EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Blockchain- Based Secure and Efficient Scheme for Medical Data

Manish Kumar Gupta[1,*], Rajendra Kumar Dwivedi[2]

[1,2] Department of Information Technology, Madan Mohan Malaviya University of Technology, U P, India, 273010.

Abstract

Internet of Things (IoT) fog nodes are distributed near end-user devices to mitigate the impacts of low delay, position awareness, and spatial spread, which aren't permitted by numerous IoT apps. Fog computing (FC) also speeds up reaction times by decreasing the quantity of data sent to the cloud. Despite these advantages, FC still has a lot of work to do to fulfill security and privacy standards. The constraints of the FC resources are the cause of these difficulties. In reality, FC could raise fresh concerns about privacy and security. Although the Fog security and privacy problems have been covered in several articles recently, most of these studies just touched the surface of these difficulties. This paper provides a unique solution for the authentication of data by using hyperledger fabric. The fog layer store data transferred by the IoT layer and calculate the hash value. These hash values are now stored in hyperledger fabric for authentication purposes. The proposed model results compared with lewako's and Fan's scheme and found that the proposed model has 25.00 % less encryption time, 09.3 % less decryption time, 17.48 % less storage overhead, and 23.38 % less computation cost as compared to Fan's scheme.

Keywords : IoT, Data, Fog Computing, Hyperledger Fabric, Hash value.

Received on 12 April 2023, accepted on 12 June 2023, published on 28 June 2023

Copyright © 2023 Gupta *et al.*, licensed to EAI. This is an open access article distributed under the terms of theCC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetsis.3235

*Corresponding author. Email:manish.testing09@gmail.com

1. Introduction

Medical Big Data (BD) are the more crucial historical documents that the patient will use to make the subsequent diagnoses and treatments. Cross-institutional medical data sharing has become a popular area of study to tackle the problem of data islands in the established healthcare delivery system. To enable cross-institutional medical data sharing between the traditional independent healthcare delivery system, blockchain (BC) technology has recently been used to create a distributed environment [39], [40]. Over the decennary, Cloud Computin (CC) has evolved as an efficient platform for fulfilling the needs of end consumers for cloud data servers to fulfill their demands [1]. In the last few years, there has been a significant rise in demand for IoT-based linked devices and apps. Examples include smartphones, gadgets, Google Glass, etc. [2]. Abbasi and Shah predict that by 2020, there may be 50 billion Internet-connected gadgets (each individual will have, on average, 6.58 connected devices), and by 2025, there may be 500 billion [3]. IoT devices offer a wealth of capabilities, including connectivity, and the creation of additional functionality is frequently driven by data. These IoT devices generate enormous amounts of heterogeneous data that must be evaluated, necessitating enormous amounts of storage space, computational power, and network bandwidth. Additionally, a lot of IoT applications need high-speed or real-time analysis. According to [5], the Fog system can be defined as

- It will be situated at the network's edge.
- It's own networking, computer, and storage services;
- Provides hardware and software deployment options that are affordable, adaptable, and portable.

A fog system differs from CC in several ways. The following list provides details on some of the more well-known [6-8].

- A FC will have lesser computational resources than a CC.
- They can process data produced by a variety of gadgets;
- Depending on the area, they can be both widely and sparingly dispersed;
- It is feasible to construct a Fog system using low-end hardware.

1.1 Motivation

BC is a new and advanced technology to secure near or far digital data. Most customers use online transactions for their daily life needs, which leads to an exponential amount of digital data. Motivated by BC technology, propose a new variety of security for end-user data.

1.2 Contribution

The contribution of the paper is folded by the following points.

i. Data transfer from the end user (IoT Layer) to Fog Layer.
ii. Two operations perform at Fog Layer
  a. Data directly transfer from Fog Layer to Cloud Layer.
  b. Hash value (HV) calculated at Fog layer and transferred to Hyperledger fabric.
  c. HV transfer from Hyperledger Fabric to Cloud Layer.
iii. Cloud Layer calculates the HV of data (data received from Fog Layer) and match it with the HV which is received from Hyperledger fabric.

2. Background

One of the most common noxious technologies today, BC is opening the mode for new financial and industrial applications [11]. Conceptually, it is made up of a collection of records, or blocks, where the information is kept and encrypted to provide privacy and security. Additionally, unlike previous technologies, BC is a decentralized network in which all users have full authority to peer-to-peer (P2P) monitor all network transactions [12]. Based on their fields of application, BC platforms can be divided into three categories: public, private, and hybrid BCs [13]. A public BC is open to all members of the network and does not have a single proprietor. As an example of a decentralized public BC, Bitcoin makes the consensus procedure reachable to all network users. On the other hand, private BC has access restrictions that limit who can read from and write to the BC. In hybrid BCs, only a small set of users have access to the public ledger. The consensus process is governed by rules that have been agreed upon by all stakeholders governing control and access over the BC in this somewhat decentralized environment. Table 1 provides a comparative Analysis of different BC platform and Table 2 provide an abbreviation used in a Comparative Analysis of different BC platform.

Table 1. Comparative Analysis of Different BC Platforms

		BC Platforms								
		Bitcoin	**Ethereum**	**Ripple**	**Cardano**	**Cosmos**	**Polkadot**	**Elrond**	**Avalanche**	**Solana**
	Consensus Mechanism	**PoW**	**PoW**	**RPCA**	**PoS**	**BPoS**	**NPoS**	**SPoS**	**DPoS, DAG**	**DPoS**
Technology Capabilities	**Consensus Energy Consumption**	H	H	L	L	L	L	L	L	L
	Block Time (S)	600	14	4	20	7	6	6	3	8
	Level of Decentralization	H	H	M	H	H	H	H	M	L
	Smart Contract	Y	Y	N	Y	Y	Y	Y	Y	Y
	dApps	N	Y	N	Y	Y	Y	Y	Y	Y
	DEX	N	Y	Y	Y	Y	Y	Y	Y	Y

DeFi	N	Y	N	Y	Y	Y	Y	Y	Y
OChG	N	N	Y	N	Y	Y	X	N	N
HRAdd	N	Y	N	N	Y	N	Y	N	Y
DIM	N	Y	N	N	Y	N	Y	N	N
Data Privacy	N	N	N	N	Y	N	X	N	N
DiClSt	N	Y	N	N	Y	N	X	N	N
DiClCo	N	Y	N	N	Y	N	X	N	N
Interoperability	N	N	N	N	Y	Y	N	N	N
Cross Communication	N	N	N	N	Y	N	N	N	N
Scalable	N	N	N	N	Y	Y	Y	Y	Y
Automated Slashing	-	-	-	N	Y	Y	Y	N	N

