International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/35 Volume 11, Issue 4, July – August (2024)

RESEARCH ARTICLE

Securing Data Communication in the Cloud Using Machine Learning-Based Blockchain Approach

Shanmugapriya Velmurugan
Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.
shanmugapriyav@skasc.ac.in

Amalraj Irudayasamy
Information Technology Department, College of Computing and Information Sciences, University of Technology and Applied Sciences-Nizwa, Nizwa, Oman.
amalraj.irudayasamy@utas.edu.om

Natesh Mahadev
Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysore, Karnataka, India.
natesh.m@vvce.ac.in

Rajesh Natarajan
Information Technology Department, College of Computing and Information Sciences, University of Technology and Applied Sciences-Shinas, Al-Aqr, Shinas 324, Oman.
✉ rajesh.natarajan@utas.edu.om

Sujatha Krishna
Information Technology Department, College of Computing and Information Sciences, University of Technology and Applied Sciences-Shinas, Al-Aqr, Shinas 324, Oman.
sujatha.krishna@utas.edu.om

Received: 11 June 2024 / Revised: 06 August 2024 / Accepted: 16 August 2024 / Published: 31 August 2024

Abstract – Internet of Things (IoT) devices are used to communicate with each other. Cloud Computing (CC) is utilized to store and analyze the data in IoT for solving security issues. Cloud security is vital for numerous users who are concerned about data security in cloud. Recently, many blockchain methods are developed in the CC environment but, the data confidentiality and integrity were not improved with less time. To address these problems, a new machine learning-based blockchain technology called the Universal Estimator Regressive Single-Block-Length Compressed Hash Blockchain (UERSBLCHB) Method is introduced. IoT devices are employed together patient data. The proposed UERSBLCHB Method performed data regression analysis and secured data communication. Patient data is examined with Universal Estimator Regression via bivariate correlation. Safe data broadcasts were performed with Matyas–Meyer–Oseas Cryptographic Hash-based Blockchain method. Hash values of every patient data are created by Matyas–Meyer–Oseas compression. Hashed results stored into blockchain and perform secure data communication with higher data confidentiality and integrity and less processing time. Simulation of proposed and existing methods are performed in Java with MHEALTH dataset The outcome of UERSBLCHB Method increased confidentiality of 15%, integrity of 17%, accuracy by 20%, reduced processing time by 49%, and space complexity by 38%, than the traditional approaches.

Index Terms – IoT, Secure Data Transmission, Universal Estimator Regression, Bivariate Correlation, Compression Function, Blockchain.

1. INTRODUCTION

IoT is a recent Internet progress combining smart devices and services safe data that organizations use to support applications, including precision agriculture, smart health and environment monitoring, and remote sensing data analysis. IoT is a paradigm in which physical objects, with features such as computing, communication, and sensing capabilities are employed. These sensors and IoT devices gather and transmit to the cloud. Security is demanding issue in cloud. Several research works were developed to guarantee security

RESEARCH ARTICLE

in Cloud. But the data confidentiality and integrity were not improved. In order to overcome the issue, novel machine learning-based blockchain technology is introduced for enhancing the security of data transmission in cloud.

Blockchain technology designed a data integrity auditing scheme in [1]. Dispersed data integrity verification technique was introduced with no third-party auditor. However, the degree of data privacy still needs to be improved per the anticipated plan. To address security problems, the Dueling Double Deep-Q-network with Prioritized experience replay (D3P)-based secure trust-based delegated consensus blockchain (TDCB) was introduced in [2]. TDCB-D3P scheme employed the trust system to enhance security and minimize computation costs. However, the data integrity level still needs to be improved by the TDCB scheme.

For an efficient IoT environment, a new Decentralized Blockchain-based Security (DeBlock-Sec) method was designed [3]. Decentralized Blockchain-based Authentication (DBA) protocol was used to validate devices based on several factors. However, it failed to reduce time. Access control system termed LightMED was developed [4] to provide secure data sharing in fog computing technology. A technique enabling the safe transfer and integration of IoT information has been developed, employing a digital signature with minimal encryption. However, accuracy could have been enhanced.

For Mobile Cloud Computing (MCC) environment in data auditability, a security system for access control designed around the distributed ledger blockchain has been developed [5]. With identical credentials, individuals could use numerous MCC applications with various kinds of privilege authority. However, it failed to minimize space complexity. The DistB-SDCloud framework was developed in [6] to boost security within advanced Industrial IoT applications. Security as well as integrity was attained by dispersed BC technique.

Public verifiability as well as user equality was obtained with Blockchain-basis of encryption scheme in [7]. It attained. However, the security level was not reduced by the blockchain-based encryption scheme. For optimizing placement, a blockchain-basis of safe cost-aware data caching technique was introduced [8]. However, data integrity could have been enhanced. For outsourcing services in CC, a blockchain-based fair payment method named BCPay was designed in [9]. However, complexity was not minimized.

A new framework was developed [10] to monitor activities on particular data evidence. ECIES method was designed to preserve confirmation from information. The problems recognized from the literature are minimum confidentiality, enhanced complexity, computational cost, and so on. To address these problems, UERSBLCHB Method is introduced.

1.1. Problem Statement

Security plays a vital role in cloud for data transmission. Blockchain technology is utilized to provide secure and scalable database storage solution. But, existing blockchain systems have scalability issues due to high processing time, low data integrity and confidentiality and security problems. Due to the vast amount of data gathered over the cloud, access control in the cloud storage system was developed to improve protection. However, cloud computing was unconfident in sharing sensitive data to the cloud. Also, the accuracy was not enhanced. To address this issue, the UERSBLCHB technique is proposed on cloud by secure data transmission in the cloud computing.

1.2. Contribution

The major contribution of the article is essential plan of the UERSBLCHB technique is to perform secured data communication in the cloud platform. IoT devices are employed to gather the patient's medical data. UERSBLCHB Method carried out data regression analysis and secured data communication. Universal Estimator Regression Analysis is used in the UERSBLCHB Method to examine the collected data, depending on the geometric median. Matyas–Reliable transmission of information can be accomplished by implementing the Blockchain approach centered around the Meyer-Oseas Cryptographic Hashing. The UERSBLCHB Algorithm uses the Matyas-Meyer-Oseas compression technique to produce a value known as a hash for every patient's data. The hashed results are collected and stored in the blockchain for secure data communication. In this way, the UERSBLCHB Method enhanced the data communication security with minimum processing time. Lastly, an experimental assessment is performed by UERSBLCHB as well as four conventional techniques for different metrics.

1.3. Organization of Paper

The work of fiction has been organized as such. Section 2 presents an illustrative literature analysis of current blockchain technology solutions. Section 3 explains the UERSBLCHB Method through data analysis and blockchain for safe data communication. Simulation conducted in Section 4 with dataset explanation. Section 5 presents the discussion. Lastly, the article is concluded in Section 6.

2. LITERATURE REVIEW

The audit method was designed in [11] in a shared atmosphere. It avoided communication overhead among users. Efficiency of user revocation was enhanced. Collusion among the agreement parties avoided. Blockchain uses smart contracts for enhancing data integrity. Blockchain framework employing heterogeneous peer-node and cloud-based ledger storage (HPCLS-BC) was designed in [12] for personal computer. Cloud-based ledger storage was introduced to

RESEARCH ARTICLE

eliminate the ledger storage pressure on peer nodes. Peer nodes were utilized to divide the copy of distributed ledger. Throughput and transaction delay were enhanced. However, the data integrity rate was not enhanced. Blockchain-based secure data outsourcing scheme was introduced in [13] but needed to minimize time complexity.

The blockchain model was designed in [14] to perform secured communication in HAPS networks. The designed model was stored and consume of cloud transactions. The designed model comprised many High-Altitude Platform Systems (HAPS) stations that were affected by persistent cyberattacks for infrastructure monitoring applications. Latency was reduced and attack detection rate was enhanced.

The blockchain-assisted certificateless public integrity checking (BA-CPIC) was introduced in [15] for the developed cloud storage scheme. BA-CPIC checks outsourced encrypted data in the Ethereum blockchain to identify the auditor's malicious behaviour.

BA-CPIC was employed to enhance integrity confirming on several encrypted industrial data and find privacy of users. However, the space complexity was not minimized by BA-CPIC.

A unique architecture was introduced in [16] for cloud and Blockchain technologies. Secure-Ring-Verification-based Authentication (SRVA) method was suggested to guarantee the security of distrustful accounts. Harmony Search Optimization is employed to create secret keys. Merkle Hash Tree was created with every block.

However, time complexity was not minimized by the designed architecture. For data management, the user-centric framework was introduced in [17]. Ethereum was employed to monitor and log of pertinent data operations. However, the data integrity rate still needs to be improved by the designed framework.

