up-to-date in a reasonable amount of time. Also, it means that the system has a higher capacity to detect a fault in real-time.

In Fig. 8, the robustness of the proposed system is evaluated. We assume $Pr_{CDC} = 0.6$, $C_{CDC} = 30$ seconds and $C_L = 60$ seconds. It means that suppose 60% probability of failure is encountered, then the total cost increases along with the number of CDCs. Besides, it means that as the adversary tries to compromise more CDCs, its total cost increases proportionally.

In Fig. 9, the time taken by the system to respond or request for EoI is analyzed. The elapsed time increases as the number of CDCs grows, according to the results. It means that F_T and D_T are inversely proportional. Moreover, there is a tradeoff between elapsed time and communication time. Furthermore, it means that as more CDCs wish to share EoI, communication time increases while elapsed time decreasing. Besides, elapsed time and delivery time are proportional.

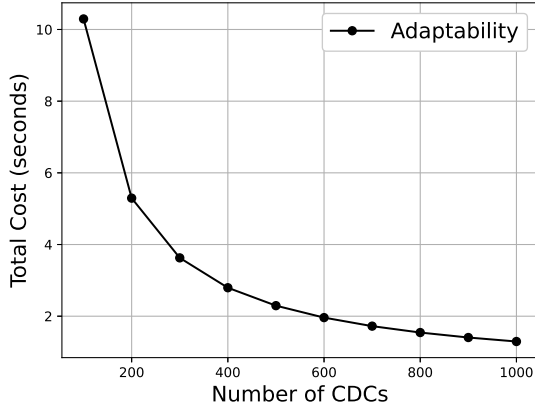


Fig. 7: Adaptability of the proposed GarliMediChain

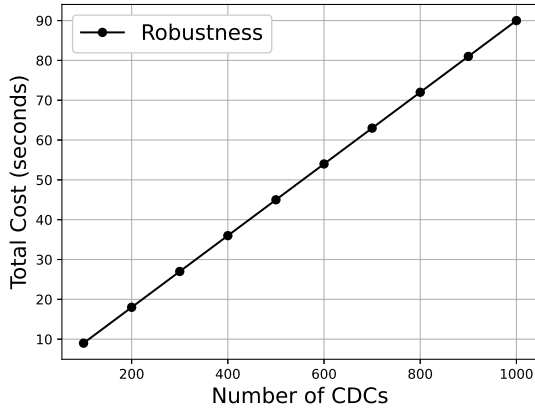


Fig. 8: Robustness of the proposed GarliMediChain

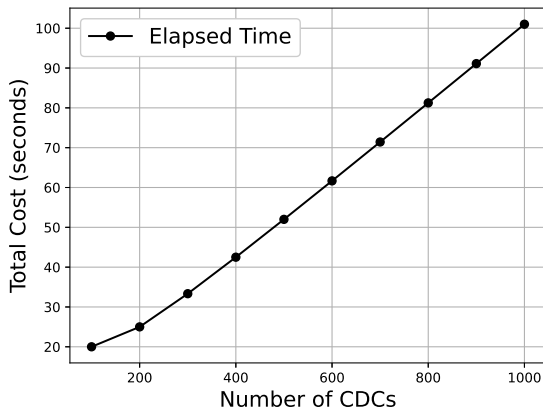


Fig. 9: Elapsed Time of the proposed GarliMediChain

B. Evaluation of the Fictitious Play for CDCs

In this section, the evaluation of the fictitious play for CDCs is provided. For the analysis, two CDCs are considered. Using Eq. (7) the total utility is calculated, and its value is shown in Fig. 10. The value of the total utility lies within 0 – 1 and

the payment negotiation parameter $q = 0.6$. Moreover, the value of q is arbitrary selected, which implies that there is a 60% probability of achieving a fair negotiation. From Fig. 10, it is observed that as the number of iterations increases, the total utility converges to a stable value after 200 iterations. It implies that both CDC1 and CDC2 consider the same strategy to update their belief by selecting the best responses of the play.

