International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain-based Solution for Securing Job Card Data Integrity and Payment System using Bi-Quad Merkle Tree

S. Jenifa Sabeena, Dr. S. Antelin Vijila

Submitted: 22/11/2023 **Revised**: 29/12/2023 **Accepted**: 10/01/2024

Abstract: Numerous individuals use cloud - based applications to store and analyse data for a variety of purposes. Because of the untrustworthy verification procedure of data integrity, the user that uploads information to a public cloud has less security. Data authentication, in particular, is critical in storing outsourced digital material and protecting it from tampering by internal or external enemies. The scheme must be equipped with cryptographic algorithms to encrypt data in order to offer privacy features like information confidentiality and authentication. This research provides a blockchain-based secured data management and trusted payment submission framework for the end users. This paper proposed a new form of merkle tree with the name Bi-Quad merkle tree with Moulded RSA and DES (MRDES) encryption algorithm. The proposed model reduces the computation overhead and time complexity of the transactions management process. The proposed model generates a block, which depends on its spatial and temporal information instead of number of transactions per block threshold. This concept helps the concern to localize the tampered or modified block easily. The data integrity is effectively achieved by the Moulded RSA and DES (MRDES) encryption algorithm. The performance of this proposed blockchain scheme is analgised with the help job card details and the results shows that the proposed scheme is significantly better in terms of latency, computation overhead. The proposed merkle tree generations verification time is compared to the traditional merkle tree based blockchain scheme.

Keywords: *Blockchain, Merkle Tree, DES, RSA.*

1. Introduction

Data storage on the cloud is becoming more and more popular. Clients those outsource their data can get a variety of advantages, including a reduction in costs for personnel upkeep and hefty storage management, unfettered access at anytime, anywhere. However, putting data on the cloud may result in a customer losing control over the management of the data, increasing security issues. Data loss or corruption in cloud servers commonly occurs due to a range of factors, including malicious attacks, internal security breaches, hardware failures, and human errors [1-3]. These elements underscore the importance of cloud users routinely employing effective methods for conducting data integrity audits on their outsourced data. Blockchain technology's integration with cloud computing [4], [5], [6], as well as employing the blockchain's security system to enhance the cloud's secure data storage and computation performance, is a promising study area.

Blockchain serves as a mechanism for securely maintaining data, rendering system alterations, hacking, and cheating either impossible or challenging [7]. A blockchain is a network of interconnected computers that replicates and shares a digital record of transactions across the entire network [8, 9]. It functions as a distributed, decentralized, and transparent digital ledger employed for recording transactions across numerous computers, ensuring that retroactive modifications cannot occur without affecting all previous blocks and the consensus of the network [10–14].

Blockchain offers a higher level of security for consumer electronics data sharing and secure payments compared to traditional methods of storing data on external computers or servers, often controlled by a single authority. Users can conduct transactions instantly without the need for approval from banks or credit card companies. The decentralized nature of blockchain enhances its

Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli.
Email: jenifasabeena1996@gmail.com
Assistant Professor, Department of Computer Science and Engineering,Manonmaniam Sundaranar University, Tirunelveli.
Email: antelinvijila@gmail.com

resilience against attacks and ensures that once data is stored, it remains immutable. Furthermore, there is no single point of failure. Blockchain is commonly employed for secure data sharing because it enables multiple parties to exchange data without relying on a central authority. This makes it an ideal platform for data exchange due to its security, transparency, and immutability.

Blockchain technology stands as a top choice for managing and securing digital interactions, maintaining a comprehensive and transparent record of assets while upholding a decentralized, shared ledger system. Notably, 'Smart Contracts' on a blockchain are commendable for automating digital transactions and interactions [15], wherein automatic payments are executed through a smart contract once parties mutually agree that their conditions have been met.

The blockchain consists of a sequence of blocks resembling linked lists, each containing information such as timestamps and transaction data, along with the encrypted hash value of the preceding block within the network. To form a chain of connected blocks, the hash value of the previous block is written onto the next block, establishing a link between them. This process is repeated in sequential order, verifying the integrity of each subsequent block up to the genesis block. The SHA-256 technique is employed to derive the hash value of each block from its contained data, generating a unique code specific to that block. Any modification to the data within a block results in a change in its hash value. Consequently, altering the data in any past block necessitates modifying the hash values of all subsequent blocks, making it infeasible to tamper with the data history.

Cryptography is a technology to prevent unauthorised access of data. Cryptography plays a pivotal role in safeguarding transactions between two nodes within a blockchain network [16]. The foundation of blockchain rests on two fundamental concepts: cryptography and hashing A type of data organisation utilised in computer science is the Merkle tree [17]. As a result, a Merkle tree appears to be a successful illustration of a blockchain contribution system. In this type of system, each tree node is thought of as a commitment, and each leaf node has the potential to be exposed and shown to be a part of the initial commitment. The majority of hash tree methods are binary, meaning each node typically has two child nodes, but they can have more child nodes if needed.

In the field of computer science, a common type of data structure is the Merkle tree, also known as the binary hash tree [18]. It is a logical data structure that aggregates hashes from multiple data blocks to create a comprehensive list of all transactions occurring within a block [19]. While the Merkle tree structure offers numerous advantages, its linear format and the numerous hash operations it requires can lead to suboptimal processing speed. Moreover, the need to store values for each node in the binary tree structure results in significant storage overhead. Consequently, this paper introduces an efficient data sharing and secure payment system utilizing Blockchain and an enhanced Merkle tree with alternating binary and quad layers, coupled with the Moulded RSA and DES (MRDES) encryption algorithm. Figure 1 illustrates the block diagram for the blockchain-based data sharing and secure payment system.

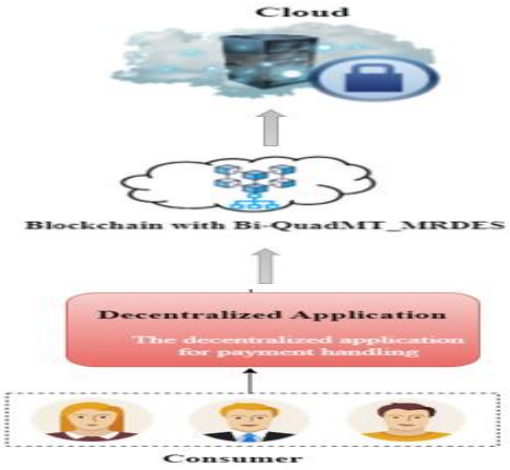

Fig 1: Secured Payment and Data Sharing via Bi-Quad Merkle Tree with Moulded RSA and DES (MRDES) based Blockchain Technology (Bi-QuadMT_MRDES)

2. Related Works

The advancement of blockchain technology has enabled the transition from the 'Internet of Information' to the 'Internet of Value,' giving rise to a genuine peer-to-peer sharing economy [20], [21]. As per a survey report from the World Economic Forum (WEF) [22], it is anticipated that by 2027, approximately 10% of the global Gross Domestic Product (GDP) will be stored on blockchain. Blockchain technology offers a seamless decentralized platform for securely recording, tracking, and managing data related to insurance, ownership documentation, patents, repairs, maintenance, and both physical and intangible assets, all while considering the potential within the automotive ecosystem. Maintaining ledger integrity is a pivotal concern when conducting transactions among stakeholders in the automotive sector.