Cloud–Blockchain Fusion Framework (CBFF) was employed in [18] to attain data liability in numerous clouds. Operation Tracing Mechanism was employed to offer efficient tracing. Data accountability was improved. However, they could have reduced computational costs. Blockchain-based secure access framework (BSAF) was introduced in [19] for privacy protection with key matrix encryption. A fully homomorphic encryption system was introduced to preserve privacy. But it failed to lessen space complexity.

A new collaboration scheme was designed in [20] for secure cloud file sharing. Blockchain performed access control between data owners and users. Access polynomial was employed to share cipher-keys. Attribute-based encryption was employed to offer user anonymity. However, the complexity level was not minimized.

The forensic technique was introduced [21] for privacy preservation. Optimal public key was attained. The designed method increased anonymity. Encryption was ensured with Elliptical curve cryptography. Though the confidentiality rate was enhanced, the computational cost was not reduced. The blockchain-based efficient tamper-proof method was designed [22] for efficient storage in the cloud. Scalability was improved. The designed operation included Electronic Healthcare Recorded (HER) and transactions on a public blockchain. However, time complexity was not minimized.

A Continues Delivery/Continuous Verifiability (CD/CV) discussed [23] for verification. User mobility information was applied to categorize interest points. CD/CV was introduced for confirming the transactions of all stage at workflow. However, it failed to improve the data integrity rate. A secure authentication scheme was introduced in [24] for blockchain technology to preserve privacy. The communication cost was lower. However, the data confidentiality rate was not enhanced.

Quantum Cloud-as-a-service was designed in [25] to attain a secure solution. Quantum Terminal Machines (QTM) were employed to improve feasibility as well as minimize computation power. A smart healthcare environment was offered. However, the accuracy level was not improved in QTM.

An integrated auction model was introduced in [26] with Bayesian game theory, and blockchain Bayesian Nash Equilibriums (BNE) presented cost-effective provider selection to construct the federated cloud services. The Timed message submission method was utilized for preserving privacy. The prototype system depended on the Ethereum blockchain. But time complexity was not reduced.

IAS protocol was designed in [27] to integrate identity. IAS protocol was executed. Reliable message delivery was guaranteed. However, computational costs remained the same. For efficient cloud storage, A blockchain-based decentralized architecture was designed [28]. It performed access control in a secure environment. Cloud storage system stores the original data with less processing time. However, the data integrity rate remained the same for the designed architecture.

The blockchain-aided searchable attribute-based encryption system was introduced in [29] for verification in electronic health records. Duplicate data was eradicated, and storage space was minimized. However, it failed to improve the data confidentiality rate. MapChain-D was introduced in [30] for effective data storage. MapChain-D was introduced for Industrial IoT with minimum latency. Though the latency was minimized, computational complexity was not reduced.

An attribute-based access control method was developed in [31] to ensure data confidentiality. However, it failed to consider space complexity. The certificateless signcryption

RESEARCH ARTICLE

scheme was introduced in [32] through public-key substitution to avoid different attack. However, integrity was not enhanced. Yet another certificateless signcryption method for Smart Home Networks was employed in [33] to provide user identity biometric verification. But the time was not reduced. A secure cloud storage approach was discussed in [34] for access control using E blockchain technology. Nevertheless, it failed to enhance data confidentiality. An improved verification scheme was examined in [35] for Remote Data Access and Sharing in Cloud. However, processing time was higher.

Several ML algorithms were employed in [36] to handle IoT data in healthcare. Adaptive neuro fuzzy inference system (ANFIS) was applied for observing human health. Simplified swarm-optimized Bayesian normalized neural network was employed in [37] for identifying anomalous data. Intelligent intrusion detection method was developed in [38] for secure data transmission. Elliptic curve cryptography-based energy-efficient routing protocol was examined in [39] with higher security. But it failed to minimize processing time. Blinder Oaxaca-based Shapiro Wilk Neutrosophic Fuzzy was utilized in [40] with less time. However, data integrity was not considered.

IoT networks create enormous amounts of data to support different applications, where the security and protection of data are significant. But most existing blockchain systems do not simultaneously consider data confidentiality, integrity, processing time, space complexity, security, and decentralization. To address the issue, machine learning-based blockchain technology is needed. The study highlights the importance of ensuring the confidentiality, integrity, and availability of data in cloud-based blockchain systems for enhancing security.

3. METHODOLOGY

The IoT plays an essential part in different real-time applications. IoT allows users to gather data using dissimilar sensors positioned at various locations. IoT sensors grant access to other services. Due to the medium of communication, it is complex to give safe access to services. An efficient data communication method called UERSBLCHB has been introduced to facilitate safe communication in IoT. The proposed UERSBLCHB method is compatible with providing security for confidential data access. The UERSBLCHB method significantly improves data communication security in different applications.

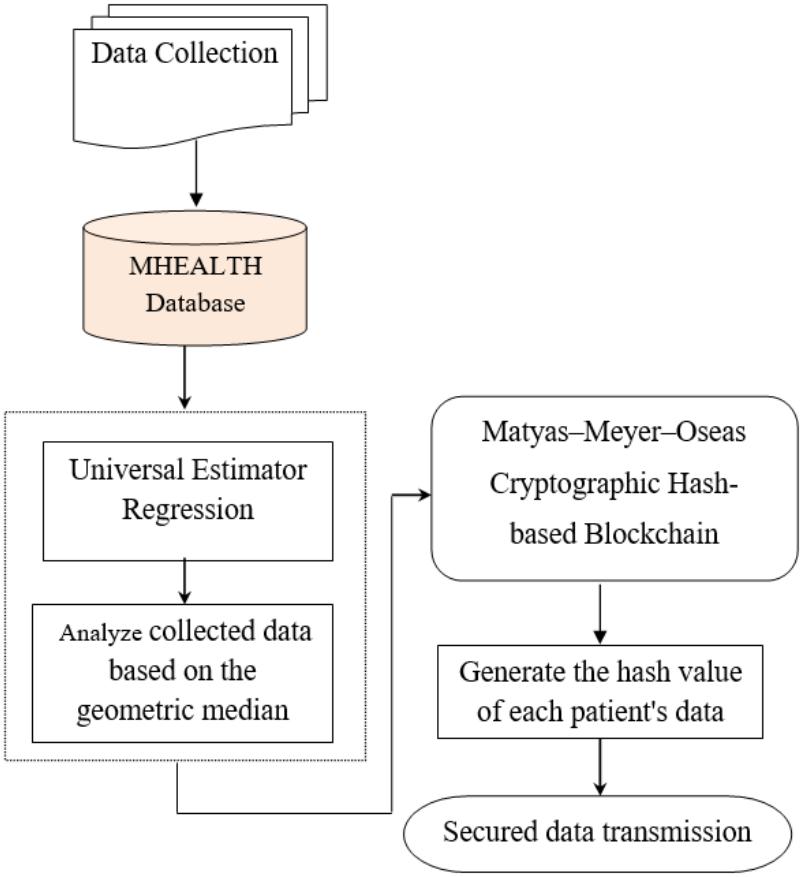

Figure 1 Architectural Representation of the UERSBLCHB Technique

RESEARCH ARTICLE

Figure 1 demonstrates the UERSBLCHB method's architectural representation, which comprises data analysis and secured communication. Number of individual patient information gathered from input dataset. Data analysis is carried out to minimize the time complexity of blockchain construction. Safe data communication is enhanced with Matyas–Meyer–Oseas Cryptographic Hash-based Blockchain during blockchain construction. UERSBLCHB of two different processes is described in sub-sections.

3.1. Bivariate Correlative Universal Estimator Regressive Analysis

After the data collection process, the data analysis is carried out to perform secure communication. Therefore, the proposed UERSBLCHB method performs the data analysis for dimensionality reduction. Universal Estimator Regressive Data Analysis is a statistical method for identifying the projections from enhanced to minimum dimensional space. Universal Estimator Regression maps the total set from maximum to minimum dimensional space.

