Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System

PRATIMA SHARMA, Bennett University, India
SUYEL NAMASUDRA, National Institute of Technology Agartala, Tripura, India
NAVEEN CHILAMKURTI, La Trobe University, Australia
BYUNG-GYU KIM, Sookmyung Women's University, Republic of Korea
RUBEN GONZALEZ CRESPO, Universidad International de La Rioja, Spain

Blockchain technology provides a secure and reliable platform for managing data in various application areas, such as supply chain management, multimedia, financial sector, food sector, **Internet of Things (IoT)**, healthcare, and many more. The recent emergence of blockchain with IoT provides significant growth in the healthcare industry to improve security, privacy, efficiency, and transparency with more business opportunities. Nevertheless, conventional healthcare schemes suffer from various security attacks like collusion, phishing, masquerade, etc. Therefore, a privacy-preserving **Distributed Application (DA)** is proposed in this paper using blockchain technology to create and maintain healthcare certificates. Here, the distributed application provides an interface between the blockchain network and system objects like healthcare centers, verifiers, and regular authorities to generate and issue medical documents. In addition, it also ensures security by specifying rules using various smart contracts. To evaluate the performance of the proposed scheme, various experimental tests are conducted using the Etherscan tool for measuring operation cost, latency, and processing time. Here, the efficiency of the proposed system is also compared to the existing systems in terms of latency, throughput, and response time. The experimental results and comparative analysis show that the proposed work is more efficient than the existing techniques.

CCS Concepts: • **Computing methodologies** → **Distributed computing methodologies** • **Security and privacy** → **Cryptography**;

Additional Key Words and Phrases: Smart contract, healthcare certificate, distributed application, Ethereum

ACM Reference format:
Pratima Sharma, Suyel Namasudra, Naveen Chilamkurti, Byung-Gyu Kim, and Ruben Gonzalez Crespo. 2023. Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. *ACM Trans. Sensor Netw.* 19, 3, Article 56 (March 2023), 17 pages.
https://doi.org/10.1145/3577926

Authors' addresses: P. Sharma, Department of Computer Science and Engineering, Bennett University, Greater Noida, Uttar Pradesh, India 201310; S. Namasudra (corresponding author), Department of Computer Science and Engineering, National Institute of Technology Agartala, Tripura, India, 799046; email: suyelnamasudra@gmail.com; N. Chilamkurti, La Trobe University, Melbourne, Australia, 3086; B.-G. Kim, Sookmyung Women's Univeristy, 100, Cheongpa-ro 47-gil, Yongsan-gu, Seoul, Republic of Korea, 04310; R. Gonzalez Crespo, School of Engineering and Technology, Universidad Internacional de La Rioja, Avda. de la Paz, 137, Logroño, La Rioja, Spain, 26006.

1550-4859/2023/03-ART56 $15.00
https://doi.org/10.1145/3577926

1 INTRODUCTION

Over the last few years, IoT-based healthcare systems arose as an emerging technology to support the smart healthcare industry by providing an effective platform to store, manage, share, and secure medical records. With the massive volume of medical data and the number of IoT devices, the data management and privacy of sensitive health records have always been a common concern of the medical industry [1]. The traditional IoT-based medical systems utilize cloud services for processing and managing health records. The cloud system suffers from the single point of failure issues, when the number of IoT devices increases, it leads to security attacks. The most common attacks that the healthcare sector experienced in the cloud are phishing, data theft, masquerade, and data breaches. As most healthcare data are communicated over the internet, the security and privacy issue of healthcare records is always a significant concern in the medical industry.

Furthermore, the security and privacy of healthcare records have been improved by using many tools, applications, frameworks, and emerging technologies. Traditional medical systems utilize encoding, advanced algorithms, and cryptographic techniques to prevent the security of healthcare information. These techniques maintain medical data using the database or cloud [2–4]. However, they fail to protect the records as they are ineffective in resisting man-in-the-middle, masquerade, and modification attacks [5]. Currently, duplication or legalization of a medical certificate's identity is very easy for attackers and hackers. The user must carry the medical certificates all the time for medical treatment. Unfortunately, if they miss carrying medical certificates, it is a lengthy procedure to retrieve them. Therefore, a blockchain-based distributed application can help to mitigate the problems mentioned above [6].

Blockchain provides a decentralized and secure solution using a distributed ledger where transactions are protected by cryptographic algorithms and verified in the Peer-to-Peer network. The technology is first proposed by Nakamoto [7] in cryptocurrency transactions, such as Bitcoin and Ether. Blockchain enables the execution of the transaction in the network without involving a trusted party or authority. Thus, it eliminates the centralized authority and removes the single point of failure issue [8, 9]. In the blockchain network, transactions are stored in the form of blocks. Each block includes transactions, timestamps, block hash, Merkle toot, parent block hash, and other information. Thus, the blockchain network provides transparency, decentralization, anonymity, and immutability with enhanced security features.

Various blockchain-based techniques have been developed by authors for the healthcare system [10–13]. For example, Rhayem et al. [10] proposed a unified model that contains information related to IoT and the healthcare sector and the link between them. Based on collected data from the gestational diabetes case study, the analysis rules are defined for the proposed model using generic ontology. It is observed that the involvement of semantic analysis with context-aware methods and IoT increases the complexity of the system. In [11], the authors analyzed the various dimensions of blockchain on the **Internet of Medical Things (IoMT)** system. They also proposed a blockchain-based architecture using smart contracts for IoMT to process, store, and manage healthcare data. However, the proposed architecture lacks the details of security analysis. Oh et al. [12] designed a framework to prevent personal information leakage from education platforms using the capture the flag scenario. The capture the flag scheme provides the evaluation platform to generate a response for personal data leakage. It analyzes the possible risks associated with personal information breaches, identifies the leading cause of the breach, and strengthens the ability to resolve it. However, this scheme faces various security and privacy issues. Sharma et al. [13] proposed a distributed scheme to maintain healthcare big medical data in the blockchain network. It utilizes the **InterPlanetary File System (IPFS)** decentralized storage system to store medical files in a distributed manner. The proposed scheme ensures the integrity of the healthcare

files using the Merkle root concept. It involves various stakeholders, such as healthcare experts, pharmacists, doctors, and researchers to store their medical data and access the medical information stored on the blockchain network. The proposed scheme lacks the details of security analysis in terms of attacks prevented by the designed architecture.

