Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Downgrade Delegated Proof of Stake Based Consortium Block Chain Espoused Anonymous and Traceable Group Data Sharing in Cloud Computing

Mr. Dorababu Sudarsa[1*], Dr. A. Nagaraja Rao[2], Dr. A.P. Siva Kumar[3]

[1*]*Research Scholar, Department of Computer Science and Engineering, JNT University Anantapur, Ananthapuramu, Andhra Pradesh, INDIA*

[2]*Senior Associate Professor, Department of Computational Intelligence, School of Computer Science & Engineering (SCOPE), VIT, Vellore.*

[3]*Professor, Department of Computer Science and Engineering, JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, INDIA*

Abstract- Group data sharing is a crucial aspect of cloud computing, enabling collaborative work and information exchange among multiple entities. However, ensuring secure and efficient data sharing within a group presents various challenges. In this manuscript, Downgrade Delegated Proof of Stake based Consortium Block Chain espoused Anonymous and Traceable Group Data Sharing in Cloud Computing (DDPS-BC-ATGDS-CC) is proposed. In this manuscript, the block chain technique uses every user in the system to rapidly and simply authenticate the shared data validity without interacting with a third-party auditor. Utilizing Downgrade Delegated Proof of Stake based consortium block chain (DDPS-BC),in construction database, which is tamper-resistant and maintained by all participants, stores the verification info for auditing. The performance metrics, like accuracy, Computation of traceability and Computation of data sharing are examined. The performance of the proposed DDPS-BC-ATGDS-CC technique provides 25.28%, 36.45%and 32.20% greater accuracy compared with the existing techniques like Secure and effective data sharing among vehicles based on consortium block chain (SEDS-BC-CC) , trusted data sharing with flexible access control based on block chain (TDS-FAC-BC) and an Accountable privacy-preserving scheme for public information sharing systems (APPS-PISS-CC).

Keywords: Data Sharing, Block chain, Anonymity, Traceability, Downgrade Delegated Proof of Stake based Consortium Block Chain, Cloud Computing.

1. Introduction

Due to its features of resource sharing and lower energy consumption, cloud computing consists of majority of researchers in comparison to traditional information sharing and communication technologies. Distributed calculating cannot just furnish clients with clearly boundless figuring assets yet additionally give clients obviously boundless capacity assets [1]. Distributed storage is perhaps of the main help in distributed computing since it empowers the association for any electronic product [2]. In addition, the cloud storage service allows for free movement for a variety of data types, including social networks, video editing, home networks [3].However, little attention is paid to group data sharing in cloud is the situation in that multiple users wish to attain group info sharing for cooperative purposes [4]. Traceable Group Data Sharing refers to a concept where groups of individuals or organizations share data in a manner that allows for traceability and accountability. It involves the exchange of data among multiple parties while maintaining transparency and visibility into how the data is being used and shared. The purpose of traceable group data sharing is to enable collaboration and

information sharing while ensuring data privacy, safety and ethical considerations. It allows different entities to pool their data resources, leading to enhanced insights, better decision-making, and the potential for innovation.

The specific scenario of group data sharing makes it possible for multi-users in a group to share information to the purpose of working together. Owing to fast improvement of distributed storage, acknowledging bunch information sharing through these administrations received a lot of attention from scholastics. [5]. Though, only situation in which all users in a group wish to share data is used in the existing literature. In this concern, a real-world situation in multiple users from various groups wish to share data, such as multiple academic institutions wishing for establish a shared medical database, multiple medical institutions wishing to share their research findings, and multiple universities wishing to share their educational resources [6]. Through storing data in cloud, users from various groups can share data in this scenario. However, users are concerned about changeable security issues brought on loss of data control because cloud is "semi-trusted". In addition, the cloud stores data from a variety of sources. Different group's users have no faith in the validity of data from other administrations [7].Users prefer to share data anonymously for safeguard their privacy. Furthermore, block chain is an arising innovation in the field of data [8]. Decentralization, openness, autonomy, and tamper-resistance are some of its characteristics. A block chain's data can't be changed or altered in any way. A trusted third party that is decentralized can be viewed as a block chain [9]. Hence, decentralization of block chain gives a feasible answer for building security plans without a confided in outsider. Simultaneously, the block tie innovation empowers clients to develop shared, dispersed, and fault-tolerant database. Additionally, it excels at system design for data sharing. Block chain is brand-new information technology. Decentralization, openness, autonomy, and tamper-resistance are some of its characteristics. The information recorded on block chain can't be messed with and modified [10]. A block chain is viewed as decentralized confided in outsider. As a result, decentralization of a block chain makes it possible to construct security frameworks without depending on confided in third party. In parallel, users can construct shared, distributed, fault-tolerant database using block chain technology. Additionally, it is excellent for creation of data sharing plans. These are motivated to carry out research work.