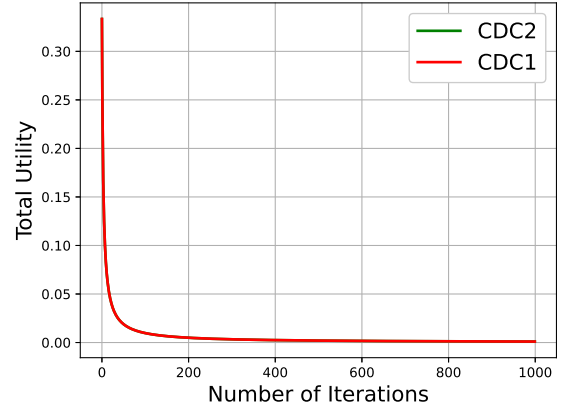


Fig. 10: Total utility versus number of iterations

C. Evaluation of Security Analysis

The results for the security analysis is given in this section. According to Eq. (11), we consider the degree of availability attack $\theta = 0.6$. In this study, if the probability is more than 0.6, the availability attack is highly possible. In Fig. 11, it is observed that as the number of unavailable nodes increases, the probability of attack reduces, which means that the degree of availability attack reduces as well. Also, with a lower probability, it is difficult for a malicious user to compromise the proposed system.

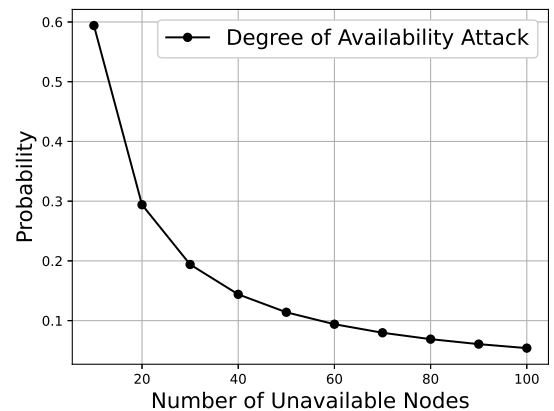


Fig. 11: Probability versus number of unavailable nodes

D. Evaluation of the Proposed PoEoI Consensus Protocol

In this paper, we compare our proposed PoEoI consensus protocol with PoW consensus protocol [28] and PoA consensus protocol [8]. As already discussed in Section II-C3, the hash rate is used to determine the computational cost per second of the proposed system. In Fig.12, it is observed that the proposed PoEoI has 15.93% less computational cost than 26.30% of PoW and 57.77% of PoA consensus protocols, respectively. The reason for the high computational cost of the PoA consensus protocol is that the Pagerank rank algorithm added to the overall cost of the system. In Fig. 13, the number of nonces versus the elapsed time is given. It is observed that as the number of elapsed time increases, the nonce increases as well. Hence, there is a direct relationship between nonce and elapsed time. Besides, nonce determines the level of difficulty for mining a block in the blockchain. Thus, our proposed PoEoI consensus protocol has the least number of nonces generated, which means that it is more efficient than other existing protocols.