Although many studies are suggested for managing healthcare documents using blockchain technology [14–17], there is still a need to better utilize the distributed approach in the medical domain to ensure security features. This paper implements a distributed application for healthcare systems with IoT devices to improve security and privacy features using blockchain technology. The front-end part of the proposed distributed application provides the user interface. Here, the users or patients can use a unique ID to access their respective medical certificates. Therefore, they need not carry the medical certificate physically. As medical certificates are maintained using the blockchain structure, the users can access the certificate at any time and from any place. Furthermore, the proposed scheme prevents unauthorized access from hackers and malicious users. The main contributions of the paper are mentioned below:

(1) This work proposes a distributed application for an IoT-based healthcare system to generate, store, and maintain medical certificates.
(2) The proposed DA works as an interface between the blockchain-based system and application users, such as hospitals, physicians, and regulatory agencies.
(3) The proposed scheme ensures the security and privacy of healthcare documents. It controls unauthorized access and maintenance of medical certificates, as well as avoids fraud on healthcare documents.
(4) Experimental results, security, and comparative analysis prove that the proposed scheme works better than the existing schemes.

The remaining paper is arranged as follows. Section 2 presents a discussion on current techniques. The proposed architecture is presented in Section 3. The security features achieved by the proposed work are given in Section 4. Section 5 deals with the results and discussion. Finally, the proposed work concludes with future direction in the last section.

2 RELATED WORKS

This section presents a discussion on existing systems related to blockchain technology in the healthcare domain. Many authors have designed advanced techniques to improve the performance and efficiency of healthcare systems [18–24]. Several studies have discussed the advantages of using blockchain to maintain the **Electronic Health Records (EHR)**. Mishra et al. [25] proposed a decentralized application to share the details of student credentials securely. It is implemented using the Ethereum platform to secure data-sharing services between various shareholders. However, the scheme lacks experimental results and comparative analysis details. Wang et al. [26] proposed a hybrid framework using blockchain, parallel healthcare systems, and artificial intelligence to model, diagnose, and treat patients. The framework constructs the consortium blockchain to link patients, healthcare experts, hospitals, and healthcare communities to provide various services, such as healthcare data storage, sharing, reviewing, and auditing. It also deploys the diagnosis and treatment functionality using artificial intelligence. The involvement of various techniques, namely blockchain, artificial intelligence, and predictive analytics increases the system's complexity. Similarly, Khatoon [27] designed a healthcare data management system using blockchain-based smart contracts. The designed system defines the multiple medical workflows using the Ethereum blockchain network to provide surgical and clinical trial procedures. It involves multiple stakeholders to provide better medical services and reduce costs. It is analyzed that the proposed scheme lacks the details for managing healthcare certificates. Ichikawa et al. [28] developed a

mobile application for healthcare systems using blockchain technology to provide a real-time monitoring system. The designed mobile application provides patients and healthcare service providers a platform to address their medical needs through real-time monitoring and treatment. It provides a tamper-resistant, trusted, and auditable healthcare system using blockchain technology. The performance evaluation of the designed applications lacks a comparative analysis with the existing techniques. In [29], Latt et al. proposed an Ethereum-based blockchain scheme to allow users to trace rice cycle information in Myanmar. The proposed scheme ensures food safety in the supply chain process and maintains the integrity of the information using the blockchain structure. The scheme is specifically designed for the rice supply chain system. Bhattacharya et al. [30] suggested an integrated healthcare architecture using deep learning and blockchain technology. It provides an electronic healthcare record-sharing method that operates in two phases. The first phase utilizes blockchain technology to implement authentication and signature-based cryptographic algorithms for healthcare authorities. The second phase deploys deep learning algorithms to predict diseases. It is analyzed that the proposed work lacks the details of security and privacy analysis. Srivastava et al. [31] proposed a light and secure model for healthcare systems using blockchain technology. This model utilizes IoT devices with remote monitoring using cryptographic tools that eliminate the need for a PoW algorithm. Yanez et al. [32] designed a novel data allocation method for IoT using blockchain based on rating value. This method utilizes the rating value to allocate the data to the on-chain storage system. It also deploys the data controller that uses fuzzy logic to decide the data allocation on the blockchain storage. This scheme takes more time to execute transactions. Bi et al. [33] proposed a deep learning-based model with privacy-preserving features for the healthcare system. The proposed model implemented the data extraction algorithm to analyze the healthcare data by separating the privacy features before. It also avoids the overfitting issue by using the data augmentation method with a customized convolution neural network to ensure security features. However, the proposed model increases the computational overhead.

Yazdinejad et al. [34] presented a novel authentication method for distributed hospital networks using blockchain technology. It utilizes the public blockchain to connect IoT devices with the distributed hospital network, and users are connected using the distributed identity. If participating users or devices migrate from one hospital to another, it does not require any authentication. Thus, it decreases the time required for authentic users or devices. Meng et al. [35] designed a medical smartphone network model to detect malicious nodes using blockchain technology. It updates the blacklist details to other nodes to obtain traffic-related information from the suspicious nodes and enhance the malicious detection process. However, this designed model lacks the details of security and privacy analysis. Akkaoui [36] suggested a blockchain-based authentication mechanism to check the authenticity of the Internet of Things Medical devices. The proposed mechanism solves the problem of duplicate or copycat devices and maintains the security of the firmware update procedure required for these devices. It is designed using consortium blockchain and guarantees confidentiality, privacy, security, and anonymity features. Further, it uses symmetric encryption to secure the medical data and leverages the zero-knowledge proof protocol for securing the keys, but lacks throughput-related details. Table 1 presents a summary of the strengths and weaknesses of the related schemes.