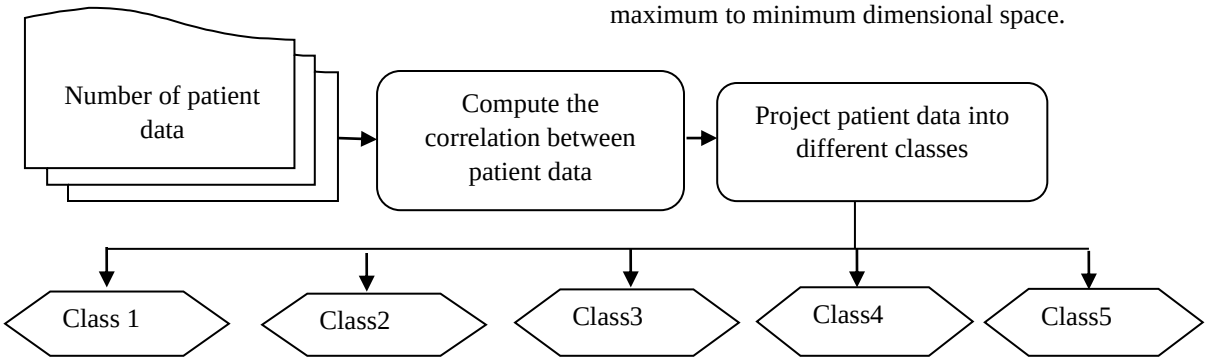

Figure 2 Block Diagram of Bivariate Correlative Universal Estimator Regressive Analysis

Figure 2 illustrates the block diagram of bivariate correlative universal estimator regressive analysis. The universal estimator identifies the best matching projection of the patient set into several classes depending on correlation value. The bivariate correlation measures the relation between patient data in the total set and the objective. Let us consider that polychotomous variable. Bivariate correlation is calculated as,

$$BC = \left(\frac{1}{Deviation}(m_{c1} - m_{c2})\right) * \left(\frac{1}{n}\sqrt{cd_{c1} * cd_{c2}}\right) \quad (1)$$

$$Deviation = \sqrt{\frac{1}{n}} * (\sum_{i=1}^{n}(cd_i - m)^2)^{1/2} \quad (2)$$

From equations (1) and (2), 'BC'represents the bivariate correlation. 'm_{c1}'denotes the mean value of patient data in class 1. 'm_{c2}' denotes the mean value for all patient data in class 2. 'd'represents the standard deviation.'cd_{c1}' and 'cd_{c2}' indicates the number of patient data in class 1 and class 2.' n 'symbolizes an entire number of patient data. 'm'represent the mean value of the particular class. The mean and deviation are employed to classify the patient data. Using a universal estimator, the data points are mapped from high dimensional space to subsets. Consequently, the mapping is carried out depending on the correlation value. Consequently, the universal estimator finds the best matching projection. It is formulated as,

$$mf: cd_i \rightarrow c_j \quad (3)$$

From equation (3), ' mf 'represents the mapping function.'cd_i'symbolizes the patient data in the healthcare dataset.' c_j ' represents the classes. The algorithm below explains the bivariate correlative universal estimator regressive analysis.

Input: Dataset, Number of patient data '$cd_1, cd_2, cd_3, \ldots cd_n$'

Output: Improves accuracy

Begin

1. For individual patient data, 'cd_i'
2. Compute the bivariate correlation 'BC'
3. Universal Regression Estimator maps patient data into different classes
4. End for

End

Bivariate correlative universal estimator regressive data analysis presented in Algorithm 1. The designed analysis maps patient information to dissimilar classes depending on correlation measures. This way, the time complexity gets minimized using bivariate correlative universal estimator regressive data analysis.

3.2. Single-Block-Length Compressed Hash Blockchain

A blockchain is defined as a communication database communicated with the help of nodes through the Bitcoin protocol. Every block in the chain included hash of preceding block, timestamp (ts), as well as communication data (cd). UERSBLCHB Method uses Fugue hash function on 512-bit blocks of input information, and it handles the random size of inputs. The blockchain is illustrated in Figure 3.

RESEARCH ARTICLE

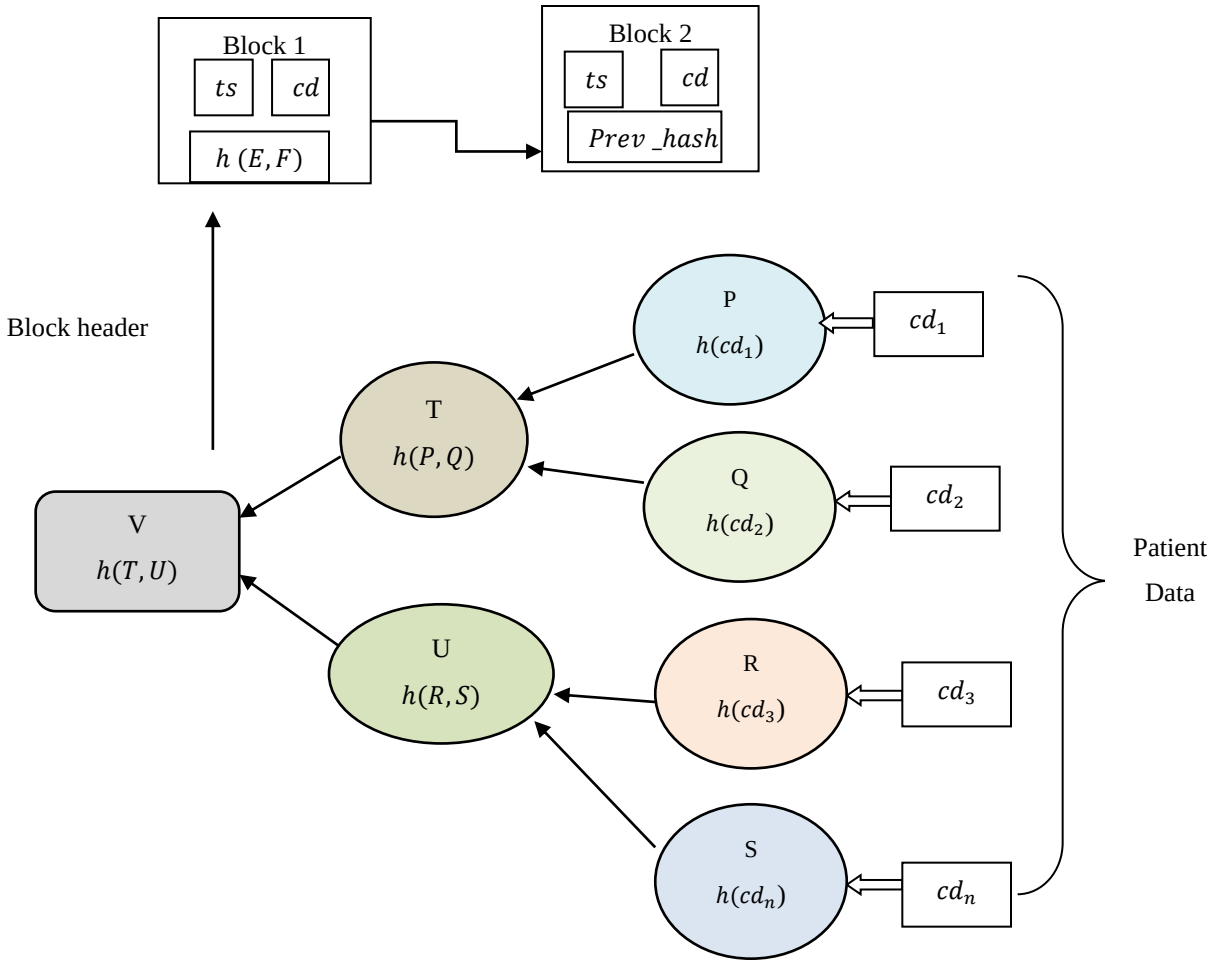

Figure 3 Blockchain Structure

The blockchain has blocks labelled ' P, Q, R, S, T, U, V '. As depicted in Figure 3, input patient data ' $cd_1, cd_2, cd_3, \ldots cd_n$ 'are sent to information block during blockchain. ' P, Q, R, S ' includes hash of information ('$h(cd_1)$,$h(cd_2)$,$h(cd_3)$,..$h(cd_n)$)'. 'T' comprises the hash of 'P' and 'Q'. The block 'U' includes the hash of 'R' and 'S'. After that, header 'V' includes the hash of the 'T' and 'U'.

Matyas–Meyer–Oseas Cryptographic Hash (MMOCH) function is used in blockchain to connect the random size data to the predetermined size of bit string termed as hash. For preserving information by arbitrary size as well as stored in database, fugue cryptographic hash function functions. MMOCH function creates a hash for every input patient information.

