International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212337 Volume 9, Issue 2, March – April (2022)

RESEARCH ARTICLE

BTDEC: Blockchain-Based Trible Data Elliptic Curve Cryptosystem with Fine-Grained Access Control for Personal Data

K. Mohamed Sayeed Khan
PG & Research Department of Computer Science, Sadakathullah Appa College, Affiliation of Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamil Nadu, India
mrkhan1031@gmail.com

S. Shajun Nisha
PG & Research Department of Computer Science, Sadakathullah Appa College, Affiliation of Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamil Nadu, India
shajunnisha_s@yahoo.com

Received: 03 February 2022 / Revised: 14 March 2022 / Accepted: 19 March 2022 / Published: 30 April 2022

Abstract – In an AI-driven era, data the board is reliant on security confirmation and open commerce. A standard data-sharing organization stage is important in the current data-sharing courses of action, and clients transmit their information to a cloud server for limitation and dispersion. Customers, on the other hand, would lose control of their data the instant it was sent off the server, making security and insurance a major worry. Even though data encryption and access control are regarded as cutting-edge innovations for storing individual data on cloud servers, they only go so far. Regardless, it continues to depend heavily on an external source of validity, the Cloud Service Provider (CSP). To tackle this challenge, they combined blockchain, 3DES ciphertext technology, ECC, and the Interplanetary File System (IPFS). This research focuses on BTDEC, a Blockchain-based Trible Data Elliptic Curve Crypto System for Personal Data. The data holder encrypts the sharing data and saves it on IPFS in this customer-driven way, boosting the decentralization of the arrangement. The standardized data area and unscrambling key will be coupled utilizing 3DES with ECC, and the data owner will disseminate his data-related information and send on keys to data customers using blockchain, according to the built-up confirmation method. The data may only be downloaded and interpreted by the data client whose credits fulfill the confirmation conditions. BTDEC enables the data owner to deny a particular data client at the individual dimension without affecting others, providing him fine-grained network access over his data. When obtaining data, the ciphertext phrase search is almost usually utilized to secure the data customer's security. They investigated BTDEC's security and recreated our technology on the EOS blockchain, proving the concept's validity. Meanwhile, they investigated the limitation and overhead and determined that BTDEC performed well.

Index Terms – Blockchain, Ciphertext, 3DES, ECC, Cloud Service Provider, BTDEC, EOS, Interplanetary File System.

1. INTRODUCTION

The Internet of Things (IoT) and 5G improvements, which supply a vast amount of planning data, have supported the quick deployment of modernized thinking (AI). Data security and assurance, on the other hand, have emerged as the most fascinating issues among information executives and sharing. Individual security has been assessed via data mining and research. The great majority of individuals have historically traded and exchanged knowledge using cloud servers.

Regardless, the majority of cloud storage is sensitive, especially data received from sensors that are close to humans. Personal data, including such lifestyle, calling, and clinical treatment, may be included in this data; if personal data is gained or transmitted unlawfully and connected to the data owner's actual person, it may have serious consequences for an individual.

As a consequence, organizing data and delivering relevant data security and protection has become a significant barrier for any cutting-edge vehicle that relies on massive amounts of data and artificial intelligence. Many safe sharing strategies have been established in the cloud [1–9].

These methods seem to meet the well-being and security concerns that occur when information is shared. Whatever the case may be, they all point to the very same conclusion: they are too dependent just on Cloud Service Provider (CSP). They treat the CSP as an untouchable trust, and most security models assume that CSP is only partly trustworthy, suggesting that CSP will be engaged in the set of data and will not delete it.

RESEARCH ARTICLE

1.1. Problem Definition

The Cloud Service Provider problems might get exposure to the owner of the data, or one of its delegates could make an error that puts the customer's security at risk. While certain approaches, including such trademark-based encryption calculations, seem to give client-defined access constraints, it needs Customer keys are thought to be produced by a trustworthy third party. It is indeed difficult close to consider the idea of these prestigious institutions working together. As a consequence, data owners who transfer sensitive When you send data on the cloud server, you lose all control over the data.

1.2. Motivation

Information is gathered on cloud servers motivated to be significantly impacted by the CSP. Customers may be unable to get information from the cloud organization due to an unavoidable weak connection. By requesting catastrophe recovery assistance, the CSP may be able to improve data security and management dependability. However, a few inevitable circumstances, for example, political concerns, will restrict customers from accessing the data via cloud companies. Every Cloud Service Provider must invest more money on servers to deliver better service, better personnel, server ranch leases, and other items. These expenditures, like the CSP and the upgrading of the organization stage, are growing at an alarming rate. Finally, the customers are held accountable for the CSP's operational expenditures. Given the above, developing a comprehensive customer-driven data sharing system to handle the aforementioned difficulties is critical to all the more probable save data security and individual protection. It doesn't have to depend on a trustworthy third party to store and transmit data, and it doesn't have to be concerned about data loss. With the launch and expansion of Bitcoin, the secret progress, decentralized and self-composed money, was sent out and generated [10]. It may be able to construct such a data security-providing approach with the use of blockchain [11–14]. This review, suggests a blockchain-based data-sharing system. The following are the audit's key responsibilities:

- BTDEC is portrayed as a customer-driven information security sharing platform that brings together blockchain, 3DES, and ECC. To further decentralization, each data holder encrypts the access data and uploads it to IPFS, while BSSPD enables data owners with fine-grained access control. It also provides for the quality-level elimination of a single data customer's privileges without impacting the distinctions of others.
- BTDEC directs that the data owner share data-related information on the blockchain and provide unscrambling keys to data buyers. Before joining up, information consumers must perform a proof of work (PoW) is a document that proves that something has been done. It would be comparable on the road to the Bitcoin extraction and processing, and indeed the information owner may alter the PoW goal wards depending on the number of knowledge customers in the framework.
- BTDEC generates ciphertext get records for each data customer associated with the data. When used in conjunction with 3DES, it assures the data customer's security during recovery and protects the data proprietor's security from data marks.

It rigorously tested this hypothesis on the EOS blockchain, completing all computations and Smart Contracts. It demonstrates that this method is feasible when used in a security evaluation.

The rest of the article is structured as follows. Section 2 elaborates related work. Section 3 discusses describes the cryptography techniques, blockchain technology, and methodology used in the proposed work. In Section 4, a detailed explanation of the proposed work is given. Section 5 describes the implementation setup used in the research work and results and discussion. Finally, section 6 concludes the paper.

2. LITERATURE SURVEY

Swan observed in 2015 that a sufficient "prosperity data house" model [15] for public sharing individual prosperity data & identity data (estimated), with appropriate security and inspiring mechanisms, is still unavailable. At the same time, the developer envisions blockchain being used to create a secure, compensated, and proprietor-controlled health data exchange stage. As per Zyskind et al's floating particular data board design [16], customers own and control the data. Only the hash function of the data collected from the customer's device is recorded on the blockchain, which would be encrypted and stored off-chain. Entry and Information, on either hand, are two permitted trade kinds, with Access being used for board access control and Data to be used for storing information and recovery. Azaria et al. suggested the MedRec framework [17], a distributed leader's platform for digital medical care records based on blockchain technology (EMRs). Because of MedRec's comprehensive and lengthy record, individuals could retrieve personal medical information anytime, across providers and regions. The engineering, on the other hand, is based on a permissionless blockchain with a PoW arrangement that isn't tied to data security, insurance, Alternatively, throughput. MeDShare [18] was initially proposed by Xia et al. as a solution to the problem of clinical huge data gatekeepers, exchanging clinical data in an uncertain environment. Dubovitskaya et al. [19] developed a method for determining and distributing EMR data related to illness patient thinking. It scans metadata and access control cutoff focuses through an assent chain, and