3 PROPOSED WORK

In this paper, blockchain-based DA is proposed to produce and maintain official health documents using various phases, namely healthcare data acquisition, representation, validation, and justification. Users manage the medical certificates using various IoT devices. The user can use any device to maintain the certificate; there is no specific requirement [37]. The DA provides the user interface to provide various services like generating, storing, and verifying medical certificates for the

Table 1. Summary of Strengths and Weaknesses of the Related Schemesc

Ref.	Findings	Platform	Features	Limitations
[25]	This scheme implements a decentralized application to secure sharing of student credentials among various stakeholders.	Ethereum with Rinkeby test network	Registration feature with access rights	It lacks the details of security and privacy analysis.
[26]	It designs a framework for a parallel healthcare system using artificial, computational, and parallel approaches with blockchain.	Consortium blockchain network	Data integrity and interoperability	Increases complexity of the system.
[27]	It proposes a smart contract-based healthcare system using blockchain technology for managing healthcare data.	Ethereum blockchain network	Data sharing with access control	Specifically designed for managing medical prescriptions.
[28]	Here, a mobile health system is designed using blockchain technology.	Hyperledger blockchain network	Tamper-resistant with audibility	The performance evaluation of the system is not justifiable.
[29]	It designs a blockchain-based Myanmar rice cycle system to manage the supply process.	Ethereum blockchain network	Data integrity with traceability	It only considers the rice supply chain system in Myanmar.
[30]	This scheme integrates the blockchain with deep learning techniques to control, share, and manage electronic health records.	Keras DL API with TensorFlow using Python	Authentication with disease prediction	The involvement of many advanced technologies increases the system's complexity.
[31]	It introduces a novel blockchain-based remote patient monitoring system using IoT devices.	ARX encryption algorithm with the ring signature	Anonymity and signature correctness	It lacks the details of performance analysis based on latency, cost, etc.
[32]	It develops a blockchain-based data allocation mechanism for IoT systems.	Fogbus with MATLAB	Data allocation	The security and privacy analysis details are not covered.
[33]	This paper proposes a deep-learning-based model for an IoT-enabled healthcare system.	Convolutional neural network with ELAN software	Supports classification	Complexity is high.
[34]	Here, a distributed hospital network system is proposed with an authentication mechanism using blockchain technology.	Network simulator version 2	Authentication	Involves high computational overhead.
[35]	It designs a novel blockchain-based trust management system using blockchain to enhance the medical smartphone network.	Bayesian inference	Trust management	Lacks the analysis of security and privacy features.
[36]	This scheme suggests a system to manage the IoT devices of the medical industry.	Ethereum blockchain with ProVerif	Confidentiality, anonymity, and privacy features	Lacks the throughput-related details.
Proposed work	Proposes a distributed application using blockchain technology for healthcare systems to generate, store, maintain, and verify medical certificates.	Ethereum framework with Remix IDE	Authentication, confidentiality, availability, and integrity	It only considers medical certificates. In future works, the architecture can be extended to include medical prescriptions.

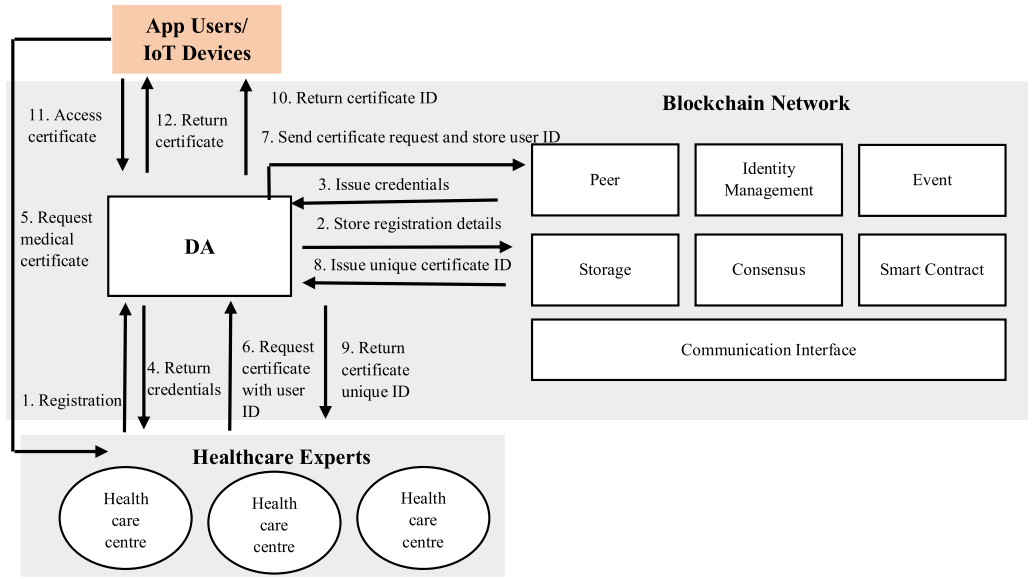

Fig. 1. Workflow of the proposed scheme.

users. It is a web application that is implemented using the distributed blockchain network. Initially, the user registers in the DA and receives the unique ID during the registration process from the involved authority. If any user or patient contacts the healthcare centers to obtain an official health document, the healthcare authorities first verify the users' records as healthcare experts. Then, the blockchain network generates the required medical certificate. Next, the DA deploys or processes the certificate on the blockchain network to generate blockchain-based documents with a unique ID. Finally, the healthcare document is stored as a transaction with a unique blockchain ID in the form of a block.

The proposed IoT-based framework supports the public blockchain (i.e., Ethereum) at the backend, i.e., a distributed file system [38–40]. At the front end, there is a user interface to communicate with the proposed system. The DA utilizes the Ethereum public network to generate medical certificate records. The proposed architecture uses **Proof of Work (PoW)** as a consensus algorithm [38, 39]. The DA maintains the distributed ledger, and provides security against unauthorized actions like insertion, deletion, and updating the healthcare records [40–43].

Figure 1 depicts the distributed application based on a blockchain system for securing medical records. The proposed system consists of four entities: (1) users/IoT devices, (2) healthcare experts, (3) DA, and (4) blockchain network. Initially, hospitals or doctors of healthcare centers send a registration request to the distributed application. Then, the DA checks registration information, obtains the credentials from the Ethereum network, and stores the information of the entity on the blockchain network. Similarly, IoT devices, such as wearable smartwatches, and many more, register in the proposed architecture by sending the request to the DA with the unique identification number and following the same registration procedure mentioned above. Next, the DA shares the obtained credentials with the healthcare experts. Then, the user of the proposed application sends a request for the healthcare documents from the healthcare experts registered in the system. Now, the healthcare experts send the respective request to the DA with the user details. After sending the request, the DA generates the requested medical document with a unique ID and maintains the user details in the proposed network. Next, the DA shares the certificate's unique ID with the user

and the healthcare center. Finally, the user can access the generated medical document using the unique shared ID. Also, the user can access the generated certificate in the registered IoT device by connecting it to the proposed architecture using Wi-Fi. The proposed system follows the below sequential steps:

Step 1: Healthcare centers send the registration request to the distributed application with the username, address, unique ID, etc.