At first, the patient data is considered as input through arbitrary size. After that, the input patient data ' cd ' is separated into 'm' of fixed-size blocks. The patient data was processed one at period Matyas–Meyer–Oseas compression function (C_F). It is formulated as,

$$cd \rightarrow block_1, block_2, block_3, \ldots block_m \quad (4)$$

From equation (4), input patient data 'cd' and 'm' symbolizes the number of fixed block size ' $block_1, block_2, block_3, \ldots block_m$ '. Matyas–Meyer–Oseas compression function transforms two different input sizes to fixed -length output. Input block combined by compression function 'CF' and output of previous round by 512 bits. '$hash_0$'symbolizes a fixed primary hash value. It joins two inputs through different sizes as well as creates a predetermined hash value. It is formulated as,

$$hash_i = R_{E_{(hash_{i-1})}}(block_i) \oplus block_i \quad (5)$$

From equation (5), hash value of current block is '$hash_i$'. '$block_i$'symbolizes information block. '$hash_{i-1}$'represents the hash of the preceding round. '⊕' represents the XOR logical operator. ' R_E 'denotes secure block cipher for encrypting blocks by symmetric key 'k'. Confidentiality protects the information from being accessed through

RESEARCH ARTICLE

unauthorized entities. Final hash block '$hash_m$' formulated as,

$$HASH(cd) = hash_m \quad (6)$$

From equation (6), '$HASH$'symbolizes the last hash value of specific patient data 'cd'. '$hash_m$' denotes hash of whole information block. This information is created as well as broadcast to receiver. The receiver de-hashes patient information to achieve novel data. De-hash is termed as a decryption procedure. It is formulated as,

$$DEHASH(cd) = HASH(cd)^{-1} \quad (7)$$

From equation (7), $HASH(cd)^{-1}$symbolizes the hash inverse. Consequently, the de-hash process is carried out on every patient information block. It is calculated as,

$$block_i = R_D(hash_{i-1}) \oplus hash_i \quad (8)$$

From equation (8), '$hash_i$' symbolizes the hash value of the present block. '$block_i$' indicates information block, hash of preceding block is '$hash_{i-1}$'.'R_D'symbolizes secure block cipher to decrypt hash to a novel data block with identical symmetric key 'k' via encryption. Safe communication carried for healthcare applications.

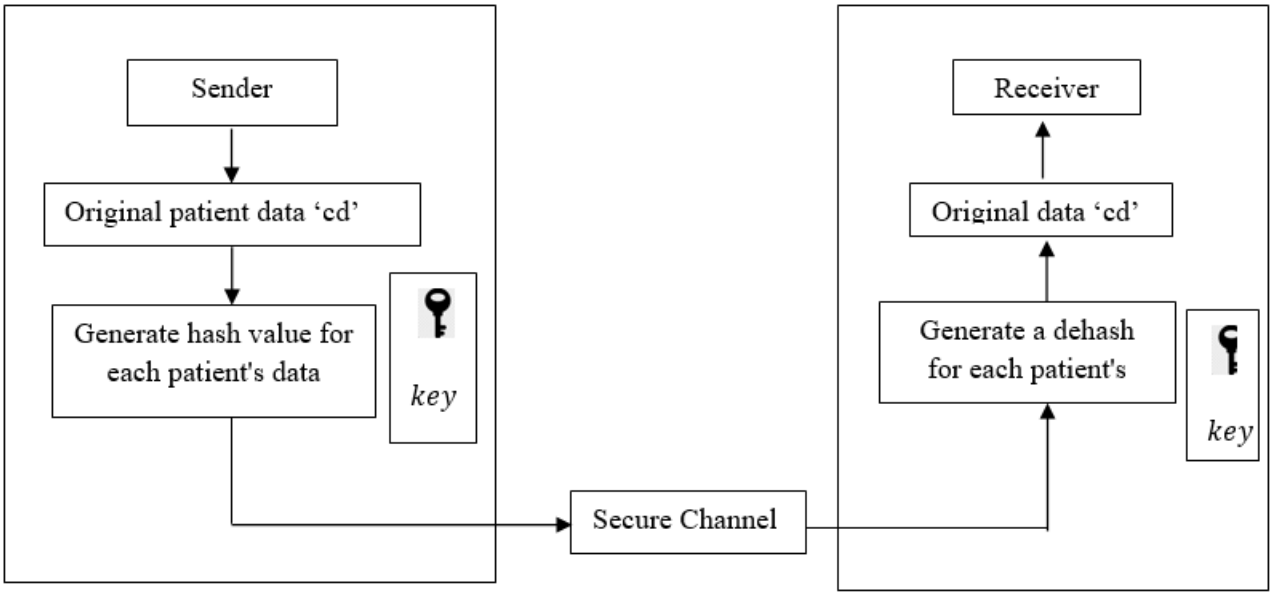

Figure 4 Secured Data Communication

Input: Dataset, patient data '$cd = cd_1, cd_2, \ldots, cd_n$'

Output: Increased data security

Begin

For individual patient data

Construction of blockchain

Partition 'cd' into blocks '$block_1, block_2, block_3, \ldots block_m$'

For individual block '$block_i$'

Generate hash value '$hash_i$' with symmetry key 'k'

End for

Ascertain the final hash $HASH(cd) = hash_m$

Sender transmits hashed data $HASH(cd)$ to the receiver

Receiver performs dehash$DEHASH(cd)$

For each hashed data

If ('k' is known to the receiver), then

Perform dehash

else

No dehash is carried out

End if

End for

Obtain original data 'cd'

End for

End

Algorithm 2 Single-Block-Length Compressed Hash Blockchain

As illustrated in Figure 4, secured data communication is performed between sender and receiver. The secret key 'k' is used to connect the sender and receiver. Encryption is carried out using the UERSBLCHB method during the hash

RESEARCH ARTICLE

generation process for every patient's data. The decryption is carried out using the UERSBLCHB Method on the receiver side to attain novel data for preserving patient data.

The algorithmic step of Single-Block-Length Compressed Hash Blockchain in the UERSBLCHB Method improves secured data communication. In the UERSBLCHB Method, the blockchain contains several blocks and data blocks. Input patient information is sent to the information block to create a hash for secured data communication. Through data communication in the UERSBLCHB Method, the blockchain uses the Matyas–Meyer–Oseascompression function. Input patient data are separated by several blocks. Matyas–Meyer–Oseascompression function creates a hash for every data block through block cypher encryption. Subsequently, novel patient data is converted to the ciphertext in hash value. After that, hashed patient information is sent to the receiver. When the receiver knows the key, the dehash process is carried out. This helps to enhance the secured data communication performance in the UERSBLCHB Method.

4. EXPERIMENTAL SETUP AND PERFORMANCE METRICS

The experimental evaluation of the UERSBLCHB Method is carried out with four existing data integrity auditing schemes [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4] are implemented using Java with the help of the MHEALTH dataset from https://www.kaggle.com/datasets/gaurav2022/mobile-health. The dataset included corresponding body activity and fundamental signs recordings attained from ten volunteers with different profiles carried out dissimilar corporal activities. The sensors are located on the chest to estimate motion registered by acceleration and so on. A sensor located on the chest provided 2-lead ECG measurements for heart monitoring and checking different arrhythmias. All sensing modalities are recorded at a sampling rate of 50 Hz to achieve human motion, which is recorded through a video camera.

Performance analysis of the UERSBLCHB technique and existing methods, namely data integrity auditing scheme [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4] are carried out with data confidentiality rate, data integrity rate, processing time, accuracy, and space complexity.

4.1. Data Confidentiality Rate

It refers to several patient healthcare data that are viewed through an authorized entity. It is estimated in in percentage (%).

$$D_{CR} = \left(\frac{n_a}{n}\right) * 100 \quad (9)$$

From equation (9), 'D_{CR}'symbolizes data confidentiality rate. 'n_a' represents the patient data accessed or viewed by an authorized entity, and 'n'symbolizes entire number of patient data.

Table 1 Tabulation of Data Confidentiality Rate

Number of Patient Data	Data Confidentiality Rate (%)				
	Data Integrity Auditing Scheme	TDCB-D3P scheme	DeBlock-Sec scheme	LightMED	Proposed UERSBLCHB Method
500	75	79	82	85	90
1000	77	81	84	87	93
1500	79	83	87	89	95
2000	76	80	85	86	94
2500	74	78	82	84	92
3000	72	76	80	82	90
3500	75	77	83	85	93
4000	77	80	84	88	95
4500	78	82	86	90	96
5000	80	84	88	93	98