The major concepts of this research work are as follows,

- Downgrade Delegated Proof of Stake based Consortium Block Chain espoused Anonymous and Traceable Group Data Sharing in Cloud Computing (DDPS-BC-ATGDS-CC) is proposed in this research.
- Sharing data with multiple groups that is based on the consortium block chain idea. Utilizing Downgrade Delegated Proof of Stake based consortium block chain (DDPS-BC). In construction database, which is tamper-resistant and maintained by all participants, stores the verification info for auditing [18].
- In data sharing structure, a mechanism that stores actual data on a storage server rather than block chain. As a result, no one in system can actually tell actual data. Additionally use bunch signature methods to accomplish unknown data trade in public block chain. Subsequently, the security of user's personalities is safeguarded.
- Finally, the proposed DDPS-BC-ATGDS-CC method will be implemented and the efficiency of proposed technique is evaluated using several performances metrics, such as as accuracy, computation of traceability and computation of data sharing are done.
- Finally, the performance of proposed DDPS-BC-ATGDS-CC is compared with existing techniques like SEDS-BC-CC [11], TDS-FAC-BC [12] and APPS-PISS-CC [13] respectively.

The remaining portion of this manuscript consists of: part 2 describes literature survey, part 3 designates proposed method, part 4 illustrates the outcome with discussion and part 5 consists of conclusion.

2. Literature Survey

Among the frequent research work on anonymous and traceable group data sharing at cloud computing using block chain were assessed in this part.

Huang et al., [11] have presented Block chain-depended multi-groups data sharing along anonymity and traceability (PBFT-ATGDS-CC). The anonymous and traceable block chain-based data sharing system for multiple groups was presented. Furthermore, the presented system cannot empower information dividing among

various gatherings with improved security anonymously yet accomplish traceability and non-frame ability. The advantage of this method was high accuracy and disadvantage was low scalability and security.

Ma et al., [12] have presented Trusted data sharing along flexible access control depended on block chain. New accessible encryption along different catchphrases was portrayed; it offers safe and dependable framework for data sharing that built on block chain, searchable encryption, and attribute base encryption (ABE). Analysis of security demonstrates technique satisfies suggested data, keyword index, trapdoor, and query security requirements. Advantages of this method are Enhanced Data Security and Fine-Grained Access Control. The disadvantage of this strategy was that security risks persist despite the fact that block chains provide increased security.

Imine et al., [13] have presented a accountable strategy for protecting privacy in public information sharing programs. It provided a new, responsible approach to protecting privacy while disseminating public data via data externalization platforms. The presented study authenticate any user of the system without affecting their privacy due to its reliance on on signatures. In addition, it distributes all accountability and privacy-preserving services without ever relying on the authority. Advantages of this method are increased ability to measure and collect data. Dis advantages of this method is low storage and high user control.

Yang et al., [14] have presented authorization, traceability, and privacy-preserving cloud auditing for multi-user systems. The presented method assures user identity anonymity and ensures that the tag was compact without requiring the use of group signatures. In the meantime, ensures that at least d managers can collaborate identify malicious user, preventing misuse of one manager authority and providing non-frame ability. Advantages of this method are easy to use and massive storage. Dis advantages of this method is low accuracy.

Liu et al., [15] have presented Block chain empowered cooperative authentication along data traceability at vehicular edge calculating. In the presented method, a secret sharing and dynamic proxy mechanism-base decentralized vehicle identification system with block chain-enabled group authentication was presented. The final validation result was transferred to the central server via the edge processing hub, which has a better reputation and is hidden in a well-planned block chain to complete the decentralized confirmation. Advantages of this method are fewer maintenance issue and high accuracy. Dis advantages of this method is need organized support and high processing power.

Yu et al., [16] have presented Block chain enhanced data sharing along traceable and direct revocation. First, block chain stores generally public keys, user characteristic sets, and withdrawal and performs unified identity authentication. Domain security, privacy protection policies and encryption operations were responsibility of domain administrator. Under Decisional Bilinear Diffie–Hellman (DBDH) supposition, malicious users were tracked and removed at any time, making the scheme secure and resistant to multiple attacks. Advantages of this method are faster operation and high data security. Dis advantages of this method is low accuracy.