Users commonly employ various strategies to assess the security of data handling and storage, ensuring the availability and integrity of outsourced data. Ren et al. [23] introduced the Identity-Based Proxy Aggregation Signature (IBPAS) approach to enhance signature verification efficiency and reduce storage and communication bandwidth requirements. Additionally, Ren et al. [24] proposed the innovative Dual Combination Bloom filter (DCOMB) technique, which leverages mining hash computation to establish a blockchain-based query model for Internet of Things (IoT) data. This approach improves data interoperability and generality in IoT database systems. To safeguard the privacy of IoT information systems, Zhao et al. [25] recommended a remote data integrity verification technique based on blockchain technology. Notably, this technique eliminates the need for a third party during the remote data integrity verification phase, making it more suitable for practical implementations in data management systems. Yu et al. [26] have developed an IoT framework that integrates blockchain technology to address privacy and security concerns in IoT devices. This framework offers a number of benefits, including the assurance of data transfer, desirable scalability with authentication, and decentralised payment methods. The authors have presented multiple solutions employing Ethereum software to exemplify the application of blockchain technology in the Internet of Things (IoT) domain, substantiating their proposed hypotheses.

Wang et al. [27] developed the inaugural secure and efficient Provable Data Possession (PDP) model based on blockchain technology for cloud data integrity verification. This model tightly integrates blockchain with the PDP scheme. Blockchain technology was suggested as part of an integration model by Wei et al. [28]. To provide dependable data storage, monitoring, and verification, they deployed a distributed VM (Virtual Machine) agent architecture on the cloud using mobile agent technology. All of the investigations mentioned above use blockchain technology to verify data integrity.

The majority of lodging providers typically speak with guests via a centralised aggregator website [29,30]. The implementation of blockchain can change these perceptions. For example, because of the promise of blockchain technology, travel companies are coming up with creative ways to connect travellers and hotels. As opposed to using a central booking site, they may now trade easily, securely, and dependably using blockchain [31]. Blockchain is a more effective and secure means to monitor activities, maintain data consistency, and archive data history [32]. In complex scenarios, blockchain can eliminate delays and simplify connections, while a traditional database may help in monitoring trades between two parties [33–36]. For instance, in the supply chain industry, certain private blockchain networks link numerous partners and clients, ensuring secure blockchain consensus for data exchange and secure payments [37]. Blockchain technology has the potential to benefit the hotel industry by facilitating increased hotel inventory booking, secure transactions, reducing the role of intermediaries, and mitigating fraud [38].

Many businesses are currently implementing various identity verification methods utilising blockchain technology. These recently created frameworks are far safer than the traditional ones. The personal data can be kept in a Blockchain identification document using ShoCard [39]. The document is hashed and encrypted when the owner digitally signs it. The decentralised application then produces a public and a private key against the document after sending it to the blockchain network. The system-generated public key may be used to verify a person's identification, but changing personal information needs a private key.

Jiang et al. [40] introduced a smart contract-based access control system for access verification,

enabling the sharing of Electronic Health Records (EHRs). This system combines data acquisition and sharing processes to facilitate the delivery of e-medical services through cloud and blockchain technologies. Medical data is collected by IoT devices, transmitted to nearby edge workers for data management and protection, and subsequently exchanged using a blockchain.

Amir et al. [41] introduced a smart contract-based framework using Remix IDE (Integrated Development Environment) for a blockchain-based healthcare system. This innovation promises to transform the healthcare sector's perception of blockchain technology by leveraging the concepts and tools of a public ledger. Health-related information, including medical records, laboratory test results, physician opinions, and precise healthcare data, can be decentralized into blocks, forming transactions. These blocks, aligned with the sequence of events, are integrated into a blockchain as distributed ledgers. The framework is implemented as an Ethereum-based application and evaluated within a hospital setting to assess its maturity. Employing this blockchain approach has the potential to enhance the efficiency of patient care.

Shaikh et al. [42] provided a system for processing transactions that offers safe transactions for online shopping as well as a model that guards against Denial of Service (DoS) attacks. The development of the transaction processing system incorporates blockchain technology, zero-knowledge proofs, and enhanced elliptic curve cryptography. These components collectively enhance the security of typical E-commerce transactions by providing privacy and integrity services.

One of the key tactics for decentralised cryptocurrency systems has emerged: blockchain. Academic and professional communities have both expressed a great deal of interest. However, the majority of modern blockchain-based systems exclusively deal with interparty transactions [43–45]. In many real-world situations, a transaction may involve multiple entities, and if these organizations adhere to the traditional blockchain rules, communication costs can escalate. This introduces a secure peer-to-peer multiparty transaction system built on blockchain technology. Through a mechanism for sharing encrypted information, multiple users can participate in a single transaction concurrently [46,47]. Besides, blockchain technology can protect forgery attacks and IP spoofing [48]. Furthermore, blockchain technology can assist certificate authorities and initiatives like Google's Certificate Transparency in preventing the issuance of fraudulent certificates [49,50].

In general, the greater security of a decentralised system makes blockchain ideal for transactions [51-53]. The data remains safeguarded against accidental destruction or tampering by any party, providing users with the advantage of possessing both a historical and continuously updated record [54]. There is no doubt that consumer electronics benefit greatly from blockchain technology. Blockchain enhances security in consumer electronics, data sharing, and secure payments [55]. Users can conduct transactions without relying on approvals from banks or credit card companies. Decentralisation of the blockchain provides no weakness and increases its resistance to attacks; in addition, information contributed to the blockchain cannot be changed [56,57].

3. Methodology

3.1 Blockchain with Merkle Tree

Blockchain often utilize hash functions like SHA-256 because they are simple to verify but very difficult to counterfeit, enabling the formation of digital signature that blockchain users require to validate themself or their data transfers in front of others. When a user sends a secure communication, a hash of the message is created, encrypted, and delivered along with the message. After the signal is received, the sender decrypts the contents and hash value. The receiver then generates other hashes from the received message. If the hashes match, the communication was secure. This procedure guarantees that an unauthorized end user does not modify the message.

Blockchain connect their blocks using hash algorithms. These blocks are interconnected chronologically, with each block containing the hash of the preceding block. Lastly, hash functions are employed in blockchain to generate user addresses or to reduce the size of public addresses. The SHA-256 algorithm is the cryptography hash function used by Bitcoin. Secure Hashing Algorithm (SHA) output is always 256 bits long. Merkle trees in cryptocurrency store and ultimately prune transactions in each block. They are built

from the ground up, using hashes of specific transactions.

Figure 2 illustrates the general structure of merkle hash tree. A block contains sixteen transactions such as JBC_1, JBC_2,….JBC_{16} and its corresponding hashing outcome is h_1, h_2,....h_{16}. The hashing of h_1 and h_2 yields h_{12} then hashing of h_3 and h_4 yields h_{34}. The two hashes are then hashed one again to get the foundation hash. This approach is often used on bigger data sets as well as subsequent transactions are frequently hashed until there is only one node at the highest level. Hashing is usually done using the SHA-2 cryptographic hash function, although other algorithms may be used as well. The merkle root summarizes all of the information included in the associated transactions and is placed in the block header. It preserves the data's integrity. A merkle tree may be used to quickly and easily determine whether or not a certain transaction is included in the collection.

