Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

An efficient dynamic access control and security sharing scheme using blockchain

Sultan Alkhliwi *

Department of Computer Science, Faculty of Science, Northern Border University, Arar, Saudi Arabia

ARTICLE INFO

Article history:
Received 9 January 2022
Received in revised form
12 April 2022
Accepted 11 May 2022

Keywords:
Blockchain technology
Encryption
Decryption
Access control
Data security

ABSTRACT

This study seeks to understand the role of institutions and organizations that have used cloud service providers to store and share data as ensuring third-party access to storage is a major challenge to avoid data theft and unwanted access. Hence, in this paper, Blockchain-Based Data Access and Secure Sharing Method (BDASS) is introduced to enhance security processes related to personal data through data access control and secure sharing method, the proposed method uses blockchain aggregation, file system (IPFS), dynamic access control (DAC), and ciphertext-attribute-based encryption (CP-ABE) to enhance the security of personal data. To keep the owner safe, a blockchain-based DAC is designed. To keep data storage and sharing secure, the blockchain-based CP-ABE is designed. In this proposed methodology, the data owner encrypts the data they have stored in IPFS, thus enhancing data security, which has been improved with the help of CP-ABE regarding detailed access policy and data owner. Policy parameters are managed by the DAC. In the proposed methodology, the data owner uses the blockchain to control security and access to the data. Finally, the paper has come up with a set of findings in order to achieve data security and access control for the data owner through the blockchain-based approach. To evaluate the performance of the proposed method, MATLAB was used. The proposed technology also contrasts with existing technologies, such as the Blockchain-Based Security Sharing Scheme for Personal Data (BSSPD) as well as the Rivest-Shamir-Adleman Algorithm (RSA) and Elliptic Curve Cryptography (ECC).

1. Introduction

In recent years, the improvement of the Internet of Things and 5G has been considered the key to enhancing the human lifestyle in various fields, such as smart grids, transportation, smart cities, and healthcare (Ghiasi et al., 2021). Interconnected IoT devices may share data with various entities and produce data gathered from neighboring environments. Similarly, privacy protection and data security have been considered the main objectives in sharing and data governance topics (Xu et al., 2021). Data analysis and powerful data mining have transferred high coercion to personal privacy security. Conventionally, numerous people select a cloud server to outsource their data, which is intended for dissemination and sharing. Moreover, the maximum of data that can be stored in the cloud is identically sensitive, especially for information gathered from IoT devices (Campanile et al., 2021). IoT devices can mostly be connected to people's devices, which contain their personal information as well as their particularities, such as healthcare, work, and life information (Chen et al., 2021). Due to the low privacy rate and security level, personal data may be leaked or stolen, which creates a major problem because the data owner's real identity may also be leaked (Esposito et al., 2021).

Generating value and integrating data while improving privacy and data security is a significant task aimed at completing modern organizations that utilize big data (Narayanan et al., 2022). Data security and privacy should be considered and empowered in storage systems. Presently, many researchers have proposed many security and privacy empowerment methods in cloud environments (Mittal et al., 2021). The designed method should provide effective security enhancement and privacy data schemes while

* Corresponding Author.
Email Address: salkhliwi@nbu.edu.sa
https://doi.org/10.21833/ijaas.2022.08.004
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-3481-549X

allowing data sharing with their different entities (Zhang et al., 2021a). The presented method has a general feature that strongly depends on the cloud service provider (CSP). Generally, a CSP is a trusted third-party company, but it may be considered semi-trustable. 'Semi-trustable' means the CSP will be curious during the information transfer mode but will not abolish it (Zhang et al., 2021c). Hence, the data privacy and security of the system are enhanced with data access control and security schemes. Many types of cryptography and data access control are available to achieve the optimal security level for the collected data (Zhang et al., 2021b).

Recently, blockchain has attracted research in cryptography for improving the security and privacy levels of data security by adding a security layer to a storage system (Hussien et al., 2021; Yan and Lee, 2021). The de-centralization feature of the blockchain enhances the security level more than conventional methods. Access control to the owner's security should be considered to enable the proper security level with data security. Many different data access control methods have been developed by researchers for empowering owner security, such as role-based access control (RBAC) Kim and Park (2021), mandatory access control (MAC) Kumar and Tripathi (2021), and discretionary access control (DAC) (Rivera Sánchez et al., 2017). These forms of data access control have been utilized to secure resources, but these methods are inferior to centralized management or solitary authority. These methods have challenges, such as privacy issues and single points of failure. Moreover, centralized access controls cannot offer the required efficient access to the IoT because of these issues. Hence, an effective and optimal security scheme for data access control should be developed to enhance the security of data stored in the system.

The main contribution and organization of the work**:** The security of systems should be improved to empower the data transactions of users in cloud storage units and IoT applications. The main contribution of the paper is as follows:

- In this paper, BDASS is introduced to enhance security operations in personal data through data access control and the secure sharing method.
- The proposed method uses a combination of blockchain, IPFS, DAC, and CP-ABE to improve the security of personal data.
- To maintain the owner's security, a blockchain-based DAC is designed. To maintain secure data storage and sharing, a blockchain-based CP-ABE is designed.
- In this proposed methodology, the sharing data is encrypted by the data owner and stored in the IPFS, which increases the scheme's de-centralization. Shared data and decryption key addresses are encrypted using CP-ABE regarding the exact access policy and the data owner.
- Additionally, the data owner utilizes blockchain to distribute the stored data and distributes keys for data access with the help of DAC. With the consideration of DAC, the data user whose attributes encounter the access policy is decrypted so they can download data. The data owner contains DAC with data, and the proposed approach supports attribute-level cancellation without disturbing other users while collecting the data for the data user.
- Finally, to maintain the data user's privacy, a ciphertext keyword search can be utilized when retrieving data.

The remainder of the paper is planned as follows: Section 2 reviews the existing work on security and privacy enhancement methods using blockchain technology. Section 3 provides a detailed explanation of the proposed methodology for enhancing security and user data access control in the stored data. Section 4 provides the outcomes of the proposed methodology, which validate the proposed method's effectiveness. Finally, the conclusion of the paper is presented in Section 5.

2. Related works

Many different methods are available to enhance the security of a system using blockchain technology. In this section, we review some of the methods for finding the problem formulation of the blockchain technology required for developing efficient security enhancement.

Guruprakash and Koppu (2020) introduced an EC-ElGamal and genetic algorithm-based extension to the lightweight scalable blockchain in the IoT domain. Their research focuses on the efficiency cost to improve security, functionality, hash rate, hash quality, block approval, transfer stream enhancement, and transaction encryption. The study evaluation was shown in the data obtained from the temperature sensor to understand the unmatched suitability of the presented work in the IoT area. Execution and conclusion testing with traditional LSP demonstrate its achievements:

1. It creates security in communication exchanges for the development of an additional layer of security of transfer encryption using the cross-race elliptical elm (EC-ElGamal) strategy.
2. It shows a 20% minimization in transaction handling time, 22% minimization in block approval preparation time, 53% enhancement in hash function, and 7% efficiency cost, resulting in extended general execution. It also improves quality and saves money on a large scale.

Guo et al. (2021) introduced efficient traceable attribute-based encryption with dynamic access control (TABE-DAC). Blockchains are also used to integrate access control and distributed storage for the sharing of personal information. Attribute-based encryption (APE) schemes that deliver unique or multiple encryptions are usually used as arrangements to ensure the classification of personal information. However, while embracing the APE

provisions, there were issues such as vulnerability, critical harassment, and the stability of the access control strategy. The presented TABE-DAC plot provisions recognition of the liability of malevolent customers to issue private keys. The proposed arrangement acknowledges dynamic access control, in which information owners have an adaptation to update their access control strategy. This demonstrates the security of the similarly presented TABE-DAC plot. Finally, through hypothetical testing, experimental testing, and confirmation of efficiency, the presented arrangement was validated.