Qureshi et al. [17] have presented Anonymous and Traceable Group Data Sharing in Cloud Computing utilizing AES Algorithm. In the presented method a hybrid encryption scheme, where the data is encrypted using a symmetric key encryption technique and the symmetric key is then encrypted using an asymmetric key encryption technique. The system also provides anonymity by using pseudonyms to represent the identities of the users in the group. Advantages of this method are Enhanced Privacy and Improved Collaboration. Dis advantages of this method is no offline access and Bandwidth issues.

3. Proposed Methodology

The DDPS-BC-ATGDS-CC is proposed in this research. This part gives a thorough explanation about the Block Chain and Group Data Sharing in Cloud Computing. The proposed method consists of three layers like user, data sharing and Public service audit layers [19]. All verification data is stored in the public service audit layer to maintain the public ledger up to date. For recording algorithm is needed, by using Downgrade Delegated Proof of Stake based Consortium Block Chain it is done. By using this algorithm the users and agencies access the block chain database. The proposed DDPS-BC-ATGDS-CC method is shown in Fig 1.

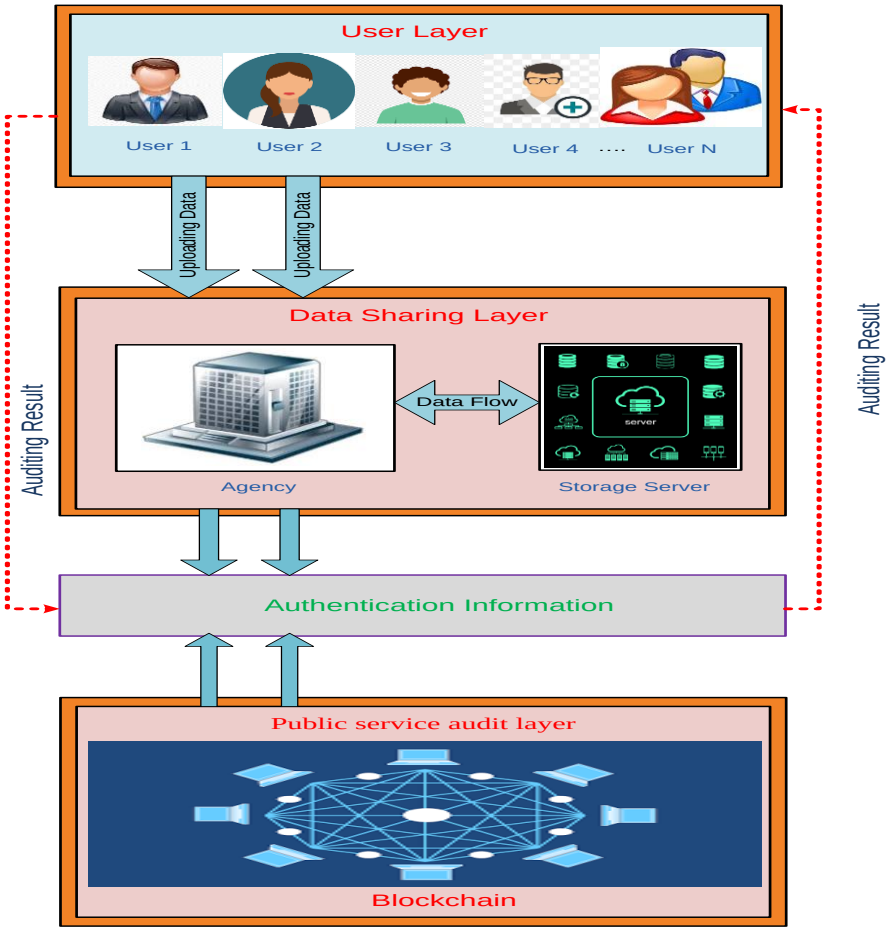

Figure 1: Proposed DDPS-BC-ATGDS-CC method

3.1 User Layer

The User Layer, also termed as Presentation Layer or User Interface (UI) Layer. Its primary purpose is to facilitate user interaction, input, and presentation of information in a user-friendly and intuitive manner. The User Layer encompasses various elements and functionalities that enable users to interact with the underlying system. This includes user interfaces, screens, forms, menus, buttons, and other graphical components that allow users to input data, make selections, and view the output or results. The User Layer acts as an intermediary between the users and the underlying layers of the system. In the user layer it consists of new user and existing users. It confirms that only authorized users able to access the system, specific functionalities and that each user is presented with a personalized experience based on their preferences.

3.2 Data Sharing Layer

The Data Share Layer includes multiple agencies and storage server. The proposed layer shares data to all the trusted users and stores, manages the data. It provides the infrastructure and services necessary for data storage, retrieval, and maintenance. Key aspects of the storage server include Data Persistence, Data Backup and Recovery. The Data Share Layer with storage server ensures that shared data is securely stored, easily accessible, and properly managed within the system. It provides the necessary functionality and infrastructure for users to collaborate, share, and store data effectively and efficiently.