Step 2: The DA receives the registration details and verifies if the healthcare expert is already registered in the system. After verification, the DA stores the experts' details in the blockchain network.

Step 3: After storing the healthcare experts' details, the blockchain network generates the login credentials for the healthcare expert and sends them to the distributed application.

Step 4: The DA shares the credentials with the healthcare expert and allows the expert to access the services of the proposed architecture.

Step 5: Users request the healthcare centers for medical certificates, such as birth, marriage, death, or sick.

Step 6: As healthcare experts, healthcare centers check the validity of received details from the user. For example, if a user wants a sick certificate, the healthcare expert verifies the user's health status and severity, treatment period, consultant doctor in the hospital, etc. Then, it decides as per the user's request, whether to proceed further or not.

Step 7: In this step, user requests are processed by healthcare centers to verify the credentials and connect with the blockchain through DA and Metamask wallet to generate a medical certificate request.

Step 8: The blockchain network saves the user details with the generated certificate details in the blockchain structure and issues the generated unique certificate ID to the DA.

Step 9: The DA shares the generated certificate ID with the user, as well as with the healthcare centers.

Step 10: The user is allowed to access the generated medical certificate with the help of the DA portal by using the certificate's unique ID.

Step 11: In response, the DA accesses the generated certificate from the blockchain network using its unique ID and shares it with the user.

The DA application implements four smart contract operations: (1) Register(), (2) $\text{Generate}_{\text{block}}()$, (3) Issue_Certificate(), and (4) Verify_Certificate(). All these operations are executed by the automated smart contract. Algorithm 1 shows the sequential steps for registering health centers in the proposed application. First, the health centers send the registration request to the DA with the username and address. Then, the DA verifies the details, i.e., whether the requested entity is already existing or not. After the verification process, the DA generates a unique HC_ID and sends it to the healthcare experts.

ALGORITHM 1: Registration of health centers (*Register*())

Input: Details of health center or domain expert.
Output: Registration is completed.

1. $Healthcare_{expert}(UnameAddress) \xrightarrow{request} DA$ //Health centers send a registration request
2. $DA(Process_{request})$ //Verify user details
3. $DA \xrightarrow{save\ details} Blockchain$
4. $Generate(HC\_ID) \rightarrow DA$ //Blockchain send a generated ID to DA
5. $Share(HC\_ID) \rightarrow Healthcare_{expert}$

Algorithm 2 shows the steps required to generate healthcare certificates for the user using blockchain technology. At first, the registered user sends a request to healthcare experts with details. Then, the healthcare expert checks whether the user is a registered one or not from the DA. On validation of the user's authenticity, the DA processes and transfers the request to the blockchain for further processing. Next, the blockchain performs cryptographic operations on the user's request to generate the certificate in the form of a block. In the end, the generated block is appended to the blockchain network. A valid user can show their health documents using U_ID without carrying any other physical documents or forms and access the generated certificate using document ID.

ALGORITHM 2: Generate healthcare certificate in the form of a block ($Generate_{block}()$)

Input: User details
Output: Generate user certificate with details store in a block

1. $User \xrightarrow{request} Healthcare_{center}$
2. Healthcare experts VERIFY authenticity from the DA
3. if $(Authenticity == True)$
4. $\quad DA(Process_{request})$
5. $\quad DA \xrightarrow{request} Blockchain$
6. $\quad Block??hain(request) \xrightarrow{perform\ cryptographic\ functions} Block(Generate_{certificate})$
7. $\quad$ Return $Document_{ID}$
8. else
9. $\quad Reject_{request}$

Algorithm 3 shows the processes of accessing a medical certificate. The blockchain-based DA assigns a unique ID for all the medical certificates that are certified by the relevant authorities. Blockchain manages each unique ID as a transaction within a specific block. The SHA256 hash algorithm is used to generate cryptographic hash values to interconnect all blocks to each other.

Algorithm 4 presents the verification process to verify the authenticity of the medical certificate. It first checks the blockchain-based unique ID of a user's medical certificate using the distributed application. If the unique ID matches within the database, it verifies the documents' correctness. Each unique ID of the user and generated certificate ID is managed as a transaction in a specific block over a blockchain. As all the blocks are interconnected using the cryptographic hash value, any change in the transaction affects the hash value of all blocks.

4 SECURITY ANALYSIS

The proposed application attains the following security features:

(1) ***Collusion Attack:*** The proposed work prevents the collusion attack by introducing the data identifier during the registration and document generation process. It uses randomly generated unique identifiers for the users and medical certificates during the registration and document generation process. In case of collusion attacks, the user colludes with the other malicious user who doesn't satisfy the valid user criteria and utilizes the access process to provide related details to the colluded user. Thus, to prevent collusion attacks, the introduced data identifier in the certificate generation process only allows access, if the document identifier matches the user identifier.

(2) ***Sybil Attack:*** The proposed work utilizes the unique identification mechanism to combat Sybil attacks. The Sybil attack is initiated by assigning several identifiers to the same node, and a hacker takes control of multiple nodes in the network to initiate the double-spending

ALGORITHM 3: Issue healthcare certificate ($Issue\_Certificate()$)

Input: Details of user and details of certificate
Output: Access generated certificate

1. User or patient REQUEST, i.e., $Request\ (User_{credentials}, Document_{ID})$ to access medical document
2. DA PROCESS the request
3. for each user
4. $Access(Document_{ID})$
5. end for

ALGORITHM 4: Verify healthcare certificate ($Verify\_Certificate()$)

Input: $Document_{ID}$
Output: Verification confirmation

1. PROVIDE $Document_{ID}$ of the medical certificate //Read BCT based unique ID of a medical certificate
2. for $\forall\ Document_{ID} \in Database$
3. if($Document_{ID} == True$)
4. Medical certificate is VERIFIED
5. else
6. Medical certificate is not VERIFIED
7. end for

attack. In the proposed work, each user is verified using a unique identity; thus, it prevents the process of assigning the same identity to a single user. Furthermore, the proposed application deploys the Proof-of-Work consensus algorithms for the mining process. Thus, the hacker must expend energy to influence the blockchain network.