Honar Pajooh et al. (2021) introduced a multi-layer blockchain security design intended to stabilize IoT systems during execution. The group's idea was used to promote multi-faceted engineering. Q-ambiguous groups are classified within the IoT network with techniques that use an evolutionary computational algorithm combination when using simulated analgesia and genetic algorithms. Selected team leaders who can respond to nearby verification and approval. The neighborhood's private blocking process promotes correspondence between cluster heads and important base stations. Such a blockchain improves reliability, stabilization, and security while, at the same time, providing an organizational verification component. The status of the open-source hyper linear fabric blockchain was reported for the projected sample events. Base stations get a global blockchain approach towards dealing with talking to each other safely. Breeding outcomes reveal that the proposed compilation calculation works best when it contradicts previously announced methods. The projected lightweight blockchain design similarly proved to be highly competent in correcting network inactivity and programming.

Eltayieb et al. (2020) introduced the idea of a blockchain with a property-based signature to provide secure information on cloud weather participation. The proposed plot meets the security prerequisites of distributed computing, as it is confidential and unforgivable. Moreover, the smart deal is concerned with the problem of distributed storage, for example, giving the same erroneous results as a regular cloud worker. Finally, the presentation contacts and restructuring outcomes show that the presented plot was more efficient than the others and that it was effective. The proposed BABSC is inverse in its use of both blockchain and quality-based signing. It delivers secure information classification and an unforgivable character. An exhibition inquiry found that BABSC not only restricts the letter overhead but also provides a quick design code on the client page. In addition, BABSC supports customer access control and is compatible with distributed computing. Future work will be zero on setting up deals interested in Ethereum.

Finally, Xu et al. (2020) introduced a blockchain-based secure data-sharing platform with fine-grained access control (BSDS-FA) aimed at preventing security leakage issues while participating in the Internet of Things. To begin with, this paper presents a progressive feature-based encryption calculation that uses a different equilibrium property system and a stumble approval center. The calculation carries out adaptive and elegant enrolment control by reporting unique client credits to different approved communities. It is coupled with fabric blockchain innovations to tackle the biggest cost problem for customers on the Internet of Things. An interesting contract in blockchain enables highly complex, incomplete decoding calculations to minimize customers' uncontrolled overheads. Blockchain can understand the detection of verifiable functions to meet the security necessities of the information range with open and direct supervision. For a long time, various equilibrium asset-based encryption calculations were CPA-secure. Hypothesis testing and research results show that BDSS-FA has yielded secure and robust information-sharing administrations for customers on the Internet of Things.

3. Background study of the blockchain model

A blockchain is an unchallengeable ledger that consists of a set of lined blocks. Blockchain technology has been justified through participants in peer-to-peer (P2P) networks. Blockchain technology was introduced subsequent to the development of bitcoin, which is an online cryptocurrency. This bitcoin method does not contain the central authority over maintaining its communications but validates and manages the blocks of participants in a de-centralized peer-to-peer network. Due to the de-centralized theory of block management and the ubiquity of bitcoin, researchers are focused on developing blockchain methodology in depth. Normally, the blockchain is a tamper-proof ledger and de-centralized distributed system that is shared between each P2P network system. Blockchain has different structures: It can be tamper-proof, traceable, or de-centralized (Yazdinejad et al., 2020). These features are enhanced to enable various applications, such as healthcare systems, smart cities, and smart cars, by maintaining transparency, ensuring traceability, and avoiding third-party access to secure data sharing. The main behavior of blockchain methodology is formulated as follows:

- Transparency: The complete parameters of the public blockchain frameworks, such as Ethereum and bitcoin, have similar access permissions, so they also contribute to the procedure of recording and validating novel blockchain communications. Hence, the recorded data in the ledger can be translucent to complete the actors in the blockchain design.
- Tamper-proof: In the blockchain model, new joining blocks are validated and authorized by complete peers in the P2P network through de-centralized agreement techniques. Additionally, the blockchain can be unchallengeable; for example, if the attacker is trying to alter the blockchain's

information, the blockchain technology checks the helpful mainstream of the contributors in the network. Hence, the attacker finds it easily.

- Traceability: Blockchain technology can be simply inspected because complete actors in the blockchain consist of duplicates in the ledger that records transactions. Hence, based on the specified blockchain address, the data exchange can be validated with the participants in the network. The complete record can be stored in the blockchain, which assigns a timestep that guarantees transaction traceability. Pseudo-anonymity is utilized in blockchains to maintain the privacy of users.
- De-centralization: The de-centralized design of the blockchain improves complete blockchain followers' networks to access the procedure for verifying communication, unlike centralization, which allows only the manager of the network to carry out validation and authorization processes.

Based on the behaviors of blockchain technology, it can be selected to enhance the security of the system. The blockchain method can be a de-centralized system that utilizes data sharing between participants across a design. The blockchain is divided based on its quality attributes and architectural behaviors: It can be fully de-centralized (permission-less blockchain) or partially de-centralized (permissioned blockchain). Blockchain is a recent technology intended to develop an efficient security level for systems. The blockchain-based security system is developed in the proposed model, which is presented in the section below.

4. Proposed system model

Open sharing and privacy protection are the most important specifications in IoT devices and cloud computing technologies. General data sharing can be crucial in traditional data-sharing outcomes. Additionally, in general, in data-sharing techniques, users may upload their data to the cloud server for dissemination and storage. When the user uploads data, the ownership of their data will be lost. Additionally, the privacy and security of the data are questionable and pose critical problems. Hence, access control and data encryption can be considered important requirements for protecting data and managing the owner's access. This access control and data security enhances the security of the system as well as offers the proper solution to security-related issues. Hence, in this paper, BDASS is introduced to enhance security operations in personal data through data access control and a secure sharing method. The proposed method uses a combination of blockchain, IPFS, DAC, and CP-ABE to improve the security of personal data. A block diagram of the proposed methodology is presented in Fig. 1 to perform the following tasks:

- To maintain the owner's security, a blockchain-based DAC is designed.
- To maintain secure data storage and sharing, a blockchain-based CP-ABE is designed.

The proposed method is designed with four important components: Data usage, data owner, blockchain, and IPFS.