RESEARCH ARTICLE

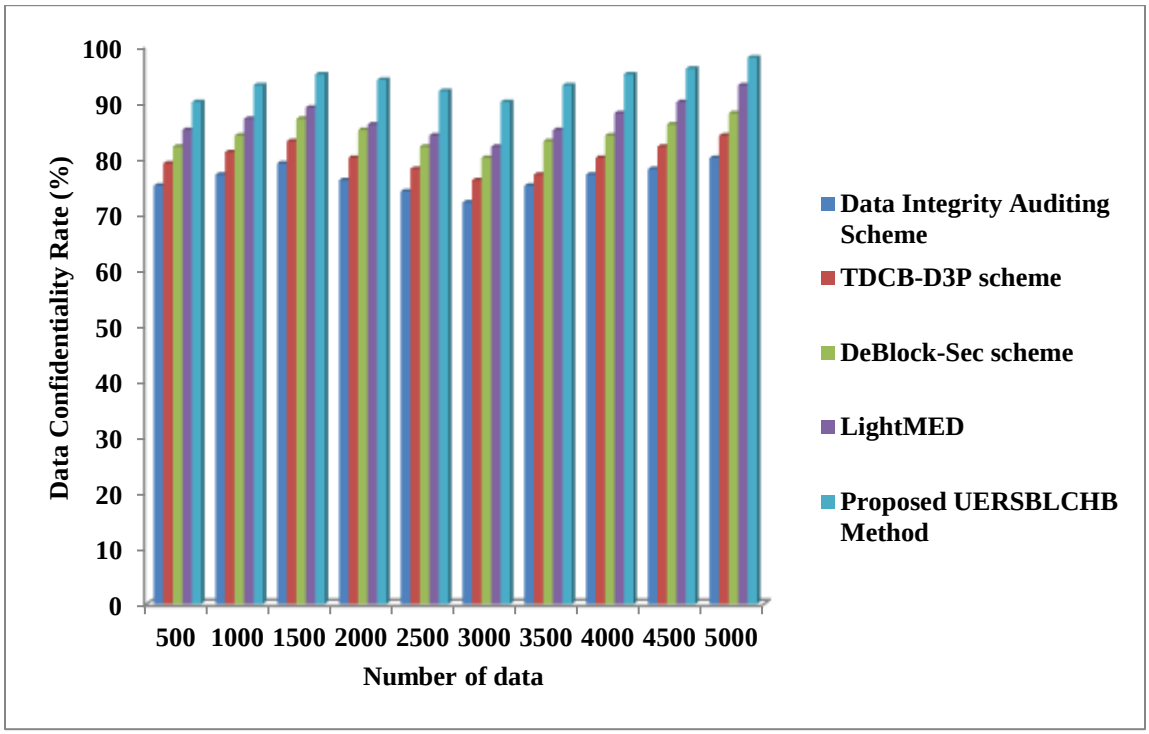

Figure 5 Measurement of Data Confidentiality Rate

Table 1 and Figure 5 explain the comparative analysis of D_{CR} for different patient data. D_{CR} of the UERSBLCHB method, data integrity auditing scheme [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4], are represented by cones, namely orange, blue, brown, green, and violet. From graph analysis, the UERSBLCHB method attains higherr D_{CR} than conventional techniques. For instance, simulations are carried out with 3500 patient data. D_{CR} was examined by 93% using the proposed UERSBLCHB method, whereas 75%, 77%, 83%, and 85% using existing [1], [2], [3], and [4], respectively. From the graph, the UERSBLCHB method attains higherr D_{CR} than other conventional methods. Contrary to existing methods, bivariate correlative universal estimator regressive data analysis and Single-Block-Length Compressed Hash Blockchain are utilized in UERSBLCHB.

Universal estimator regression is to classify the collected patient data via bivariate correlative. Matyas–Meyer–Oseas Cryptographic Hash-based Blockchain carried out safe data communication through hash value generation for each patient data via block cipher encryption. The original patient data is modified into the ciphertext in hash value. Hashed patient data are transmitted to the receiver. When the receiver knows the key, dehash process is performed. In this way, the data confidentiality is enhanced. Overall performance outcomes represent that D_{CR} using the UERSBLCHB method is considerably enhanced by 23%, 17%, 11%, and 8% than the [1], [2], [3], and [4].

4.2. Integrity

It is defined as a number of patient data not modified via some illegal entity.

$$D_{IR} = \left[\frac{nn_a}{n}\right] * 100 \quad (10)$$

From equation (10), ' D_{IR} 'represents the data integrity rate.' nn_a ' symbolizes several patient information not modified through unauthorized entities. It is measured in percentage (%).

Table 2 and Figure 6 illustrate the comparative analysis of D_{IR} for dissimilar patient data. The $D_{IR}$of proposed UERSBLCHB method, data integrity auditing scheme [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4] are represented as orange, blue, brown, green, and violet. From graph analysis, the UERSBLCHB method attains enhanced D_{IR} than the other conventional methods. For instance, simulations are carried out with 4500 patient data. Integrity obtained as 94% using proposed UERSBLCHB method, whereas 73%, 77%, 83%, and 86% using existing [1], [2], [3], and [4], respectively. From the graph, the UERSBLCHB method attains enhanced D_{IR} when compared to conventional methods. Contrary to obtainable methods, bivariate correlative universal estimator regressive data analysis and Single-Block-Length Compressed Hash Blockchain are developed in UERSBLCHB. The bivariate correlative is used to examine patient data by Universal estimator regression.

RESEARCH ARTICLE

Protected data communication is obtained with Matyas–Meyer–Oseas Cryptographic Hash-based Blockchain during hash value generation for every patient data. Hash value is stored in blockchain with higher data integrity. Overall performance of ten outcomes indicates that D_{IR} using the UERSBLCHB method is considerably increased by 26%, 10%, 13%, and 8% than the [1], [2], [3], and [4].

Table 2 Tabulation of Data Integrity Rate

Number of Patient Data	Data Integrity Rate (%)				
	Data Integrity Auditing Scheme	TDCB-D3P scheme	DeBlock-Sec scheme	LightMED	Proposed UERSBLCHB Method
500	73	79	82	87	92
1000	75	81	84	89	94
1500	74	78	81	86	93
2000	72	76	79	83	90
2500	73	77	82	85	92
3000	76	79	84	87	95
3500	74	76	82	85	93
4000	72	74	81	83	91
4500	73	77	83	86	94
5000	75	79	85	88	96

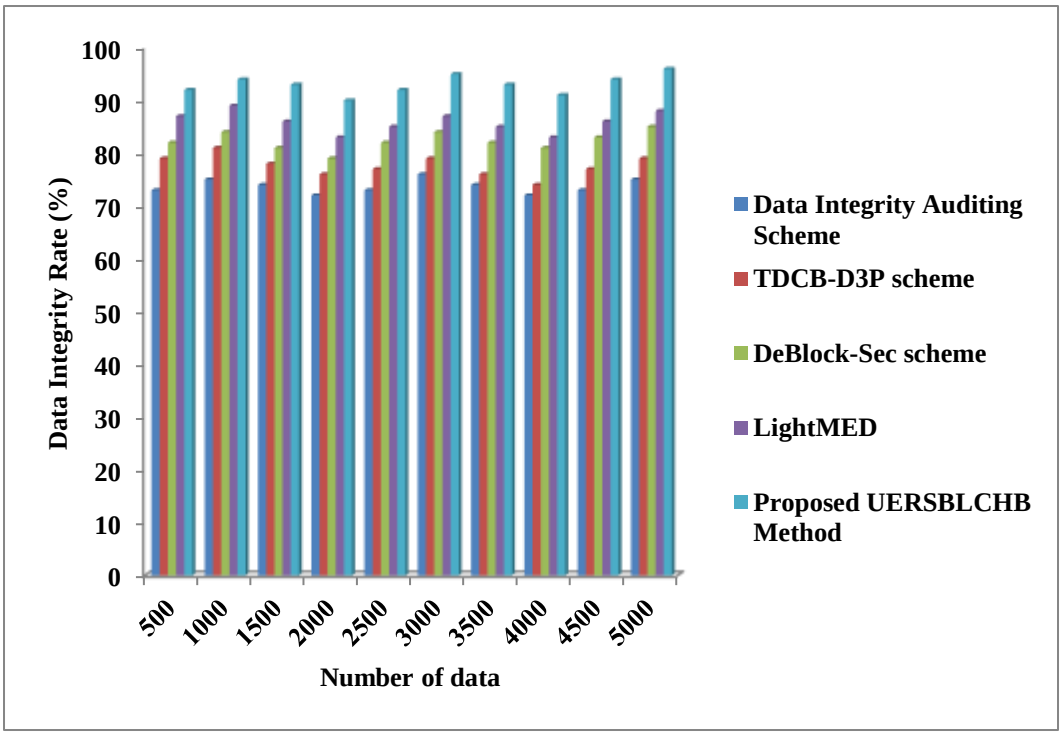

Figure 6 Measurement of Data Integrity Rate

RESEARCH ARTICLE

4.3. Processing Time

It is described as time consumed through an algorithm to carry out safe data transmission. It is determined as,

$$T_{Pro} = n * t[cd] \quad (11)$$

From equation (11),'T_{Pro}' symbolizes the processing time. From equation (11),'T_{Pro}' symbolizes the processing time. Time utilization for processing one patient data is '$t[cd]$'. It is computed in milliseconds (ms).