(3) ***Masquerade Attack:*** The masquerade attack allows the unauthorized user to use fake credentials or information to get access to the system. The proposed application deploys the registration service for the users to prevent the masquerade attack. In the proposed work, all users need to register in the system, and then after successful login, the user can access the services. Thus, unauthorized, or malicious users cannot access the proposed application services using a fake identity. In the worst case, if a malicious user enters the system and requests any medical documents, the proposed system validates the user's identity with the requested medical certificate before granting access.

(4) ***Phishing Attack:*** The phishing attack occurs when the attacker or malicious user obtains the user's personal or sensitive information, such as user ID, login credentials, and so on. Then, the attacker utilizes the authorized data of the user to avail of the service of the application. In the proposed scheme, the blockchain network stored all user details using the blockchain structure in the form of hash values. When the user sends the access request to the distributed application, it checks the information using the blockchain structure and verifies the user details with the requested document. Thus, the attacker or the malicious user cannot get the user's details as all details are stored in the blockchain structure using the hashing algorithms.

(5) ***51% Attack:*** The 51% attack is also termed a majority attack. It occurs when a single person or group controls more than 50% of the blockchain network mining's hash power. Thus, the attacker may halt transactions or payments between some users in the blockchain network. The proposed architecture implemented the PoW algorithm, which requires more energy resources to mine the block in the blockchain network. Hence, the hacker would

Table 2. Notations and Description

Notation	Description
$Uname$	Name of health center
$Address$	Address of health center
HC_ID	Health center's ID
U_ID	User ID
T_ID	Transaction ID
$Healthcare_{expert}$	Healthcare expert
$User_{credentials}$	User's credentials
$Certificate_{details}$	Details of certificate
$Generate(HC\_ID)$	Function to generate unique ID for healthcare center
$Healthcare_{expert}(Uname, Address)$	Healthcare expert details
$Process_{request}$	Function to process user's request
$Share(HC\_ID)$	Function to share generated healthcare center ID
$Document_{ID}$	Generated medical certificate ID
$Block(Generate_{certificate})$	Function to generate medical certificate in the form of block
$Blockchain(request)$	Function to process user's request and apply cryptographic operations in the blockchain network
$Access(Document_{ID})$	Function to access the stored healthcare document using unique ID
$Request(User_{credentials}, Certificate_{details})$	Function to send access request with user and certificate details

require vast amounts of power and hardware resources to control more than 50% nodes of the proposed blockchain network, which is almost impossible to attain. Table 2 represents all the notations and their description used in this paper.

5 PERFORMANCE ANALYSIS

This section presents the experimental environment, evaluates the performance parameters, and compares the proposed work.

5.1 Experimental Environment

The proposed work is implemented using the Ethereum platform. Ethereum is a public blockchain network that is open source and used to deploy smart contracts. The smart contract provides various functions of the proposed distributed application. It allows users to register, generate, verify, and access medical certificates. The smart contract also identifies unauthorized access and illegal manipulation, and prevents attacks on the proposed architecture. The experiment environment involves the Ganache tool for setting up the blockchain network, smart contracts for defining the basic functionalities, and Testnet for executing tests on the proposed work based on various performance evaluation parameters, namely latency, processing time, throughput, and response time. The front-end of the DA is designed using React Native, which provides a compatible environment with the Ethereum platform. NodeJS provides an interaction between the Ethereum framework and the distributed application. The essential components of smart contracts, namely variables, modifiers, states, and events, are implemented using Solidity language. The smart contracts are deployed using a remix text network on the Testnet. Remix IDE is mainly utilized to design smart contracts to be included locally and globally. For connecting the Ethereum platform, the MetaMask browser plugin is used that provides a wallet as an extension of the browser.

Table 3. Proposed System Operations Cost

Caller	Function	TestRPC (Gas cost)	Remix (Gas cost)
Healthcare center	$Register()$	0.000426	0.000761
Healthcare center	$Generate_{block}()$	0.000562	0.000798
Healthcare center	$Issue\_Certificate()$	0.000765	0.000843
Healthcare center/user	$Verify\_Certificate()$	0.000312	0.000345

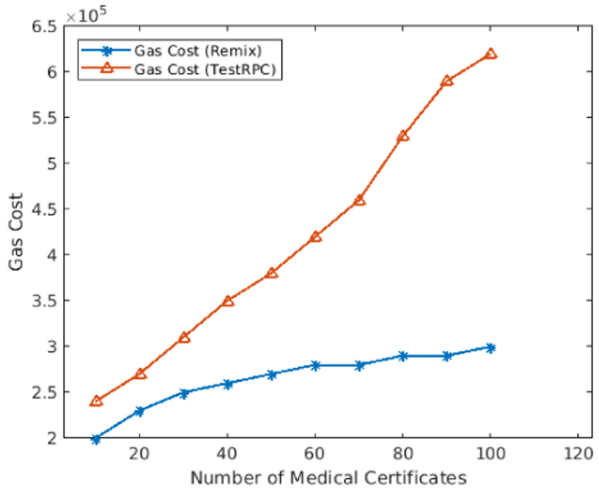

Fig. 2. Platform wise gas cost for medical certificates.

5.2 Results and Discussion

The Etherscan tool is utilized to evaluate the operational costs of the proposed work. It is an analytics tool that explores the block in the blockchain network. Etherscan acts as an Ethereum platform Gas tracker that tracks the transactions, verify the performance of smart contracts, and checks the process's state. The execution of the transaction requires Gas as the cost in the Ethereum blockchain network. Gas represents the unit of the cost required to perform a function in a blockchain network. Based on supply and demand, the miners set the price of the Gas. This cost depends on the execution, deployment, and transfer process involved in running the blockchain network transaction. Generally, Gas involves two parameters that are limit and price. The limit depends on the willingness of the user to execute a transaction, and it is presented as 'gwei'. The execution of smart contracts and transactions involves lots of computation power over the blockchain network. In the proposed work, the smart contracts are deployed on TestRPC, and the Etherscan tool collects details of all executed tasks.

The proposed approach's operational costs on TestRPC-based Ethereum blockchain network and using Remix platforms have been shown in Table 3. In Table 3, the caller means the entity which requests the execution of the smart contract function. Here, four operations, namely Register(), $\text{Generate}_{\text{block}}()$, Issue_Certificate(), and Verify_Certificate(), are considered. The proposed blockchain network deploys these functions using the distributed application and calculates the Gas cost of each operation.