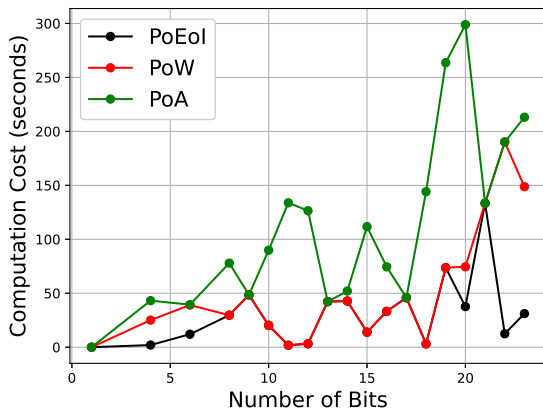


Fig. 12: Computation cost versus number of bits

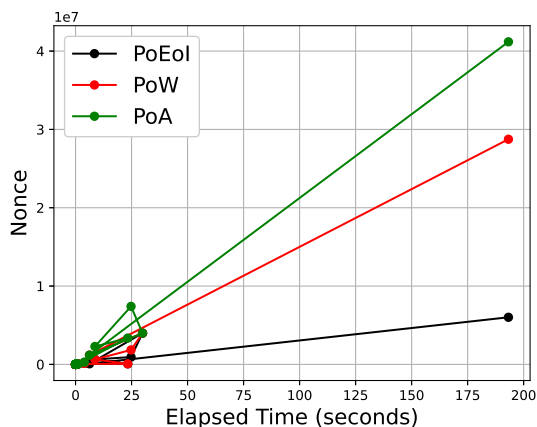


Fig. 13: Nonce versus elapsed time

V. CONCLUSION

This study proposes a blockchain-based anonymous system that provides anonymity and privacy of COVID-19 patients' information in IoT. Garlic routing and blockchain have been combined in the system to provide low-latency communication, privacy, anonymity, trust, and security. Additionally, COVID-19 data is encrypted numerous times before being sent to a series of network nodes. To facilitate secure COVID-19 information exchange, a blockchain-based coalition system is being developed. The coalition method enables healthcare institutions to exchange data while simultaneously improving profitability. Furthermore, each institution uses the proposed fictitious play to examine other institutions' strategies to update its beliefs by choosing the best responses from them. The simulation findings demonstrate that the proposed system is robust, adaptive, and efficient, preventing an honest-but-curious health institution from attacking it. From the results, the PoEoI consensus protocol has 15.93% less computational cost as compared to 26.30% of PoW and 57.77% PoA consensus protocol, respectively.

In future, we intend to analyze the overall cost of the proposed system and the scalability of the proposed system will be investigated for real-time implementation. Furthermore, we want to improve the proposed system in collaboration with other health institutions, practitioners, and government organizations.

ACKNOWLEDGMENT

We are thankful to Prof. Chung-Chian Hsu for his valuable feedback in revision.

REFERENCES

- [1] Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. *IEEE Systems Journal*, 15(1), 85-94.
- [2] Hu, F., Xie, D., & Shen, S. (2013, August). On the application of the internet of things in the field of medical and health care. In *2013 IEEE international conference on green computing and communications and IEEE Internet of Things and IEEE cyber, physical and social computing*, 2053-2058.
- [3] Qian, Y., Shen, J., Vijayakumar, P., & Sharma, P. K. (2021). Profile Matching for IoMT: A Verifiable Private Set Intersection Scheme. *IEEE Journal of Biomedical and Health Informatics*, 25(10), 3794-3803.
- [4] De Boer, T., & Breider, V. (2019). Invisible Internet Project (I2P), *System and Network Engineering*, 1-16.
- [5] Naik, A., Saksena, A., Mudliar, K., Kazi, A., Sukhija, P., & Pawar, R. (2018, March). Secure Complaint bot using Onion Routing Algorithm Concealing identities to increase effectiveness of complain bot. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 1777-1780.
- [6] Parizi, R. M., Homayoun, S., Yazdinejad, A., Dehghantanha, A., & Choo, K. K. R. (2019, May). Integrating privacy enhancing techniques into blockchains using sidechains. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, Edmonton, AB, Canada, 1-4.
- [7] Dakhnovich, A., Moskvina, D., & Zeghzda, D. (2019, March). An approach for providing industrial control system sustainability in the age of digital transformation. In *IOP Conference Series: Materials Science and Engineering*, 497(1), 1-10.
- [8] Samuel, O., & Javaid, N. (2021). GarliChain: A privacy preserving system for smart grid consumers using blockchain. *International Journal of Energy Research*, 1-17.
- [9] Precht, H., & Marx Gómez, J. (2021, October). Usage of Multiple Independent Blockchains for Enhancing Privacy Using the Example of the Bill of Lading. In *International Congress on Blockchain and Applications*, Springer, Cham, 300-309.

