Optimization with Blockchain based Secure Authentication and Collaborative Data Sharing Model in Cloud

Shelke Kavita
Assistant Professor, Department of Computer Engineering
Fr. C. Rodrigues Institute of Technology, Vashi
Navi Mumbai, India
kavita.shelke@fcrit.ac.in

Dr. Shinde S.K.
Professor, Department of Computer Engineering
Lokmanya Tilak College of Engineering, Koparkhairane
Navi Mumbai, India
skshinde@ltce.in

Abstract—
Cloud computing has become a critical technology to meet infrastructure and data service needs cost-effectively, with minimal effort, and with a high degree of scalability. It is widespread in many facets. Although the use of cloud computing has increased significantly, concerns about information security have not yet been fully addressed. With the exponential growth of cloud computing, many new web services have emerged, making it difficult for customers to choose the services they want. This research study has attempted to create a powerful framework for data exchange called blockchain-based secure authentication and collaborative data sharing in the cloud to overcome this hurdle. The entities used in this research are third parties, data owners, smart contracts, and blockchain networks. The steps involved in this process are initialization, registration, authentication, data sharing, and decryption. The safety operators are created using Fire Hawks Optimization (FHO). In addition, the evaluation metrics are revenue, storage usage, and compute costs. Finally, the results proved that FHO-based OptiBC-SecAuth-DS achieved maximum revenue, minimum storage usage, and minimum computational costs.

Keywords: Cloud Computing, Blockchain, Collaborative data sharing, security, Revenue distribution.

I. INTRODUCTION

Cloud computing [1], an internet-based network technology, has contributed to the rapid advancement of communication technology by serving customers with a variety of needs. It includes resources such as hardware and software applications, software development platforms, and testing tools. [2][3][4]. The security of cloud computing [5] is a crucial area within computer security, and it presents a significant obstacle to the broad use of cloud technology. Due to the fact that cloud computing services are essentially based on an Internet connection, they are susceptible to numerous attacks and other security risks, which could have potentially disastrous effects. Examples of these risks include data breaches, malware injections, denial-of-service (DoS) attacks, data loss, and insecure application programming interfaces (APIs). The infrastructures for collaborative product development (CPD) in contemporary socio-technical systems are collaborative computing and collaborative environments. A wealth of information and resources have been made available to all types of users as a result of the recent expansion of collaborative data sharing, which has advantages in the fields of education and research, medicine, and entertainment [6]. Additionally, cloud customers can employ the developing technology known as Blockchain to increase trust and ensure data security when outsourcing and purchasing services from the Cloud. [7].

Blockchain, with its potent decentralized mechanism, has drawn an increasing number of academics and offers workable solutions to address the effects of cloud computing because the data stored on a chain is visible and tamper-resistant [8]. The distributed ledger described by blockchain technology offers a safe and transparent data exchange between the supply chain stakeholders [9]. A decentralized approach to facilitating trustworthy interactions between data owners and energy service providers for personal data sharing and data consumption audits with transparency and provenance tracking is provided by upcoming blockchain and smart contract technology [10]. Due to its decentralization, immutability, traceability, and executable smart contracts, a blockchain is a useful tool for solving verifiable and traceable transactions. It is widely employed in a variety of situations, including virtual currency, electronic bidding, and the Industrial Internet of Things (IoT), thanks to the properties of its distributed data ledger [11]. Blockchain does not employ an incentive mechanism to encourage cooperating parties to offer secure and trustworthy data during data sharing across several clouds. Given that the data collection may occur separately in various organizations, the data sharing should have incentives to enhance the quality and revenue of services [12].