RESEARCH ARTICLE

stores encoded data in the cloud. To maintain data security and transparency, patients may create entry control measures. Even though the newly presented blockchain-based data trade plans provide a solid framework, the vast majority of them merely express the arrangement's concept while excluding the required show execution subtleties. A few researchers have now designed and published all of the most amazing access control processes on blockchain to secure data security and protection while exchanging data in the next years. Liang et al. built a client medical data-sharing architecture using the Ethereum Platform consortium chain [20], in which transmitted capacity is employed as a knowledge stockroom and a blockchain record is used to document activities such as pursuits and updates. Simultaneously, the Hyperledger component of the main organization is utilized to construct consumers' integrity assessments, and the channel model is employed to get the insurance. Fan et al. developed a proof-of-stake smart sharing service for diverse relationship information exchange and secure certification inside the 5G future [21]. The primary purpose is to construct a cryptocurrency trading strategy that can be utilized to illustrate a segment strategy. The system offers a task-based inductive control model that considers the transit requestor, content supplier, visitor, and enter start and end. Zhang et al. [22] created a smart contracts data sharing system for Automation association assignments. This method creates two sorts of chain systems: DataChain and BehaviorChain. DataChain is used to govern internet connectivity, whereas BehaviorChain maintains access records and ensures that they cannot be manipulated. It might examine these distinct degrees of access. Zhou et al. developed cryptography archives sharing architecture [23] to reduce unnecessary reporting sharing during the examination of logical articles. The arrangement uses Authorization Language to control access to information kept on-chain (ALC). A subsection system should be developed for every combination of consumers and services on the blockchain. Patel described a ledger merge media sharing architecture [24], wherein the patients may establish access conditions and blockchain is employed as a file storage structure. It underlined that, although this strategy may obtain data through a few stitches, no controls or safety procedures have been adopted. BacCPSS, a blockchain-based authorization system for huge amounts of data, was submitted by Tan et al, at the Cyber-Physical Social System Conference (CPSS). BacCPSS detects customers using a blockchain address and keeps an analyzed customer framework on the Blockchain System to guarantee that the critical errands permitted in the passage cross-section are satisfied. Previously, data-sharing system access control approaches either required a huge number of access rules to be recorded just on the network or have been utterly incapable of delivering fine-grained admission control. Although neither the sector administration system nor the RBAC is suitable for conveying circumstances such as blockchain.

DES is often considered the best method for managing information security and insurance concerns in a distributed setting. As a consequence, researchers have exploited DES to offer perfectly all-right network access to blockchain data. Jemel and Serhrouchni [26] presented a decentralized verification control system. Surprisingly, experts employed blockchain nodes to confirm the legality of customer access consents using the 3DES estimation. The framework differentiates between two sorts of trades: policy creation and access acquisition. It was unable to adapt to more complicated demands since it does not utilize Smart Contracts. Sun et al. presented a system for safe collection and useable availability of digital healthcare data that incorporates expanded affirmation control via the use of ABE and blockchain [27]. Trained practitioners used 3DES to encode patients' clinical information, saving money on ECC. Excellent ideas, on the other hand, are seldom carried out. As a consequence, only a subset of the DES constraints encoded in transactions is transmitted, making more complex commercial transactions harder to execute. Customers exchange secret keys using the approach developed by Wang et al [28]. It recognizes that the owner of the data possesses fine-grained access control. Meanwhile, ciphertext watchwords are obtained using the Ethereum Smart Contract. However, it prefers stable off-chain customer interactions and does not enable authorization repudiation. Pthisnaghi et al. introduced MedSBA [29], a blockchain-based clinical data collection and limitation method. Updates and approval rejections are handled using a distinct specialized method to cover the prior transaction; nonetheless, clients who do not want the keys denied will be needed to recharge the keys.

The phrase "distribution registration" consists of assets or organizations made accessible over the internet. The creators of [10] sought to emphasize most well security problems in inappropriate registration so that salesmen, investigators, and customers are aware of the main dangers, what to look out for, and the numerous solutions available to solve these concerns. [11–13] created a method for identifying Distribution Denial of Service (DDoS) attacks, which may produce a big quantity of traffic for a company and endanger Internet Service Providers. Early results indicate that the proposed structure outperforms existing solutions in terms of acknowledgment execution. [14] Created a security model that examines the exploratory boundaries of an opponent affirmation architecture for moving data in a circulated registering design to tackle the risks of appropriated figuring. The review findings show that the suggested structure is more effective than the current ones. [15–17] proposed the use of an I-AES-based strategy in the creation of a private informational index. It also offers a speculative technique for controlling the overwhelming amount of 5G devices that might be employed in IoT. The first results suggested that the new strategy beat the existing services in respect of processing time and

RESEARCH ARTICLE

throughput. [18–20] created a practicable energy board estimate to aid an IoT connection and its design. It utilizes a cringeworthy condition progression-based vital organization plan to find secure and dependable data bundle transmission easy approaches to the target. Automotive organizations also use a bug monkeys synchronization approach to reduce the amount of time it requires for packets of data to transit without spending a great deal of effort. The testing results show that the proposed approach works well to reduce energy consumption, data bundle construction, and long-distance transmission. [21] Developers handled the issue of data confidentiality and execution by providing a perspective for trust translation, generating rare situations center point password protection, and building a guide for implementing changes in consumers and the locations.

The researchers of [22] conducted an Artificially Intelligent estimate to reduce response time and organize traffic by allocating different tasks to clouds and fog servers. Exploratory findings indicated that this cycle greatly lowers reaction time when compared to earlier strategies. The authors of [23] hoped to show how much a fog figure structure may lessen the security problems that afflict typical IoT computing framework, as well as how it could be enhanced in the future by developing an architecture examining at applications with the proposed framework at its heart. In [24, 25], the authors investigated data storage, transparency, trustworthiness, and the idea of organization, as well as what the suggested design may mean for fog registration, the cloud architecture, and fluctuating edge management. The [26] planners presented a blockchain-based remedy to the board's security data leakage concern. Centre and energy terminals are connected towards the model it displays, making data collecting easier. The creators advocated for blockchain-based security.

3. PRELIMINARY

3.1. 3DES and ECC are Two Cryptographic Algorithms

Bethencthist et al. [30] endorsed the 3DECS approach. 3DES is yet another encryption system, as contrasted to RSA and ECC, and those are both public-key encryption schemes. In AES, the secret key correlates to the client's characteristics, and indeed the entry approach is incorporated in the encrypted message [31]. If the characteristics of the decompiling application match the admission strategy, the contents must be decrypted. 3DECS is also used for selective access control. In summation, these steps of 3DECS are essential to age, and decryption, which corresponds to the calculations:

$$Setup\ (\lambda, S)\ \rightarrow\ (PSK, MSK) \qquad (1)$$

As shown in equation (1), the installation calculations are a randomness method that is used on a trustworthy key distribution network regularly. To generate the frameworks digital certificates PSK and the environment ace key, the technique traverses a protected perimeter and sets the characteristics S. MSK

$$KeyGen(PSK, MSK, \omega)\ \rightarrow\ USK \qquad (2)$$

As shown in equation (2), based on the methodology digital certificates PSK, the infrastructure private key MSK, and indeed the informational client's properties, the classification method calculation offers a virtual need USK for the informational client.

$$Encrypt\ (PSK, M, A)\ \rightarrow\ CM \qquad (3)$$

As shown in equation (3). a knowledge holder is the one who conducts the encryption computation. This same foundation data encryption PSK, the compressed communication M, and indeed the authorized access structure are combined to create the cipher-text CM. A note on the entrance strategy.

$$Decrypt\ (PSK, CM, USK)\ \rightarrow\ M \qquad (4)$$

As shown in equation (4), the information client performs the unscrambling computation. The new framework asymmetric key Packet switching, the customer's encryption key USK, and indeed the ciphertext CM are the bits of feedback used in the computation. The cryptosystem will be demodulated and the subtext M retrieved if somehow the intelligence client's quality set fits the entry strategy.