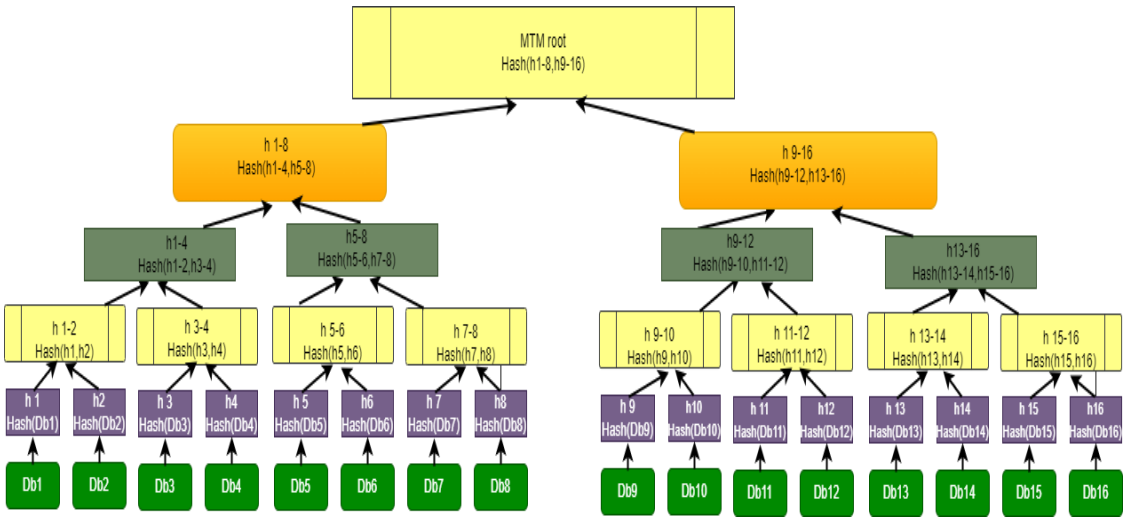

Fig 2: Merkle Hash Tree's Organizational Framework

The hash of non-leaf nodes is referred to as the 'path hash,' whereas leaf nodes' hash represents the actual data. When transmitting data from A to B, ensuring data integrity involves a simple check: comparing the root nodes of the Merkle trees constructed on A and B. If they match, the data remains unaltered during transmission. If not, it indicates data tampering during transmission. Additionally, identifying the tampered node within the Merkle tree is a straight forward process.

3.2 Proposed Blockchain Bi-QuadMT_MRDES Model

The traditional Merkle tree offers numerous advantages, but it requires a substantial amount of hashing processing when dealing with a large number of transactions. It definitely affects the speed of process for huge collection of payment enrolling process. Merkle tree is based on the binary tree concept, hence it reduces the amount of the transaction’s computation into half. Hence this paper proposes an alternate level of enhanced merkle tree to do the tree concept. In this model, at the odd level, the hashing is performed as like the traditional binary mode, in the even level, the hashing is performed as quad mode. This alternative Bi-Quad mode of the Merkle tree enhances performance in terms of computational efficiency and conserves storage space. The search time complexity of a quad tree is O(log2N). In this work a novel merkle tree was introduced, the alternate binary and quad mode of merkle tree is represented as Bi_QuadMT. Its complexity is $(O(\log_2 N) + O(\log_2 N))/2$.

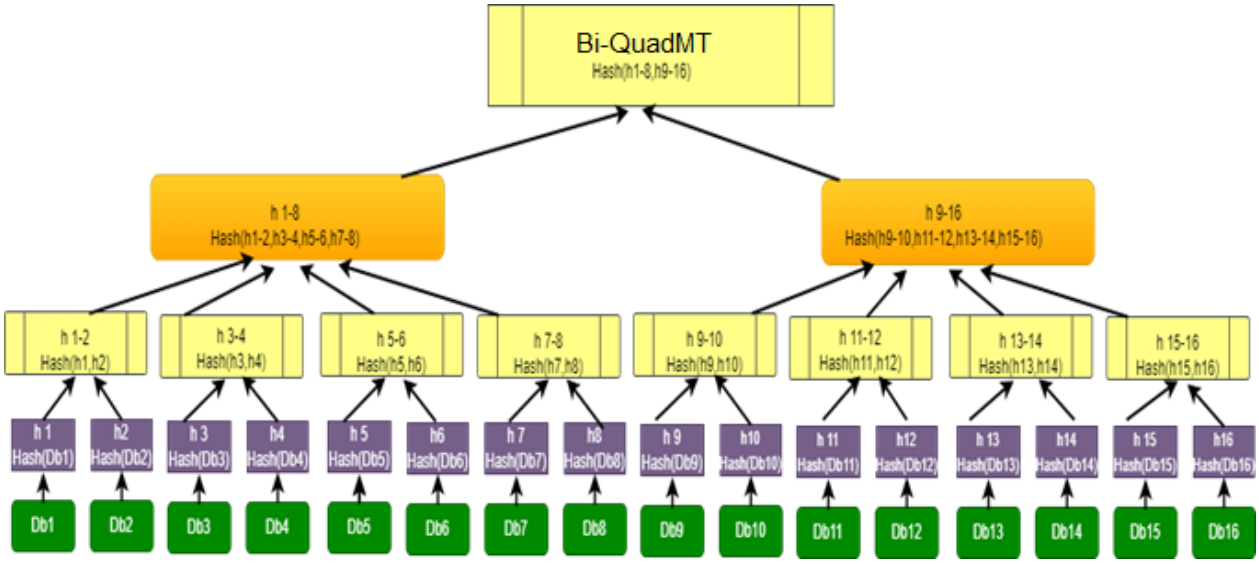

Fig 3: Structure of Bi-QuadMT

This Bi-Quad Merkle Tree reduces the complexity of intermediate node generation and hash calculations. The following example illustrates the operational process of the proposed Bi-Quad Merkle Tree using 16 transactions, as depicted in Figure 3. First, the transactions undergo encryption with the Moulded RSA and DES (MRDES) [62] encryption algorithm, as shown in Figure 4. Subsequently, the SHA-256 algorithm is employed for the hash function within the Bi-Quad Merkle Tree.

A block contains sixteen transactions such as JCT_1, JCT_2,.. JTC_{16} and its corresponding encrypted form with the help of MRDES is represented as $EJCT_1$, $EJCT_2$,…$EJTC_{16}$ and its corresponding hashing outcome is h_1,h_2,... h_{16}. The hash of h_1 and h_2 results in $h_{1\text{-}2}$, and the hash of h_3 and h_4 results in $h_{3\text{-}4}$. Similarly, at the odd level of the first level of the tree, $h_{5\text{-}6}$, $h_{7\text{-}8}$, $h_{9\text{-}10}$, $h_{11\text{-}12}$, $h_{13\text{-}14}$, $h_{15\text{-}16}$ and $h_{17\text{-}18}$ are generated in the same manner.

Then in the second level which is even level, the hashing is done in the accumulated for four hash outputs from its previous level. The hashing of $h_{1\text{-}2}$, $h_{3\text{-}4}$, $h_{5\text{-}6}$, $h_{7\text{-}8}$ produce the first output from the second level as $h_{1\text{-}8}$. Similarly, the output $h_{9\text{-}16}$ is generated as second output in the second level. The third level has an odd depth, and as a result, the traditional binary mode is employed to generate the ultimate output, which serves as the root of the tree. This root is then placed in the block header.