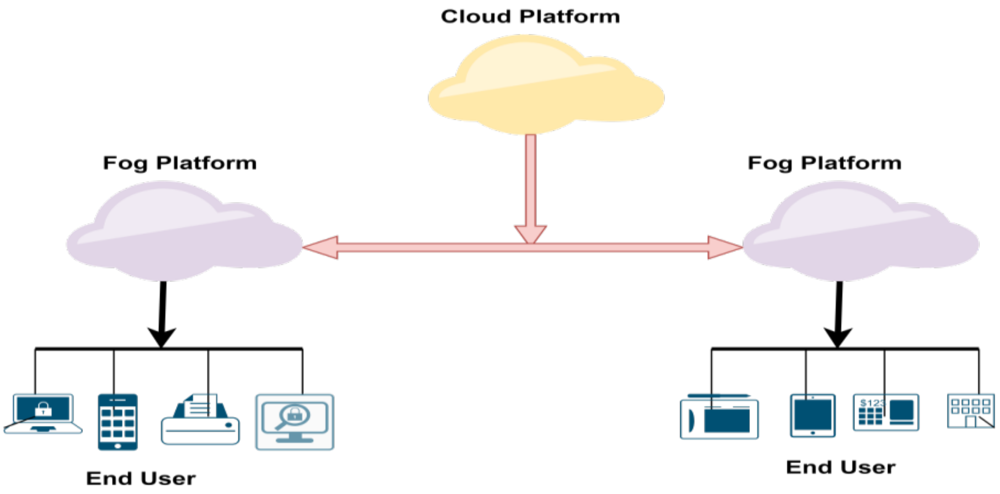

Figure 1. Fog Computing. This figure depicts how end users communicate with Fog Computing

Applications that use FC in real-time demand a faster connection and a better response than those that can tolerate delays [10]. Additionally, these applications need to check for available resources. Resource management is a significant challenge in FC due to the latency-sensitive and resource-constrained behavior of fog applications. Fig. 2 depicts the technological layout of a Fog platform [9]. The Linux and Cisco IOS networking operating systems are part of the Cisco IOx API, which is used to develop the Fog IaaS platform.

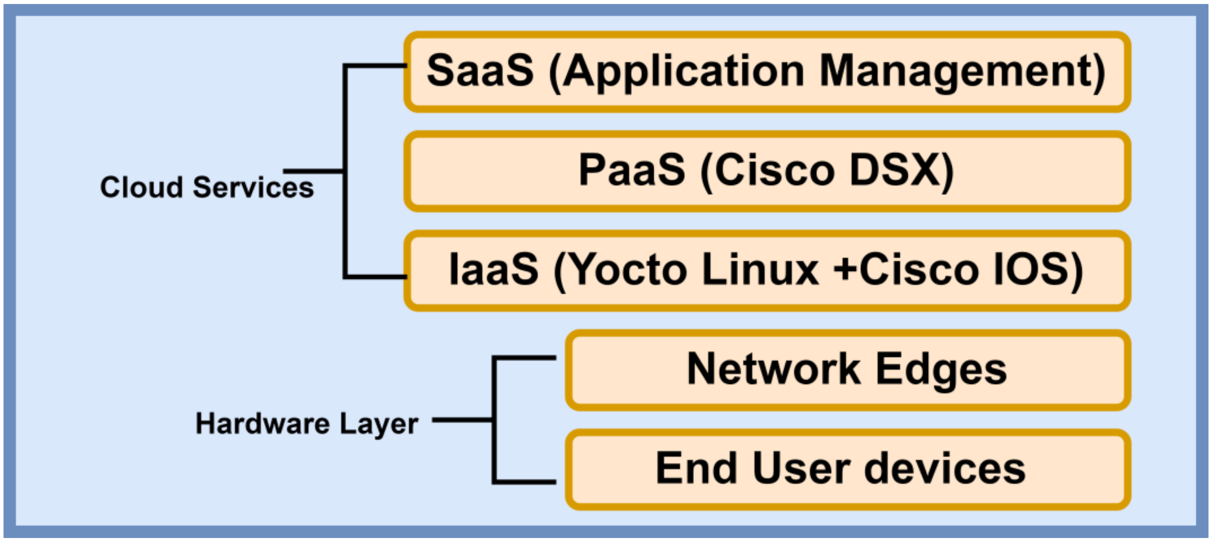

Figure 2. The Architecture of Fog Computing

Table 2. Abbreviation used in Comparative Analysis of the different BC platforms

Abbreviation	Description	Abbreviation	Description
dApps-	Decentralized Apps	DIM-	Digital Identity Management
DEX-	Decentralized Exchange	DiClSt-	Distributed Cloud Storage
DeFi-	Decentralized Finance	DiClCo-	Distributed CC
OChG-	On-Chain Governance	PoW –	Proof of Work
HRAdd-	Human Readable Address	RPCA -	Ripple Protocol consensus algorithm
PoS-	Proof of Stake	SPoS-	Secure Proof of Stake
BPoS-	Bonded Proof of Stake	H-	High
NPoS-	Nominated Proof of Stake	L-	Low
DPoS-	Delegated Proof of Stake	M-	Medium
DAG-	Direct Acyclic Graph	Y-	Yes
		N-	No

3. Related works

Lin et al. [16] introduced a unique access control mechanism for protecting cloud data privacy. This strategy encompasses three steps: user registration, data generation, and data access. At each level, consumers can select between direct and indirect interaction with the cloud service provider. However, several issues are not addressed in this study. On the one hand, more efforts should be made to enable a more complicated trust architecture that addresses circumstances such as a malevolent TTP attempting to divulge users' information. On the other hand, our continuing research will investigate tradeoffs between cloud service quality and privacy protection, some of which may be supplementary to PriGuarder. To ensure patients' privacy, Seol et al. [17] presented an EHR cloud. EHR model conducts partial encryption and employs electronic signatures. Liu et al. [18] suggested a role-based access management architecture for specific users' permission-assigning requests based on certain roles. An optimum authorization route is defined in this study. Automatic authorization procedures for collaborative multidomain RBAC models will be the subject of future study. Chatterjee et al. [19] allowed identity identification for users and provided specific services for approved users. Future work will entail implementing and testing the proposed method in a real-world setting. By offering anticipatory offloading, Zhang et al. [20] investigated how complexity may be reduced. The optimization happened in the area that makes decisions. Liu et al. [21] aimed to use the benefits of edge computing, such as computation offloading and content caching, to reduce the computational cost of BC. The performance of BC systems was assessed in this study. The findings demonstrated that leveraging idle edge computing resources might significantly improve the efficiency of BC deployments. Other research [22, 23] found comparable results, arguing that dumping workload via edge computing was superior when the governance system was effective. Li et al. [24] proposed an energy BC, a safe energy trading system that addresses security issues while eliminating the use of trusted mediators, using the consortium BC technique. Kang et al. [25] approved consortium BC to secure the security of electricity transactions. A BC system's network nodes might be formed from a variety of edge devices. Sharma et al. [26] showed that using BC in fog/edge computing might result in safe energy transfers due to the benefit of BC approaches in protecting anonymity. Another research [27] presented a use case for combining edge computing and BC to provide a secure electric car cloud. Recent research [28] indicated that centralized computing (cloud data center) was no longer the best option for some smart grid applications due to the possibility of energy loss and delay time from different electric devices and widely dispersed geographic embedded systems. Stolfo et al. [29] provide an alternative strategy for protecting data stored in the cloud by utilizing offensive decoy technology. Chen et al. [30] proposed CP-ABE method. The problem that Hur's system can't withstand collusion attack is solved by the proposed technique, which utilizes DH tree to revoke characteristics statelessly for the first time. Additionally, combines two granular revocation techniques and offloads difficult processes to fog nodes to improve performance on more resource-constrained devices. For vehicular fogs, Fan et al. [31] suggest a revocable data-sharing method. To implement data access control in a vehicular network system, develop a novel CP-ABE method with effective decryption.