Figure 2 presents the platform-wise Gas consumption for generating the medical certificates using two platforms, namely Remix and testRPC Ethereum blockchain. Gas consumption is

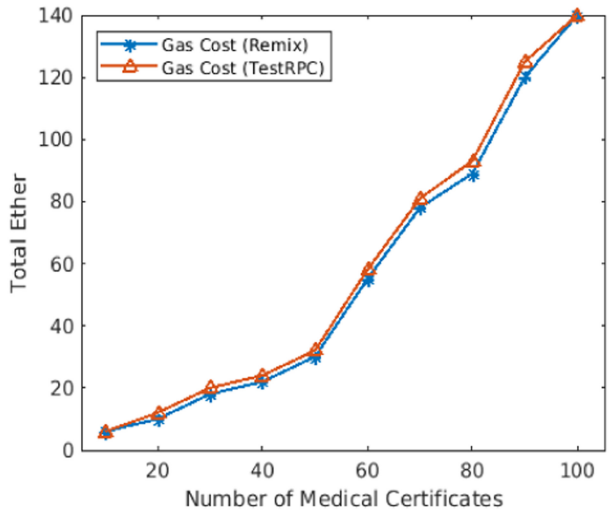

Fig. 3. Total ether consumption for certificates generation.

Table 4. Cost Analysis of Smart Contracts

Smart contract function	Transaction cost (Gas)	Execution cost (Gas)
$Request()$	2165431	1587652
$Generate_{block}()$	863212	682101
$Issue\_Certificate()$	1154324	818553
$Verify\_Certificate()$	975438	832233

measured in terms of ETH and gwei. Here, the proposed application is tested by considering up to 100 certificates. As depicted in Figure 2, the proposed application Gas cost increases with the number of medical certificates as the number of blocks increases in the blockchain structure. As each block stores the certificate details with user details. Thus, as the number of medical certificates increases, the Gas cost increases on both platforms, i.e., Ethereum and testRPC. The proposed application deployed on the Ethereum platform requires less Gas cost than the testRPC platform.

Figure 3 presents the operational cost of the proposed system deployed on the Ethereum blockchain-based Ropstern network with the remix-based system. The proposed application increases the total Ether as the number of medical certificates increases due to the processing required for completing the medical certificate generation process transactions. Table 4 shows the transaction cost and execution cost of the proposed scheme. Usually, any blockchain network takes a modest time to read the application's information, i.e., from a DA or a system application. The transaction cost denotes the cost required to complete the execution of the transaction. In contrast, execution cost denotes the total cost required to append the newly created block having multiple transactions in the blockchain structure. The cost analysis of the smart contract functions of the proposed application in terms of transaction and execution cost is represented in Table 4.

Table 5 shows the proposed application's performance by considering two non-functional characteristics: latency and processing time. The results indicate the variance between the proposed scheme with blockchain and without blockchain deployment. The time consumption is more on the system deployed in the blockchain platform than the without blockchain system due to its

Table 5. Performance Analysis of the Non-functional Operations

Blockchain-based platform	Properties	Operations	
		Issue_Certificate ( )	Verify_Certificate ( )
Yes	Latency time	5.66	7.45
Yes	Processing time	6.70	11.03
No	Latency time	4.15	3.04
No	Processing time	5.55	8.45

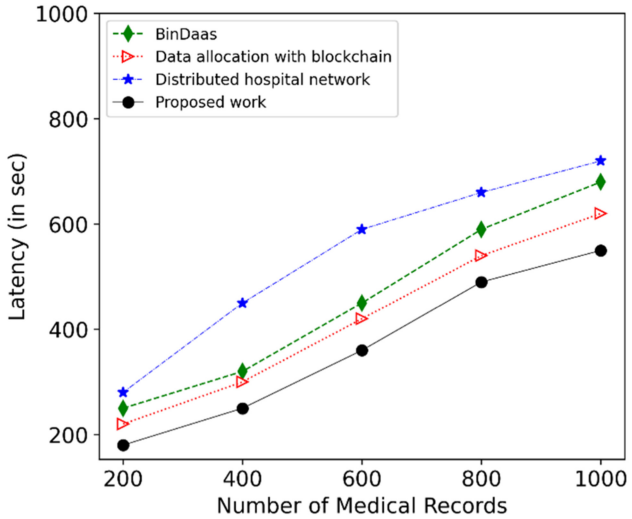

Fig. 4. Latency comparison among the proposed work and other related works.

internal computations, such as mining, crypto hash evaluation, transaction, block creation, and adding the new block in the blockchain network.

Furthermore, the proposed work is compared with related works, namely BinDaaS [30], data allocation with blockchain [32], and distributed hospital network [34]. The proposed work's different aspects, i.e., latency, throughput, and response time are evaluated and compared with the related works. This comparative analysis evaluates the proposed work's performance, robustness, and efficiency compared to the existing works. As shown in Figure 4, the proposed work performance is analyzed based on the latency involved in generating and verifying medical certificates and compared with the existing works. The latency parameter measures the delay between the time the user initiated the transaction and the transaction appended as a block in the blockchain network. The BinDaaS involves more delay to generate the prediction for the medical documents. During this phase, the involved entities first verify the correctness of the message requested by the other entities and then generate the prediction result. Next, the data allocation with blockchain work involves the network propagation delay to transfer the request from the blockchain network to the cloud virtual machine.

In contrast, the distributed hospital network scheme requires more latency than BinDaaS and data allocation with blockchain due to the implementation of complex authentication techniques. Thus, the existing works required more latency for processing the medical documents. At the same time, the proposed work involves less latency time for processing the medical certificates

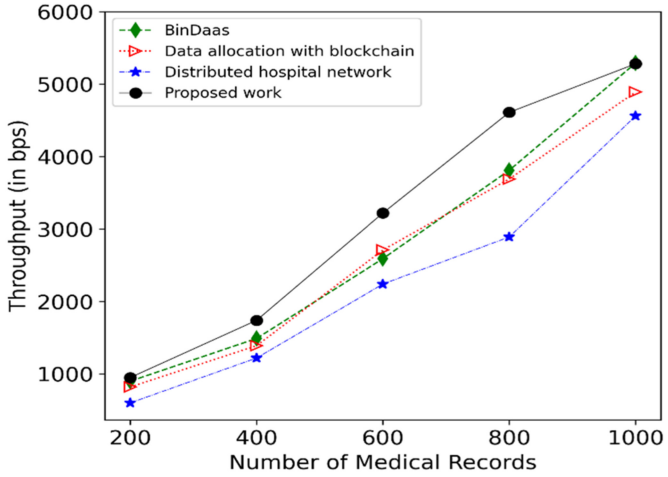

Fig. 5. Throughput comparison among the proposed work and other related works.