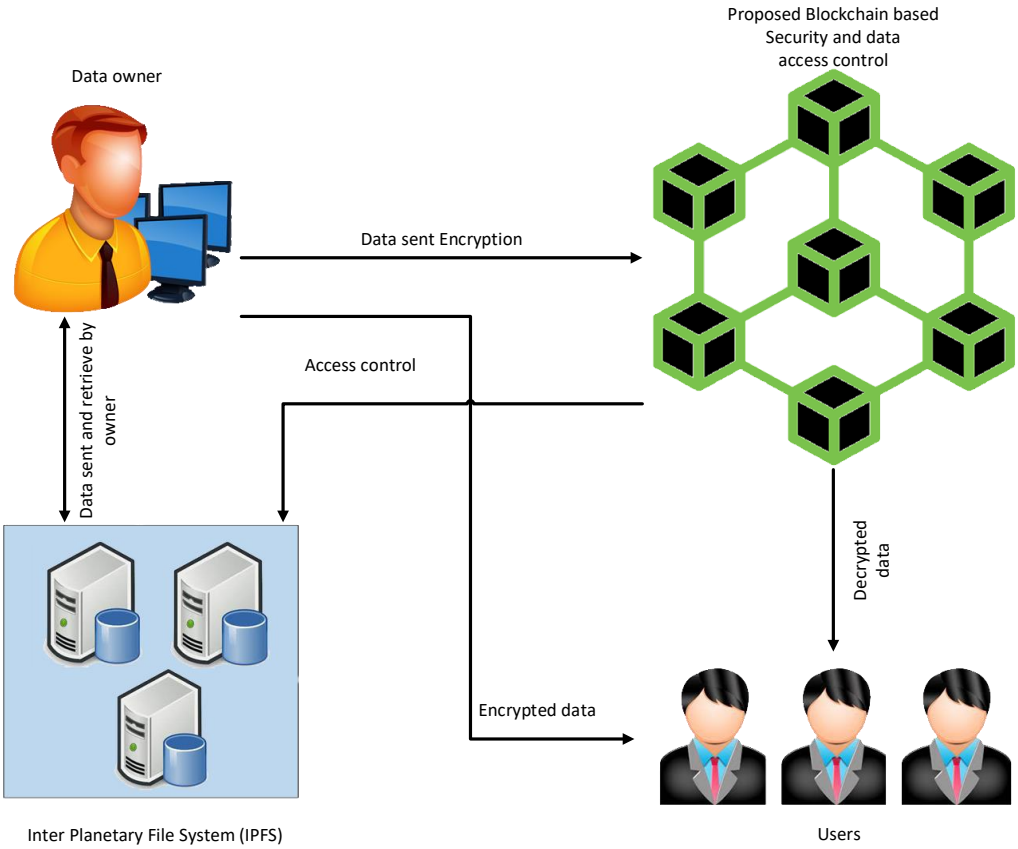

Fig. 1: System architecture of the proposed methodology

Initially, the data owner's data are encrypted with the help of blockchain-based CP-ABE and stored in the IPFS through the uploading process with their decryption key. Additionally, the blockchain-based DAC is utilized to maintain data access control for the data owner as well as the data user. The data owner provides the encryption key to data users with the consideration of blockchain technology and verifies the access policy of the users. The proposed method is completely de-centralized in terms of its data access and security algorithms. The encryption algorithm can be utilized to empower data security, as well as data accessibility. The specific operation of the four proposed components is explained below:

- Data user: The data user can be defined as the user who needs to access the data. The data user is checked against the data access control policies and permission strategy. Only after that is the encrypted key provided to the user by the data owner for accessing the data.
- Data owner: The data owner is responsible for developing the data access policies in the proposed methodology. The data owner has the sole privacy to manage their data and provide access to data users by providing the encryption key.
- Blockchain: The blockchain stores the operational records and public information in a complete section. The blockchain can be utilized with reliable broadcast channels intended to exchange messages between the data owner and the data user. Without a trusted third party, it can be a cornerstone of security.
- IPFS: The IPFS can be utilized as a reliable and secure storage device. The incentive method empowers the data on the IPFS so that it is never unavailable.

In this proposed methodology, the shared data are encrypted by the data owner and stored in the IPFS, which increases the scheme's de-centralization. Shared data and the decryption key address are encrypted using CP-ABE regarding the exact access policy and the data owner. Additionally, the data owner utilizes blockchain to distribute the stored data and keys for data access with the help of DAC. With the consideration of DAC, the data user whose attributes encounter the access policy decrypts and downloads the data. The data owner contains DAC with data, and the proposed approach supports attribute-level cancellation without disturbing other users while collecting the data from the data user. Finally, to maintain the data user's privacy, a ciphertext keyword search can be utilized when retrieving data. The proposed methodology empowers security by using blockchain technology with security as well as data access control. A detailed description of data security and data access control is presented in the section below.

4.1. Blockchain-based dynamic access control (DAC)

Blockchain-based DAC was developed to enable secure access to the data transaction process. The proposed DAC Wang et al. (2018) is designed. with different stages, such as the initialization stage, the application and registration stage, and the updated policy, verify policy, key check, and tracing stages. The complete architecture of the DAC is illustrated in Fig. 2.

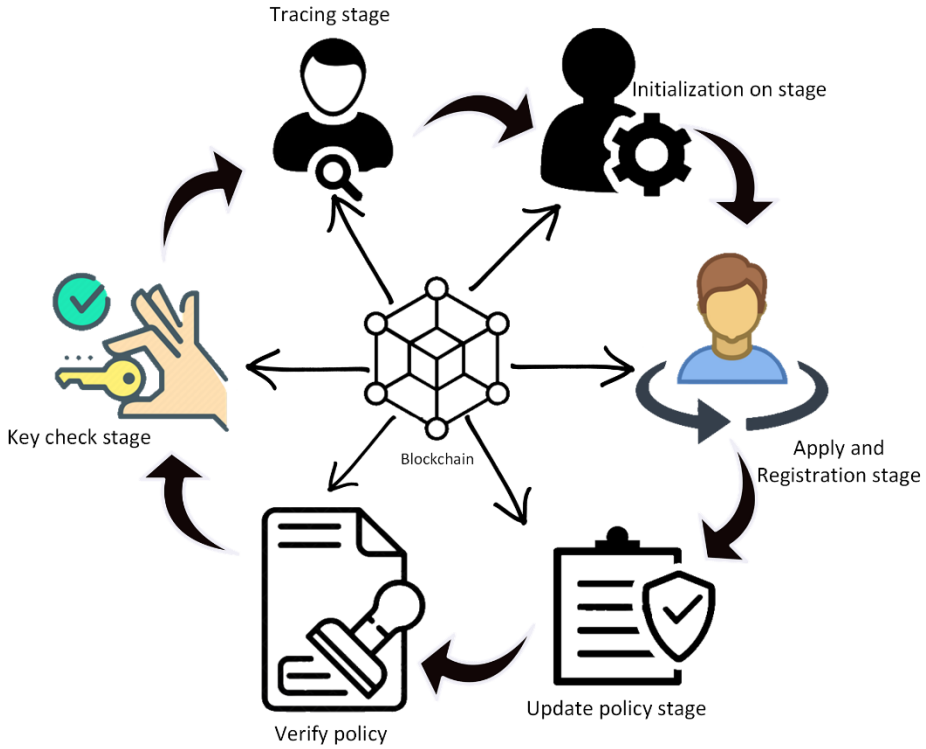

Fig. 2: Different stages of the proposed blockchain-based DAC

The steps of the proposed DAC are presented as follows:

- Initialization stage: The basic function of the initialization stage is that the data owner generates the master key and public key and the general parameters. The main step of this proposed security algorithm is to initiate the key parameters. The initialization stage is mathematically formulated as follows:

$$Initialisation \rightarrow (MK, PK) \quad (1)$$

where, MK can be described as a master key and PK is denoted as a public key. These keys are selected by the data owner. The master key is kept secret by the data owner, and a public key is stored in blockchain technology. This is utilized by the data owner to initiate the transaction.

- Apply and register stage: The main operation of the register and apply stage is that the data user starts to apply for registration, and a public encryption algorithm key is needed while applying. Once applied, the data owner is assigned a unique ID and provides a private key for the data usage, which is formulated as follows:

$$Key\ generation\ (MSK, PK, UID, W) \rightarrow \big(SK(data), SK(search)\big) \quad (2)$$

In this stage, the input of the algorithm is the master key, unique ID, and general attribute set (W) of the data user. The output is the private attribute key $(SK(data))$ and search key $SK(search)$ of the data user. The data user's private key is stored in blockchain technology. In this manner, the data user collects the private key reliably and securely.

- Update policy stage: The policy for permission is generated by the data owner. The private key is utilized to check the policy conditions with the consideration of encrypted data (data encrypted by the proposed security method). The policy checking condition is validated with the help of a key and policies. This condition is mathematically formulated as follows:

$$Update\ policy \rightarrow (PK, CT, Policy) \quad (3)$$

where, $Policy$ can be described as the policy of the data owner.

- Verify policy: In this stage, the policy of the data owner is matched with the data use policy to provide data access permission. That the policy of the data user is matched with the required policy means that access is provided by the data owner. The policy verification stage is completed with the consideration of blockchain technology. The verification stage is mathematically formulated as follows:

$$Verify\ policy \rightarrow (PK, CT, user\ Policy) \quad (4)$$

- Key check**:** The policy is checked with the data owner and the data user. Once satisfied with the policies of the data owner are reported by the data user, the private key is shared with the data user. The key is also checked with blockchain technology, which checks the data using a key with their data owner keys. The key check condition is mathematically formulated as follows:

$$Key\ check \rightarrow (PK, MSK, SK - UID) \quad i.e., 0\ or\ 1 \quad (5)$$

In this stage, the secret key is either correct or not. The key is correct if it is displayed at 1; otherwise, it is displayed at 0.