3.2. Blockchain

Satoshi Nakamoto first proposed the blockchain idea in his Blockchain publication [10], and it has been based on encryption and a traditional structure. The blockchain's data is divided into frames, including one that corresponds to a new solicitation. Private information and non-forgery are provided via cryptography and arranging methods. In its most basic form, A distributed ledger, or blockchain, is a historical reminder that can't be addressed, and it's the technology that enables cryptographic monetary forms like Bitcoin.

3.2.1 Smart Contract

The terminology "savvy contract" refers to a situation in which large computerized monetary forms, such as In the early stages of blockchain innovation, BTC and LTC have more successful uses. In his white paper about Ethereum [32], he says, Buterin introduced the notion of Smart Contracts, which established the main blockchain platform with an extrapolated Fully complete language. Shrewd Contract [33] defines an automation trade show as "a mechanized tech conference which thus performs out the possible options of the understanding." A Smart Contract is a computer program that functions naturally inside the blockchain's trusted environment, enabling the blockchain to handle more complicated transactions. As shown Figure 1 displays a blockchain-savvy understanding of how things function. From a strong educational background, blockchain may be

RESEARCH ARTICLE

considered as a control structure bound by transactions, with a publicly available report that can be traced all the history long to the Genesis Block. Customers may make and transmit transactions at any point inside the blockchain organization. All rectangle manufacturers will adopt the vital system after the transaction.

All centers will finally achieve the anticipated finish as well as upgrade the global state as a consequence of the arrangement approach. A transaction may do tasks like transmitting one Smart Contract or calling a blockchain Smart Contract and running it in a sandbox. The elements of a superb blockchain agreement are as follows:

- The Smart Contract's execution and current global state are accessible to everybody on a publicly available report that cannot be changed.
- Trusted spread channel: after scrambling the message that used the recipient's public key, the transporter may send it via the blockchain. The communication will be conveyed to the recipient and will be documented on the blockchain securely and irrefutably.

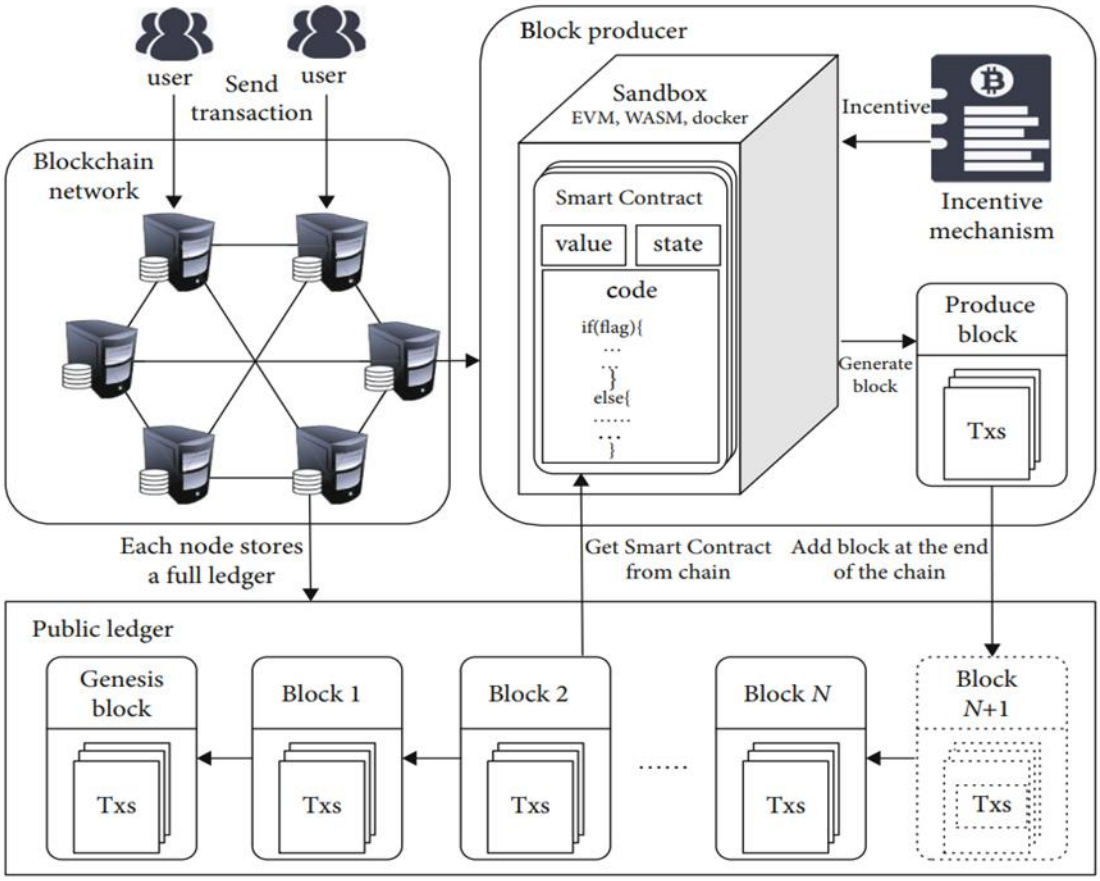

Figure 1 The Smart Contract's Functioning Mechanism on the Blockchain

3.2.2. EOS Transaction

The three most important components of the EOS blockchain are address, record, and exchange.

Every client in EOS has a record, which implies it is all addressed by different ECDSA key sets (pk,sk). To generate an EOS address, the public key employs hash work and base58 coding. The transaction is tagged and validated to ensure that the private and public keys are used independently. If a customer intends to utilize a Smart Contract on the blockchain, he must first conduct an exchange to do so Tx [34].

$$Tx = (Ref\ block, t, Sigu(Chain\ ID, Tx), Action\ (Code, Name, Authu, Data)) \quad (5)$$

The Reference blocks allude to that same square quantity and header of a freshly created square to avoid transactions from surfacing on a spreading chain. This same identification of the client who started the transaction using his public key is confirmed using the client's particular data on the exchange.

RESEARCH ARTICLE

Sigu(Chain ID, Tx) represents the child's specific data on the exchange. While Software is the identifier of something like the Smart Contract to somehow be called, Name is a Smart Contract method to be used, and Authu is used to assess whether the client who began the trade have agreed. Data refers to the parameters that will be provided into the agreement, while Action refers to the action that will be carried out.

3.2.2. EOS Data Persistence

It is essential to maintain the knowledge in the Smart Contract since the involved restricts will be freed when the Smart Contract is done, and all the knowledge in the applications will be erased. The data must be kept in Ethereum Smart Contract key-value sets, making it more difficult to address more complex requests. It emulates Multiindex Containers in the Boost library using a C++ class entitled eosio::multi index (henceforth referred to as multi-list) in EOS. In a common data collection, each multi-file may be considered as a table. Each table line may store one item, and the credits for the article could have been any C++ type of data. As a consequence, the table formed by EOS's multi-record is almost as adaptable as traditional databases. One of the most essential aspects of multi-list is the ability to employ an important key as both the main pages and 16 supplementary records. Consumers may obtain any of these lists and add, delete, edit, and select information that uses the list emplace, remove, alter, and search features.