Table 3. Review papers and their description & challenge

[citation]	**Methodology**	**Features**	**Challenges**
[16]	PriGuarder	Three stages of cloud service access control method. At each stage, there are two modes of interaction – direct and indirect.	More work should be put into promoting a more intricate trust framework. Trade-offs between privacy protection and cloud service features
[17]	attribute-based access control using XML	Use XML encryption and XML digital signature	Real-world use of the prototype model and quantitative performance analysis.
[18]	Intelligent planning theory	Authorization routes are supported by PGAO for external review.	Automated authorization techniques for a multidomain collaborative RBAC model
[19]		identity identification for users and provided specific services for approved users	Implementing and testing the proposed method in a real-world setting
[29]	Offensive Decoy Technology	Monitoring data access patterns through user behavior profiling can help identify if and when a malevolent insider improperly accesses someone's Cloud service documents.	Only valid for social media and networking sites.
[30]	CP-ABE scheme	Data secrecy, forward and backward	multi-authority will be improved.

		security, and resistance to collusion attacks are all achieved by the technique. It is clear from the performance study that, the system has comparatively low encryption and decryption costs for consumers.	
[31]	revocable data-sharing method	a new multi-authority CP-ABE technique with effective decryption was proposed	The communication cost for attribute revocation will be quite high.
[26]	BC-based DMM scheme	DMM can manage hierarchical security concerns without changing the network architecture. By utilizing three BCs, it meets the demands of completely distributed security and fixes the de-registration problems that plague the current DMM systems.	Different broadcasting techniques will be used to assess the proposed BC-based DMM.

The distributed solution for security with BC has been the subject of a lot of writing in recent years. Simple summaries and comparisons are provided in Table 4. A MediBchain was introduced by Al et al. [17], which can assist users in encrypting and storing their EMRs. The requirement for the user to transmit his passcode when sharing his EMRs with other users is a drawback of MediBchain. To improve the powers of access control and compatibility for EMRs based on smart contracts, a distributed privacy-preserving system, Dagher et al. [18] employed the Ethereum-based BC. Wang et al. [19] suggested parallel healthcare systems baes on BC-powered, in which they employ a synthetic system to maintain patients' electronic medical records, computational experiments to choose treatment plans, and parallel execution to reach a decision. BC technology was used by Xu et al. [20] to create a platform that allows users to freely access their EMRs and choose the doctor they want from among several medical facilities. For healthcare 4.0 applications, Tanwar et al. [21] took advantage of an EMRs administration system based on BC technology. They also enhanced data access with an access control policy algorithm. A secure healthcare record management system based on a hybrid of private and consortium BCs was suggested by Rahoof et al. [22] and has the potential to reduce storage requirements while increasing scalability. A HealthBlock using BC technology for managing medical data was presented by Zaabar et al. [23]. Chenthara et al. [43] proposed HealthChain, a novel blockchain-based smart contract system for eReferral in healthcare. It utilizes blockchain technology to improve transparency, security, and efficiency in the referral process. Chenthara et al. [44] presented HealthChain, a framework for the privacy preservation of electronic health records using blockchain technology. It aims to enhance data privacy and security while ensuring the accessibility and integrity of healthcare records. You et al. [45] introduced a knowledge graph-empowered online learning framework for access control decision-making. The framework utilizes a knowledge graph to improve the accuracy and adaptability of access control systems. You et al. [46] proposed a minority class-boosted framework for adaptive access control decision-making. The framework addresses the challenge of imbalanced data in access control and employs machine learning techniques to improve decision-making accuracy. Wang and Sun [47] presented a trust-involved access control mechanism for collaborative open social networks. The mechanism aims to enhance security and privacy in social networks by considering trust relationships between users in the access control process.

In summary, we found that all previous models faced threats from scalability, interoperability issues, and privacy and security measures in blockchain-based healthcare record management systems. the proposed technique utilizes a decentralized and distributed ledger blockchain system to address scalability and interoperability issues. This approach ensures transparency and prevents tampering by intruders. Additionally, authorized personnel can access data from distributed blockchains installed on different fog layers.

Table 4. Related works comparison for BC-enabled security

[citation]	Methodology	Features	Challenges
[17]	Permission BC	Encryption of data and storing medical records	a receiver needs to know the passcode
[18]	Ethereum-based BC	Access control	Confusion in medical records
		Interoperability	
[19]	Public BC	Parallel healthcare system	Interoperability
			Confusion in medical records
[20]	Public BC	Healthchain system	Double chain (user chain & doc chain) Cooperation
			Confusion in medical records
[21]	Public BC	Data access control	Interoperability
			Confusion in medical records
[22]	Private BC	Scalability	Double chain cooperation
	Consortium BC		
[23].	Private BC	Scalability	Double chain cooperation
	Consortium BC		
[43]	HealthChain	Blockchain-based smart contract system for eReferral	Addressing scalability and centralized issues
[44]	HealthChain Framework	Privacy preservation of electronic health records	Ensuring data privacy and security
[45]	Knowledge Graph Online Learning Framework	Knowledge graph empowered access control decision-making	Handling complex and dynamic access control scenarios
[46]	Minority Class Boosted Framework	Adaptive access control decision-making with imbalanced data	Dealing with imbalanced datasets and biased decision-making
[47]	Trust-Involved Access Control in Collaborative Social Networks	Trust-involved access control mechanism	Establishing trust relationships in social networks

4. Proposed Methodology

The proposed model uses hyperledger fabric to store the HV of data. HV is calculated by SHA256 algorithms. By using HV, the authenticity of data will be defined. Architecture and algorithms will be discussed in this section.

4.1 Hyperledger Fabric

Hyperledger Fabric, an open-source initiative that offers a modular BC foundation, has become the de facto standard for business BC systems. The open, modular framework uses plug-and-play components to support a range of use cases and is intended to serve as a foundation for developing business solutions and enterprise-grade apps. Together with more than 15,000 engineer contributors and more than 120,000 contributing companies, The unique consensus approach provided by Hyperledger Fabric enables efficiency at scale while upholding the needs of companies for data protection [14]. With the use of BC technology, apps may be created where many parties can record transactions directly without the requirement for a reliable central authority to guarantee that the transactions are valid. With the use of a peer-to-peer network, which gives each member access to a common ledger where the transactions are recorded, BC makes this possible. These exchanges are immutable and cryptographically provable by design. Three main elements make up BC technology: a distributed ledger, a consensus method, and smart contracts [15].

4.2 Proposed Model

Fog layer is a middle layer connecting the Cloud layer and end-user devices. FC is a form of distributed computing that links several "peripheral" devices to a cloud. To reduce bandwidth requirements and send processed data rather than raw data, FC aims to process as much data as possible utilizing computer units that are situated close to data-generating sources. The fog layer is linked to the hyperledger fabric and the cloud layer, as shown in Figure 3; the fog layer sends data to the cloud layer and the HV of that data to the HF. The HV is now safe in HF due to the nature of immutability. At the time of computation, the Cloud layer calculates the HV of the data and compares it to the HV stored in the HF. If the HVs are the same, there is no eve-teasing with the original data.