A quad Merkle tree processes 16 input data points and consists of only 4 layers, requiring 27 hash operations. In the case of merkle tree, the structure constructed with 6 layers and 31 hashing functions. As a result of this reduction, the proposed Bi-Quad Merkle Tree model offers lower storage space requirements and computational complexity compared to the standard Merkle tree. The overall overhead is reduced by this alternate model.

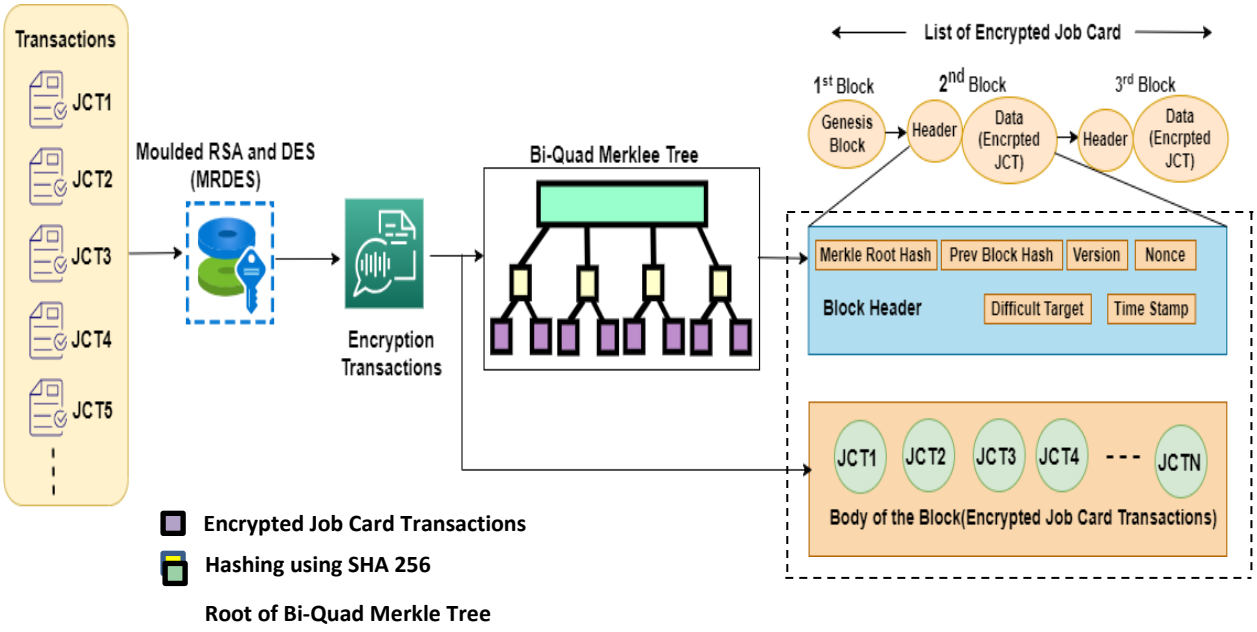

Fig 4: System Model of Bi-Quad Merkle hash tree and MRDES

3.2.1 System Model

As depicted in Figure 4, the system model for blockchain-based cloud storage for job card payment encompasses four key entities: the customer, the first-level security facilitated by MRDES [62], the cloud, and the blockchain with Bi-quad Merkle Tree.

1) Customer: The customer refers to the data owner, who is going to do the secured payment for the posted job card details of very big vehicle servicing network. Job card details from several service centers of the company are maintained by this system. The sample job card details are shown in the following Figure 5. It has corresponding service department number from various area along with the transaction entry date information along general and cost oriented details.

2) Data Security Panel: In this framework the two level of security is maintained by blockchain based and data encryption module. In this data encryption module, all the incoming job card details in the form of transactions are encrypted with the help of the Moulded RSA and DES encryption algorithm. In this algorithm, key generation is carried out by the RSA algorithm due to its good key generation ability. The encryption is carried out by the DES algorithm because of its low power consumption. The performance of MRDES algorithm provides better security to data by setting high key value is clearly stated in the previous work [62].

3) Cloud: The cloud server is maintained by the service provider to manage extensive storage and resources. The blockchain based data are properly managed by the cloud and provide highly verification and integrity of those job card data to the vehicle service-based organization owners.

	A	B	C	D	E	F	G	H	I	J
1	Dept	JobDate	jobno	Vehicleid	UnitNo	Reason	Notes	CostParts	CostLabor	CostTotal
2	1020	1/14/2021	14073	118743	14	04 DRIVER S REPORT	PM SERVICE CHECK TURN SIGNAL CLUNKING NOISE	493.85	0	493.85
3	1020	1/15/2021	14232	230973	13	08 PM SERVICE	SERVICEROB EXT 5604	38.87	0	38.87
4	2111	1/15/2021	14006	1243	116	04 DRIVER S REPORT	NEED 4 PLOW PINS	45	0	45
5	2111	1/15/2021	14140	B39109	178	04 DRIVER S REPORT	INSTALL SPINNER ASSY	175	0	175
6	1020	1/15/2021	14163	574950	215	13 SNOW BREAKDOW	DONT START	140	0	140
7	1020	1/15/2021	14169	A00413	283	04 DRIVER S REPORT	DOG BONE PIN BROKEN	358.58	0	358.58
8	2111	1/15/2021	14000	766153	248	08 PM SERVICE	NEED SERVICE CHECK BRAKES	2139.35	0	2139.35
9	2111	1/15/2021	14155	525670	232	04 DRIVER S REPORT	HYD CAP CHECK ENGINE LIGHT ON	163.47	0	163.47
10	1020	1/15/2021	14157	621909	213	40 NEGLIGENCE	TARP VALVE STICKINGRIGHT SIDE MIRROR BRACKET E	241.33	0	241.33
11	1020	1/15/2021	14164	1226	117	13 SNOW BREAKDOW	HANDLES IN CAB LOOSE	233.42	0	233.42
12	2111	1/15/2021	14165	525999	114	04 DRIVER S REPORT	NO PLOW LIGHTS	11.91	0	11.91
13	2111	1/15/2021	14172	B34632	276	10 ROADCALL	WILL NOT START	1.79	0	1.79
14	1020	1/15/2021	14174	1469	122	10 ROADCALL	WILL NOT START	98.08	0	98.08
15	1020	1/15/2021	14175	68932	147	10 ROADCALL	WILL NOT START	397.87	0	397.87
16	2111	1/15/2021	14176	68933	148	10 ROADCALL	WILL NOT START	358.58	0	358.58
17	2111	1/15/2021	14177	621907	208	10 ROADCALL	WILL NOT START	2139.35	0	2139.35
18	2111	1/15/2021	14181	337657	218	04 DRIVER S REPORT	CONVEORY NOT WORKING	163.47	0	163.47
19	1020	1/15/2021	14182	D1920	164	10 ROADCALL	DONT START	241.33	0	241.33
20	1020	1/15/2021	14183	525998	217	10 ROADCALL	DONT START	233.42	0	233.42
21	2111	1/15/2021	14184	526000	225	10 ROADCALL	DONT START	11.91	0	11.91

Fig 5: Sample Dataset of Job Card Details

4) Blockchain with Bi_Quad Merkle Tree: In this approach, the blockchain concept involves storing the encrypted root of the proposed Merkle tree derived from the customer's job card transactions. This facilitates data verification and ensures data integrity. In this model two Bi_Quad merkle trees are constructed separately for general meta data information and cost details information which is already in encrypted form.