- Tracing**:** The final stage of the proposed DAC is the tracing stage. The trace algorithm input is the public parameters' private key, master key, and user decryption key. The tracing algorithm provides the output as 1 if the tracing algorithm can extract the user identity; otherwise, the trace algorithm output is 0. The trace stage is mathematically formulated as follows:

$$Tracing \rightarrow (PK, MSK, SK - UID) \quad i.e., 0\ or\ 1 \quad (6)$$

With the help of the proposed DAC, the permission policy of the data owner is checked with the data user, which empowers the security of the system during transactions. The proposed DAC enables the data access process in the system. Once data access is completed, the stored data can be encrypted with the data user. The encryption and decryption processes of the proposed methodology are explained in the following section.

4.2. Blockchain-based ciphertext-policy attribute-based encryption

This blockchain-based CP-ABE method can be utilized to enhance the security of the proposed methodology. This proposed security algorithm is mainly designed to use the user's ID as an attribute to give support to permission revocation (Lin et al., 2018). The proposed security algorithm proceeds in two stages: The encryption and uploading phase and the decrypted and downloading stage. The complete architecture of the proposed blockchain security algorithm is illustrated in Fig. 3.

The two stages of the proposed security algorithm are presented in what follows.

- Encryption and uploading stage: This stage is important for securing the data with optimal functions that proceed through the data owner for encrypting shared data and uploading them to the IPFS. Subsequently, the decryption key and address are encrypted and uploaded to the IPFS. Additionally, ciphertext keyword indices can be recognized to ensure relevant data users. The encryption process of the proposed algorithm is mathematically formulated as follows:

$$Encrypt\left(F,(A^{l\times k},\rho),\{R^{\rho(x)}\}_{x\epsilon 1,\ldots,l}PK\right) \quad (7)$$

The encryption process can be implemented by the data owner. The encryption procedure is followed in the three steps below:

- Step 1**:** The main inputs of the data encryption algorithm are the shared collected data denoted as F, the IPFS address, which is denoted as $REF(loc)$, and the key of the symmetric encryption algorithm (KF). The complete process can normally choose a private key (KF) and encrypt the input data (F), which generates the ciphertext (CF). The encrypted ciphertext (CF) is uploaded to the IPFS to obtain the address. This step is mathematically formulated as follows:

$$Encrypt\ File\ (F) \rightarrow (KF, REF(loc) \quad (8)$$

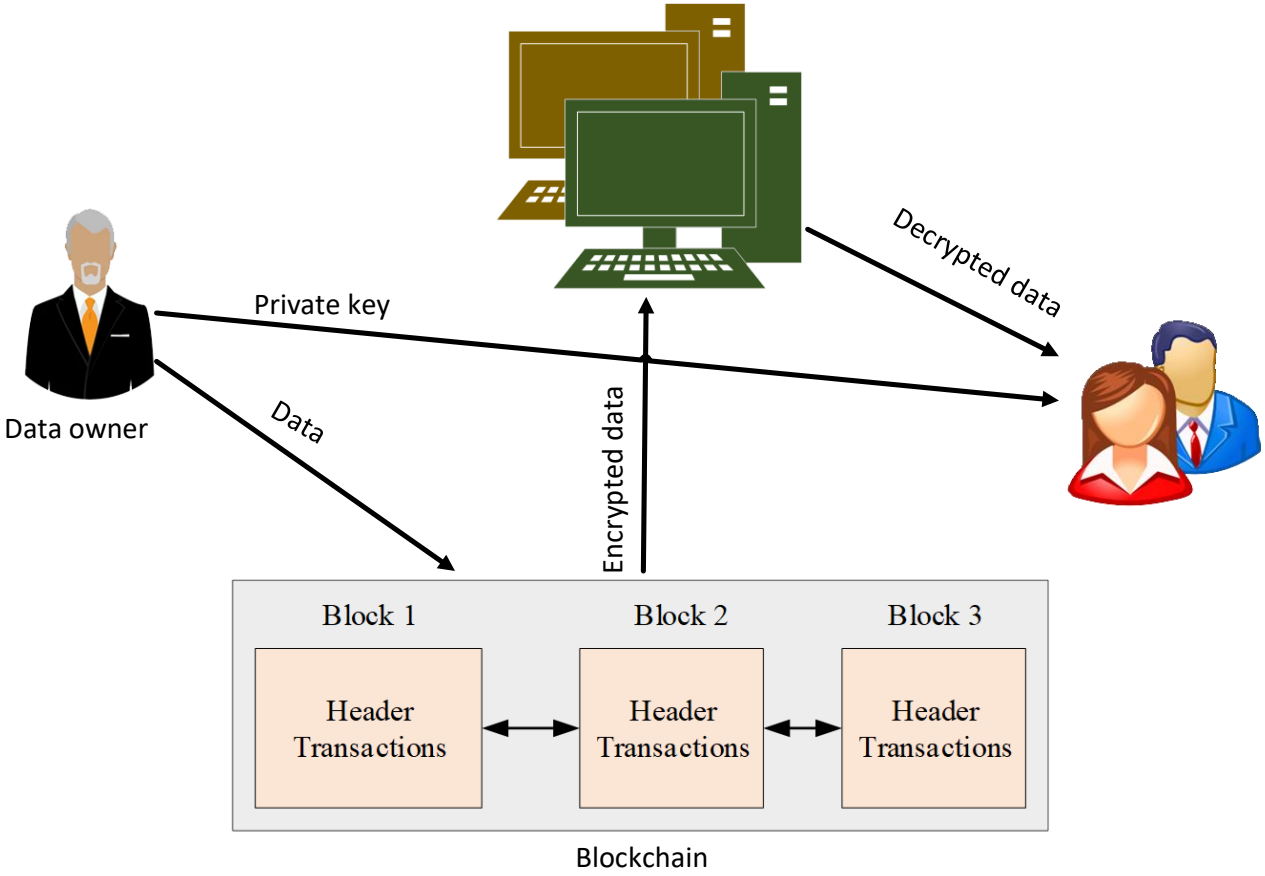

Fig. 3: Process of blockchain-based security algorithm

- Step 2**:** This encryption algorithm can be utilized to encrypt the address. This step's input is the decryption key and the IPFS address site, the public parameters (PK), each attribute (A), the revocation list (R), and the access policy (AP). The output of this step is the ciphertext of the encryption and encrypted key. This process is mathematically formulated as follows:

$$(KF, REF\ (loc), A, R, PK)(KF|REF(loc) \quad (9)$$

- Step 3**:** In the proposed security algorithm, the ciphertext keyword index is generated, and the data owner chooses a keyword for the data. The keyword can be utilized as an input combined with the secret key. The keyword index generation is mathematically formulated as follows:

$$IndexGen(kw, SK(search) \rightarrow t_{tw} \quad (10)$$

- Decryption and downloading stage: The major operation of the downloading and decryption stage is that the data user utilizes their private attribute key. With the utilization of a private key (Wu et al., 2019) the data can be decrypted and downloaded from the IPFS with the permission of the data owner. The decryption stage of the proposed method is mathematically formulated as follows:

$$Decrypt(SK-UID, CT, PK) \rightarrow (KF, REF(loc) \quad (11)$$

where, $SK-UID$ can be described as the private attribute key of the data user, CT can be described as data-related information, and PK can be described as public system parameters. In this process, the data user can encrypt and download data. Finally, the intent of the proposed method is to enhance security with blockchain-based data access and security control. The performance of the proposed methodology is validated in the following section.

5. Performance evaluation

In this section, the projected technique performances are validated through performance

and comparison analyses. To validate the presence of the projected blockchain-based security and data access control, the proposed method is implemented on an Intel Core i5-2450M CPU 2.50GHz laptop with 6 GB of RAM and MATLAB software R2016b. To validate the performance of the proposed method, the databases were collected from Asuncion and Newman (2007), which consisted of more than 10,000 attributes. The projected method implementation parameters are given in Table 1. The proposed method is implemented and validated using performance metrics such as storage overhead, initialization time, waiting time, encryption time, decryption time, uploading time, downloading time, and processing time.