The contribution of this work is to generate an influential approach for blockchain-based secure authentication and collaborative data sharing in the cloud, where an ecological system is intended to be provided by a blockchain-based platform. Through the blockchain, it authorizes diverse participants and ensures the protection of data privacy. The third parties act as sending parties and the data owners will act as receiving parties. At first, the user data is fed up to the senders and it is subjected to the smart contract. Moreover, it sends the data acquisition to senders. The components of smart contracts share the revenue distribution to the cloud. When the sender requests data, the receiver will send the data to the cloud through a smart contract. After that, collaborative data sharing takes place and the proposed approach regards the revenue

distribution based on Multiple Services (MS) and the authentication is done by security operators with key generation utilizing FHO.
The novelty of this article is FHO based OptiBC-SecAuth-DS, an influential framework is introduced that utilises proposed FHO based OptiBC-SecAuth-DS to secure data using blockchain-based secure authentication and collaborative data sharing in cloud.
The remaining part of this work is ordered as the conventional techniques reviewed are deliberated in segment II, the proposed strategy is explicated in segment III and the outcomes obtained by the devised technique are elaborated in segment IV and segment 5 describes the conclusion of the proposed FHO-based OptiBC-SecAuth-DS.

II. MOTIVATION

Blockchain is a viable application area in the privacy and security sector, where the potential reach of an application is quite small. Therefore, this research inspired the development of the privacy-preserving, decentralized data sharing method (PPDS) technique in the e-governance system. The papers examined for this work are described below along with their drawbacks.

A. Literature survey

Wu, Y., et al [6] presented a brand-new grid-based geometric deformation technique for the security mechanism to facilitate secure product data transmission in a cloud-based collaborative design environment. This approach is content-based, which is different from generic cloud security mechanisms.

Hong, L., et al; [8] the newly introduced Inter Planetary File System-equipped blockchain and attribute-based encryption (ABE) (IPFS). This method addresses the problems of malicious decryption in typical cloud computing scenarios and storage strain on the block chain by outsourcing decryption and data storage using the blockchain and IPFS. It sacrificed some efficiency to seek stronger security.

Chinnaraj, G. et al [9] introduced Intelligent secured inventory management strategy with the reduced cost. In this method, lot of iterations were required. Hence, the computational time was high.

Wang, Y., et al [10] proposed Secure and Auditable Private Data Sharing Scheme (SPDS). In this approach, a trust-free framework provided the privacy-preserving data computation, fine-grained data non-reputable data usage tracking, access and usage control. Moreover, the smart contract execution mechanism was employed for confidential user data processing and the alleviation of computation overhead in blockchain. The memory-efficient inference algorithm for knowledge extraction in trusted execution environment (TEEs) was not analyzed. Furthermore, it was failed to investigate the optimal contract design without prior knowledge of user type distribution.

Feng, T., et al [11] presented Blockchain privacy protection scheme based on zero-knowledge proof. This method combined the zero-knowledge proof and smart contracts to achieve data validity and consistency between the data owners and cloud service providers. This method was failed to analyze the realization of secure sharing of data without third-party server and the realization of Completely decentralized data sharing scheme.

Shen, M., et al; [12] introduced the reliable collaboration model was designed to provide the dynamic distribution of revenue by Shapley value. Moreover, the solution encouraged that more clouds contributed their data and improved data authenticity Failed to achieve the fair distribution of benefits. Moreover, it was difficulty of judge the contributions when roles or data are unknown.

Yan, B., et al; [13] designed the collaborative service recommendation system using Blockchain (BC-SRDS). The cloud platforms easily got the shared data and used to maximize the profits, meanwhile, the BC-SRDS was capable of achieving data confidentiality, data integrity and tampering-proof. This model takes more time while sending the request to cloud platform.

Deng, H., et al; [14] Identity-based broadcast encryption (IBBE) was used by the recently established Policy-based Broadcast Access Authorization (PBAA) method to enable multi-recipient data sharing and also realized a fine-grained re-encryption mechanism adopting linear secret sharing technique. However, in order to provide a more effective result, the identity authentication, hash function, and digital signature procedures were not combined.

B. Major Challenges

The various difficulties that come across the existing techniques are as follows.