Table 3 Comparison of Processing Time

Number of Patient Data	Processing Time (ms)				
	Data Integrity Auditing Scheme	TDCB-D3P scheme	DeBlock-Sec scheme	LightMED	Proposed UERSBLCHB Method
500	54	48	35	27	15
1000	57	50	38	29	18
1500	59	52	40	31	20
2000	61	55	42	34	23
2500	63	58	45	37	25
3000	65	60	48	39	27
3500	68	62	50	42	29
4000	70	64	52	43	31
4500	72	67	55	46	33
5000	75	70	58	49	35

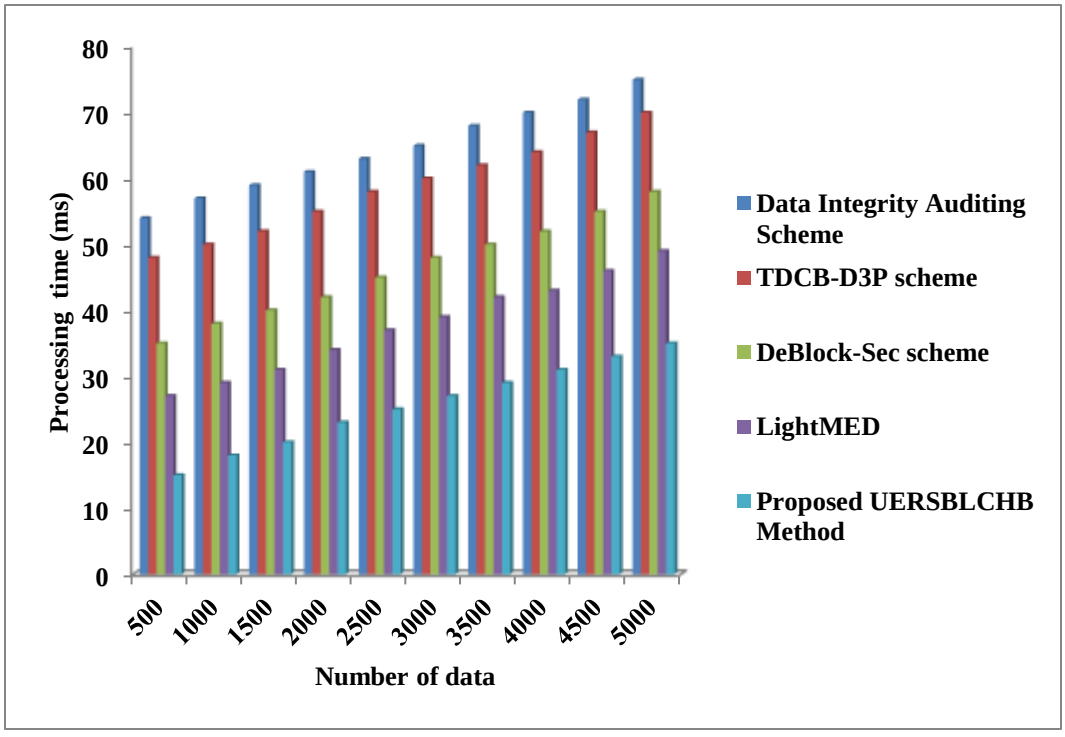

Figure 7 Measurement of Processing Time

RESEARCH ARTICLE

Table 3 and Figure 7 illustrate the processing time for dissimilar patient data. Processing time of the proposed UERSBLCHB method, data integrity auditing scheme [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4] are indicated by orange, blue, brown, green, and violet. From graph analysis, the UERSBLCHB method attains lesser processing time than other existing methods. For instance, simulations are conducted with 3000 patient data. The processing time was observed to be 27ms using the proposed UERSBLCHB method, whereas 65ms, 60ms, 48ms, and 39ms using existing [1], [2], [3], and [4], respectively. From graph analysis, the UERSBLCHB method attains lesser processing time than the other conventional methods. This is because of the use of universal estimator regression to categorize the collected data. Matyas–Meyer–Oseas broadcasts safe data through hash value generation for every patient data. Then, the hashed results are saved to the blockchain. This helps to reduce processing time. The overall performance of ten outcomes indicates that processing time using the UERSBLCHB technique is considerably minimized by 61%, 57%, 46%, and 33% than the [1], [2], [3], and [4], respectively.

4.4. Accuracy

It referred to the proportion of number of patient data categorized.

$$Acc = \frac{Number\ of\ patient\ data\ that\ are\ correctly\ analyzed\ and\ classified}{n} \quad (12)$$

From equation (12), 'Acc' symbolizes the accuracy level. It is measured in percentage (%).

Table 4 Comparison of Accuracy

Number of Patient Data	Accuracy (%)				
	Data Integrity Auditing Scheme	TDCB-D3P scheme	DeBlock-Sec scheme	LightMED	Proposed UERSBLCHB Method
500	68	72	79	84	91
1000	70	73	81	86	93
1500	69	71	80	85	92
2000	67	69	78	83	90
2500	69	70	79	86	91
3000	68	72	81	87	94
3500	70	74	83	89	92
4000	72	76	84	90	95
4500	71	75	82	88	94
5000	73	77	83	89	96

Table 4 and Figure 8 illustrate the accuracy of different patient data. Accuracy of the proposed UERSBLCHB method, data integrity auditing scheme [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4] are indicated by orange, blue, brown, green, and violet. For instance, simulations are conducted with 2000 patient data. Here, the accuracy was observed to be 90% using the proposed UERSBLCHB method, whereas 67%, 69%, 78%, and 83% using existing [1], [2], [3], and [4], respectively. From graph analysis, the UERSBLCHB method attains higher accuracy than conventional techniques. This is because of the use of universal estimator regression in the proposed UERSBLCHB method for analyzing and classifying the collected data with maximum accuracy. This helps to improve the accuracy level. The overall performance of ten outcomes indicates that accuracy using the UERSBLCHB technique is considerably enhanced by 61%, 57%, 46%, and 33% than the [1], [2], [3], and [4].

RESEARCH ARTICLE

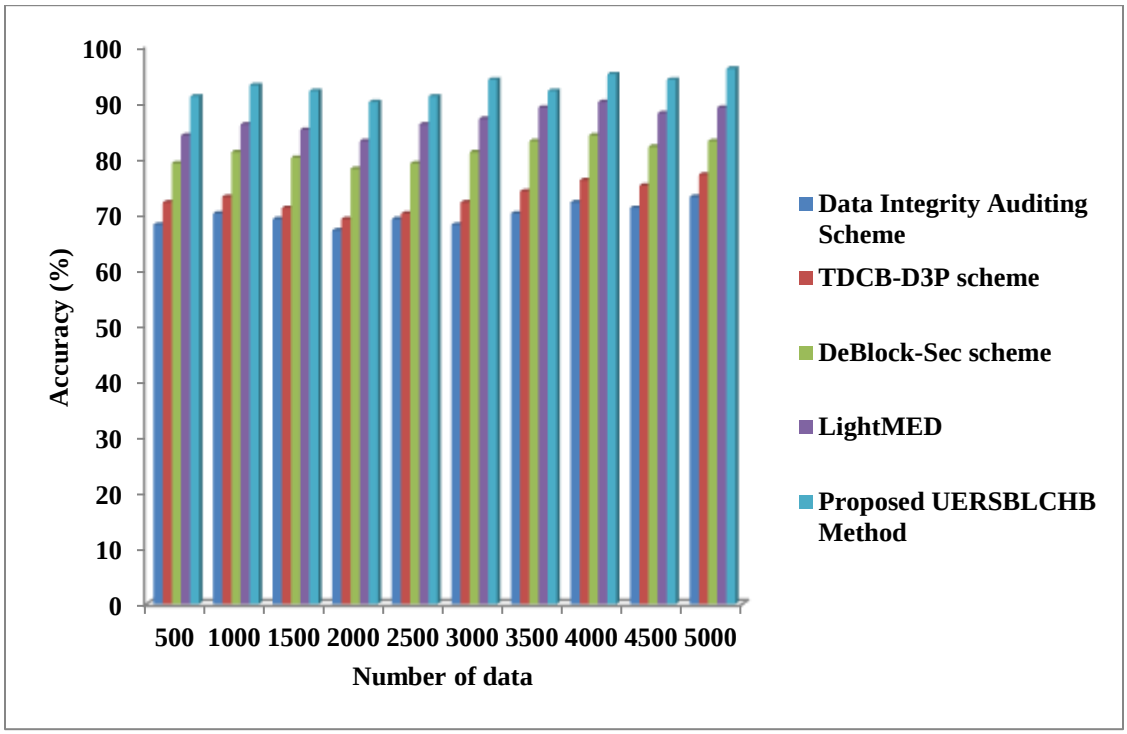

Figure 8 Measurement of Accuracy

4.5. Space Complexity

It is referred to as a product of several patient data and the amount of memory space of storage space consumed by the algorithm for storing the values such as block generation, hashing, and dehashing during data communication. The space complexity is computed in kilobytes (KB).

$$SC = n * MC(block\ generation + Hasing + Dehasing) \quad (13)$$

From equation (13), 'SC' symbolizes space complexity. 'MC' represents memory consumption. It is computed in terms of kilobytes (KB).