Table 1: Proposed method parameters

S. No	Method	Description	Value
1	Proposed method	Send rate	20.2
2		Maximum Latency	0.38
3		Minimum Latency	7.05
4		Average Latency	0.18
5		Throughput	20.1

The performance of the proposed method is analyzed with the performance metrics, which validate the security as well as the data access control. The proposed method is analyzed through performance analysis and comparative analysis.

5.1. Performance analysis

The proposed method was analyzed with performance metrics such as storage overhead, initialization time, waiting time, encryption time, decryption time, uploading time, downloading time, and processing time. The storage overhead of the proposed method, with the three stages of initialization, registration encryption, and uploading, is illustrated in Fig. 4. The storage overhead in the initialization phase is 5 kb at 25 attributes. Similarly, the storage overhead in the registration phase is 9 kb at 25 attributes. The storage overhead in the encryption and uploading stage is 8 kb at 25 attributes. The initialization stage time of the proposed method is illustrated in Fig. 5. The maximum and minimum times of the initialization phase are 40 m/s and 75 m/s, respectively. The waiting time for the proposed methodology is illustrated in Fig. 6. The waiting time was analyzed with 100 users, 200 users, and 300 users and determined as 60 m/s, 85 m/s, and 100 m/s, respectively.

The encryption time of the projected technique was analyzed with different key lengths, such as 1,500 bits, 1,000 bits, and 500 bits, as illustrated in Fig. 7. The maximum and minimum encryption times of the projected method are 1.7 m/s and 11 m/s, respectively. The decryption time of the projected method is analyzed with different key lengths, such as 1500 bits, 1000 bits, and 500 bits, as illustrated in Fig. 8. The maximum and minimum decryption times of the projected method are 2 m/s and 11 m/s. The uploading and downloading times of the proposed methodology are illustrated in Fig. 9. In Fig. 9, the uploading time of the proposed method is 3 ms and the downloading time is 4 m/s for 10 MB. The uploading and downloading times change based on the data size. The processing time of the proposed methodology is illustrated in Fig. 10. The proposed method processing time is analyzed with different counts of users, such as 100, 200, and 300. The processing time increases due to the large number of users being connected in data transactions.