3.3 Public audit Service Layer

The proposed layer consists of block chain network with authentication information. The public verification data of users is stored in an immutable database. The availability and integrity of shared data are ensured by the maintenance of this database by all collaborating authorities. The block chain database is accessible to both

users and agencies for providing a secure and transparent platform for data sharing. For satisfying the properties such as Data confidentiality, Anonymity, Public verifiability, Non-frame ability and Traceability in the block chain an algorithm is used.

3.3.1 Block Chain based Multiple Group Data Sharing Scheme

Block chain is a distributed, decentralized digital ledger system that allows several parties to manage a single database without the need for a central authority. It is designed to ensure transparency, security, and immutability in recording and verifying transactions on data.In a block chain, data's are grouped into blocks, which are then linked together in a chronological and cryptographic manner for forming block chain.

A transparent and unchangeable record of all the data kept on the block chain is produced by combining the hash of the previous block with a unique identifier called a hash found in each block. The decentralized nature of block chain is one of its primary characteristics. The block chain is distributed among a network of computers, or nodes, as opposed to depending on a single central authority.

Block chain technology uses point-to-point network communication technology, distributed consistency protocols, smart contract programming languages, and contemporary cryptography to combine data transmission, processing, and storage technologies across several users. There are three types of block chain networks at the moment: consortium, private, and public. To get Data confidentiality, Anonymity, Public verifiability, Non-frame ability and Traceability an Downgrade Delegated Proof of Stake based Consortium Block Chain algorithm is used.

3.3.2 Downgrade Delegated Proof of Stake based Consortium Block Chain

Downgrading Delegated Proof of Stake based Consortium Block Chain (DDPS-BC) refers to the process of transitioning a different consensus algorithm in a block chain network. DDPS-BC is a consensus mechanism commonly used in block chain networks, particularly those focused on Data confidentiality, Anonymity, Public verifiability, Non frame ability and Traceability. In DDPS-BC, a limited number of selected nodes, known as delegates or validators, are chosen to produce blocks and validate transactions.

Token holders conducted votes to choose these delegates and are responsible for maintaining the network's integrity and reaching consensus on the order of transactions. However, there might be situations where downgrading DDPS-BC becomes necessary. This could be due to changing network requirements to explore alternative consensus mechanisms that better suit the specific needs of the block chain network. The process of DDPS-BC requires careful planning and consideration of various technical and governance aspects.

It involves implementing the new consensus mechanism, modifying the network's software, protocol, migrating existing data if needed, and ensuring a smooth transition for the participating nodes and stakeholders. By downgrading DDPS-BC networks can explore alternative consensus mechanisms that align better with their evolving needs, and optimize the network's overall Data confidentiality, Anonymity, Public verifiability, Non-frame ability and User Traceability.

The proposed DDPS-BC system utilizes the consortium block chain, where every agency represents a member within the block chain network. The system operates through four distinct phases: initialization, data sharing, Data auditing and tracing user.

Initialization:

The initialization of the block chain environment is by agencies, the set of all agencies is expressed as N whose size of the agencies is $l(l \in n^*)$, where each agencies is denoted by $N_j(j \in [1,l])$,agencies is at the value of $N = \{1,2,3,4...l\}$.To find the consensus agencies it is expressed in equation (1).

$$N_{CON} = \begin{bmatrix} N_{j,} \in N, & j \in [1, l] \\ N_{j,} \in N_{CON,} & j \in [1, m] \\ N_{j,} \in N_{U}, & j \in [1, (l-1)] \\ N_{J} \in N_{X,} & j \in [1, n] \\ N_{j} \in N_{B,} & j \in [1, (1-n)] \end{bmatrix} \quad (1)$$

here, N_{CON} denoted as consensus agencies, N_j denoted as agency numbered with j, N_U denoted as the set of trading agencies, N_X denoted as set of witness agencies and N_B denoted as set of agencies nodes. Here the parameters are initialized for the security purpose. User registration is a process in which individuals or entities provide their information and create an account or profile within a system or platform. It typically involves collecting essential details from users to establish their identity, establish credentials, and grant them access to specific features or services. In DDPS-BC Registration is done with manager and then if manager accepts the data will be transferred. User registration in the DDPS-BC is expressed in equation (2).

$$N_{REG} = \left[\frac{M_{th} * l}{C * M_{th} * l} \right] + 1 \quad (2)$$

where N_{REG} denoted as user registration, M_{th} denoted as manager, C denoted as Member certificate and size of the agencies is denoted as l.