- In [8], the method ABE and IPFS are used to lessen the chain's storage burden without tampering. However, the overall effectiveness of the blockchain-based access control and data sharing system was not promoted by this method, which did not investigate more significant features like attribute revocation, user revocation, policy concealing, or attribute revocation.
- In the reliable collaboration model [12], the challenge with the collaborative data sharing technique is that the communication overhead across cloud platforms was greatly increased by the data storage across multiple distributed platforms. This problem is not promptly addressed.
- The planned approach BC-SRDS in [13] was exceeded, however, it took a longer time to transmit the request to the cloud platform.
- Cloud storage architecture offered users practical services. The data is not evenly dispersed among cloud servers, despite the distributed cloud storage systems.

III. PROPOSED METHODOLOGY

The aim of this paper is to create a blockchain-based system for collaborative data exchange and secure authentication. Entities like third parties, data owners, smart contracts, and blockchain networks will be taken into account in this case. It will provide a platform for all users to share data and distribute profits. In this case, the sending parties for numerous clouds of data in the blockchain-based data sharing system will be third parties, and the receiving parties will be the data owners. In the beginning, user will send data service request to third parties, and it will submit a data request to a smart contract. The smart contract will also distribute the data acquisition to outside parties. The Smart contracts will also contribute the revenue distribution to the cloud and be seen as model control components. Owners of the requested data will transmit it to the cloud when a third party publishes a request for it. The third parties will receive cloud data via smart contracts. The process of collaborative data sharing will involve processes like initialization, registration, authentication, data exchange, and validation. In addition, the suggested data sharing model would use the Numerous Services (MS) Mechanism revenue distribution model to enhance multiple cloud services. The authentication method will be developed using several security operators, including encryption, hashing, passwords, and keys, with the keys being ideally generated via Fire Hawks optimization [1]. Figure 1 shows the systemic view of the proposed FHO-based OptiBC-SecAuth-DS. The steps involved are initialization, registration, authentication, data sharing, revenue sharing, and decryption.

A. Initialization

In this segment, initialization is the first step to initialize the random numbers. The random numbers are signified by $c, d, w,$ and z in the range of 0 and 4. Thus, f , K_p , and s characterized as a hash function, a public key, and a security parameter respectively. Figure 2 shows the Initialization phase of FHO-based OptiBC-SecAuth-DS

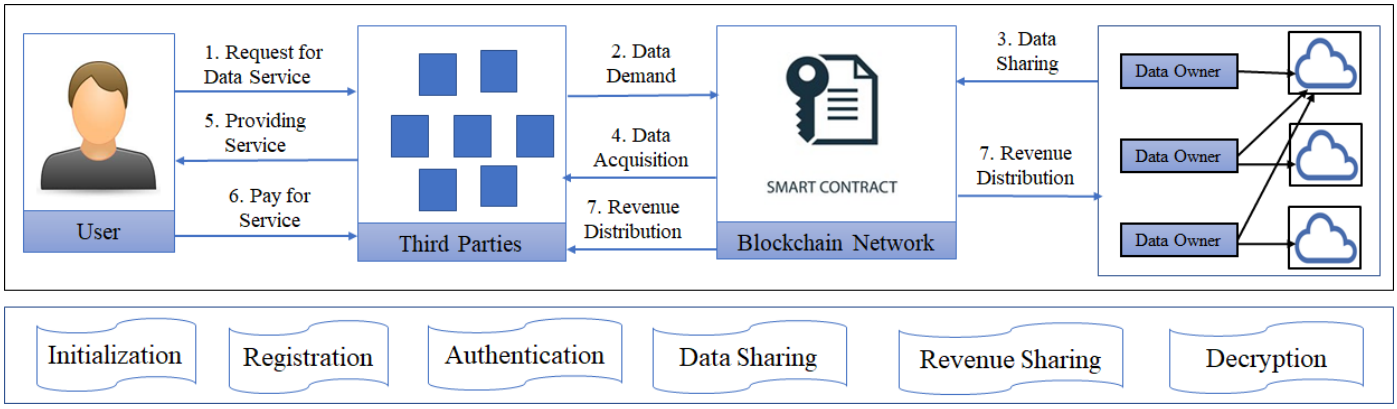


Figure 1. Methodology view of proposed FHO-based OptiBC-SecAuth-DS

User	Third Parties	Smart Contract	Miner	Data Owner	Blockchain
				Initalize Random Number $c, d, w, z = [0 - 4]$ $f \rightarrow$ *Hash Function* $K_p \rightarrow$ *Public Key* $s \rightarrow$ *Security Parameter*	