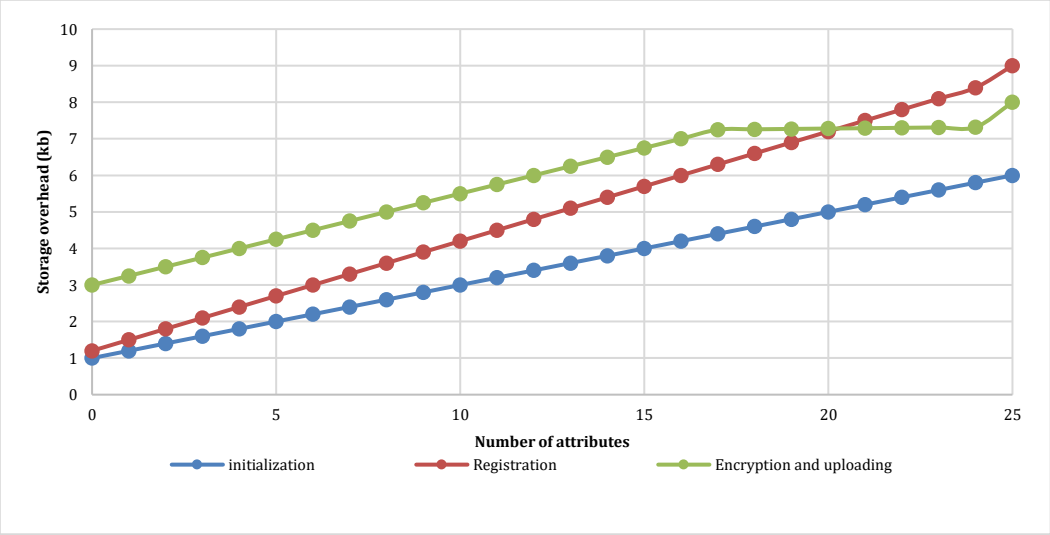

Fig. 4: Analysis of storage overhead

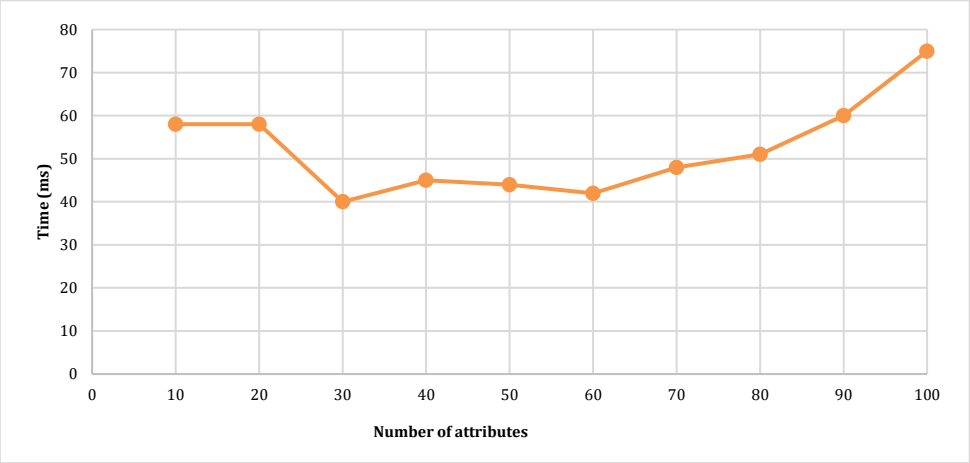

Fig. 5: Analysis of initialization time

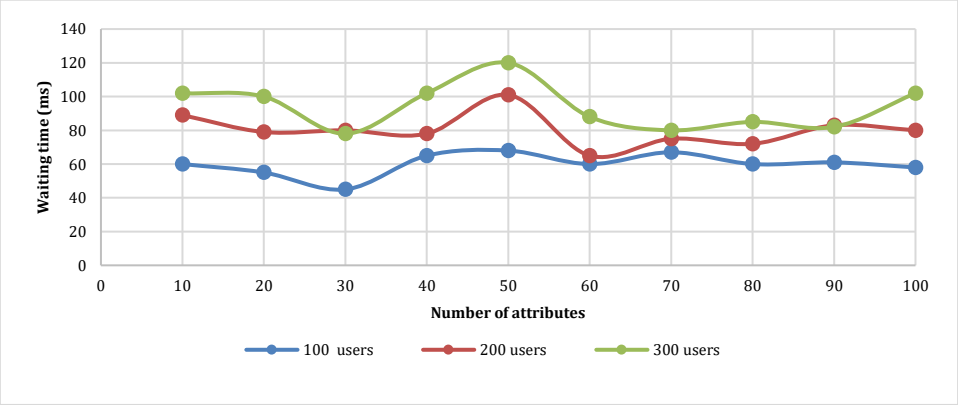

Fig. 6: Analysis of waiting time

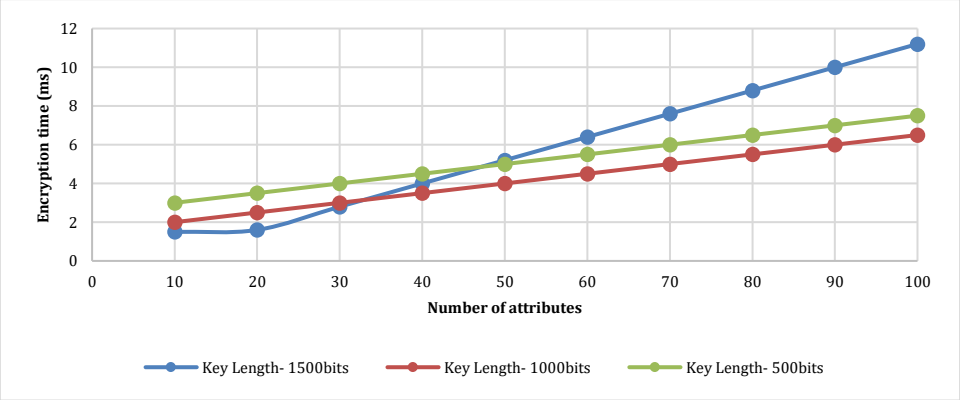

Fig. 7: Analysis of encryption time

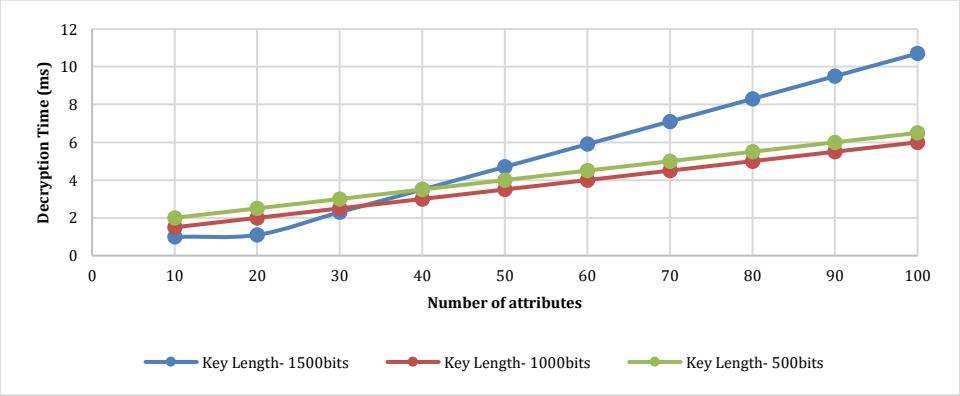

Fig. 8: Analysis of decryption time

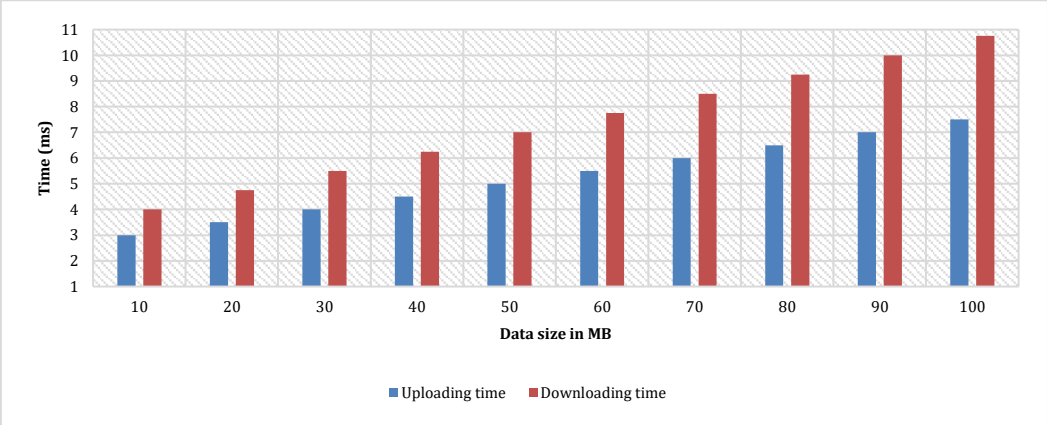

Fig. 9: Analysis of uploading and downloading time

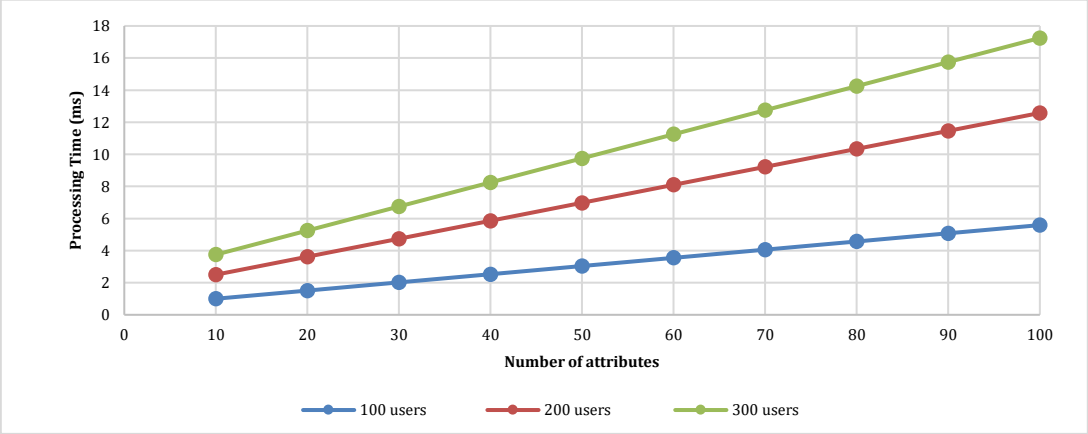

Fig. 10: Analysis of processing time

5.2. Comparison analysis

The comparison analysis is essential to validate the proposed methodology with the conventional methods, such as BSSPD-(Ex-1), ECC-(Ex-2), and RSA-(Ex-3). The comparison analysis is validated with the performance metrics, such as encryption time, decryption time, uploading time, downloading time, processing time, and received packets.

As shown in Fig. 11, the proposed method spent lower encryption time for the data encryption process when the number of attributes is increased compared with other techniques, where the maximum value was (2 ms) and the minimum value was (11 ms) of encryption times.

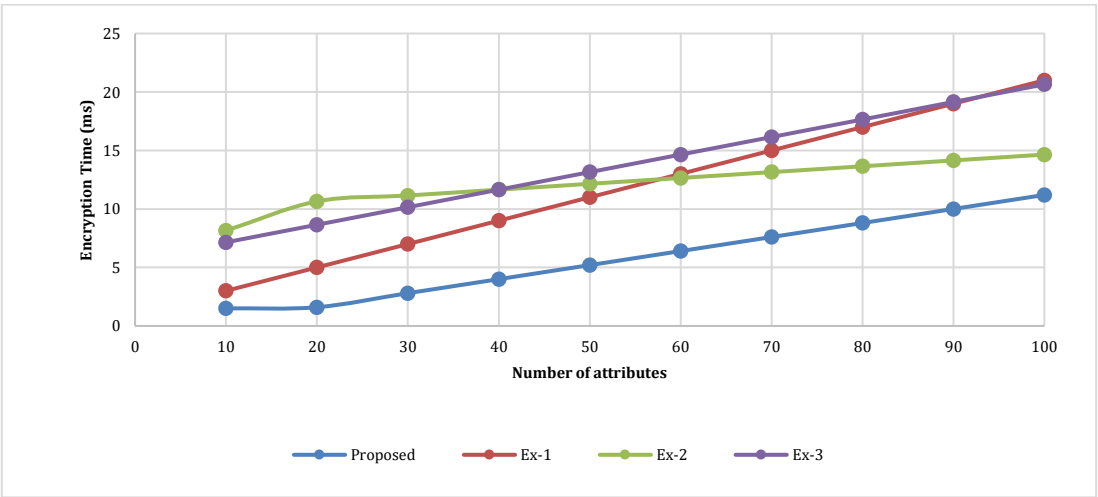

Fig. 11: Analysis of encryption time

As shown in Fig. 12, the proposed method only consumes a lower decryption time for the data decryption process when the number of attributes is increased compared with other techniques where the maximum value was (1 ms) and the minimum value was (10.5 ms) of decryption times.