Data sharing.

Data sharing refers to the process of distributing and exchanging data among individuals, organizations, and systems. It involves making data available to authorized users, entities in a secure and controlled manner. Effective data sharing practices consider privacy, security, and compliance requirements, as well as the need for collaboration and innovation. The shared file is classified by using equation (3)

$$D_{TSG} = \left[\frac{\sqrt{W_{idth} \times H_{eght} \times Q}}{2(H_{eight} + W_{dith})} \right]_{l} + 1 \quad (3)$$

where D_{TSG} denoted as the shared files with data, The data consists of elements such as width W_{dth}, height H_{ght} and Total number of data's with blocks is denoted as Q. To generate group signature in DDPS-BC file ID is created. The manager receives the data sent by the user. Then, the file is uploaded to the cloud, creating the block. The shared file's authentication details are included in a transaction that the manager creates. The data used by the nodes to confirm DDPS-BC makes up the authentication information. The transaction is then transferred to the block chain network by the management. After receiving the transaction, the block chain nodes check the authentication data. The block chain nodes is verified using equation (4)

$$B_{Nodes} = \frac{T}{\sqrt{2\Pi}} \frac{F_{gt}}{F} \frac{M}{e^2 toBS} \quad (4)$$

where B_{Nodes} denotes the block chain nodes, $e^2 toBS$ is denoted as transaction of the block chain, M Is denoted as hash of the DDPS-BC, T is denoted as structure of nodes , F_{gt} is denoted as file and F is denoted as average distance from all nodes. once the verification process is successfully completed, the Downgrade Delegated Proof of Stake based Consortium Block chain algorithm is executed by the nodes. The algorithm

ensures the synchronization of authentication information for the shared file within the block chain. This leads to the creation of a novel block in the block chain. Each block consists of four main components. Firstly, it includes the previous block hash value which aids to preserve the the block chain integrity and continuity. Secondly, it contains the shared file itself along with the corresponding number of file blocks. This allows for the identification and retrieval of the shared file within the block chain. The third component of the block is the signature S_{Ver} , which provides verification and authentication of the block's content. It ensures the integrity and origin of the shared file and its associated information. Lastly, the block includes a random number for additional security and cryptographic purposes. All the data within the block, including the hash value, shared file, signature, and random number, are accessible to all members in system. Users peruses the ledgers and obtain information across the whole block chain due to this transparency. To facilitate efficient access to specific blocks and files, each manager of every agency maintains a pointer list. This list enables users to locate specific blocks by referencing the data IDs. The pointer directly points to the corresponding block that contains the desired file. The manager publishes the provided pointer list to every users within the same group, ensuring easy access and verification of specific blocks. By utilizing this approach, users within the consortium block chain can browse and retrieve information from the shared ledger while maintaining the security, integrity, and accessibility of the system.

Data Auditing

Data auditing is a process that involves examining and evaluating data to ensure its Data confidentiality, Anonymity, Public verifiability, Non-frame ability and Traceability. By regularly auditing data, organizations can identify and resolve issues, maintain data integrity, and make informed decisions based on trusted information. The use of block chain technology enables the authentication information to be stored in a transparent and decentralized manner, eliminating the need for a trusted auditor. This allows all users within the system to independently verify the shared data. In our scheme, users can acquire the Downgrade Delegated Proof of Stake based Consortium Block chain (DDPS-BC) and the associated signature from the public block chain. By utilizing the block chain's inherent transparency and cryptographic mechanisms, our scheme allows users to autonomously validate the shared data without relying on a centralized authority. This decentralized approach enhances trust, security, and efficiency in the verification process, promoting a more robust and reliable data sharing. The verification of the signature can be represented by the following equation (5)

$$S_{Ver} = U_C + M \times T_f \tag{5}$$

where S_{Ver} is denoted as verification of signature, U_C is denoted as digital signature generated for the message, M is denoted as data or message that has been signed and T_f is denoted as public key associated with the entity of user who generated the signature. In this instance, the user receives the relevant data from the cloud server. Once the data is acquired, the user can create a route to the DDPS-BC.