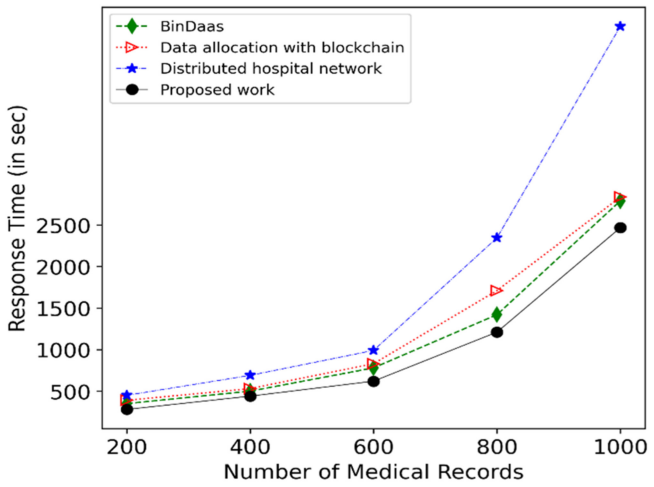

Fig. 6. Response time comparison among the proposed work and other related schemes.

as compared to existing works. The proposed work generates unique identifiers for the medical documents; thus, it fastens the overall medical certificate generation and verification process. As depicted in Figure 4, the proposed work involves less latency than the existing literature. Therefore, the proposed work provides a more robust solution for handling medical documents than the existing works.

As shown in Figure 5, the proposed work performance is analyzed based on throughput and compared with the existing works. The throughput measures the number of transactions handled by the user in a given amount of time. The proposed architecture's throughput is high for executing the transactions initiated by the users randomly as compared to the existing work. The existing works require a two-step process for executing the transactions for different users; thus, throughput is less than the proposed work. Also, the proposed architecture directly executes the transaction as per the user's request because it only allows the validated user to initiate the transaction. Thus, it executes faster. As shown in Figure 6, the response time required for processing

the medical documents is considered for comparing the proposed scheme's performance with the current work. The response time includes the time required to process the transaction by the system and generates the response as per the request. The response time is evaluated for processing the different-sized medical files on the proposed system. However, the proposed work requires less response time to process the medical data on the system than the existing work. The existing work involves the extra overhead for processing the healthcare documents that require more time than the proposed system.

6 CONCLUSIONS AND FUTURE WORKS

This paper introduces a novel distribution architecture for healthcare systems with privacy-preserving features using blockchain technology. The proposed architecture provides a distributed application for generating and accessing medical certificates. It deploys various smart contracts for registering users, generating certificates, verifying certificates and users, preventing attacks, and providing access to the users. Various experimental tests are conducted to evaluate the performance of the proposed scheme, and here, various parameters, namely latency, processing time, throughput, and response time, are considered for evaluation purposes. The results and discussion validate that the proposed architecture outperforms other well-known schemes. The proposed work can be further extended in the future by considering government policies and standards to generate medical certificates with stamps using smart contracts. As the proposed work only considers medical certificates, there are also possibilities to extend the proposed work by including medical prescriptions. Furthermore, a novel access control method can also be developed to achieve mutual authentication.

REFERENCES

[1] D. Kao, S. Hsiao, and R. Tso. 2019. Analyzing WannaCry ransomware considering the weapons and exploits. In *Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT)*, PyeongChang Kwangwoon_Do, South Korea. 1098–1107.

[2] J. Sun, X. Zhu, C. Zhang, and Y. Fang. 2011. HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. In *Proceedings of the 31st International Conference on Distributed Computing Systems*. 373–382.

[3] E. Daraghmi, Y. Daraghmi, and S. Yuan. 2019. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* 7 (2019), 164595–164613.

[4] S. Namasudra, R. Chakraborty, A. Majumder, and N. R. Moparthi. 2020. Securing multimedia by using DNA based encryption in the cloud computing environment. *ACM Transactions on Multimedia Computing, Communications, and Applications* 16, 3s (2020).

[5] A. I. Newaz, N. I. Haque, A. K. Sikder, M. A. Rahman, and A. S. Uluagac. 2020. Adversarial attacks to machine learning-based smart healthcare systems. In *Proceedings of the GLOBECOM 2020 - 2020 IEEE Global Communications Conference*. 1–6.

[6] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi. 2021. The revolution of blockchain: State-of-the-art and research challenges. *Archives of Computational Methods in Engineering* 28, 3 (2021), 1497–1515.

[7] S. Nakamoto. 2020. Bitcoin: A peer-to-peer electronic cash system, 2008. Available: http://www.bitcoin.org/bitcoin.pdf. [Accessed on 15 September 2020].

[8] A. Monrat, O. Schelén, and K. Andersson. 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* 7 (2019), 117134–117151.

[9] S. Zhang and J. H. Lee. 2020. Analysis of the main consensus protocols of blockchain. *ICT Express* 6, 2 (2020), 93–97.

[10] A. Rhayem, M. B. A. Mhiri, K. Drira, S. Tazi, and F. Gargouri. 2020. A semantic-enabled and context-aware monitoring system for the Internet of Medical Things. *Expert Systems*, 1–33.

[11] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B. G. Kim. 2020. Blockchain based smart contracts for Internet of Medical Things in e-healthcare. *Electronics* 9, 10 (2020), 1–14.

[12] S. Oh, B. G. Kim, and N. Park. 2020. Framework for accessing responsiveness to personal data breaches based on Capture-the-Flag. *Journal of Multimedia Information System* 7, 3 (2020), 215–220.

[13] P. Sharma, M. D. Dorah, and S. Namasudra. 2021. Improving security of medical big data by using blockchain technology. *Computers and Electrical Engineering Journal* (2021).

[14] P. Sharma, R. Jindal, and M. D. Borah. 2021. A blockchain-based secure healthcare application. *Blockchain in Digital Healthcare*, CRC Press, 35–54.