- [10] Vaishya, R., Javaid, M., Khan, I. H., & Haleem, A. (2020). Artificial Intelligence (AI) applications for COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, 14(4), 337-339.
- [11] Jelodar, H., Wang, Y., Orji, R., & Huang, S. (2020). Deep sentiment classification and topic discovery on novel coronavirus or covid-19 online discussions: Nlp using lstm recurrent neural network approach. *IEEE Journal of Biomedical and Health Informatics*, 24(10), 2733-2742.
- [12] Gomez-Exposito, A., Rosendo-Macias, J. A., & Gonzalez-Cagigal, M. A. (2021). Monitoring and tracking the evolution of a viral epidemic through nonlinear kalman filtering: Application to the covid-19 case. *IEEE Journal of Biomedical and Health Informatics*.
- [13] Samuel, O., Omojo, A.B., Onuja, A.M., Sunday, Y., Tiwari, P., Gupta, D., Hafeez, G., Yahaya, A.S., Fatoba, O.J., & Shamshirband, S. (2022). IoMT: A COVID-19 Healthcare System driven by Federated Learning and Blockchain. *IEEE Journal of Biomedical and Health Informatics* 1-12.
- [14] Chen, Y. C., Lu, P. E., Chang, C. S., & Liu, T. H. (2020). A time-dependent SIR model for COVID-19 with undetectable infected persons. *IEEE Transactions on Network Science and Engineering*, 7(4), 3279-3294.
- [15] Chayu, Y., & Jin, W. (2020). A Mathematical Model for the Novel Coronavirus Epidemic in Wuhan, China. *Mathematical Biosciences and Engineering*, 17(3), 2708-2724.
- [16] Abhimanyu, S. A., Vineet P. R., Oge M. (2020). Artificial intelligence and COVID-19: A multidisciplinary approach. *Integrative Medicine Research*, 9(1), 1-3.
- [17] Marbouh, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., & Ellahham, S. (2020). Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arabian Journal for Science and Engineering*, 1-17.
- [18] Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. *Research on Biomedical Engineering*, 1-8.
- [19] Kalla, A., Hewa, T., Mishra, R. A., Yliantila, M., & Liyanage, M. (2020). The role of blockchain to fight against COVID-19. *IEEE Engineering Management Review*, 48(3), 85-96.
- [20] Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. J., & Imran, M. A. (2020). Beeprace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond. *IEEE Internet of Things Journal*, 8(5), 3915-3929.
- [21] Choudhury, H., Goswami, B., & Gurung, S. K. (2021). Covidchain: An anonymity preserving blockchain based framework for protection against covid-19. *Information Security Journal: A Global Perspective*, 30(5), 257-280.
- [22] Sowmiya, B., & Poovammal, E. (2021). A Heuristic K-Anonymity Based Privacy Preserving for Student Management Hyperledger Fabric blockchain. *Wireless Personal Communications*, 1-18.
- [23] Kumar, M., & Chand, S. (2021). MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. *Journal of Network and Computer Applications*, 179, 102975.
- [24] Jutila, M. (2016). An adaptive edge router enabling internet of things. *IEEE Internet of Things Journal*, 3(6), 1061-1069.
- [25] Al-Naami K, El Ghamry A, Islam MS, Khan L, Thuraisingham BM, Hamlen KW, Alrahmawy M, Rashad M. BiMorphing: A bi-directional bursting defense against website fingerprinting attacks. *IEEE Transactions on Dependable and Secure Computing*. 2019 1-15.
- [26] Ye L, Yu X, Zhao J, Zhan D, Du X, Guizani M. (2018). Deciding your own anonymity: user-oriented node selection in I2P. *IEEE Access*. 2018 Nov 16;6:71350-9.
- [27] Samuel, O., Javaid, N., Almogren, A., Javed, M. U., Qasim, U., & Radwan, A. (2022). A Secure Energy Trading System for Electric Vehicles in Smart Communities using Blockchain. *Sustainable Cities and Society*, 79, 1-21.
- [28] Wang, Y., Su, Z., & Zhang, N. (2019). BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. *IEEE Transactions on Industrial Informatics*, 15(6), 3620-3631.
- [29] Kong, W., Li, X., Hou, L., Yuan, J., Gao, Y., & Yu, S. (2022). A Reliable and Efficient Task Offloading Strategy Based on Multi-feedback Trust Mechanism for IoT Edge Computing. *IEEE Internet of Things Journal*.
- [30] Egoschin, N. S., Konev, A. A. & Shelupanov, A. A. (2020). A Model of Threats to Confidentiality of Information Processed in Cyberspace based on Information Flows Model. *Symmetry*, 1-18.
- [31] Mohapatro, M., & Snigdha, I. (2021). An Experimental Study of Distributed Denial of Service and Sink Hole Attacks on IoT based Healthcare Applications. *Wireless Personal Communications*, 121(1), 707-724.
- [32] Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., & Boutaba, R. (2021). Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Transactions on Industrial Informatics*, 18(3), 2053-2062.
- [33] Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K. D., & Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, 97, 132-145.
- [34] Akinyele, J. A., Garman, C., Miers, I., Pagano, M. W., Rushanan, M., Green, M., & Rubin, A. D. (2013). Charm: a framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering*, 3(2), 111-128.