Tracing user

In this scheme the manager in each agency has the capacity to disclose the data owner true identity. Each manager in the agency acts as a member of the block chain network, contributing to the overall functionality and transparency of the system. When a dispute arises, the manager, can holds relevant information regarding the data owner's identity. By doing this, the manager assists in establishing the authenticity and accountability of the data owner within the block chain ecosystem. The involvement of managers as block chain members adds an additional layer of trust and accountability to the system. Their role in disclosing the real identity of the data owner enhances the integrity and reliability of the information stored and shared within the block chain network. The group member is traced using signature S_{Ver} and traced using equation (6)

$$T_{user} = \sum_{n=1}^{M_{th}} a(n) * S_{Ver} + M \tag{6}$$

where T_{user} is denoted as traced used, S_{Ver} is signified as signature, M implies content in the message, n is denoted as total number of users and M_{th} is denoted as manager. Hence our proposed consortium block chain network, known as DDPS-BC-ATGDS-CC, involves collaborative efforts from all participating agencies. Each agency serves as a representative member within the consortium block chain, with each member functioning as a node. In the block chain network, nodes are carefully chosen, ensuring strong network connectivity between them. The block chain network's distributed consensus process must be used by the nodes to agree transactions that creates a new block. We use the DDPS-BC consensus method in the proposed consortium block chain network. The DDPS-BC algorithm involves the selection of a leader node, tasked with generating a new block in each round based on predetermined rules. If a node acquires support from more than two-thirds of all nodes, it participates in each step. The DDPS-BC algorithm operates under the assumption that the amount of faulty nodes g is less than one-third of total nodes. Consequently, the system necessitates a minimum of $3g+1$ nodes for optimal functioning.

3.4 Security Analysis of Proposed DDPS-BC-ATGDS-CC

The brief security analysis of the proposed scheme is performed using various properties and are verified here.

3.4.1 Property of Completeness

The real data is stored on a cloud server instead of a block chain in the proposed data sharing arrangement. Users within the system obtains verification information through a public ledger, which is the sole data stored on the block chain. Consequently, the data remains concealed from the block chain nodes. Conversely, we employ group signature techniques within the public block chain to facilitate anonymous information exchange, safeguarding the users' identity privacy. This approach eliminates the need for encrypting the shared data before storing it in the storage server. In addition, the session key established utilizing the symmetric balanced incomplete block design technique to guarantee data security in particular situations. Using a shared conference key, the shared data is encrypted to prevent unwanted users from access.

3.4.2 Property of Anonymity

In the proposed method, the user's group signature and the data verification details are publicly available on the block chain. Even in the improbable case that an attacker manages to gain the group signature, it presents a challenge for them to identify the signer. This is due to the statistically zero-knowledge nature of the underlying interactive protocol. As a result, valuable information cannot be obtained without possessing the group signature. However, it is important to note that only the DDPS-BC process is capable of performing this procedure, ensuring anonymity is guaranteed.

3.4.3 Property of Traceability

The manager M_{th} of every group has the ability to access user details and, consequently, can disclose the signers actual identity by cross-referencing the maintained user list. In the event of a dispute, the manager can calculate and retrieve the identity of the signer.

3.4.4 Property of Public Auditability

In the described data sharing structure, Users of the system validate their data independently of a reliable third party by saving verification information in a public block chain. The proposed approach raises privacy issues and creates serious data security threats, because the third party acquires private information from the auditing data. The data stored on the cloud server is susceptible to tampering in an attempt to address these issues. Since the verification data is derived from the entire dataset, DDPS-BC is used in the proposed structure. This enables the rapid identification of even minute changes in the data. Additionally, the immutability of the block chain protects the DDPS data. The data cannot be altered after the registration in the block chain.

3.4.5 Property of Non-frame ability

The proposed research proves that the manager must first launch a traitor tracing request on the block chain network in the event of a dispute before revealing the user's identify. Only once the request has received confirmation from at least two thirds of the nodes will the management move forward with it. This lowers the manager's tracking authority and removes the possibility of power concentration. The proposed method guarantees non-frame ability and maintains equity while tracing the actual identity of a malevolent user.

4 .Results and Discussion

The stimulation is conducted on an Amazon cloud server, utilizing a Dual Core i5 CPU with RAM8.0 GB. The operating system utilized was Ubuntu 16.04. The implementation of group signature with verification algorithms was done using Python, with key parameters set to be 1024-bit long. The obtained results of proposed DDPS-BC-ATGDS-CC technique are compared with existing SEDS-BC-CC, TDS-FAC-BC and APPS-PISS-CC methods.

4.1 Performance measures

Analysis of performance metrics such as accuracy, Computation of traceability and Computation of data sharing are done.

4.1.1 Accuracy

It is the capacity to calculate the precise value. This is calculated by equation (7),

$$Accuracy = \frac{(TP + TN)}{(TP + FP + TN + FN)} \tag{7}$$

where TP denotes as True Positive, TN signifies as True Negative, FP symbolizes as False Positive , FN denoted as False Negative.

4.1.2 Computation of traceability

To compute the traceability of a system, It is measured by following equations (8)

$$TR = \frac{NTI}{TI} \tag{8}$$

where TR is denoted as Traceability Ratio, NTI is denoted as Number of traced items and TI is denoted as total number of items.