3.3. InterPlanetary File System (IPFS)

IPFS is a moment in time decentralized version of the File System aimed at establishing everlasting and diverse and powerful along with network storage network transmission protocols. IPFS is a high amount block storage format that combines content addressing hyperlinks by merging current infrastructure including BitTorrent, DHT, Git, and SFS (self-certifying File System). Any restricted, such as text, images, music, video, and website code, is converted to a permanently protected hash algorithm unique to the address once transferred to the IPFS network, and indeed the participating nodes do not need to trust each other. On the internet, this address is known as a URL (Uniform Resthisce Locator). If the user wants to utilize the information, it should go to this place first.

4. PROPOSED SCHEME

4.1. BTDEC's System Model

They've formulated the following plan: IPFS, blockchain, data proprietor, and data client are the four components of BTDEC. The DO encrypted his data and transferred it to IPFS, where it is then recorded and the key unscrambled using a blockchain Smart Contract. Fine-grained access to information control is provided using 3DES and ECC. Only individuals who meet the entrance conditions are permitted to retrieve and decrypt the shared data, which is stored on the DO's blockchain. The strategy is decentralized in its entirety. To guarantee data security and transparency, the data is represented and stored in the IPFS. The DO and DU are stored in the blockchain and are irreversible. These four sections have the following particular functions and responsibilities:

- Create a safe and reliable stockpiling solution using IPFS. The motivating factor structure ensures that IPFS knowledge will never be blocked.
- Blockchain: The blockchain contains all of the publicly available information and processes new information for the whole plan. Similarly, it may have been used to send secure communications first from DO to the DU. It is the plan's foundation of trust, yet there might not be a single reliable outsider to be found. In BTDEC, there are two different types of Smart Contracts. Client information is provided to DSContract from UMContract, which keeps track of them.
- Data owner: this individual is responsible for creating and spreading the Smart Contract, according to the plan. The DO may be forced to divulge his information-sharing methods and institutional capacity over who had the access to it. Furthermore, the DO has the power to give or cancel admission authorizations for a DU.

Data user: the DU is the individual who wishes to use the shared data. DU will unwind the placement and key to acquire the common information when his qualities match the approach given in the ciphertext.

It implemented a 3DES, ECC approach based on [35], with the entire client's ID included as nothing more than a component to handle authorization denial. [36]. with the help, it learned how to utilize BTDEC's watchword ciphertext search. The accompanying interpretation for each advancement point in Figure 2 is as follows:

1 The Department of the Interior is responsible for creating and spreading Smart Contracts. In our configuration, individuals have two Smart Contracts. Clients' participation, a commodity the administrators, the individuality of the committee, and ratification are all widely remembered for UMContract. Everything concerning transferring information, changing access arrangements, refusing permission, and retrieving information is remembered by DSContract.

2 The DO creates the environment private keys and premise public key on the fly, then saves the foundation public key in DSContract.

RESEARCH ARTICLE

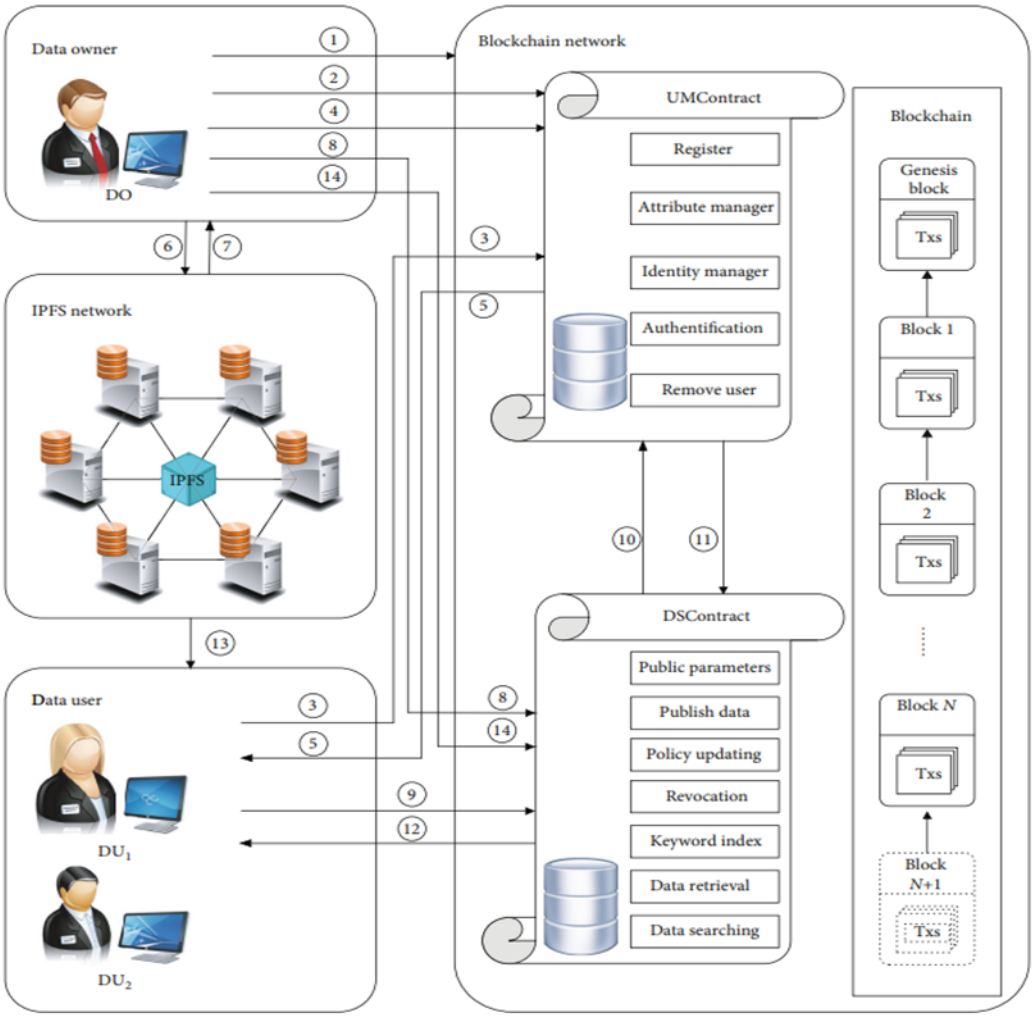

Figure 2 System Model of the Proposed Approach

3 The DU must utilize UMContract to apply for enlistment and supply his EOS accounts and public key. The DO utilizes the public key to interact with it, and even before disseminating the encrypted message to the blockchain, it encrypts the message. Again, when the encryption key has been unscrambled, the message must be acquired by the appropriate DU.

4 Each DU whom applications for a DU is given a remarkable uid, which functions similarly to a personal personality key and a mystery inquiry key. The DO will deposit those same two keys, together with all the uid, in the Smart Contract after encrypting them using the DU's matching public key.

5 The DU gets and decrypts the certificates' ciphertext data using its corresponding key.

6 The DO chooses the topsy-turvy encrypted calculation key at random, encryption the offering data with it, transmits the cryptographic hash to the IPFS organizational, and IPFS assigns a location to the ciphertext.

7 The DO develops an entrance technique for spreading knowledge and a disavowal list for each characteristic in the approach and then encapsulates the position with the available information unscrambling key. There are no characteristics related to the information in the DUs in the denial list.

8 The DO chooses watchwords to produce plaintexts files for knowledge DUs, and then uses DSContract to save the files and data.

RESEARCH ARTICLE

9 The DU picks a passphrase from the knowledge to be obtained and creates an inquiry token using the disguised entrance work.