In this work the blocks are maintained based on the spatial information. In the traditional approach, a new block is generated when the length of transactions in the current block reaches a predefined threshold. First it will check the incoming transactions information such as location and time stamp based on that it will add the corresponding encrypted transactions into the specified spatial and temporal matching block. This concept is introduced in this proposed system model which has the ability to localize the tampers on particular branch of the company. This approach also uses SHA-256 hash algorithm to connect the blocks. Finally, it forwards the root, along with the encrypted data, to the cloud for secure storage.

When the concern seeks to access the data, it initiates a request to the cloud server, which subsequently sends this information to the blockchain module, accompanied by its spatial and temporal key-related information. The blockchain utilizes the information forwarded by the cloud to compute the new Bi_Quad Merkle hash tree root. It then compares this newly computed root with the root stored in the block header to validate the data's integrity. The spatial and temporal blockchain hashing based system can identify whether any data is tempered or altered by the malicious user or attacker and can localize in which service branch it happened and its corresponding ledger date of entry. With the help of Bi-Quad Merkle Tree proof verification this proposed model can identify which transaction fall in alteration or tampered.

The following algorithm 1 and 2 shows the process of proposed Bi-Quad Merkle tree Blockchain process with MRDES and its corresponding verification process.

Algorithm 1: Bi-Quad Merkle Tree Blockchain with MRDES

Input: Job Card Transaction JCT with N number of transaction

Output: Bi-Quad Merkle tree (M)

Fetch each transaction JCT_i where (i = 1 to N) and find its corresponding block based on its spatial location and time period

2. Encrypt JCT_i by JCT_i^e=$MRDESE_k(JCT_i)$
3. Generate Bi-Quad Merkle tree M by taking JCT_i^e as the leaf node of tree
4. Store JCT_i^e and the Bi-Quad Merkle Root of M in the blockchain

Algorithm 2: Job Card Details Verification
Input: Unverified Job Card Transaction JCT

Output: Assign Tampered Block vector $TB_i=(tr_1,tr_2,\ldots,tr_N)$,

$$tr_i\begin{cases}0, attack\ free\ block\\1,\ tampered\ block.\end{cases}$$

1. Generate Merkle tree M_{new} of JCT by using the Bi-Quad Merkle tree
2. Find the block from which details has to be extract using the spatial(location) and time period data. Extract the Bi-Quad merkle tree M_{ret} from the identified block.
3. Verify the size of the two trees M_{new} (Merkle Tree generated) and M_{ret} (returned from the block) are same, if so do the following steps for transaction verification otherwise there may be some data missing, hence return the block based output as tampered as tr_i to 1 and stop the further progress
4. The proper comparison is done in recursive mode for both M_{new} and M_{ret}
5. Initial checking is done from the root to the left of the tree and checks the hash values are same, then forward the checking from root to the right side and do the same progress recursively
6. If the node does not match, then set the tampered block vector tr_i to 1 and stop the process.
7. If the hash values are matched form root to end leave nodes means, then it is attack free information and traverse the same progress for child node until all nodes hash values are analyzed.
8. Go to Step 4, until all nodes have been checked.

4. Experiment Analysis

This section evaluates the performance of the proposed B-Quad Merkle Tree based blockchain with MRDES encryption algorithm with various state arts of approaches in terms of latency, throughput, Bi-QuadMT generation time and audit verification time. The latency is measured by the time difference from the Task Completion time (TC) and actual Deployment Time (DT) as (TC-DT) in seconds.

The throughput is measured in terms of number of successful transactions per second. The mean or average latency means it is an average latency of all transactions in the job card datasets. Whereas the average throughput is measured by the average of throughput over the entire simulation or execution time. In this work, the entire simulation is conducted using Python libraries. The data utilized for the simulation is sourced from a vehicle service concern encompassing various units. The system is evaluated with the different size of data transactions up to 1GB.

The following Figure 6 shows the performance of the latency versus workload represented with different size of transactions. The estimated latency of the proposed Bi-QuadMT_MRDES is significantly improved than existing MT_MRDES approach latency in all size of workload. The average latency of the proposed Bi-QuadMT_MRDES is 1.33 seconds faster than the MT_MRDES.