Table 5 Comparison of Space Complexity

Number of Patient Data	Space Complexity (KB)				
	Data Integrity Auditing Scheme	TDCB-D3P scheme	DeBlock-Sec scheme	LightMED	Proposed UERSBLCHB Method
500	48	41	34	29	21
1000	50	43	36	32	23
1500	52	46	39	34	24
2000	55	48	41	37	26
2500	58	51	43	39	28
3000	60	53	45	42	31
3500	63	55	47	44	33
4000	66	58	50	46	35
4500	68	60	53	48	37
5000	70	62	56	49	40

RESEARCH ARTICLE

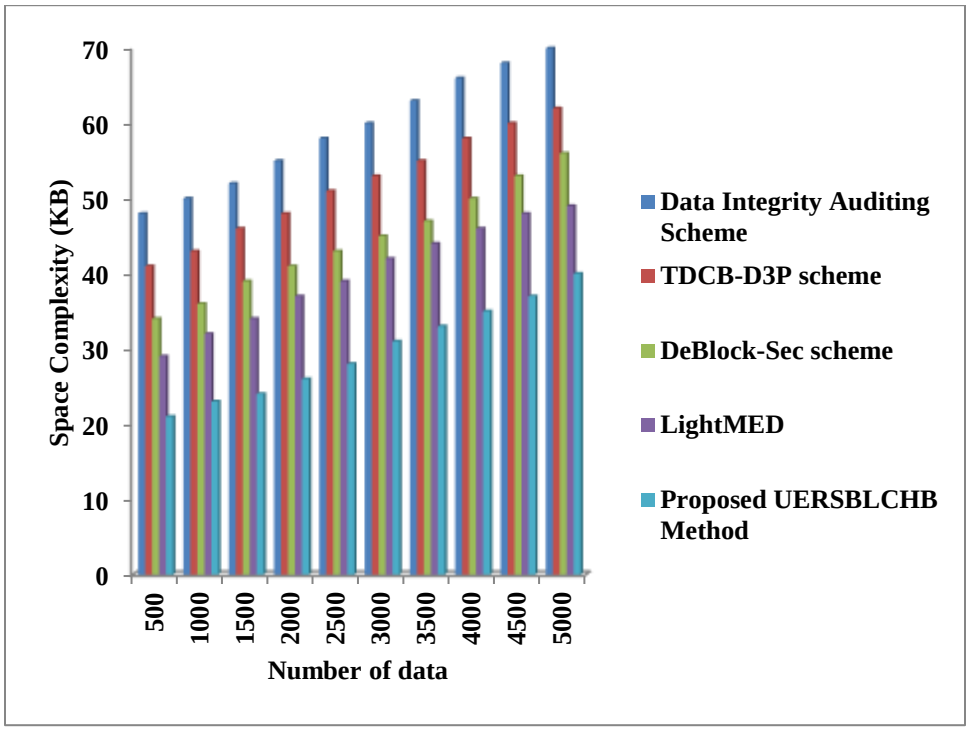

Figure 9 Measurement of Space Complexity

Table 5 and Figure 9 illustrate the comparative space complexity analysis for different patient data. Space complexity of the proposed UERSBLCHB method, data integrity auditing scheme [1], TDCB-D3P scheme [2], DeBlock-Sec scheme [3], and LightMED [4] are indicated by orange, blue, brown, green, and violet. From graph analysis, the UERSBLCHB method attains lesser space complexity than other existing methods. For instance, simulations are conducted with 4000 patient data. The space complexity was observed to be 35KB using the proposed UERSBLCHB method, whereas 66KB, 58KB, 50KB, and 46KB using existing [1], [2], [3], and [4], respectively. From graph analysis, the UERSBLCHB method attains lesser space complexity than conventional methods. Contrary to conventional, UERSBLCHB method attains lesser space complexity. Universal Estimator Regression for analyzing and classifying the collected data based on the geometric median. Safe data broadcast achieved by Blockchain through hash value generation for each patient data. After that, hashed results are saved to the blockchain. This helps to reduce SC. Overall performance of ten outcomes indicates that the SC using the UERSBLCHB method is considerably reduced by 50%, 43%, 33%, and 26% than the [1], [2], [3], and [4], respectively.

5. DISCUSSION

In this section, the objective of the proposed UERSBLCHB method is to enhance accuracy, data integrity and confidentiality and minimum time. Based on this objective, the proposed UERSBLCHB, existing [1], [2], [3] and [4] are compared by using the MHEALTH dataset. The reason for less processing time is to apply Universal Estimator Regression for analyzing the patient information. The reason for higher accuracy, confidentiality, and integrity is to apply Matyas–Meyer–Oseas Cryptographic Hash-based Blockchain for secure data transmission. From the overall analysis of results, the following summary key findings are achieved: The proposed UERSBLCHB method achieved higher accuracy by 20%, confidentiality by 15%, and integrity by 17% when compared [1] [2] [3] and [4]. The UERSBLCHB method also minimizes the processing time by 49% and space complexity by 38% when compared to existing methods. In a comparative analysis, the UERSBLCHB method provides better performance for secure data transmission in cloud.

6. CONCLUSION

Secure data communication helps to improve the user experience in different IoT applications. However, the communication resulted in data leakage. To guarantee data confidentiality and integrity, a secure data communication called the UERSBLCHB method is proposed using blockchain technology to protect data privacy. Universal Estimator Regression analyzes and classifies the collected data. Matyas–Meyer–Oseas Cryptographic Hash-based Blockchain method performed safe data broadcast. Data broadcast is attained by Matyas–Meyer–Oseas Cryptographic

RESEARCH ARTICLE

Hash-basis of Blockchain. Hash value generated with Matyas–Meyer–Oseas. Through this method, effective data communication is performed with higher security and minimum processing time. The assessment performance analysis demonstrates that it outperforms well in attaining enhanced data confidentiality and integrity rates by minimum processing time and space complexity compared to conventional techniques.

REFERENCES

[1] Yi Li and Meiqin Tang, “Blockchain-powered distributed data auditing scheme for cloud-edge healthcare system”, Cyber Security and Applications, Elsevier, Volume 1, December 2023, Pages 1-15.

[2] Yunyeong Goh, Jusik Yun, Dongjun Jung, and Jong-Moon Chung, “Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning”, IEEE Access, Volume 10, November 2022, Pages 118498 – 118511.

[3] Uma Narayanan, Varghese Paul and Shelbi Joseph, “Decentralized blockchain based authentication for secure data sharing in Cloud-IoT”, Journal of Ambient Intelligence and Humanized Computing, Springer, Volume 9, 2023, Pages 349–368.

[4] Somchart Fugkeaw, Leon Wirz and Lyhour Hak, “Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing”, IEEE Access, Volume 11, June 2023, Pages 62998 – 63012.

[5] Yin Zhang, Ling Xiong, Fagen Li, Xianhua Niu and Hanzhou Wu, “A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing”, Journal of Systems Architecture, Elsevier, Volume 142, September 2023, Pages 1-17.

[6] Anichur Rahman, Md Jahidul Islam, Shahab S. Band, Ghulam Muhammad, Kamrul Hasan and Prayag Tiwari, “Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT”, Digital Communications and Networks, Elsevier, Volume 9, Issue 2, April 2023, Pages 411-421.

[7] Xixi Yan, Suwei Feng, Yongli Tang, Pei Yin and Dazhi Deng, “Blockchain-based verifiable and dynamic multi-keyword ranked searchable encryption scheme in cloud computing”, Journal of Information Security and Applications, Elsevier, Volume 71, December 2022, Pages 1-15.

[8] Chunlin Li, Song Yu Liang, Jing Zhang, Qiao-e Wang and Youlong Luo, “Blockchain-based Data Trading in Edge-cloud Computing Environment”, Information Processing & Management, Elsevier, Volume 59, Issue 1, January 2022, Pages 1-14.

[9] Yinghui Zhang, Robert H. Deng, Ximeng Liu and Dong Zheng, “Blockchain based efficient and robust fair payment for outsourcing services in cloud computing”, Information Sciences, Elsevier, Volume 462, September 2018, Pages 262-277.

[10] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand and V. Vasudevan, “Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm”, Materials Today: Proceedings, Elsevier, Volume 37, Part 2, 2021, Pages 2653-2659.

[11] Zhenpeng Liu, Shuo Wang and Yi Liu, “Blockchain-based integrity auditing for shared data in cloud storage with file prediction”, Computer Networks, Elsevier, Volume 236, November 2023, Pages 1-15.

[12] Changping Liu, “HPCLS-BC: A novel blockchain framework using heterogeneous peer-node and cloud-based ledger storage for Internet of Things applications”,Future Generation Computer Systems, Elsevier, Volume 150, January 2024, Pages 364-379.

[13] T. Benil, J. Jasper “Blockchain based secure medical data outsourcing with data deduplication in cloud environment”, Computer Communications, Elsevier, Volume 209, 1 September 2023, Pages 1-13.