Figure 2. Initialization phase of FHO-based OptiBC-SecAuth-DS

B. Registration

The registration phase of FHO-based OptiBC-SecAuth-DS is shown in Figure 3. In the registration phase, the registration takes place between the user and the third party. The user contains the user id C_{id} and password C_{pwd} . The user id and passwords are sent to the third parties and stored as C_{id}^{*} , C_{pwd}^{*} , and again it will be stored in the blockchain as C_{id}^{**} and C_{pwd}^{**} . The message is formed by the concatenation of the user's password and a random number in the hash function and this message will send to the user. If the given message to the user is verified with the third parties and the user is registered. Here, the message is indicated as, which is formulated as,

$$N_1 = f\left(C_{pwd} \| z\right) \quad (1)$$

C. Registration between the third party and data owner

In this phase, the registration between the third party and the data owner (DO) is processed. The third parties are denoted as Q_{id}^{r}, Q_{pwd}^{r} those stores in the smart contract, miners, data owners, and finally in the blockchain. The saved id and password will be verified by the data owner and it produced the verified message (EN_1) by the third party password concatenated with the public key and XOR operation with a random number by the hash function. After that, EN_1 is subjected to the user and stored in it. Again EN_1 return to the DO to verify and register the data between the third party and the DO. Figure 4 shows the Registration phase between the third party and DO.