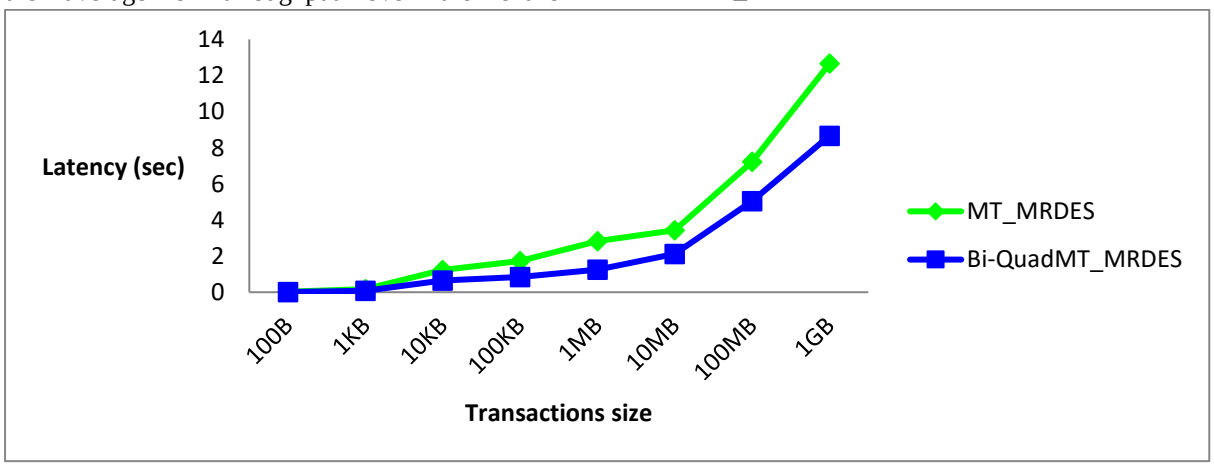

Fig 6: Latency vs Work Load (Transactions Size) Analysis

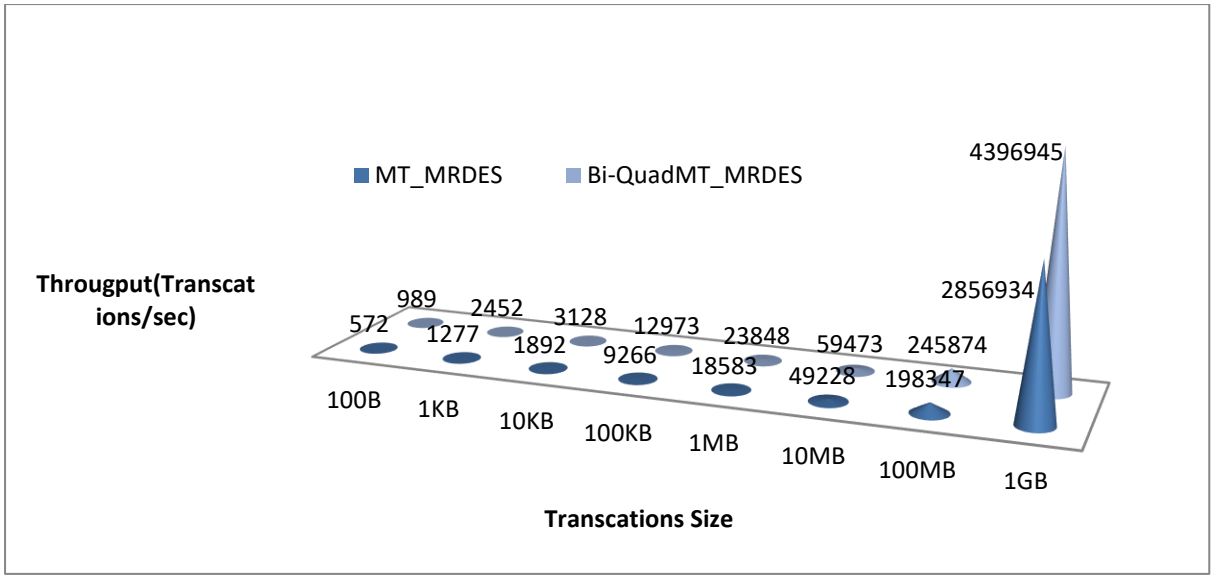

Fig 7: Analysis on Throughput with different Transactions size

Figure 7 shows the throughput analysis on different transactions size. Normally the query process in blockchain method is somewhat more than the normal data storing approach. When compared to blockchain-based data sharing, the proposed enhanced Merkle tree approach demonstrates a significantly higher throughput, allowing for the processing of a greater number of transactions per second in contrast to the existing model. The average throughput of the proposed approach with different transactions size is 0.201 million of instructions per second better than the average throughput of the MT_MRDES.

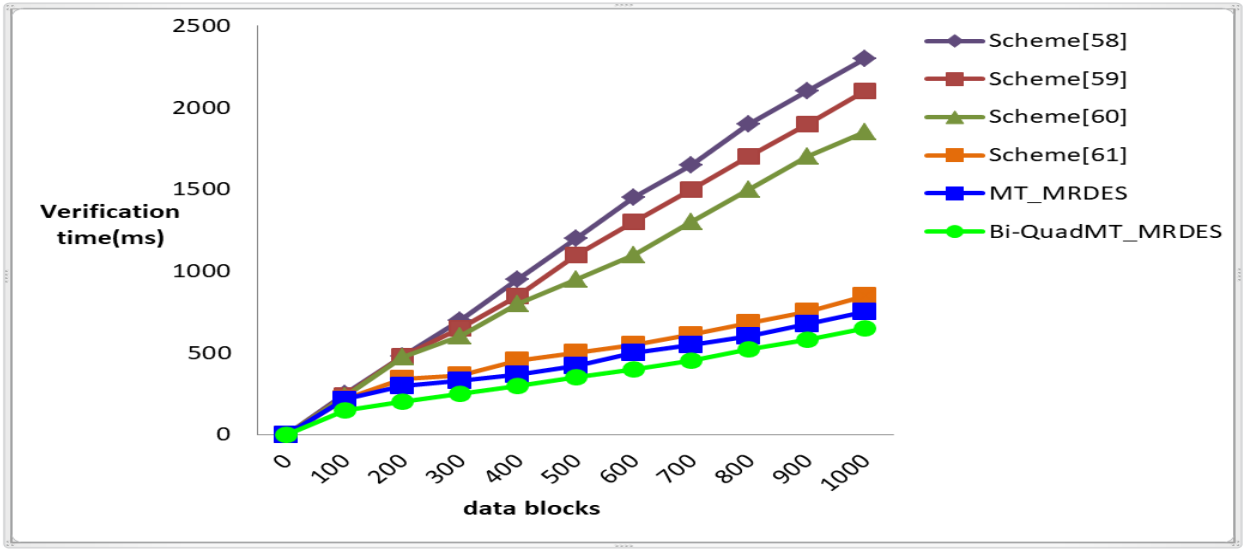

Fig 8: Verification phase time vs Number of data blocks

The Figure 8 shows the verification phase overhead with respect to number of blocks. From the figure 8, it is clear that the verification time (in ms) of the proposed model is 100 ms less than the general merkle tree based blockchain as well as 200 ms less than the scheme described in [61]. When compared with other schemes, the scheme [60] is less than the scheme [59] and scheme [58].

Table 1: Analysis on Computation time (in milliseconds) for Tree generation and Sibling path generation with different size of transactions

	Merkle Tree Generation		Sibling path Generation	
	MT_MRDES	Bi-QuadMT_MRDES	MT_MRDES	Bi-QuadMT_MRDES
100B	0.033	0.011	0.002	0.002
1KB	0.012	0.003	0.003	0.002
10KB	0.15	0.08	0.052	0.047
100KB	0.88	0.12	0.06	0.046
1MB	10.72	6.22	0.083	0.062
10MB	111.6	86.87	0.114	0.0953
100MB	1120	792.76	0.138	0.0991
1GB	10,743.40	6,834.82	0.173	0.131

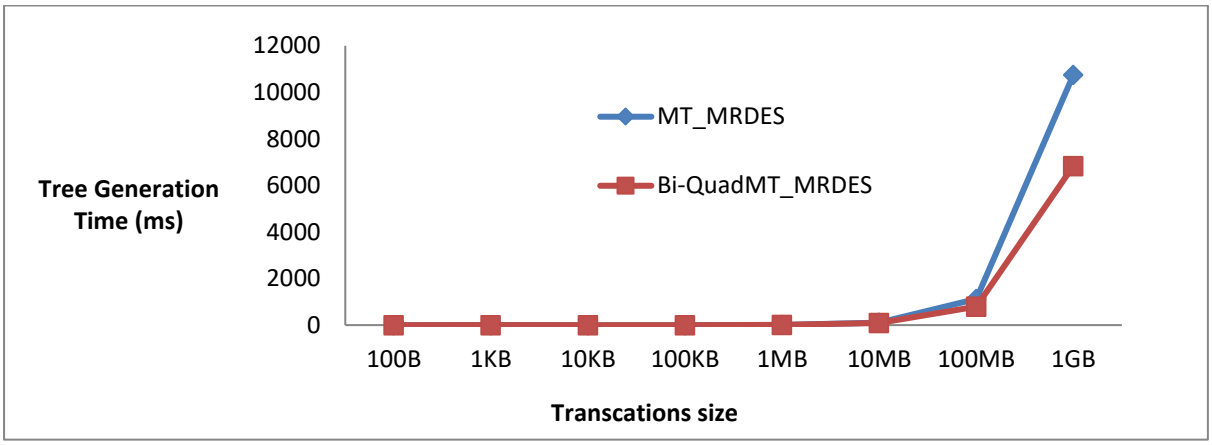

Fig 9: Average computation time for generating Merkle trees in MT_MRDES and Bi-QuadMT_MRDES

Figure 9 illustrates the total tree generation time for the proposed scheme utilizing the default Merkle tree concept. From the table 1 and figure 8, it is clear that the proposed approach attains less tree generation time compared to merkle tree based blockchain algorithm. When the transactions size is 1GB, for MT_MRDES the tree generation time is 10743.40(ms) whereas for Bi-QuadMT_MRDES the tree generation time is 8834.82(ms). The sibling path generation time is average of 0.173 for MT_MRDES and 0.131 for Bi-QuadMT_MRDES on 1GB.