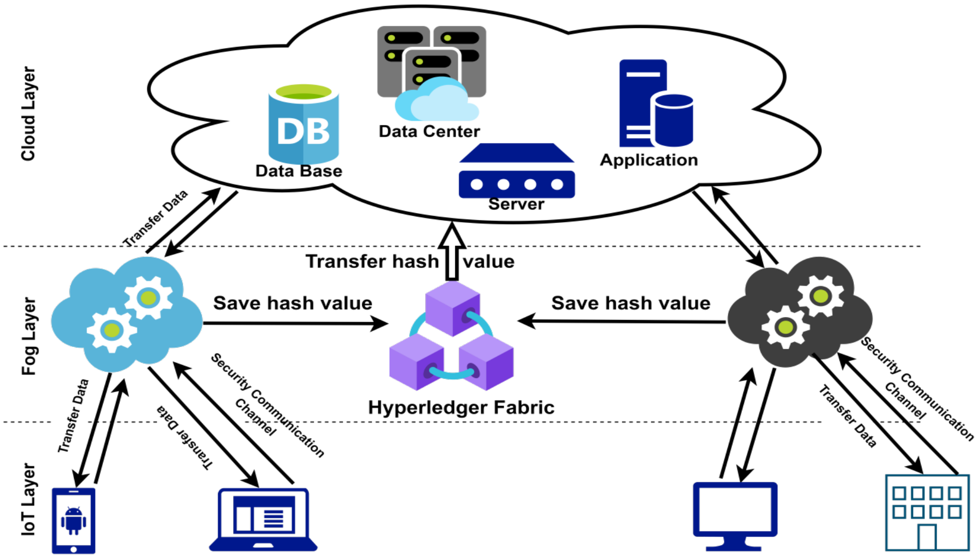

Figure 3. Integration of Fog Computing with Hyperledger Fabric

4.3 Flow chart

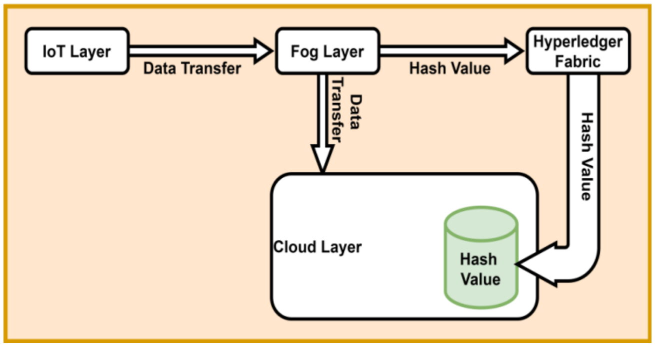

Figure 4. Flow chart of the proposed model

Figure 4 depicted the flow of the proposed model. The fog layer collects data generated from different IoT devices. The HV is computed at the fog layer and transferred to the hyperledger fabric and simultaneously original data is transferred to the cloud layer. The cloud layer received a HV from the hyperledger fabric. The cloud layer computes the HV of data received from the fog layer and compares it with a HV of the hyperledger fabric. If both are the same, means there is no tempering with the original data.

4.4 Algorithms

Algorithm 1: Data Authenticity

Input: Data
Output: Authenticity of the data

Begin
Step1. End-user devices encrypt the data using **ES256 Algorithm** and send encrypted data to the fog layer
Step2. Fog layer store data and calculate the HV by using **HV256 Algorithm**
Step3. The calculated HV transmitted to HF
Step4. The same data send to the Cloud layer.
Step5. The cloud layer calculates the hash and compares it with HF's HV
Step6. Check the authenticity of comparing both HVs.
End

Mathematical model of HV256 Algorithm

Initialize:
rr ← Right Rotate
hsv ← HV
ch← Chunk

Create message schedule (m):

$$\mu_0^{256}(m-15) = (m[i-15]rr\ 7 \oplus m[i-15]rr\ 18) \oplus (m[i-15] \gg 3$$

$$\mu_0^{256}(m-2) = (m[i-2]rr\ 17 \oplus m[i-2]rr\ 19) \oplus (m[i-2] \gg 10$$

$$\text{m[i]=}\ \mu_0^{256}(w-15) + m[i-16] + \mu_0^{256}(m-2) + m[i-7]$$

Compression Function:

$$\text{tmp1} = hsv + \sum_{i=1}^{256}(\text{e}) + \text{ch} + k_{i=1}^{256} + w$$

$$\text{tmp2} = \sum_{i=1}^{256}(\text{a}) + \text{mj}$$

Mathematical model of ES256 Algorithm

```
Initialize Plain Text (P), c[i], nc[i]
a[i][j]← P
Initialize Key (K)
$X_0$ ←P ⊕ K
for (r=1,r<=14,r++)
{
                    Substitution of the bytes
                    S-box
          {
                    Invert in GF($2^8$)
                    Multiply by a matrix $L$
                    Add a constant $c$.
          }
          Shifting the rows
          {
                              a[i][j]
                              value of i ranging from 1 to 4.
                              value of j ranging from 1 to 4.
                              {
                                        if (i=2)
                                        1 bit left← Shift a[2][j]
                              if (i=3)
                              2 bit left← Shift a[3][j]
                              if (i=4)
                              3 bit left← Shift a[4][j]
                    }
          }
                    Mixing the columns
                    {
                              Value of i ranging from 1 to 4
                              Value of j ranging from 1 to 4
                              {
                                        a[i][j] * c[i] =nc[i]
                    }
                    }
Adding the round key
{
                    Value of i ranging from 1 to 4
                    Value of j ranging from 1 to 4
          a[i][j] ⊕ k[i][j]
}
}
```

Algorithm 2: SHA256

Initialize: rr ← Right Rotate, >> ← Right Shift, && ← and, ! ← Not, ⊕ ← xor
Input: User Data
Output: HV

Step 1. Pre-processing plain text using **Algorithm 3**
Step 2. Initialize HV (hsv)
Step 3. Initialized round constant (k)
Step 4. Chunk loop
Step 5. Create message schedule (w) using **algorithm 4**
Step 6. Compression using **algorithm 5**
Step 7. Modify the final value by adding the current HV to the compressed block using **algorithm 6**
Step 8. Concatenate final hash

Message digest =
$$hsv_0^i + hsv_1^i + hsv_2^i + hsv_3^i + hsv_4^i + hsv_5^i + hsv_6^i + hsv_7^i$$
End

Algorithm 3: Pre-processing plain text

Input: Plain text
Output: Padding plain text

Step 1. Convert plain text into binary.
Step 2. Append 1 at last.
Step 3. Pad with 0 until data will multiple of 512.
End

Algorithm 4: Create message schedule (w)

Input: Text
Output: Message Schedule

```
Array[w]←Plain text (entry will be 32-bit format).
w[0….63]
for (i=16,i<=63,i++)
{
X0=(w[i-15] rr 7) ⊕ (w[i-15] rr18) ⊕ (w[i-15] >> 3)
X1=(w[i-2]rr17) ⊕ (w[i-2] rr19) ⊕ (w[i-2] >> 10)
W[i]=w[i-16] + X0 + w[i-7] +X1
}
End
```