10 The DU tells DSContract to start looking for the best data. To verify the DU and establish whether it is legitimate, DSContract will contact UMContract.

11 The verification result is returned to DSContract via UMContract. If the DU is sold legally, the harvesting capacity will increase.

12 DSContract provides the indexed lists to the DU.

13 The DU decodes the obtained information-related data using his quality private key. If his unrevoked characteristics meet the admittance requirements, the IPFS destination for the decrypted contents, and even the decompression key, will be sent to the DU. By acquiring the cryptographic hash of the shared information from IPFS, the DU may very well be able to decode it.

14 A DO may revoke a DU's characteristics. Access to particular common information and add the DU's uid to the reliability. A renouncement lists. The DO will then build a new ciphertext and use DSContract to change the information associated with it.

5. RESULTS AND DISCUSSIONS

To put this idea into reality, it will construct a 3DEECS that allows authorization repudiation and connect it to the EOS blockchain. This section delves into the details of with us EOS-based Smart Contracts, as well as BTDEC's unique architecture.

5.1. Design of Smart Contracts

It divided the Shared Ledger in the plan into two pieces, UMContract and DSContract, to make the rationale more transparent. UMContract is used to monitor DU's identity, whereas DSContract is utilized to control data exchange activities. It'll look into the documentation of the DO having signed the _self agreement.

5.1.1. Contract for User Management (UMContract)

As shown in algorithm (1) SetTarget, GetUserByUid, Apply, Register, and Authenticate are the five function interfaces that make up the UMContract. The following is how it set up UMContract. Create a multi-index called table user for the three-tuple A, uid, Pkcom to represent a DU, where A is the DU's EOS account, uid is the DO's unique ID, and Pkcom is The DO's public key is used to communicate with DU. Let A represent the table user's primary key, and account idx represent the matching index. Allowing uid idx to be used as a complement to uid. Let target be the value of the PoW's target.

```
Input: newTarget
Output: bool
Begin
if msg.sender is not _self then
   throw;
else
   target = newTarget;
return true;
end
```

Algorithm 1 SetTarget

- SetTarget: These capabilities point of interaction will be programmed to execute whenever UMContract accepts an engagement (UMContract, SetTarget, Auth, (new objective)). To alter the difficulty of PoW, it must be utilized by the DO who agreed. The DO may create PoW issues when there are a large number of consumers in the framework.
- GetUserUid: This capacity connection point will be programmed to execute whenever UMContract receives transaction (UMContract, GetUserByUid, Auth, (account)). It must be utilized by the DO who negotiated the deal to receive so now all of DU's data, which again is depending on his uid.
- Apply: This capacity connection point will be set to run when UMContract gets an activity (UMContract, Apply, Auth, (from, pk, nonce)). The DU uses it to submit an application for enrolment in the system.
- Register: This capacity connection point will be set to execute when UMContract receives the action (UMContract, Register, Auth, (record, and id)). It must be utilized by the agreement's creator to complete a DU's enrollment.
- Authenticate: This function interface will be triggered to run when UMContract receives a given operation (UMContract, Authenticate, Auth, (from, method, account, id, args)). It verifies the identity of a DU that has already been requested by another contract before informing the caller of the findings.

5.1.2. Date-Sharing Agreement (DSContract)

As shown in the algorithm (2), (3), (4), (5) SetPK, SetSK, AddData, PolicyUpdate, Search and EndSearch, and Remove are the six function interfaces that make up the DSContract. This is how it went about getting DSContract up and running. The public parameters of the system will be referred to as PK. The multi_ index table sk constructed for the two tuples (A,

RESEARCH ARTICLE

SK) matching connection between both the DU's membership and his attribute private key. For table sk, let A be the primary key and aidx be the corresponding index. Assume two tuples (fid, cf) represent shared data, with fid denoting the shared data's id and cf denoting data-related metadata. Introduced a multi-data table for it, using fid as the primary key and fid idx as the index. As an index of DU connected to shared data, develop a non-linear and non-search table with this tuple (id, A, t, fid), where Someone who is the DU's EOS account, t is the searches means of exchange, and fid is the id of shared data in the data table. saidx, t idx, and sf idx are the secondary indices in the search table, which stand for A, t, and fid, respectively.

```
Input: uid
Output: all information of DU
Begin
if msg.sender is not _self then
   throw;
else
   user_row = uid_idx.find(uid);
return user_row;
end
```

Algorithm 2 GetUserByUid

```
Input: from, pk, nonce
Output: bool
Begin
u = account_idx.find(from)
if u != null then
   u:Pkcom = pk;
      account_idx.modify(u);
   return true;
else
   pow = SHA256(SHA256(f rom | pk | nonce));
   if pow > target then
      return false;
   else
      u.A = from; 1
         u:Pkcom = pk;
      account_idx.emplace(u);
      return true;
   end
end
```

Algorithm 3 Apply

```
Input: account, id
Output: bool
Begin
if msg.sender is not _self then
   throw;
else
   u = account_idx.find(account);
   if u==null then
      return false;
   else
      u.uid=id;
      account_idx.modify(u);
      return true;
   end
end
```

Algorithm 4 Register

```
Input: from, method, account, id, args
Output: null
Begin
u=account_idx.find(account)
if u != null then
   if u.id == id then
      send_action(from, method, (_self, true, args));
   else
      send_action(from, method, (_self, false, args));
   end
else
   send_action(from, method, (_self, false, args));
end
```

Algorithm 5 Authenticate

RESEARCH ARTICLE

5.1.3. Security Analysis

As shown in algorithm (6) the 3DECS technique used in this study is based on the plan [37], which refers to a denial list for each characteristic in [35]. The framework [38] is completely safe. The broad evidence technique contrasts with the security focus in [39], which will be predicated on the conventional model and depends on reaction forces suspicions to guarantee security. This article focuses on the usage of blockchain to communicate security data. The main focus of this presentation isn't on the security of 3DECS. Following the addition of a trait renouncement mechanism to the plan [40], it'll conduct a quick security analysis.

```
key = 'Sixteen byte key'
iv = Random.new().read(DES3.block_size)
cipher_encrypt = DES3.new(key, DES3.MODE_OFB, iv)
plaintext = 'sona si latine loqueri  '
encrypted_text = cipher_encrypt.encrypt(plaintext)
cipher_decrypt = DES3.new(key, DES3.MODE_OFB, iv)
cipher_decrypt.decrypt(encrypted_text)
cipher_decrypt.decrypt(encrypted_text)
```

Algorithm 6 3DECS

5.2. Additional Security Issues

5.2.1. Data Protection

Information security encompasses the categorization, integrity, and accessibility of shared information. The Department of Defense's massive limit-sharing data is obtained using a strong differential encryption technology like AES and sent to IPFS in this process. IPFS will partition the encoded data and store it on separate IPFS hubs in a suitable way. The admission will be managed by each hub's dynamic hash table, and an excess method will ensure adaptability to non-critical failure. IPFS, like Git, also includes adaption control. As a result, information encryption and the impossibility of hoarding maintain up with the mystery of shared data. Information uprightness is guaranteed via dynamic hash table steering, and modified information squares are unavailable. Because of IPFS' surplus storage and incentive mechanisms, clients may retrieve the data at any time. This architecture protects the information kept on IPFS as long as it is safe.

5.2.2. Privacy Assessment

The content of the DO's common information, as well as the trail left by the DU while utilizing the information, are both protected in an information-sharing architecture. The DO will use CP-ABE to scramble the location of the common information and the corresponding decoding key according to the defined admission method. The ciphertext is then recorded on the blockchain, and the data is only accessible to DUs with a characteristic set that fits the entry strategy. The content of the information will not be exposed. It scrambles the catchphrases that correspond to the sharing information in the DUs' following. The DU used the hidden entrance capability to generate the quest token for the keyword he required, then used the hunt token to get the data into the blockchain without revealing anything he didn't want to expose. Even more urgently, the client's identity is examined as a location on the blockchain, and the client's real data will not be revealed.