5. Conclusion

Due to the tremendous increase in information sharing and financial transactions in digital form, it needs a specialized framework to protect those transactions and maintain it in secured form. In this paper a new enhanced form of merkle tree is proposed along with the spatial and temporal based block construction to handle the job card details and its corresponding transactions. The proposed alternate mode of tree construction (Bi-QuadMT) leads a model with less computational overhead than the traditional merkle tree generation. The information confidentiality and data integrity are properly handled by the Bi-QuadMT and the data protection is maintained by the Moulded RSA and DES algorithm. The blockchain hashing helps to identify where the tamper had occurred and the Bi-QuadMT proof checking helps find the exact transactions. With the help Bi-Quad merkle tree and MRDES it attains the data integrity and security for the job card transactions process, which helps the customer and the car servicing owners to make secured payment without any alteration in transaction amount. The assessment of the proposed framework's performance focused on factors such as latency and overhead, particularly concerning tree generation and proof verification time. The outcome reveals that the proposed approach incurs lower computational overhead compared to conventional blockchain-based secure digital transformations.

This model holds potential for future enhancements, where lightweight cryptography based on block contents can be integrated to further reduce complexity and enhance resilience against security threats.

References

[1] M. Li and P. P. C. Lee, ‘‘STAIR codes,’’ ACM Trans. Storage, vol. 10, no. 4, pp. 1–30, Oct. 2014.

[2] J. Toutouh, A. Muñoz, and S. Nesmachnow, ‘‘Evolution oriented monitoring oriented to security properties for cloud applications,’’ in Proc. 13th Int. Conf. Availability, Rel. Secur., Hamburg, Germany, Aug. 2018, pp. 1–7.

[3] M. Antonio, M. Antonio, and G. Javier, ‘‘Dynamic security properties monitoring architecture for cloud computing,’’ in Security Engineering for Cloud Computing: Approaches and Tools. Pennsylvania, PA, USA: IGI Gobal, 2012, pp. 1–18.

[4] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ‘‘Identity-based public data integrity verification scheme in cloud storage system via blockchain,’’ J. Supercomput., vol. 78, no. 6, pp. 8509–8530, Apr. 2022.

[5] G. Xie, Y. Liu, G. Xin, and Q. Yang, ‘‘Blockchain-based cloud data integrity verification scheme with high efficiency,’’ Secur. Commun. Netw., vol. 2021, pp. 1–15, Apr. 2021.

[6] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, ‘‘Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain,’’ Inf. Sci., vol. 485, pp. 427–440, Jun. 2019.

[7] Bistarelli, S.; Mazzante, G.; Micheletti, M.; Mostarda, L.; Tiezzi, F. Analysis of Ethereum Smart Contracts and Opcodes. In Advanced Information Networking and Applications; Barolli, L., Takizawa, M., Xhafa, F., Enokido, T., Eds.; Advances in Intelligent Systems and Computing; AINA 2019; Springer: Cham, Germany, 2019; Volume 926

[8] Huh, S.; Cho, S.; Kim, S. Managing IoT Devices using Blockchain Platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 19–22 February 2017.

[9] Hlaing, K.M.; Nyaung, D.E. Electricity Billing System using Ethereum and Firebase. In Proceedings of the 2019 International Conference on Advanced Information Technologies (ICAIT), Yangon, Myanmar, 6–7 November 2019; pp. 217–221

[10] Wood, G. Ethereum: A secure decentralized generalized transaction ledger. EthereumProj. Yellow Pap. 2014, 151, 1–32.

[11] Pee, S.J.; Nans, J.H.; Jans, J.W. A simple blockchain-based peer-to-peer water trading system leveraging smart contracts. In Proceedings of the International Conference on Internet Computing (ICOMP), Las Vegas, NV, USA, 26 April 2019; The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), pp. 63–68.

[12] Gür, A.Ö.; Öksüzer, ¸S.;Karaarslan, E. Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network. In Proceedings of the 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 25–26 April 2019; pp. 204–208.

[13] Albrecht, S.; Reichert, S.; Schmid, J.; Struker, J.; Neumann, D.; Fridgen, G. Dynamics of Blockchain Implementation-A Case Study from the Energy Sector. In Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 3–6 January 2018.

[14] Adeyemi, A.; Yan, M.; Shahidehpour, M.; Botero, C.; Guerra, A.V.; Gurung, N.; Paaso, A. Blockchain technology applications in power distribution systems. Electr. J. 2020, 33, 106817.

[15] Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. Future Gener. Comput. Syst. 2018, 89, 746–764

[16] Li, X., Wang, Z., Leung, V. C., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks: A survey and outlook. *ACM Computing Surveys (CSUR)*, *54*(3), 1-38.

[17] Rahman, M. A., Rahim, M. A., Rahman, M. M., Moustafa, N., Razzak, I., Ahmad, T., &Patwary, M. N. (2022). A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics. *IEEE Transactions on Intelligent Transportation Systems*, *23*(10), 19727-19742.

[18] Zhang, W., Bai, Y., &Feng, J. (2022). Tiia: A blockchain-enabled threat intelligence integrity audit scheme for iiot. *Future Generation Computer Systems*, *132*, 254-265.

[19] Appasani, B., Mishra, S. K., Jha, A. V., Mishra, S. K., Enescu, F. M., Sorlei, I. S., ...

&Bizon, N. (2022). Blockchain-enabled smart grid applications: architecture, challenges, and solutions. *Sustainability*, *14*(14), 8801.

[20] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York, NY, USA: Random House, 2016.

[21] T. M. Fernández-Caramés and P. Fraga-Lamas, ‘‘Design of a fog computing, blockchain and IoT-based continuous glucose monitoring system for crowdsourcing mHealth,’’ in Proc. 5th Int. Electron. Conf. Sensors Appl., Nov. 2018, pp. 1–6.

[22] World Economic Forum. (Sep. 2015). Deep Shift Technology Tipping Points and Societal Impact. Survey Report. Accessed: Jul. 2018. [Online]. Available: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[23] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, and A. Tolba, ‘‘Multiple cloud storage mechanism based on blockchain in smart homes,’’ Future Gener. Comput. Syst., vol. 115, pp. 304–313, Feb. 2021.

[24] Y. Ren, F. Zhu, P. K. Sharma, T. Wang, J. Wang, O. Alfarraj, and A. Tolba, ‘‘Data query mechanism based on hash computing power of blockchain in Internet of Things,’’ Sensors, vol. 20, no. 1, p. 207, Dec. 2020.

[25] Zhao. Q, S. Chen, Z. Liu, T. Baker, and Y. Zhang, ‘‘Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems,’’ Inf. Process. Manage., vol. 57, no. 6, 2020, Art. no. 102355, doi: 10.1016/j.ipm.2020.102355.

[26] Yu Y, Li Y, Tian J, Liu J (2018) Blockchain-based solutions to security and privacy issues in the internet of things. IEEE WirelCommun 25(6):12–18

[27] H. Wang, Q. Wang, and D. He, ‘‘Blockchain-based private provable data possession,’’ IEEE Trans. Dependable Secure Comput., vol. 18, no. 5, pp. 2379–2389, Oct. 2019.