Algorithm 5: Compression

Input: Normal text
Output: Compressed text

```
Initialized variables and set them equal to the current HV.
α=hsv0, β=hsv1, μ=hsv2, £=hsv3, €=hsv4, ¥=hsv5, $=hsv6, ¢=hsv7
for (i=0,i<=63,i++)
{
X1= (e rr 6) ⊕ (e rr 11) ⊕ (e rr 25)
ch= (e && f) ⊕ ((!e) && g)
tmp1= h+ X1 +ch+ k[i] +w[i]
X0 = (a rr 2) ⊕ (a rr13) ⊕ (a rr 22)
Mj= (a && b) ⊕ (a && c) ⊕ (b && c)
tmp2 = X0 + mj
¢=$, $=¥, ¥=€, €=£ + tmp1, £= μ, μ = β, β = α, α =  tmp1+ tmp2
}
End
```

Algorithm 6: Modify the final value by adding the current HV to the compressed block

$$hsv_0^i = hsv_0^{(i-1)} + \alpha$$
$$hsv_1^i = hsv_1^{(i-1)} + \beta$$
$$hsv_2^i = hsv_2^{(i-1)} + \mu$$
$$hsv_3^i = hsv_3^{(i-1)} + \text{£}$$
$$hsv_4^i = hsv_4^{(i-1)} + \text{€}\ hsv_5^i = hsv_5^{(i-1)} + \text{¥}$$
$$hsv_6^i = hsv_6^{(i-1)} + \$$$

5. Performance Evaluation

The proposed model presents an evaluation to access the performance in terms of flexibility analysis, and efficiency analysis (Storage Overhead, Communication Cost, and Computation Cost). Tabular and graphical visualization are shown in the experimental result section.

5.1 Experiment Configuration

Ethereum Client Geth and Ethereum Wallet running on Window based computer. The hardware configuration includes Intel i5-12400CPU@2.5 GHz, 10GB RAM, 64-bit OS, X64-based processor, and 1TB of HDD. Edge nodes ranging from 50 to 500 to simulate the scenario.

$$hsv_7^i = hsv_7^{(i-1)} + \text{¢}$$

Algorithm 8: Proof of Stack

```
Input: Transaction
Output: Rewards

Step 1: Transaction←Nodes
Step 2: validate [next[blocks]]←Contending[Nodes]
Step 3: Publish [block]←validator[verifies[nodes]]
Step 4: if validate [block]→ OK
            reward ++
        else
            reward - -
End:
```

5.2 Experiment Result

The proposed model demonstrates the evaluation result generated from the experiment in terms of flexibility and efficiency analysis.

5.2.1 Flexibility Analysis

Concerning the type of access structure, the type of authority, security attacks, and revocation, the proposed model compares with prior multi-authority CPABE schemes in Table 5. We can infer from Table 4 that the proposed model is more adaptable than others. It is simple to see that Lewko's and our schemes are comparable in terms of adaptability. Consequently, we will contrast our plan with its in terms of storing expenses.

Table 5. Comparison of flexibility

Scheme	Access Structure	Authority	Against Collision Attack	Revocation
Chase	AND	More than one	✓	X
Hur	Access tree	One	✓	Attribute and user
Lewko	LSSS	More than one	✓	X
Ruj	Access tree	More than one	✓	User
Proposed Scheme	LSSS	More than one	✓	Attribute and user

Encryption and decryption techniques are very important metrics for a security mechanism. The proposed model compares with Lewko's scheme and Fan's scheme and is shown in Tables 6 & 7.

Table 6. Analysis of the Decryption Time of the proposed model with lewako's and Fan's scheme

Number of Authorities	Time for Data Decryption (S)		
	Lewako's Scheme	Fan's scheme	Proposed Scheme
1	0.081	0.075	0.06
2	0.0811	0.077	0.0611
3	0.0832	0.078	0.0612
4	0.0833	0.079	0.0623
5	0.0845	0.08	0.0635
6	0.0846	0.081	0.0646
7	0.0857	0.082	0.0657
8	0.0858	0.083	0.0668
9	0.0869	0.084	0.0679
10	0.0872	0.085	0.069

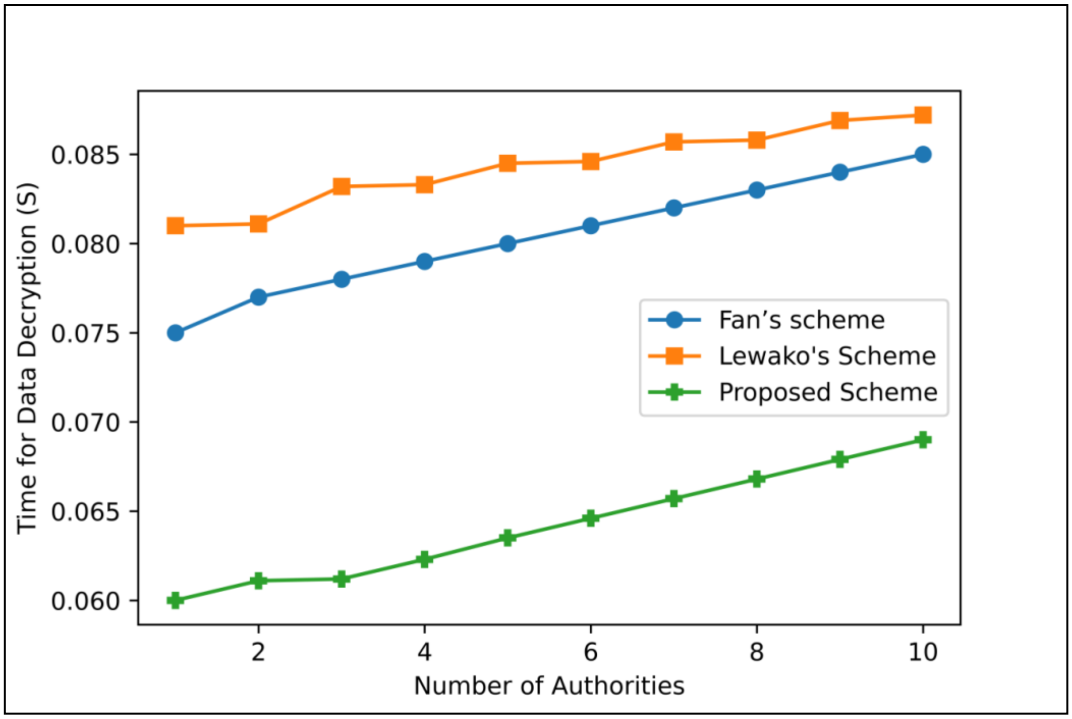

Figure 5. Analysis of the Decryption Time of the proposed model with lewako's and Fan's scheme

Encryption time concerning the number of authorities is compared with other models and it is found that the proposed model has less encryption time. Table 7 shows a comparative analysis of the encryption time of the proposed model with the other two models.