5.2.2.1. Access Control on a Fine-Grained Scale

In this engineering, 3DECS performs fine-grained admission control of shared information. The DO may use LSSS to create several entry controls that can give DUs a different quality. Controlling admissions on a finer scale, on the other hand, should also include fine-grained renunciation. The suggested approach is based on the DO's personality-based transmission encryption mechanism, in which each DU has a one-of-a-kind uid, which is employed as a client quality in the ciphertext alongside the overall characteristics. The ciphertext includes a renouncement list for each wide attribute, and any relevant property is no longer held by any DU member uid belongs in this list, achieving the goal of quickly repudiating a DU's characteristic.

5.2.2.2. A single point of failure should be avoided

Unlike traditional distributed storage systems, this proposed technique does not rely on a third-party vendor. Blockchain and IPFS are two of the technologies used in BSSPD. Regardless of whether any of the hubs fail, the framework as a whole will continue to operate. Furthermore, the BitTorrent protocol used by IPFS might achieve high throughput by paying a little amount of money to augment hoarding hubs. Clients may be able to access the EOS blockchain for free, with the exception that the DO may be required to contract a few framework tokens in exchange for capacity and CPU assets that may be reclaimed.

5.2.2.3. Centered on the user

Under this suggested approach, the DO may construct public bounds and the framework ace key, as well as develop and distribute private keys for DUs based on the features. Furthermore, the DO may establish access limits that allow DU consents to be freely relegated and withdrawn. The DO has complete control over everything without the help of a trustworthy outsider. The DO has complete control over his common knowledge in this area.

5.2.2.4. Verify User Identity

The customer constructs his identity on the blockchain by employing an asymmetric encryption approach that produces

RESEARCH ARTICLE

inadequate key sets. Because the uid is a parameter integrated into the cryptography of 3DECS, in this recommended strategy, The DUs may deploy a huge proportion of uids and use a variety of uids to find and decode the data. Common information, increasing the DO's responsibility. BTDEC demands a personality examination to prevent such assaults. Before requesting enlistment, the DU must carry out a PoW, comparable to Bitcoin mining. Depending on the overall volume of DUs mostly in the framework, the DO may change the PoW difficulty. The blockchain manages the consumer board and personality verification, and only approved consumers can conduct transactions. All of this is achieved via the use of a Smart Contract, which guarantees transparency and security.

Table 1 The BSSPD and Other Blockchain-Based Sharing of Information Activities are Examined for Potential Value

Data Sharing Scheme	BTDEC	Ref [18]	Ref [21]	Ref [28]
Privacy and security	YES	YES	YES	YES
Managing your identity	YES	FALSE	FALSE	YES
Access control with finer granularity	YES	FALSE	FALSE	FALSE
Revocation of access immediatel y	YES	FALSE	FALSE	FALSE
Ciphertext retrieval keyword	YES	FALSE	FALSE	YES

5.3. BTDEC Experiments and Analysis of Performance

5.3.1. Functional Comparison

As shown in Table 1, compared the approach proposed in this paper to current blockchain-based information sharing models in terms of security and protection, executive character, fine-grained access control, fast access renouncement, and ciphertext recovery. According to the conclusions of the table, DOs may establish access control constraints for information thought-provoking blockchain-based information exchange models, assuring security and safety for everyone. Early approaches, such as Ref. [18], mostly stated the model's result line without going into detail about how it was implemented. In most cases, it simply explains how blockchain may help with security and safety while sharing, making the concept relatively evident. Even though RBAC is a job-based access control system, Reference [21] used the blockchain to create a job-based access control viewpoint.

In a conveyed situation, it isn't ideal for fine-grained admission control and renouncement. ECC was used in reference [28] to establish fine-grained admission control; however, consent disavowal was not achieved. Nonetheless, instantaneous access repudiation is necessary for a 3DEES-based admittance control component. In this suggested design, it used 3DEES to accomplish fine-grained admittance control and characterize the board for DUs. For registered DUs, the DO provides and retains unusual uids and characteristics. You may reject a single DU attribute without renewing the keys of others if you keep a repudiation list for each characteristic in the ciphertext. BTDEC ensures the secrecy of DUs on-chain, ciphertext watchword search is used. As a result, this suggested strategy is more suitable and practical, As Shown in Figure 3.

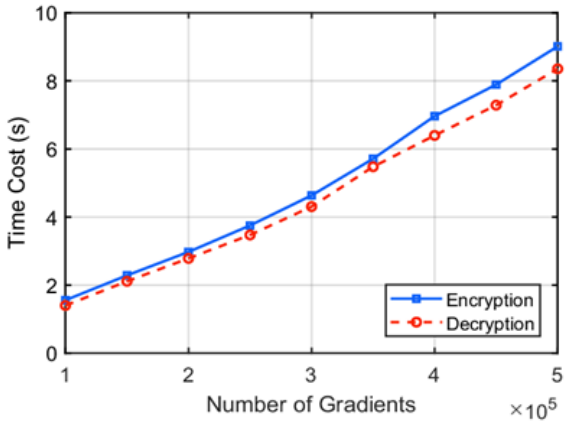

Figure 3 Encryption and Decryption Time Slots

5.3.2. Analysis of Storage

Depending on the EOS blockchain, BTDEC is a contract information exchange strategy. Maintains public framework boundaries, client information, and information-related data in the exceptionally durable data set of a Smart Contract. Because on-chain stockpiling is costly, and increasing RAM on the EOS blockchain necessitates the sale of framework tokens, it's vital to assess the quantity of data stored in the Smart Contract.

5.3.3. Performance Analysis

The technological execution of modern blockchains is frequently addressed, and computing transactions somewhat on the blockchain are restricted. It takes 10 minutes to produce a block in Bitcoin, for example. Even though Ethereum has cut the amount of time needed to build a square

RESEARCH ARTICLE

in half, it still takes around 15 seconds. It will test this recommended method in this part, evaluating its presentation and client adaptability.

As illustrated in Figure 4, raising the number of traits doesn't increase the number of attributes. This affects AddData's computation overhead. When there is a modified measure of characteristics, AddData's computational cost is consistently stable. AddData's computational cost is influenced by the number of DUs, particularly how many DUs are involved with sharing information. The computational time of 500 DUs is larger than even 100 DUs, and the bulk of the time is spent creating expedition files for the significant DUs.

As the qualities increase, the capacity overhead will continue to grow, as shown in the first section. However, as shown in Figure 5, the computational expenditure will not be much influenced when the attributes improve at this level. During the scrambling and transferring phase of this plan, the actions that should be led on-chain include moving information-related data to Smart Contracts and creating catch-lists for information-related DUs. As shown in Figure 4 measured the data size Cryptographic techniques key levels.