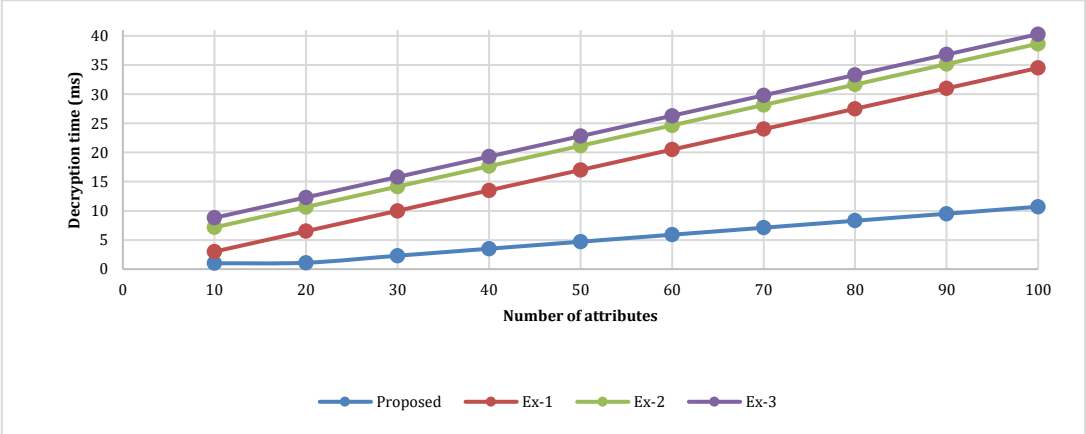

Fig. 12: Analysis of decryption time

As shown in Fig. 13, the proposed method only consumes a lower uploading time for the data process. The maximum and minimum uploading times of the proposed method are (3 ms) and (6 ms). Whereas the maximum and minimum uploading times of the BSSPD-(Ex-1) method was (5 ms) and (30 ms). Similarly, the maximum and minimum uploading times of ECC-(Ex-2) and RSA-(Ex-3) were (6 ms/10 ms) and (18 ms/20 ms), respectively.

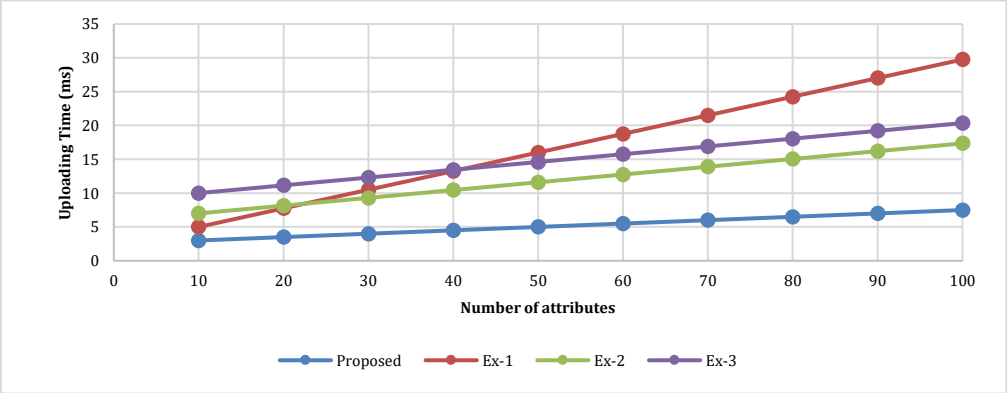

Fig. 13: Analysis of uploading time

A comparative analysis of the downloading time is illustrated in Fig. 14. Based on the analysis, the proposed method only consumes a lower downloading time for the data process compared with other techniques. In the proposed method, the maximum and minimum values of downloading time were (4 ms) and (10 ms), respectively. On the other hand, with the BSSPD-(Ex-1), the maximum and minimum values of downloading times were (6 ms) and (28 ms). Similarly, the maximum and minimum values of uploading times at ECC-(Ex-2) and RSA-(Ex-3) were (9 ms/11 ms) and (34 ms/40 ms), respectively.

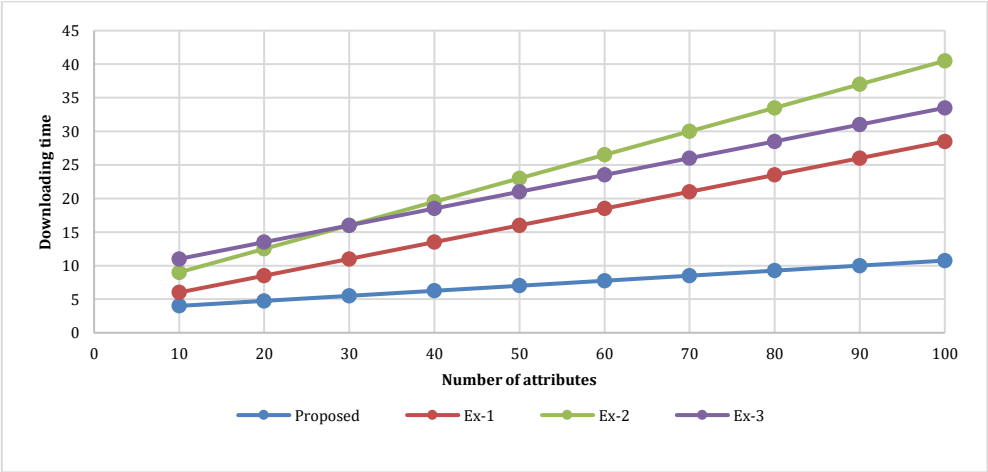

Fig. 14: Analysis of downloading time

A comparative analysis of the processing time is illustrated in Fig. 15. The maximum and minimum processing times of the proposed method were (2 ms) and (5 ms). The maximum and minimum processing times of the BSSPD-(Ex-1) method was (5 ms) to (36 ms). Similarly, the maximum and minimum processing times of ECC-(Ex2) and RSA-(Ex-3) were (8 ms/9 ms) and (45 ms/36 ms), respectively. Therefore, the proposed method only consumes a lower processing time for the data process.

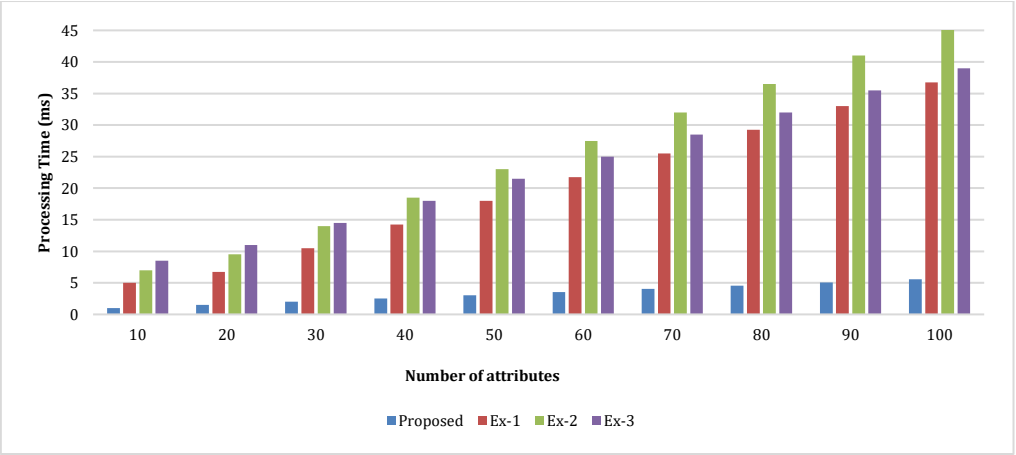

Fig. 15: Analysis of processing time

A comparative analysis of the received packets is illustrated in Fig. 16. The proposed methodology receives 97% of the packets from the data owner. The existing BSSPD-(Ex-1), ECC-(Ex-2), and RSA-(Ex-3) methods received 87%, 85%, and 82%, respectively. Based on the analysis of the received packets, the proposed methodology receives a high percentage of packets.