Table 7. Analysis of the Encryption Time of the proposed model with lewako's and Fan's scheme

Number of Authorities	Time for Data Encryption (S)		
	Lewako's Scheme	Fan's scheme	Proposed Scheme
1	0.5	0.4	0.3
2	1	0.8	0.6
3	1.5	1.2	0.9
4	2	1.6	1.2
5	2.5	2	1.5
6	3	2.4	1.8
7	3.5	2.8	2.1
8	4	3.2	2.4

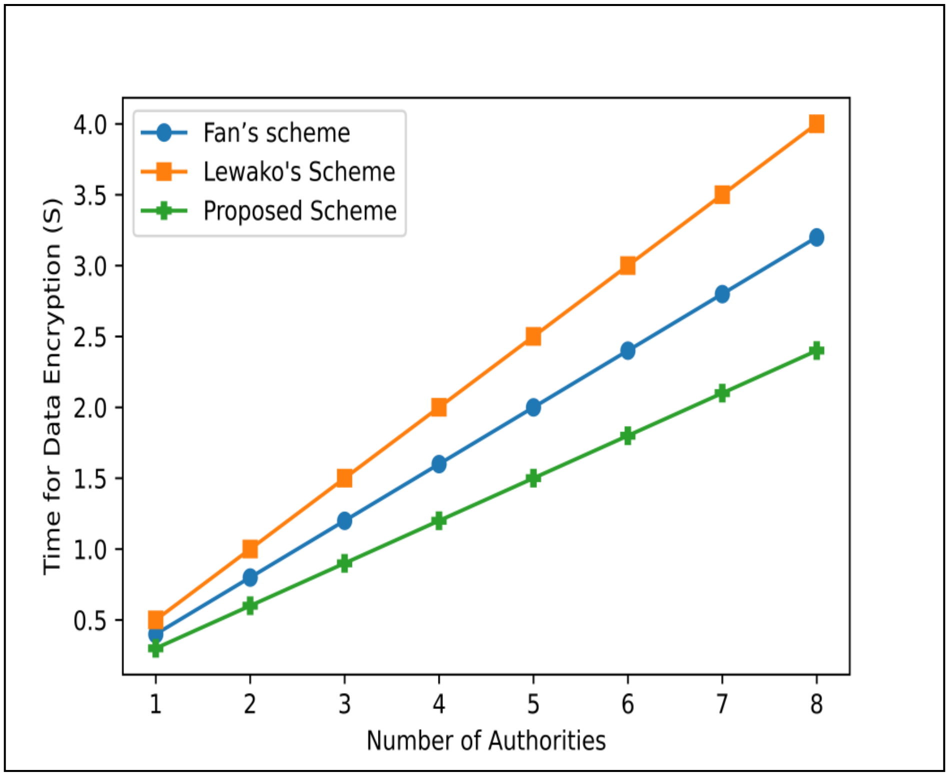

Figure 6. Analysis of the Encryption Time of the proposed model with lewako’s and Fan’s scheme

Figures 5 and 6 indicate the performance of encryption and decryption time for the proposed model with lewako’s and fan’s schemes. With these tables, it is clearly understood that the proposed scheme is more flexible than other schemes.

5.2.2 Efficiency Analysis

This section provides a comparative analysis of efficiency in terms of storage overhead, communication, and computation cost of the proposed model with lewako’s and fan’s scheme.

5.2.2.1 Storage Overhead

The proposed model’s version keys for each characteristic serve as the authority's storing overhead. While Lewko's strategy on it involves additional storage costs because of the authority's private keys. Every visible attribute in the proposed model is used to calculate the storage overhead for each data proprietor. The size of each user's ciphertext and transformation keys determine the storage overhead for the cloud, so each user's storage overhead is just their private keys, which can be almost completely disregarded.

Table 8. Comparison of Storage Overhead of the proposed model with lewako’s and Fan’s scheme

	Storage Overhead in KB				
Number of Edge Nodes	1000	2000	3000	4000	5000
Lewako's Scheme	19.58	39.03	58.49	77.59	97.4
Fan’s scheme	25	40.6	62.57	79.51	101.1
Proposed Scheme	**15.73**	**32.14**	**51.77**	**68.78**	**86.33**

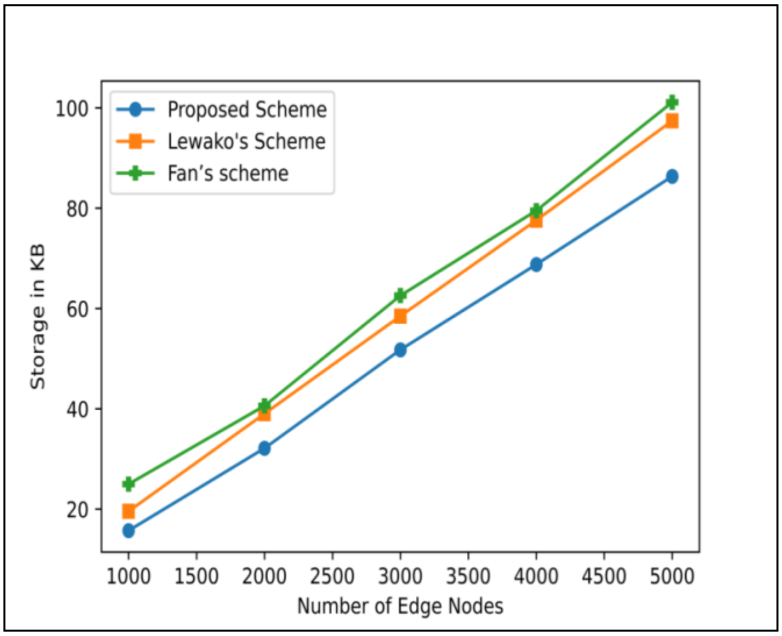

Figure 7. Comparison of Storage Overhead of the proposed model with lewako's and Fan's scheme

5.2.2.2 Communication Cost

The proposed model compares the communication cost with Lewako's and Fan's scheme as shown in Table 9. From the table, it is easy to say that the proposed model has high accuracy in terms of percentage.

Table 9. Comparison of Communication Cost of the proposed model with lewako's and Fan's Scheme

Communication Cost in GB	**Accuracy in %**				
	10	15	20	25	30
Lewako's Scheme	7	14	19	25	30
Fan's scheme	5	7	9	11	13
Proposed Scheme	**9**	**17**	**22**	**28**	**35**