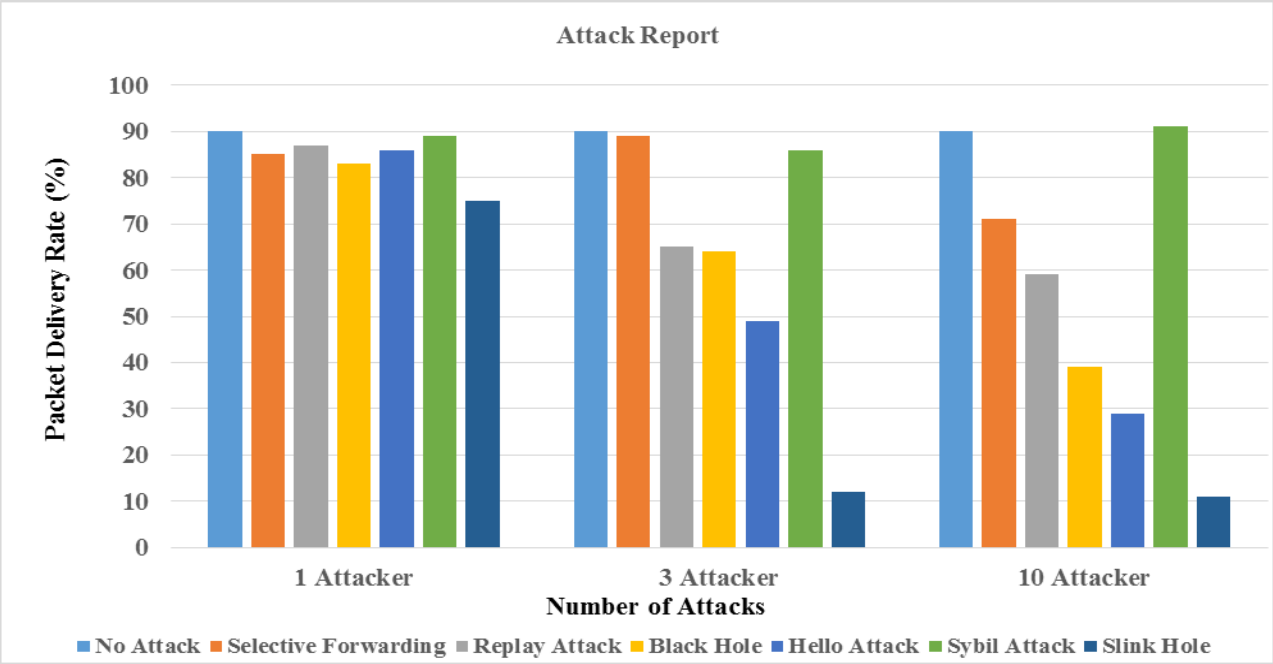

Figure 4 Attack Report

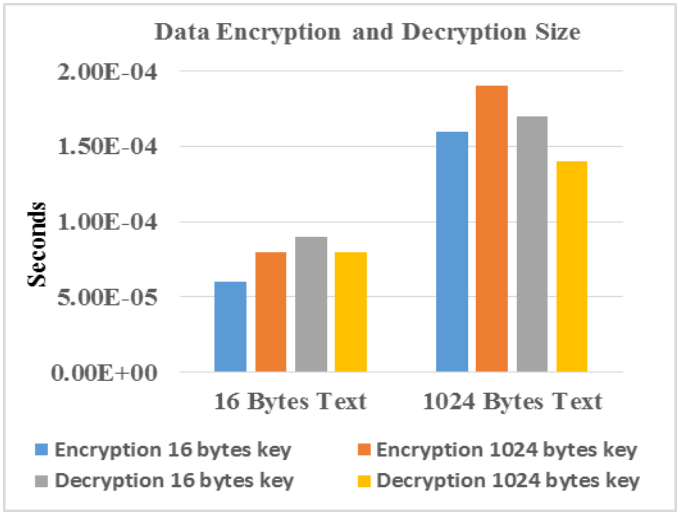

Figure 5 Size of Data Encryption and Decryption

RESEARCH ARTICLE

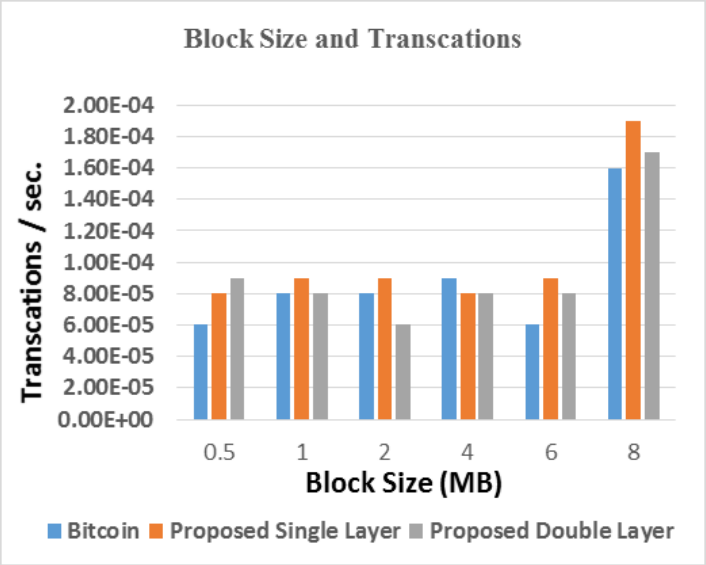

Figure 6 Block Size and Transaction

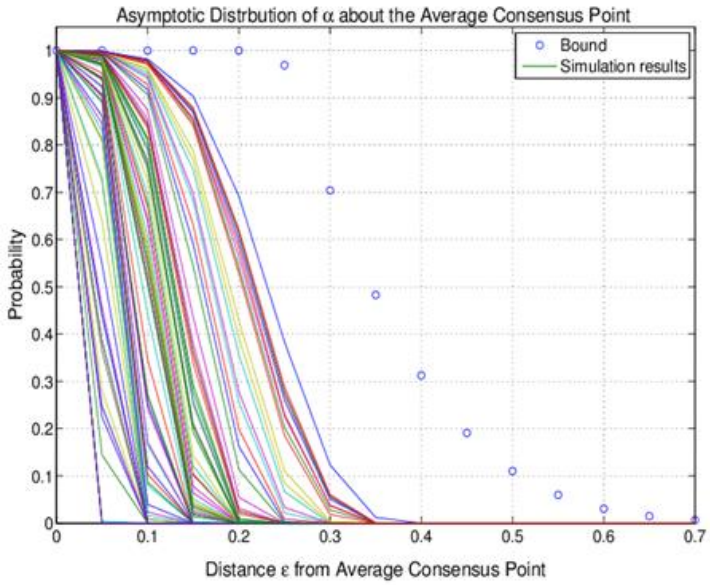

Figure 7 Average Smart Contracts Point

The temporary complexity of retrieving as per the hunt token is O since BTDEC sets up the pursue means of exchange as a supplementary list of the investigation table in the Smart Contract, paying little mind to the number of elements of devices and objects that exist in the framework (1). Since there seem to be 10 billion pieces of evidence in the file, the search duration is ten minutes. Comparable to a million, the pursuing process can take in milliseconds, As shown in Figure 6.

Deleting explicit information, like erasing information files, removes all information-related data. As the number of information-related DUs grows, so does the cancellation handling cost. The majority of my time is spent removing the data's seek lists. There is no compelling reason to work on the significant records because only the ciphertext information should be refreshed by the common information's essential key id while denying a DU's quality of specific common information, and the figuring overhead is comparable to setting and refreshing the public framework boundaries in the introduction stage, which is constant.

Overall, in this suggested technique, the aggregate total of characteristics will have minimal influence on the

RESEARCH ARTICLE

computation overhead on-chain. As far as it knows, mostly off operations including key creation, encrypting, and decrypting are affected.

When, on either hand, the user base develops, the time costs of various techniques will increase. Since search records will be created, the number of DUs associated with particular shared information will increase. As the number of connected quest lists for solitary information grows the processing time lowers in milliseconds as the number is increased to 500. Below published a list of all on-chain exercises. The computational cost of this technique is less than 100 milliseconds.