[15] S. Namasudra, D. Devi, S. Kadry, R. Sundarsekar, and A. Shanthini. 2020. Towards DNA-based data security in the cloud computing environment. *Computer Communications* 151 (2020), 539–547.

[16] S. Ndichu, S. Kim, and S. Ozawa. 2020. Deobfuscation, unpacking, and decoding of obfuscated malicious JavaScript for machine learning models detection performance improvement. *CAAI Transactions on Intelligence Technology* 5, 3 (2020), 184–192.

[17] R. M. Alguliyev, R. M. Aliguliyev, and L. V. Sukhostat. 2020. Efficient algorithm for big data clustering on single machine. *CAAI Transactions on Intelligence Technology* 5, 1 (2020), 9–14.

[18] H. S. Jennath, V. S. Anoop, and S. Asharaf. 2020. Blockchain for healthcare: Securing patient data and enabling trusted artificial intelligence. *International Journal of Interactive Multimedia and Artificial Intelligence* 6 (2020), 15–23. http://doi.org/10.9781/ijimai.2020.07.002

[19] D.-J. Munoz and D.-A. Constantinescu. 2021. Decentralised blockchain-based solutions for electronic healthcare record with interacting social networking components. In *Proceedings of the 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. 488–493. DOI: 10.1109/3ICT53449.2021.9581525

[20] R. Fantacci and B. Picano. 2020. Federated learning framework for mobile edge computing networks. *CAAI Transactions on Intelligent Technology* 5, 1 (2020), 15–21.

[21] M. El Ghazouani, M. A. E. Kiram, E. R.-R. A. J. Y. Latifa, and Y. El Khanboubi. 2020. Efficient method based on blockchain ensuring data integrity auditing with deduplication in cloud. *International Journal of Interactive Multimedia and Artificial Intelligence* 6 (2020), 32–38. DOI: http://doi.org/10.9781/ijimai.2020.08.001

[22] A. Kishor, C. Chakraborty, and W. Jeberson. 2021. A novel fog computing approach for minimization of latency in healthcare using machine learning. *International Journal of Interactive Multimedia and Artificial Intelligence* 6 (2021), 7–17. DOI: http://doi.org/10.9781/ijimai.2020.12.004

[23] J. Gao et al. 2021. Decentralized federated learning framework for the neighborhood: A case study on residential building load forecasting. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, ACM, Portugal*. 453–459. DOI: https://doi.org/10.1145/3485730.3493450

[24] H. T. Raut et al. 2021. Enhanced bat algorithm for COVID-19 short-term forecasting using optimized LSTM. *Soft Computing* 2021. https://link.springer.com/article/10.1007/s00500-021-06075-8.

[25] R. A. Mishra, A. Kalla, N. A. Singh, and M. Liyanage. 2020. Implementation and analysis of blockchain-based DA for secure sharing of students' credentials. In *Proceedings of the IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA. 1–2.

[26] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F. Y. Wang. 2018. Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Transactions on Computational Social Systems* 5, 4 (2018), 942–950.

[27] A. Khatoon. 2020. A blockchain-based smart contract system for healthcare management. *Advances in Blockchain and Distributed Ledger Technology (DLT) for Industry 4.0 Technologies* 9, 1 (2020).

[28] D. Ichikawa, M. Kashiyama, and T. Ueno. 2017. Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth Uhealth* 5 (2017).

[29] C. N. Z. Latt, S. Rahmadika, and K. H. Rhee. 2021. A data provenance system for Myanmar rice cycle based on ethereum. *Journal of Multimedia Information System* 8, 1 (2021), 35–44.

[30] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar. 2020. BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE Transactions on Network Science and Engineering* (2020).

[31] G. Srivastava, J. Crichigno, and S. Dhar. 2019. A light and secure healthcare blockchain for IoT medical devices. In *Proceedings of the IEEE Canadian Conference of Electrical and Computer Engineering (CCECE'19)*.

[32] W. Yanez, R. Mahmud, R. Bahsoon, Y. Zhang, and R. Buyya. 2020. Data allocation mechanism for Internet of Things systems with blockchain. *IEEE Internet of Things Journal* 7, 4 (2020), 3509–3522.

[33] H. Bi, J. Liu, and N. Kato. Deep learning-based privacy preservation and data analytics for IoT enabled healthcare. *IEEE Transactions on Industrial Informatics*. DOI: 10.1109/TII.2021.3117285

[34] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari. 2020. Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE Journal of Biomedical and Health Informatics* 24, 8 (Aug. 2020), 2146–2156. DOI: 10.1109/JBHI.2020.2969648

[35] W. Meng, W. Li, and L. Zhu. 2020. Enhancing medical smartphone networks via blockchain-based trust management against insider attacks. *IEEE Transactions on Engineering Management* 67, 4 (Nov. 2020), 1377–1386. DOI: 10.1109/TEM.2019.2921736

[36] R. Akkaoui. Blockchain for the management of Internet of Things devices in the medical industry. *IEEE Transactions on Engineering Management*. DOI: 10.1109/TEM.2021.3097117

[37] S. Namasudra, P. Sharma, R. G. Crespo, and V. Shanmuganathan. 2022. Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. *IEEE Consumer Electronics Magazine* (2022).
[38] P. Sharma, R. Jindal, and M. D. Borah. 2022. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. *Journal of Supercomputing* (2022), 1–29.
[39] P. Sharma, R. Jindal, and M. D. Borah. 2022. A review of smart contract-based platforms, applications, and challenges. *Cluster Computing* (2022), 1–27.
[40] H. Wu, A. D. Dwivedi, and G. Srivastava. 2021. Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications* 17, 2s (2021), 1–17.
[41] Z. Chen. 2022. Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm. *Journal of Computational and Cognitive Engineering* 1, 3 (2022).
[42] R. Khan, K. Ullah, D. Pamucar, and M. Bari. 2022. Performance measure using a multi-attribute decision making approach based on complex T-spherical fuzzy power aggregation operators. *Journal of Computational and Cognitive Engineering* 1, 3 (2022).
[43] M. Yang. 2022. Research on vehicle automatic driving target perception technology based on improved MSRPN algorithm, *Journal of Computational and Cognitive Engineering* 1, 3 (2022).

Received 29 September 2021; revised 12 October 2022; accepted 15 December 2022