$$EN_1 = f\left(Q_{pwd}^{***} \| K_p\right) \oplus s \tag{2}$$

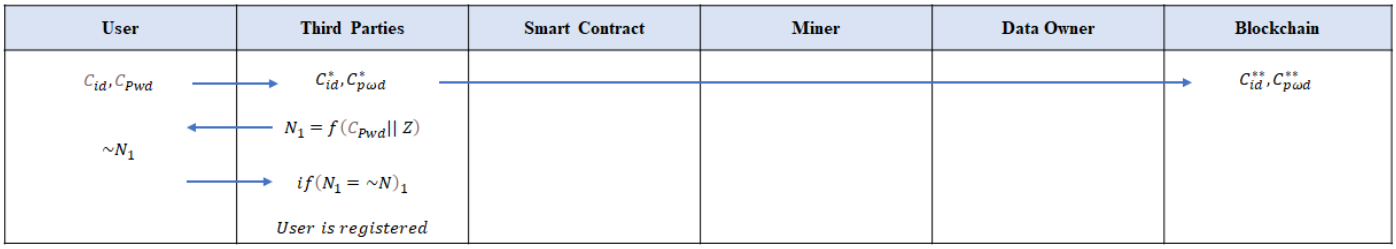


Figure 3. Registration phase of FHO based OptiBC-SecAuth-DS

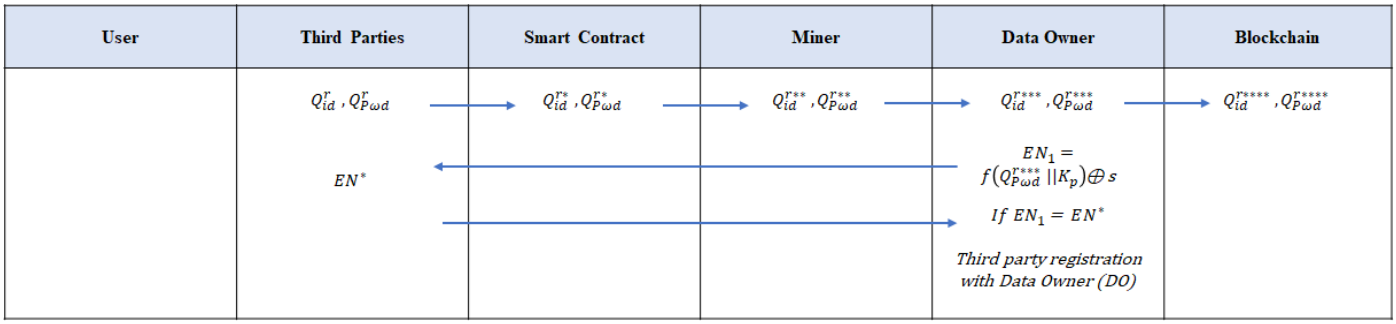


Figure 4. Registration phase between third party and data owner

D. Authentication

In the authentication segment first, the user sends the authentication request to the third party which is given below,

$$R_1 = f\left(c \| K_p\right) \oplus f\left(C_{pwd} \| w\right) \oplus s \tag{3}$$

The third party received the request and verifies whether the user id is matched or not. If it is equal then the third party sends a request to smart control otherwise, it will get rejected.

$$R_2 = f\left(Q_{pwd}^{r} \| z\right) \oplus f\left(s \| c\right) \oplus V \tag{4}$$

Where V is indicated as a timestamp. If the time stamp is confirmed with the request, it creates a message to a third party or else it rejects the session. Whether the time stamp is valid, the message is represented as M_2. After that, M_2 send to the third party stored. The third party is authenticated after the verification of the message.

The third party sends another authentication request to DO using Eq. (5) to create one time token (OTT). After the generation of OTT Eq. (6) the third party will get authenticated.

$$R_3 = f\left(Q_{id}^{r} \| Q_{pwd}^{r} \| K_p\right) \oplus s \tag{5}$$

$$OTT = f\left(Q_{pwd}^{r***} \| d\right) \oplus f\left(s \| w\right) \tag{6}$$

Where the authentication requests are illustrated as R_1, R_2 and R_3 respectively. Authentication of FHO-based OptiBC-SecAuth-DS is viewed in Figure 5.

E. Data Sharing

After the authentication, the DO sends the encrypted data to the blockchain and stores them using Eq. (7). Thereafter, the third party receives a data access request from the user and checks if the received data was similar to the saved data. If it is similar, the third party sends a request to DO through the miner and verifies the data with existing data. When the data is verified, it generates a message to block the chain and send the data to the DO. Data sharing of FHO-based OptiBC-SecAuth-DS is drawn in Figure 6.