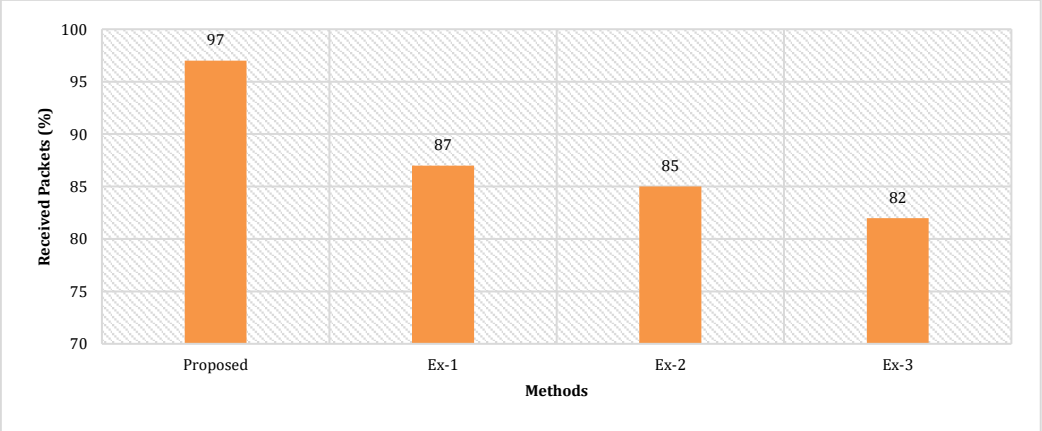

Fig. 16: Analysis of processing time

6. Conclusion

In this paper, BDASS was developed to enhance security operations in personal data through data access control and a secure sharing method. The proposed method uses a combination of blockchain, IPFS, DAC, and CP-ABE to improve the security of personal data. To maintain the owner's security, a blockchain-based DAC was designed. To maintain secure data storage and sharing, blockchain-based CP-ABE was designed. In this proposed methodology, the data owner encrypted the data and stored it in the IPFS, which empowers the security of the data. The proposed methodology was validated by implementing it in the MATLAB platform. The performance of the proposed methodology was verified using performance metrics such as storage overhead, initialization time, waiting time, encryption time, decryption time, uploading time, downloading time, and processing time. The proposed method was compared with conventional data access and security methods, such as BSSPD, ECC, and RSA. It was validated through performance analysis and comparative analysis. Based on the comparison analysis, the proposed method achieved the best performance metrics results. In the future, a new method will be introduced to reduce the processing time of data access and enhance security.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Asuncion A and Newman D (2007). UCI machine learning repository. University of California, School of Information and Computer Science, Irvine, USA.

Campanile L, Iacono M, Marulli F, and Mastroianni M (2021). Designing a GDPR compliant blockchain-based IoV distributed information tracking system. Information Processing and Management, 58(3): 102511. https://doi.org/10.1016/j.ipm.2021.102511

Chen J, Wang W, Zhou Y, Ahmed SH, and Wei W (2021). Exploiting 5G and blockchain for medical applications of drones. IEEE Network, 35(1): 30-36. https://doi.org/10.1109/MNET.011.2000144

Eltayieb N, Elhabob R, Hassan A, and Li F (2020). A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. Journal of Systems Architecture, 102: 101653. https://doi.org/10.1016/j.sysarc.2019.101653

Esposito C, Ficco M, and Gupta BB (2021). Blockchain-based authentication and authorization for smart city applications. Information Processing and Management, 58(2): 102468. https://doi.org/10.1016/j.ipm.2020.102468

Ghiasi M, Dehghani M, Niknam T, Kavousi-Fard A, Siano P, and Alhelou HH (2021). Cyber-attack detection and cyber-security enhancement in smart dc-microgrid based on blockchain technology and Hilbert Huang transform. IEEE Access, 9: 29429-29440. https://doi.org/10.1109/ACCESS.2021.3059042

Guo L, Yang X, and Yau WC (2021). TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain. IEEE Access, 9: 8479-8490. https://doi.org/10.1109/ACCESS.2021.3049549

Guruprakash J and Koppu S (2020). EC-ElGamal and genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain. IEEE Access, 8: 141269-141281. https://doi.org/10.1109/ACCESS.2020.3013282

Honar Pajooh H, Rashid M, Alam F, and Demidenko S (2021). Multi-layer blockchain-based security architecture for internet of things. Sensors, 21(3): 772. https://doi.org/10.3390/s21030772 **PMid:33498860 PMCid:PMC7865640**

Hussien HM, Yasin SM, Udzir NI, Ninggal MIH, and Salman S (2021). Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration, 22: 100217. https://doi.org/10.1016/j.jii.2021.100217

Kim J and Park N (2021). Role-based access control video surveillance mechanism modeling in smart contract environment. Transactions on Emerging Telecommunications Technologies, 33: e4227. https://doi.org/10.1002/ett.4227

Kumar R and Tripathi R (2021). Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model. Journal of Ambient Intelligence and Humanized Computing, 12(2): 2321-2338. https://doi.org/10.1007/s12652-020-02346-8

Lin C, He D, Huang X, Choo KKR, and Vasilakos AV (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications, 116: 42-52. https://doi.org/10.1016/j.jnca.2018.05.005

Mittal A, Gupta MP, Chaturvedi M, Chansarkar SR, and Gupta S (2021). Cybersecurity enhancement through blockchain training (CEBT)–A serious game approach. International Journal of Information Management Data Insights, 1(1): 100001. https://doi.org/10.1016/j.jjimei.2020.100001

Narayanan U, Paul V, and Joseph S (2022). Decentralized blockchain based authentication for secure data sharing in Cloud-IoT. Journal of Ambient Intelligence and Humanized Computing, 13(2): 769-787. https://doi.org/10.1007/s12652-021-02929-z

Rivera Sánchez YK, Demurjian SA, and Gnirke L (2017). Attaining role-based, mandatory, and discretionary access control for services by intercepting API calls in mobile systems. In the International Conference on Web Information Systems and Technologies, Springer, Porto, Portugal: 221-248. https://doi.org/10.1007/978-3-319-93527-0_11

Wang S, Zhang Y, and Zhang Y (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 6: 38437-38450. https://doi.org/10.1109/ACCESS.2018.2851611

Wu A, Zhang Y, Zheng X, Guo R, Zhao Q, and Zheng D (2019). Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Annals of Telecommunications, 74(7): 401-411. https://doi.org/10.1007/s12243-018-00699-y

Xu H, He Q, Li X, Jiang B, and Qin K (2020). BDSS-FA: A blockchain-based data security sharing platform with fine-grained access control. IEEE Access, 8: 87552-87561. https://doi.org/10.1109/ACCESS.2020.2992649

Xu Z, Zhang J, Song Z, Liu Y, Li J, and Zhou J (2021). A scheme for intelligent blockchain-based manufacturing industry supply chain management. Computing, 103(8): 1771-1790. https://doi.org/10.1007/s00607-020-00880-z

Yan Z and Lee JH (2021). BGPChain: Constructing a secure, smart, and agile routing infrastructure based on blockchain. ICT Express, 7(3): 376-379. https://doi.org/10.1016/j.icte.2020.12.005

Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, and Choo KKR (2020). An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Transactions on Services Computing, 13(4): 625-638. https://doi.org/10.1109/TSC.2020.2966970

Zhang J, Lu C, Cheng G, Guo T, Kang J, Zhang X, and Yan X (2021a). A blockchain-based trusted edge platform in edge computing environment. Sensors, 21(6): 2126. https://doi.org/10.3390/s21062126 **PMid:33803561 PMCid:PMC8003011**

Zhang Y, Liu T, Cattani C, Cui Q, and Liu S (2021b). Diffusion-based image inpainting forensics via weighted least squares filtering enhancement. Multimedia Tools and Applications, 80(20): 30725-30739. https://doi.org/10.1007/s11042-021-10623-7

Zhang Y, Liu W, Xia Z, Wang Z, Liu L, Zhang W, and Fang B (2021c). Blockchain-based DNS root zone management decentralization for internet of things. Wireless Communications and Mobile Computing, 2021: 6620236. https://doi.org/10.1155/2021/6620236 **PMid:35573891**