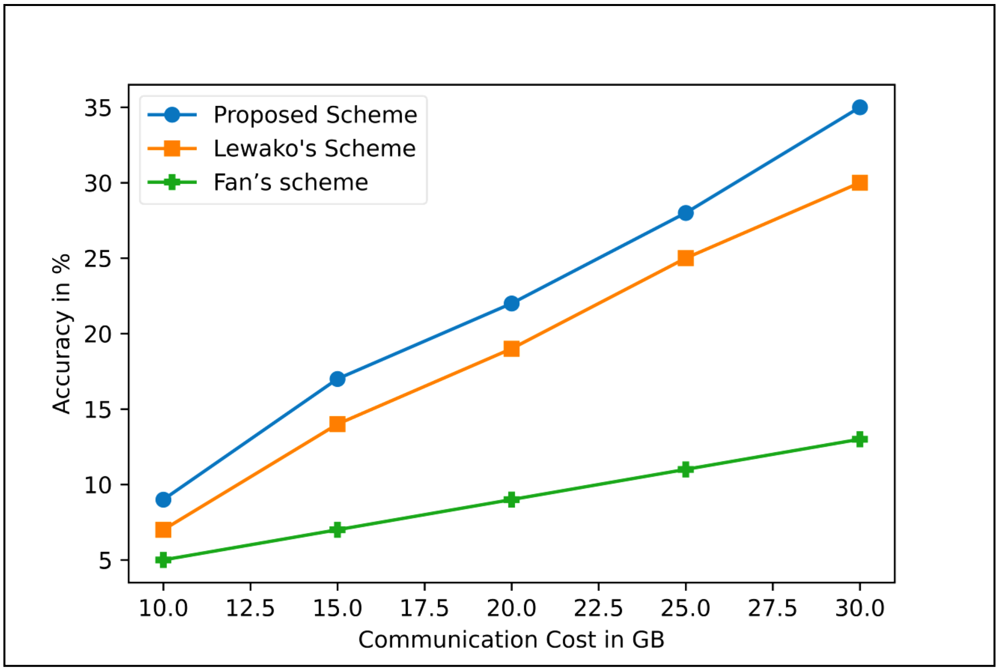

Figure 8. Comparison of Communication Cost of the proposed model with lewako’s and Fan’s scheme

5.2.2.3 Computation Cost

Computation cost comparison with edge nodes is shown in Table 10. The proposed model compares with the other two old models and analyzes that the proposed model has the lowest computation cost even if the number of edge nodes increased.

Table 10: Comparision of Computation Cost of the proposed model with lewako’s and Fan’s scheme

Number of Edge Nodes	**Storage Overhead in KB**				
	100	120	140	160	180
Lewako's Scheme	18	19	21	25	27
Fan’s scheme	20	22	24	28	30
Proposed Scheme	15	17	19	21	23

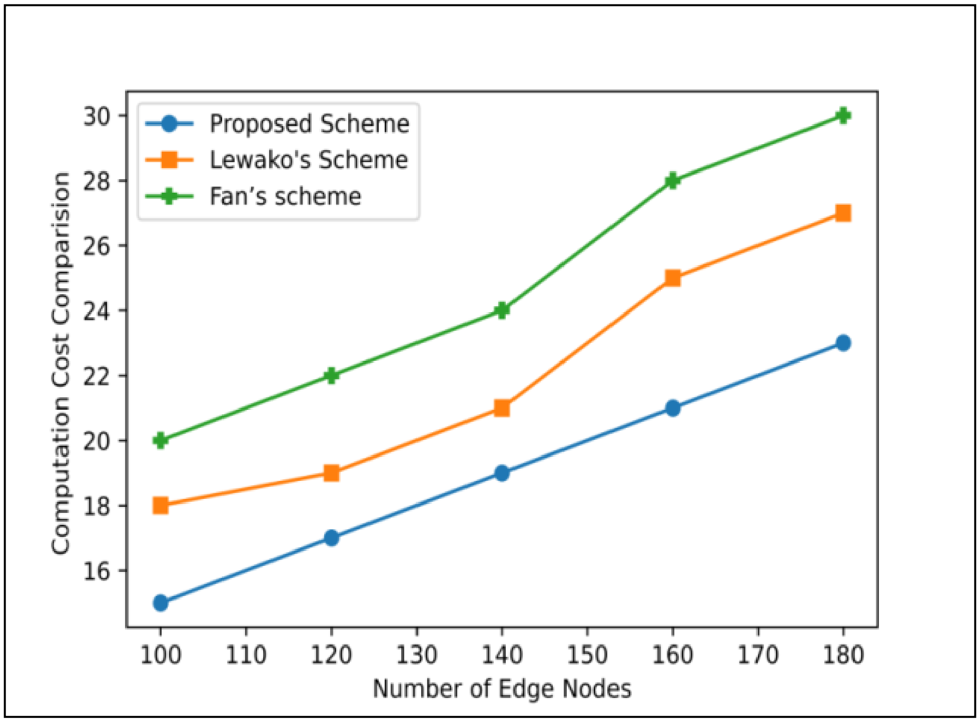

Figure 9. Comparison of Computation Cost of the proposed model with lewako's and Fan's scheme

5.3 Result Summary

To minimize the security concerns in the BD storage process in the Cloud, the intended method is used. To demonstrate the effectiveness of the suggested combined technique, we contrasted its various outcomes with some of the currently used security techniques. To further minimize data and security overheads, the proposed technique provides improved efficiency. A comparison table of performance matrices is shown in Table 11.

Table 11. Comparison of proposed Vs. previous approach

Performance Metrics	**Proposed Vs Previous Models (Average)**		
	Lewako's	**Fan's scheme**	**Proposed**
Encryption Time	2.25	1.8	**1.35**
Decryption Time	.704	.075	**.068**
Storage overhead	58.41	61.75	**50.95**
Communication Cost	19	9	**22.2**
Computation Cost	22	24.8	**19**

5.4 Discussions

To lessen the security concerns in the BD storage operation in the Cloud, the intended approach is used. To demonstrate the effectiveness of the suggested technique, we contrasted its various outcomes with some of the currently used security techniques. Additionally, the suggested method provides improved compression effectiveness to lower data and security overheads. Figures 5–9 demonstrate that the suggested strategy outperforms existing approaches. The experimental findings thus show that the suggested system is superior to and safer than all other ones that are currently in use. We concluded that our suggested strategy meets all of our objectives because we got improved results using the two BD methods that are outlined in it.

6. Conclusion and Future Work

To guarantee data authenticity, we proposed a model which consists of 3 stages ie. IoT layer, Fog layer, and Cloud layer. The end user transfer data to the fog layer. Two operations perform at the fog layer, 1st one is Data directly transfer from Fog Layer to Cloud Layer, and the secondary HV is calculated at the Fog layer and transferred to the Hyperledger Fabric and HV is transferred from Hyperledger Fabric to Cloud Layer. In the end, Cloud Layer calculates the HV of data (data received from Fog Layer) and match it with the HV which is received from Hyperledger fabric.

However, this model is tested only on a single user cluster and some issues are not addressed in this article. On the one hand, more work needs to be done to support a more intricate confidence paradigm. On the other hand, our continuing research will examine the trade-offs between data security and cloud service features.

Acknowledgments.

We thank the anonymous referees for their useful suggestions.

Reference

[1] R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: a taxonomy, survey and future directions, in: Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives, Springer, Singapore, 2018, pp. 103–130.

[2] Q.-V. Pham, F. Fang, V.N. Ha, M. Le, Z. Ding, L.B. Le, W.-J. Hwang, A survey of multi-access edge computing in 5G and beyond: fundamentals, technology integration, and state-of-the-art, arXiv preprint, arXiv:1906.08452, 2019.

[3] Abbasi BZ, Shah MA. Fog computing: security issues, solutions and robust practices. Paper presented at: Proceedings of 2017 23rd International Conference on Automation and Computing (ICAC); 2017: 1–6

[4] Sagiroglu S, Sinanc D (2013) Big data: A review. In: Collaboration Technologies and Systems (CTS), 2013 International Conference On. IEEE. pp 42–47

[5] Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile CC. ACM. pp 13–16

[6] Sareen P, Kumar P (2016) The fog computing paradigm. Int J Emerging Technol Eng Res 4:55–60

[7] Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev 44(5):27–32

[8] Saharan K, Kumar A (2015) Fog in comparison to cloud: A survey. Int J Comput Appl 122(3):10–12

[9] Cisco (2015) Cisco Fog Computing Solutions: Unleash the Power of the Internet of Things. Online: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-solutions.pdf. Accessed 13 Dec 2016

[10] Bushra J et al (2020) A job scheduling algorithm for delay and performance optimization in fog computing. Concurren Comput Pract Exper 32(7):5581

[11] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of BC: A survey," IEEE Access, vol. 8, pp. 16 440–16 455, 2020.