4.1.3 Computation of data sharing

The data sharing computation is measured using equation (9)

$$DSR = \frac{SDS}{TDS} \tag{9}$$

where DSR is denoted as Data Sharing Ratio, SDS is denoted as Shared Data Size and TDS is denoted as Total Data Size.

4.2 Performance Analysis

The performance analysis of DDPS-BC-ATGDS-CC is analyzed using various performance metrics. The performance of proposed DDPS-BC-ATGDS-CC is evaluated with existing SEDS-BC-CC , TDS-FAC-BC and APPS-PISS-CC techniques.

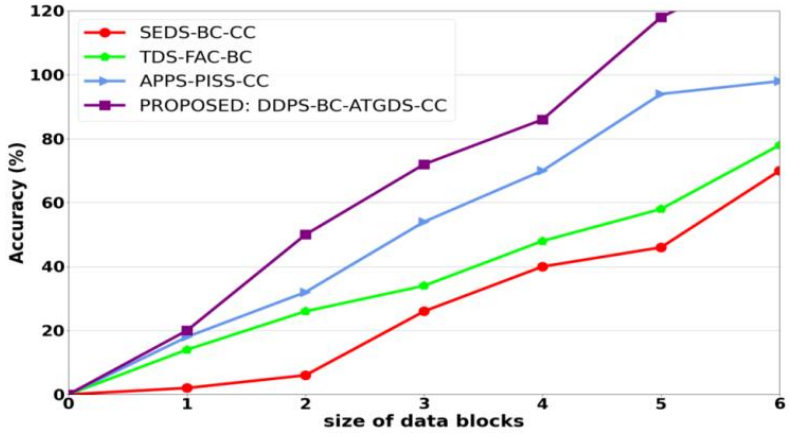

Figure 2: Comparative analysis of Accuracy with various methods

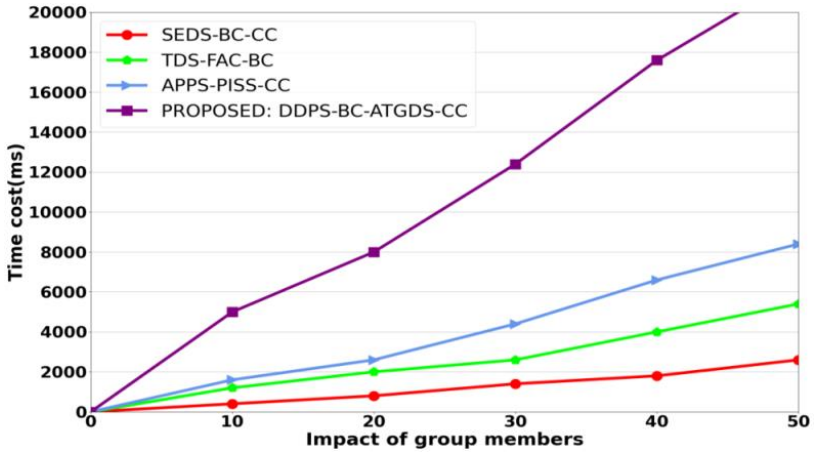

Figure 3: Comparative analysis of Computation of traceability with various methods

Figure 2 shows Accuracy analysis. Here, the proposed method provides 25.28%, 36.45%and 32.20% higher accuracy. Figure 3 shows Computation of traceability analysis and it provides 12.34%, 18.33% and 23.34% higher traceability. Figure 4 shows Computation of data sharing analysis and it provides 29.33%, 22.5% and 12.45% lower time while sharing the data.

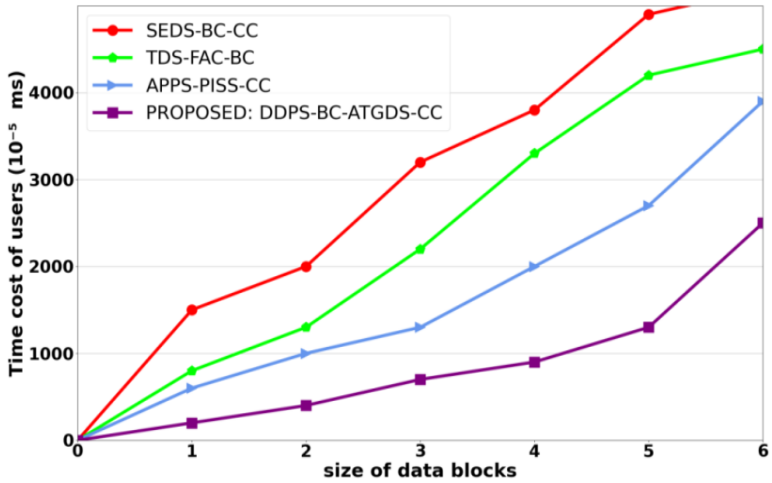

Figure 4: Comparative analysis of Computation of data sharing with various methods