[28] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ‘‘Blockchaindatabased cloud data integrity protection mechanism,’’ Future Gener. Comput. Syst., vol. 102, pp. 902–911, Jan. 2020

[29] Gul, M.J.J.; Paul, A. IoT Geography Chain: Blockchain-Based Solution for Logistics Ecosystem. In The Fifth International Conference on Safety and Security with IoT; Springer: Cham, Germany, 2023; pp. 191–194.

[30] Bhadoria, R.S.; Das, A.P.; Bashar, A.; Zikria, M. Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections. Electronics 2022, 11, 3359.

[31] Butt, G.Q.; Sayed, T.A.; Riaz, R.; Rizvi, S.S.; Paul, A. Secure Healthcare Record Sharing Mechanism with Blockchain. Appl. Sci. 2022, 12, 2307

[32] Shrestha, A.K.; Vassileva, J. Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners. In International Conference on Blockchain; Springer: Cham, Switzerland, 2018; pp. 259–266.

[33] Zhang, Z.; Zhao, L. A Design of Digital Rights Management Mechanism Based on Blockchain Technology. In International Conference on Blockchain; Springer: Cham, Switzerland, 2018; pp. 32–46.

[34] Wu, A.; Zhang, Y.; Zheng, X.; Guo, R.; Zhao, Q.; Zheng, D. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann. Telecommun. 2019, 74, 401–411.

[35] Bisht, D.; Singh, R.; Gehlot, A.; Akram, S.V.; Singh, A.; Montero, E.C.; Priyadarshi, N.; Twala, B. Imperative Role of Integrating Digitalization in the Firms Finance: A Technological Perspective. Electronics 2022, 11, 3252

[36] Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. Future Gener. Comput. Syst. 2019, 91, 527–535.

[37] Li, J.; Wu, J.; Chen, L. Block-secure: Blockchain based scheme for secure P2P cloud storage. Inf. Sci. 2018, 465, 219–231.

[38] Flecha-Barrio, M.D., Palomo, J., Figueroa-Domecq, C., Segovia-Perez, M. (2020). Blockchain Implementation in Hotel Management. In: Neidhardt, J., Wörndl, W. (eds) Information and Communication Technologies in Tourism 2020. Springer, Cham. https://doi.org/10.1007/978-3-030-36737-4_21

[39] Prashant. MY., Deepak. NP.,Abhijeet. RP.,Rushikesh. VK., William. P., 2023. Integrated identity and auditing management using blockchain mechanism, Measurement: Sensors, 27, 2023, https://doi.org/10.1016/j.measen.2023.100732.

[40] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma and J. He, “BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange,” 2018 IEEE International Conference on Smart

Computing (SMARTCOMP), Taormina, Italy, 2018, pp. 49-56.
[41] Amir Latif, R. M., Hussain, K., Jhanjhi, N. Z., Nayyar, A., &Rizwan, O. (2020). *A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. Multimedia Tools and Applications.* doi:10.1007/s11042-020-10087-1
[42] J. R. Shaikh, G. Iliev, "Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security" In 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 155-158, 2018
[43] Hong, H.; Sun, Z. A flexible attribute-based data access management scheme for sensor-cloud system. J. Syst. Archit. 2021, 119, 102234.
[44] Suratkar, S.; Shirole, M.; Bhirud, S. Cryptocurrency Wallet: A Review. In Proceedings of the 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 22–23 April 2020; pp. 1–7.
[45] Thapliyal, H. Internet of Things-Based Consumer Electronics: Reviewing Existing Consumer Electronic Devices, Systems, and Platforms and Exploring New Research Paradigms. IEEE Consum. Electron. Mag. 2018, 7, 66–67
[46] Caldarola, F.; d'Atri, G.; Zanardo, E. Neural Fairness Blockchain Protocol Using an Elliptic Curves Lottery. Mathematics 2022, 10, 3040.
[47] Hamledari, H.; Fischer, M. Role of blockchain-enabled smart contracts in automating construction progress payments. J. Leg. Aff. Disput. Resolut. Eng. Constr. 2021, 13, 04520038.
[48] N. Kshetri, ''Can blockchain strengthen the Internet of Things?'' IT Prof., vol. 19, no. 4, pp. 68–72, 2017
[49] Google's Certificate Transparency. Accessed: Nov. 2018. [Online]. Available: https://www.certificate-transparency.org
[50] T. M. Chen and S. Abu-Nimeh, ''Lessons from Stuxnet,'' Computer, vol. 44, no. 4, pp. 91–93, Apr. 2011.
[51] Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017, 5, 14757–14767.
[52] Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Comput. Secur. 2018, 78, 126–142.
[53] Gao, X.; Zhang, W.; Zhao, B.; Zhang, J.; Wang, J.; Gao, Y. Product Authentication Technology Integrating Blockchain and Traceability Structure. Electronics 2022, 11, 3314.
[54] Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 2652–2657.
[55] Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K.C. A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things. IEEE Trans. Ind. Inform. 2019, 15, 358–3592.
[56] Steichen, M.; FizPontiveros, B.; Norvill, R.; Shbair, W. Blockchain-Based, Decentralized Access Control for IPFS. In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1499–1506.
[57] Gaby, G.; Chandra, L.; Enderson, T. Towards Secure Interoperability between Heterogeneous Blockchains Using Smart Contracts. In Proceedings of the Future Technologies Conference (FTC), Vancouver, BC, Canada, 15–16 November 2017; pp. 73–81.
[58] J. Li, H. Yan, and Y. Zhang, ''Efficient identity-based provable multicopy data possession in multi-cloud storage,'' IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 356–365, Mar. 2019, DOI: 10.1109/TCC.2019. 2929045.
[59] M. Long, Y. Li, and F. Peng, ''Integrity verification for multiple data copies in cloud storage based on spatiotemporal chaos,'' Int. J. Bifurcation Chaos, vol. 27, no. 4, Apr. 2017, Art. no. 1750054.
[60] K. He, C. Huang, J. Shi, X. Hu, and X. Fan, ''Enabling decentralized and dynamic data integrity verification for secure cloud storage via Tmerkle hash tree based blockchain", Mobile Inf. Syst., vol. 2021, pp. 1–17, Nov. 2021.
[61] Z. Liu, L. Ren, Y. Feng, S. Wang and J. Wei, "Data Integrity Audit Scheme Based on Quad Merkle Tree and Blockchain," in IEEE Access, vol. 11, pp. 59263-59273, 2023, doi: 10.1109/ACCESS.2023.3240066.
[62] Jenifa Sabeena.S, & Antelin Vijila. S, (2023). Moulded RSA and DES (MRDES) Algorithm for Data Security. International Journal

on Recent and Innovation Trends in Computing and Communication, 11(2), 154–162. https://doi.org/10.17762/ijritcc.v11i2.6140
[63] Dhanikonda, S.R., Sowjanya, P., Ramanaiah, M.L., Joshi, R., Krishna Mohan, B.H., Dhabliya, D., Raja, N. K. An Efficient Deep Learning Model with Interrelated Tagging Prototype with Segmentation for Telugu Optical Character Recognition (2022) Scientific Programming, 2022, art. no. 1059004,
[64] Venu, S., Kotti, J., Pankajam, A., Dhabliya, D., Rao, G.N., Bansal, R., Gupta, A., Sammy, F. Secure Big Data Processing in Multihoming Networks with AI-Enabled IoT (2022) Wireless Communications and Mobile Computing, 2022, art. no. 3893875,