[12] W. Viriyasitavat and D. Hoonsopon, "BC characteristics and consensus in modern business processes," Journal of Industrial Information Integration, vol. 13, pp. 32–39, Mar. 2019.

[13] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of BC-based applications: current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55–81, Mar. 2019

[14] https://www.ibm.com/in-en/topics/hyperledger

[15] https://aws.amazon.com/BC/what-is-hyperledger-fabric/

[16] L. Lin, T. Liu, S. Li, C. M. Sarathchandra Magurawalage, and S. Tu. Priguarder: A privacy-aware access control approach based on attribute fuzzy grouping in cloud environments. IEEE Access, 6:1882–1893, 2018.

[17] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik. Privacy-preserving attribute-based access control model for xml-based electronic health record system. IEEE Access, 6:9114–9128, 2018.

[18] Q. Liu, H. Zhang, J. Wan, and X. Chen. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. IEEE Access, 5:7001–7011, 2017

[19] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, A. G. Reddy, K. Park, and Y. Park. On the design of fine grained access

control with user authentication scheme for telecare medicine information systems. IEEE Access, 5:7012–7030, 2017.

[20] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang. Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading. IEEE Vehicular Technology Magazine, 12(2):36–44, 2017

[21] Mengting Liu, Richard Yu, Yinglei Teng, Victor CM Leung, and Mei Song. Computation offloading and content caching in wireless BC networks with mobile edge computing. IEEE Transactions on Vehicular Technology, 2018

[22] R. Yu, J. Ding, X. Huang, M. Zhou, S. Gjessing, and Y. Zhang. Optimal resource sharing in 5g-enabled vehicular networks: A matrix game approach. IEEE Transactions on Vehicular Technology, 65(10):7844–7856, 2016.

[23] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang. Mobile edge computing and networking for green and low-latency internet of things. IEEE Communications Magazine, 56(5):39–45, 2018.

[24] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang. Consortium BC for secure energy trading in industrial internet of things. IEEE Transactions on Industrial Informatics, 14(8):3690–3700, Aug 2018

[25] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain. Enabling localized peer-to-peer electricity trading among plugin hybrid electric vehicles using consortium BCs. IEEE Transactions on Industrial Informatics, 13(6):3154–3164, Dec 2017.

[26] V. Sharma, I. You, F. Palmieri, D. Jayakody, and J. Li. Secure and energy-efficient handover in fog networks using BC-based DMM. IEEE Communications Magazine, 56(5):22–31, 2018

[27] H. Liu, Y. Zhang, and T. Yang. BC-enabled security in electric vehicles cloud and edge computing. IEEE Network, 32(3):78–83, 2018

[28] Y. Zhang and N. Ansari. Hero: Hierarchical energy optimization for data center networks. IEEE Systems Journal, 9(2):406–415, 2015.

[29] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. EE Symposium on Security and Privacy: 125-128

[30] Shan Chen, Mi Wen, Rongxing Lu. Jinguo Li, Sijia Chen. Achieve Revocable Access Control for Fog-based Smart Grid System. IEEE 90th Vehicular Technology Conference, 2019

[31] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "Secure, efficient and revocable data sharing scheme for vehicular fogs," Peer-to-Peer Networking and Applications, vol. 11, no. 4, pp. 766–777, 2018.

[32] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A BC based privacy preserving platform for healthcare data," in Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage, 2017, pp. 534–543.

[33] G. Dagher, J. Mohler, M. Milojkovic, and B. Praneeth, "Ancile: Privacypreserving framework for access control and interoperability of electronic health records using BC technology," Sustain. Cities Soc., vol. 39, pp. 283–297, May 2018

[34] S. Wang et al., "BC-powered parallel healthcare systems based on the ACP approach," IEEE Trans. Comput. Social Syst., vol. 5, no. 4, pp. 942–950, Dec. 2018.

[35] J. Xu et al., "Healthchain: A BC-based privacy preserving scheme for large-scale health data," IEEE Internet Things J., vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[36] S. Tanwar, K. Parekh, and R. Evans, "BC-based electronic healthcare record system for healthcare 4.0 applications," J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102407.

[37] T. A. Rahoof and V. R. Deepthi, "HealthChain: A secure scalable health care data management system using BC," in Proc. Int. Conf. Distrib. Comput. Internet Technol., 2020, pp. 380–391.

[38] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure BC-based healthcare data management system," Comput. Netw., vol. 200, Dec. 2021, Art. no. 108500.

[39] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "BC technology in the healthcare industry: Trends and opportunities," J. Ind. Inf. Integration, vol. 22, Jun. 2021, Art. no. 100217.

[40] P. P. Ray, N. Kumar, and D. Dash, "BLWN: BC-based lightweight simplified payment verification in IoT-assisted e-healthcare," IEEE Syst. J., vol. 15, no. 1, pp. 134–145, Mar. 2020.

[41] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in CC," Future Gener. Comput. Syst., vol. 67, pp. 133–151, Feb. 2017.

[42] G. Li, M. Dong, L. T. Yang, K. Ota, J. Wu, and J. Li, "Preserving edge knowledge sharing among IoT services: A BC-based approach," IEEE Trans. Emerg. Topics Comput. Intell., vol. 4, no. 5, pp. 653–665, Oct. 2020

[43] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F. (2020). A Novel Blockchain Based Smart Contract System for eReferral in Healthcare: HealthChain. In: Huang, Z., Siuly, S., Wang, H., Zhou, R., Zhang, Y. (eds) Health Information Science. HIS 2020. Lecture Notes in Computer Science(), vol 12435. Springer, Cham. https://doi.org/10.1007/978-3-030-61951-0_9

[44] Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLOS ONE, 15(12), e0243043. https://doi.org/10.1371/journal.pone.0243043

[45] You, M., Yin, J., Wang, H. et al. A knowledge graph empowered online learning framework for access control decision-making. World

Wide Web 26, 827–848 (2023). https://doi.org/10.1007/s11280-022-01076-5

[46] You, M., Yin, J., Wang, H., Cao, J., Miao, Y. (2021). A Minority Class Boosted Framework for Adaptive Access Control Decision-Making. In: Zhang, W., Zou, L., Maamar, Z., Chen, L. (eds) Web Information Systems Engineering – WISE 2021. WISE 2021. Lecture Notes in Computer Science(), vol 13080. Springer, Cham. https://doi.org/10.1007/978-3-030-90888-1_12

[47] H. Wang and L. Sun, "Trust-Involved Access Control in Collaborative Open Social Networks," *2010 Fourth International Conference on Network and System Security*, Melbourne, VIC, Australia, 2010, pp. 239-246, doi: 10.1109/NSS.2010.13.