5. Conclusion

This study proposes a block chain-based data exchange strategy that guarantees traceability and anonymity for numerous organizations. The proposed strategy makes safe and dependable data sharing possible without requiring a dependable auditor. Public verification data is maintained by members utilizing consortium block chain technology and kept in a tamper-resistant database, doing away with the need for a reliable auditor. A group signature approach is used to further ensure user identity traceability and anonymity. The group manager has the authority to disclose the identity of the data owner in the event of a dispute to ensure fairness in the dispute resolution process.

Reference:

[1] L. Ogiela, M.R. Ogiela. Cognitive security paradigm for cloud computing applications. Concurrency and Computation: Practice and Experience. 32(8):e5316 2020.
[2] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, M. Guizani. Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. IEEE Journal on Selected Areas in Communications. 38(6):1229-41 2020.
[3] U. Narayanan, V. Paul, S. Joseph. A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. Journal of King Saud University-Computer and Information Sciences. 34(6):3121-35 2022.
[4] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, Z. Zhou. SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain. IEEE Transactions on Industrial Informatics. 17(11):7688-99 2020.
[5] M. Muzny, A. Henriksen, A. Giordanengo, J. Muzik, A. Grøttland, H. Blixgård, G. Hartvigsen, E. Årsand. Wearable sensors with possibilities for data exchange: Analyzing status and needs of different actors in mobile health monitoring systems. International journal of medical informatics. 133:104017 2020.
[6] S.A. Bello, L.O. Oyedele, O.O. Akinade, M. Bilal, J.M. Delgado, L.A. Akanbi, A.O. Ajayi, H.A. Owolabi. Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction. 122:103441 2021.
[7] D. Srivaishnavi, T. Arjun, K. Dhyaneshwaran, R. Deepak. Secure Ring Signature based privacy preserving of Public Auditing mechanism for outsourced data in cloud computing paradigm. InJournal of Physics: Conference Series 2021 (Vol. 1916, No. 1, p. 012079). IOP Publishing.
[8] A. Manzoor, A. Braeken, S.S. Kanhere, M. Ylianttila, M. Liyanage. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. Journal of Network and Computer Applications. 176:102917 2021.
[9] T. White, E. Blok, V.D. Calhoun. Data sharing and privacy issues in neuroimaging research: Opportunities, obstacles, challenges, and monsters under the bed. Human Brain Mapping. 43(1):278-91 2022.
[10] S. Shamshirband, M. Fathi, A.T. Chronopoulos, A. Montieri, F. Palumbo, A. Pescapè. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Journal of Information Security and Applications. 55:102582 2020.
[11] H. Huang, X. Chen, and J. Wang. Blockchain-based multiple groups data sharing with anonymity and traceability. Science China Information Sciences, 63, pp.1-13, 2020.
[12] X. Ma, C. Wang, X. Chen. Trusted data sharing with flexible access control based on blockchain. Computer Standards & Interfaces. 78:103543 2021.
[13] Y. Imine, A. Lounis, A. Bouabdallah. An accountable privacy-preserving scheme for public information sharing systems. Computers & Security. 93:101786 2020.
[14] X. Yang, M. Wang, T. Li, R. Liu, C. Wang. Privacy-preserving cloud auditing for multiple users scheme with authorization and traceability. IEEE Access. 8:130866-77 2020.
[15] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, Y. Zhang. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing. IEEE Transactions on Vehicular Technology. 69(4):4221-32 2020.

[16] K. Yu, L. Tan, M. Aloqaily, H. Yang, Y. Jararweh, Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. IEEE transactions on industrial informatics. 17(11):7669-78 2021.
[17] H. Qureshi, F.U. Rehman, M. Ismail, L. Vaishnavi. Anonymous and Traceable Group Data Sharing in Cloud Computing Using AES Algorithm. Mathematical Statistician and Engineering Applications. 72(1):1469-75 2023.
[18] F. Yang, W. Zhou, Q. Wu, R. Long, N.N. Xiong, M. Zhou. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access. 7:118541-55 2019
[19] J. Cui, F. Ouyang, Z. Ying, L. Wei, H. Zhong. Secure and efficient data sharing among vehicles based on consortium blockchain. IEEE Transactions on Intelligent Transportation Systems. 23(7):8857-67 2021.