Because the square maker on the EOS fundamental organization is much more organized than this reproduction, the handling overhead will be much reduced if the agreement is completed on the EOS fundamental organization. Because a square on EOS takes 0.5 seconds to create, the functioning of this solution will be authorized shortly after it is implemented. This technique is effective as a result of the preliminary.

6. CONCLUSION

A stakeholder-sharing philosophy is provided in the AI-driven era to provide information while ensuring information security. If proposed a blockchain-based protection sharing information framework for quite well identity management and permission revocation by merging the blockchain, BTDEC, and IPFS. The DO encrypts his information and transfers it to IPFS employing this recommended methodology, subsequently scrambles the return location and uses 3DEECS to unscramble the key. The data must be encrypted and acquired by DUs that match the admission method's criteria. The structure has no embedded hub, and the DO has complete control over the information he shares, assuring its secrecy and security. Some built this structure on the EOS blockchain to prove this point. This method is rational, practical, and effective, according to security and execution analyses. It may also employ digital money to create a monetary framework for knowledge exchange and increase the potential of this plan. On the other hand, there are a few weaknesses in this plan. The 3DEECS are established with revocable consents, for example, do not operate effectively. Several research initiatives have been conducted on BTDEC. To improve this plan, it could require a 3DEECS with a more visible execution. Furthermore, the DO should indeed carry and preserve a secret key to every DU on-chain to employ this methodology's transparent encryption mechanism. It would also have to keep track of a huge number of datasets for each data transmission, which may be done more quickly. Several researchers have suggested that blockchain be utilized to alleviate the present encryption approach's reasonableness issue. Later on, it looks at and evaluates the option of using a better plaintext accessible computation to improve this approach. Conversely, may combine expert knowledge with this own to come up with a more practical data management plan.

REFERENCES

[1] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," in Computers & Security, 2018, vol. 72, pp. 1–12.
[2] S. Sundareswaran, A. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," in IEEE Transactions on Dependable and Secure Computing, 2012, vol. 9, no. 4, pp. 556–568.
[3] Cheng-Kang Chu, S. S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," in IEEE Transactions on Parallel and Distributed Systems, 2014, vol. 25, no. 2, pp. 468–477.
[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1–9.
[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," in IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.
[6] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," in IEEE Transactions on Dependable and Secure Computing, 2018, vol. 15, no. 4, pp. 1–590.
[7] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," in IEEE Transactions on Network Science and Engineering, 2020, vol. 7, no. 2, pp. 766–775.
[8] X. Zhou, W. Liang, K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data," in IEEE Transactions on Emerging Topics in Computing, no. 1, 2018.
[9] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flow estimation via taxi companies," in IEEE Transactions on Industrial Informatics, 2019, vol. 15, no. 12, pp. 6492–6499.
[10] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf.
[11] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled de-duplicatable data auditing mechanism for network storage services," in IEEE Transactions on Emerging Topics in Computing, 2020.
[12] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," in IEEE Transactions on Services Computing, 2020, vol. 13, no. 2, pp. 289–300.
[13] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," in IEEE Transactions on Network Science and Engineering, 2020.
[14] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," in IEEE Transactions on Industrial Informatics, 2019, vol. 15, no. 6, pp. 3632–3641.
[15] M. Swan, "Blockchain thinking: the brain as a decentralized autonomous corporation [commentary]," in IEEE Technology and Society Magazine, 2015, vol. 34, no. 4, pp. 41–52.
[16] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180–184.
[17] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25–30.
[18] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: trust-less medical data sharing among cloud service

RESEARCH ARTICLE

providers via blockchain," in IEEE Access, 2017, vol. 5, pp. 14757–14767.
[19] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in AMIA Annual Symposium Proceedings, 2017, vol. 2017, pp. 650–659.
[20] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1–5.
[21] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy-preserving and data sharing scheme of a content-centric network in 5g," in IET Communications, 2017, vol. 12, no. 5, pp. 527–532.
[22] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, "Blockchain-based data sharing system for AI-powered network operations," in Journal of Communications and Information Networks, 2018, vol. 3, no. 3, pp. 1–8.
[23] I. Zhou, I. Makhdoom, M. Abolhasan, J. Lipman, and N. Shariati, "A blockchain-based file-sharing system for academic paper review," in 2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, Australia, 2019, pp. 1–10.
[24] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," in Health informatics journal, 2018, vol. 25, no. 4, pp. 1398–1411.
[25] L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," in IEEE Access, 2020, vol. 8, pp. 77215–77226.
[26] M. Jemel and A. Serhrouchni, "Decentralized access control mechanism with temporal dimension based on blockchain," in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, 2017, pp. 177–182.
[27] X. Sun, S. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in ipfs," in IEEE Access, 2020, vol. 8, pp. 59389–59401.
[28] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," in IEEE Access, 2018, vol. 6, pp. 38437–38450.
[29] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," in Journal of Ambient Intelligence and Humanized Computing, 2020, vol. 11, no. 11, pp. 4613–4641.
[30] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, 2007, pp. 321–334.
[31] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography, PKC'11, Berlin, Heidelberg, 2011, pp. 53–70.
[32] V. Buterin, "Ethereum: a next-generation smart contract and decentralized application platform," 2013, https://github.com/ethereum/wiki/wiki/White-Paper.
[33] N. Szabo, "Smart Contracts," 1994, https://szabo.best.vwh.net/smart.contracts.html.
[34] H. Gao, Z. Ma, S. Luo, and Z. Wang, "Bfr-mpc: a blockchain-based fair and robust multi-party computation scheme," in IEEE Access, 2019, vol. 7, pp. 110439–110450.
[35] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in Proceedings of the 3rd International Conference Palo Alto on Pairing-Based Cryptography, pairing '09, Berlin, Heidelberg, 2009, pp. 248–265.
[36] H. Li, F. Zhang, J. He, and H. Tian, "A searchable symmetric encryption scheme using blockchain," 2017, https://arxiv.org/abs/1711.01030.
[37] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT'10, Berlin, Heidelberg, 2010, pp. 62–91.
[38] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," in IEEE Systems Journal, 2018, vol. 12, no. 2, pp. 1767–1777.
[39] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, "An efficient privacy-enhanced attribute-based access control mechanism," in Concurrency and Computation: Practice and Experience, 2020, vol. 32, no. 5, article e5556.
[40] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," in IEEE Transactions on Industrial Informatics, 2020, vol. 16, no. 9, pp. 6182–6192.

Authors

K. Mohamed Sayeed Khan, Ph.D. Research scholar, currently pursuing at Sadakathullah Appa College, Tirunelveli. I had completed my UG B.Sc. (IT) and PG M.Sc. (CS) and M.Phil. at Sadakathullah Appa College. My research area is Blockchain Security.

Dr. S. Shajun Nisha, Assistant Professor and Head of the PG & Research Department of Computer Science, Sadakathullah Appa College, Tirunelveli. She has completed M.Phil. (Computer Science) M.Tech (Computer and Information Technology) at Manonmaniam Sundaranar University, Tirunelveli, and completed Ph.D. (Computer Science) at Bharathiyar University, Coimbatore. She has been involved in various academic activities and attended so many national and international seminars, conferences and presented numerous research papers. She is a member of ISTE and IEANG and her specialization in Image Processing and Neural Network.

How to cite this article:

K. Mohamed Sayeed Khan, S. Shajun Nisha, "BTDEC: Blockchain-Based Trible Data Elliptic Curve Cryptosystem with Fine-Grained Access Control for Personal Data", International Journal of Computer Networks and Applications (IJCNA), 9(2), PP: 214-228, 2022, DOI: 10.22247/ijcna/2022/212337.