[14] Khaleel Mershad and Hayssam Dahrouj, “Blockchain model for environment/infrastructure monitoring in cloud-enabled high-altitude platform systems”,Vehicular Communications, Elsevier, Volume 42, August 2023, Pages 1-15.

[15] Qing Liu, Xiaojun Zhang, Jingting Xuea, Rang Zhou, Xin Wang and Wei Tang, “Enabling blockchain-assisted certificateless public integrity checking for Industrial cloud storage systems”, Journal of Systems Architecture, Elsevier, Volume 140, July 2023, Pages 1-15.

[16] Ragu, G., and S. Ramamoorthy. "A blockchain-based cloud forensics architecture for privacy leakage prediction with cloud." Healthcare Analytics 4 (2023): 100220.

[17] Ahmad, Haris, and Gagangeet Singh Aujla. "GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment." Computers and Electrical Engineering 109 (2023): 108747.

[18] Li, Qi, et al. "CBFF: A cloud–blockchain fusion framework ensuring data accountability for multi-cloud environments." Journal of Systems Architecture 124 (2022): 102436.

[19] Duan, Li, et al. "BSAF: A blockchain-based secure access framework with privacy protection for cloud-device service collaborations." Journal of Systems Architecture 140 (2023): 102897.

[20] Almasian, Mohammadpayam, and Alireza Shafieinejad. "Secure cloud file sharing scheme using blockchain and attribute-based encryption." Computer Standards & Interfaces 87 (2024): 103745.

[21] Shinde, Sahadev Maruti, and Venkateswara Rao Gurrala. "Securing trustworthy evidence for robust forensic cloud-blockchain environment for immigration management with improved ECC encryption." Expert Systems with Applications 229 (2023): 120478.

[22] Dharavath Ramesh, Rahul Mishra, Pradeep K. Atrey, Damodar Reddy Edla, Sanjay Misra and Lianyong Qi “Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage”,Alexandria Engineering Journal, Elsevier, Volume 68, 1 April 2023, Pages 205-226.

[23] Martinez-Rendon, Cristhian, et al. "CD/CV: Blockchain-based schemes for continuous verifiability and traceability of IoT data for edge–fog–cloud." Information Processing & Management 60.1 (2023): 103155.

[24] Aggarwal, Priya, et al. "BPADTA: Blockchain-based privacy-preserving authentication scheme for digital twin empowered aerospace industry." Computers and Electrical Engineering 111 (2023): 108889.

[25] Azzaoui, Abir EL, Pradip Kumar Sharma, and Jong Hyuk Park. "Blockchain-based delegated Quantum Cloud architecture for medical big data security." Journal of Network and Computer Applications 198 (2022): 103304.

[26] Zeshun Shi, Huan Zhou, Cees de Laat and Zhiming Zhao, “A Bayesian game-enhanced auction model for federated cloud services using blockchain”,Future Generation Computer Systems, Elsevier, Volume 136, November 2022, Pages 49-66.

[27] Prasad, S. Navin, and C. Rekha. "Block chain based IAS protocol to enhance security and privacy in cloud computing." Measurement: Sensors 28 (2023): 100813.

[28] Sharma, Pratima, Rajni Jindal, and Malaya Dutta Borah. "Blockchain-based decentralized architecture for cloud storage system." Journal of Information Security and Applications 62 (2021): 102970.

[29] Shufen Niu, Mi Song, Lizhi Fang, Fei Yu, Song Han and Caifen Wang, “Keyword search over encrypted cloud data based on blockchain in smart medical applications”, Computer Communications, Elsevier, Volume 192, 1 August 2022, Pages 33-47.

[30] Tiantong Wu, Guillaume Jourjon Kanchana Thilakarathna and Phee Lep Yeoh, “MapChain-D: A Distributed Blockchain for IIoT Data Storage and Communications”, IEEE Transactions on Industrial Informatics, Volume 19, Issue 9, September 2023, Pages 9766 – 9776.

[31] Marrium Yusuf & Dr. Bhupesh Gour, “An Efficient Signcryption Based Data Sharing in Public Clouds with Message Verification”, International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February 2016, Pages 1-8.

RESEARCH ARTICLE

[32] Y. Sreenivasa Rao, "A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing", Future Generation Computer Systems, Volume 67, 2017, Pages 133-151.
[33] Deepnarayan Tiwari and G. R. Gangadharan, "SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation", International Journal of Communication Systems, Volume 31, Issue 5, 2018, Pages 1-28.
[34] Shangping Wang, Xu Wang, Yaling Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain", IEEE Access, Volume 7, 2019, Pages 112713 –112725.
[35] Leyou Zhang, Yilei Cui , and Yi Mu "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing", IEEE Systems Journal, Volume 14, Issue 1, 2020, Pages 387-397.
[36] Shivi Chaturvedi, "Clinical Prediction on ML based Internet of Things for E-Health Care System", International Journal of Data Informatics and Intelligent Computing, Volume 2, Issue 3, 2023, Pages 29–37.
[37] Shivi Chaturvedi, "IoT-Based Secure Healthcare Framework Using Blockchain Technology with A Novel Simplified Swarm-Optimized Bayesian Normalized Neural Networks", International Journal of Data Informatics and Intelligent Computing, Volume 2, Issue 2, 2023, Pages 63–71.
[38] Priyanka Tyagi, S. K. Manju Bargavi. "Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain", International Journal of Data Informatics and Intelligent Computing, Volume 2, Issue 1, 2023, Pages 1–10.
[39] Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta. "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0", Infrastructures, Volume 8, Issue 2, 2023, Pages 22.
[40] Osamah Ibrahim Khalaf, Rajesh Natarajan, Natesh Mahadev, Prasanna Ranjith Christodoss, Thangarasu Nainan, Carlos Andrés Tavera Romero, Ghaidaa Muttasher Abdulsaheb "Blinder Oaxaca and Wilk Neutrosophic Fuzzy Set-based IoT Sensor Communication for Remote Healthcare Analysis", IEEE Access, 2022.

Authors

Shanmugapriya Velmurugan received her Ph.D Degree from Periyar University, Salem in the year 2020. She has received her M.Phil Degree from Periyar University, Salem in the year 2007. She has received her M.C.A Degree from Madurai Kamaraj University, Madurai in the year 2002. She is working as Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College Coimbatore, Tamilnadu, India She has 19 years of experience in academic field. She has published 1 book, 15 International Journal papers and 26 papers in National and International Conferences. Her areas of interest include Big Data, Artificial Intelligence and Data Mining.

Amalraj Irudayasamy completed his Ph.D. in Computer Science from Peiyar University, Master of Science from Bharadhidasan University and Bachelor's in Computer science from Madras University. He is currently working as a Lecturer at University of Technology and Applied Sciences-Nizwa, Sultanate of Oman. His research interest includes Cloud Computing, Data Science and Big Data Analytics. He has presented articles in the National and International conferences also published articles in reputed indexed journals and SCOPUS.

Natesh Mahadev completed his PhD in computer science and engineering in Visveswaraya technological university (VTU), MTech from Visvesvaraya Technological University (VTU), B.E (CSE) from VTU. Currently he is working as Associate professor in the department of Computer science and engineering in Vidya vardhaka college of engineering, Mysore, Karnataka, India. His research interests include Digital image processing, Blockchain, Machine learning, Artificial Intelligence, Data science. He has published a various paper in reputed National and international journals.

Rajesh Natarajan completed his PhD in Computer Science from Bharathiar University, Master of Computer Application from Thiruvalluvar University and BSc in Computer Science from Madras University. He works as a Lecturer at the University of Technology and Applied Sciences-Shinas, Sultanate of Oman. His founder and chief editor for the International Journal of Data Informatics and Intelligent Computing. His research interests include Data Mining, Machine Learning, Big Data Analytics, Blockchain Technology, and Data Privacy and Security. He has presented articles at national and international conferences and has published articles in reputed indexed journals like WoS and SCOPUS.

Sujatha Krishna received the B.E. and M. Tech degrees in Computer Science and Engineering from Visvesvaraya Technological University, Karnataka, India. She received Ph.D. degree in Computer Science and Engineering from REVA University, Karnataka, India. She is currently working as a Lecturer at University of Technology and Applied Sciences-Shinas, Sultanate of Oman. Her research interests include big data, data mining, machine learning and privacy preserving algorithms.

How to cite this article:

Shanmugapriya Velmurugan, Amalraj Irudayasamy, Natesh Mahadev, Rajesh Natarajan, Sujatha Krishna, " Securing Data Communication in the Cloud Using Machine Learning-Based Blockchain Approach ", International Journal of Computer Networks and Applications (IJCNA), 11(4), PP: 540-555, 2024, DOI: 10.22247/ijcna/2024/35.