$$F = H\left(e, j\right) \tag{7}$$

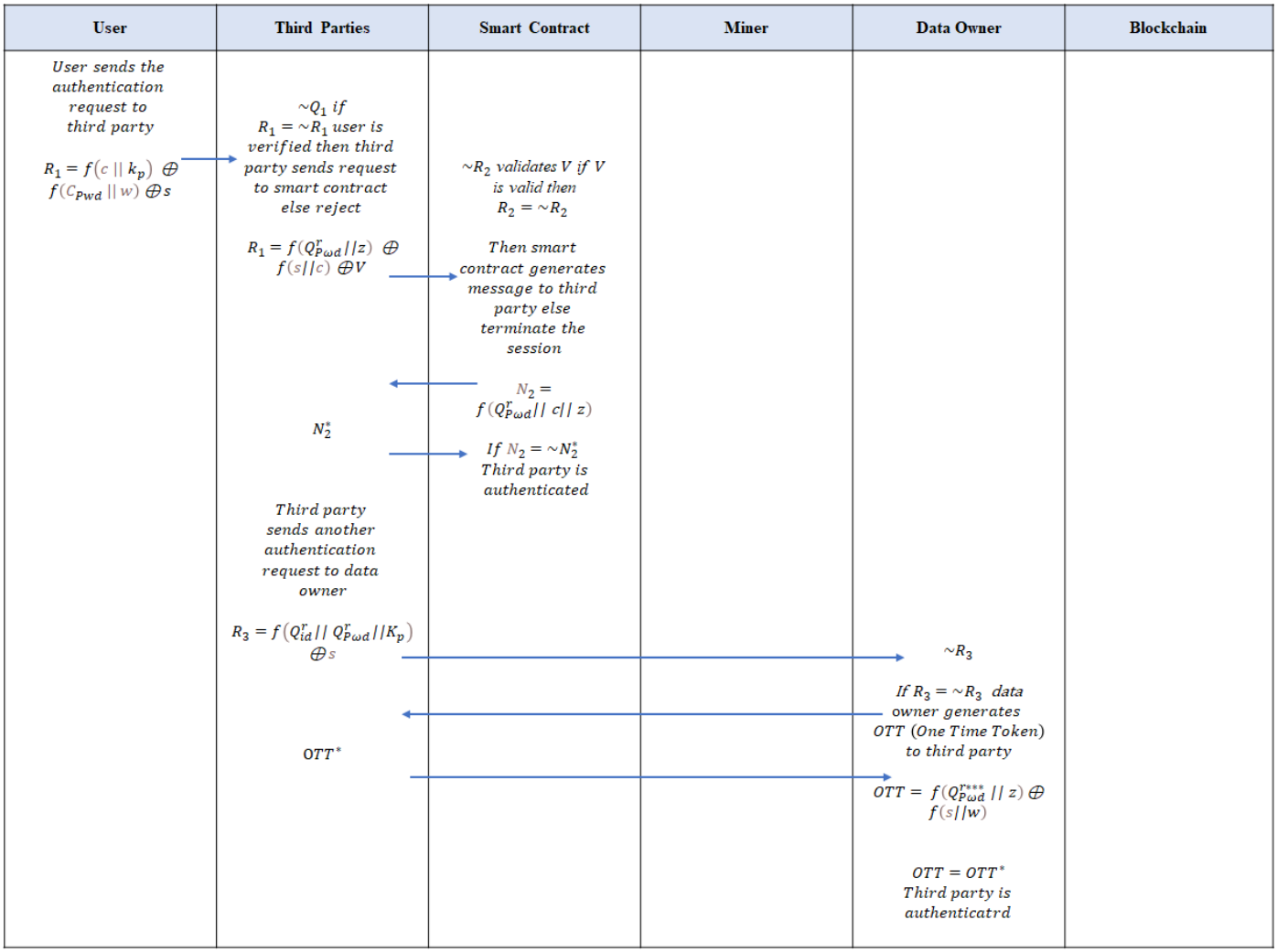


Figure 5. Authentication of FHO-based OptiBC-SecAuth-DS

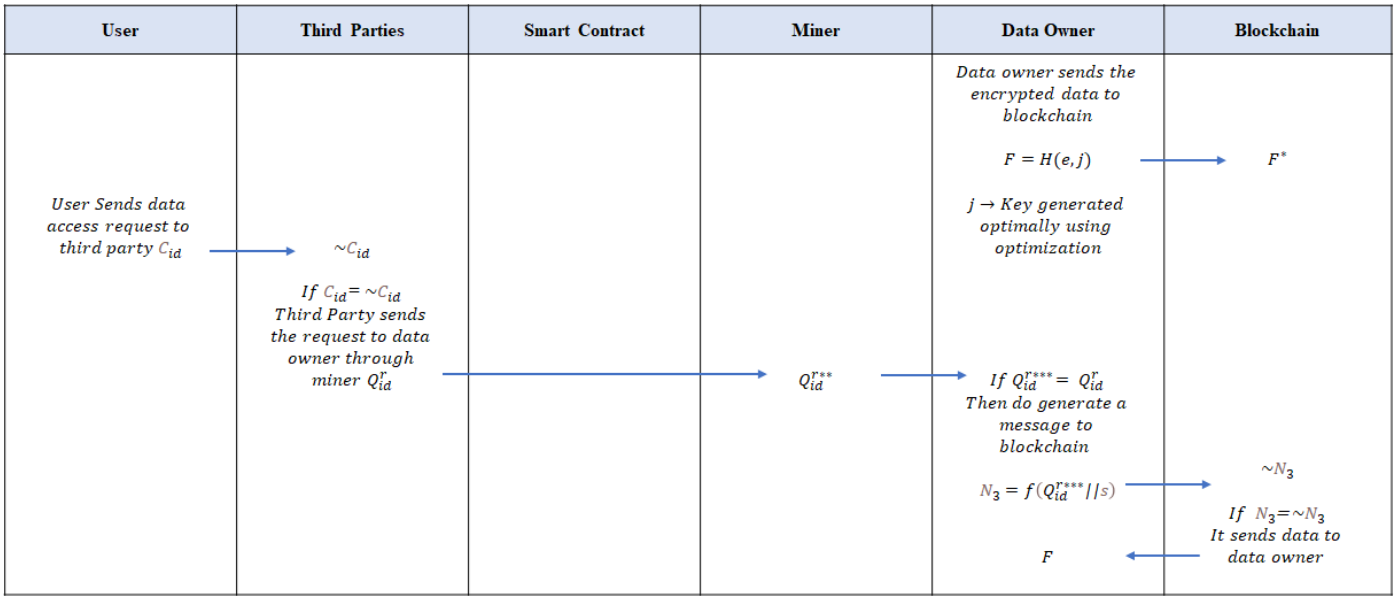


Figure 6. Data sharing of FHO-based OptiBC-SecAuth-DS

F. Revenue sharing

The DO shares the data, so that share values are equally distributed to miners.

$$Y = f\left(Q_{id}^{r}\right) \oplus I \tag{8}$$

Where, Y and I indicates share value and revenue respectively. Data owner send the share values to miner with third party id and revenue, which is illustrated as,

$$I = Y \oplus f\left(Q_{id}^{r}\right) \tag{9}$$

G. Decryption

In this segment, the encrypted data should send the data to the miner and the data attained in the miner is stored as F^{*}. After that, the data send to the user through a third party which is deliberated in Figure 7 as,

$$F_e = e\left(F^{**}, h\right) \tag{10}$$

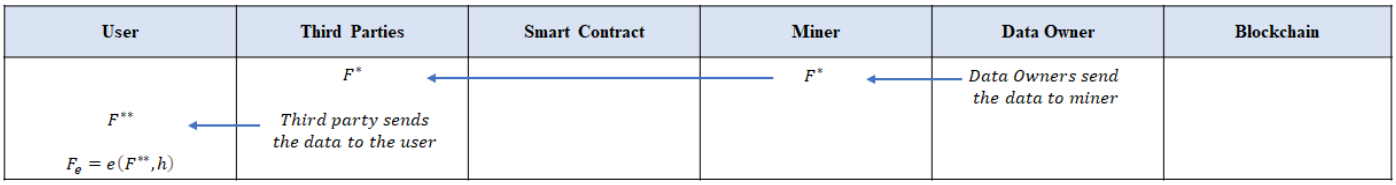


Figure 7. The decryption of FHO-based OptiBC-SecAuth-DS

H. Key generation using FHO

In this segment, the concept of FHO is employed along with key generation to create an optimization approach named optimization blockchain secure authentication data sharing in the cloud.

- Solution encoding: In solution encoding, the key is optimally generated using FHO.
- Fitness Measure: The fitness measure [15] is to evaluate the optimal features which is formulated as,

$$A=(L+M)/2 \tag{11}$$

Algorithmic steps	
Step 1	Initialization: In search space, a random process is initialized to recognize the initial position of the feature vectors.
Step 2	Evaluate Fitness measure: The fitness measure A analyzed using Eq. (11) to choose the exact aspect for further purpose.
Step 3	Evaluate Total distance between fire hawks and prey: Between fire hawks and prey, the total distance is analyzed which results in the effectual region of these birds being distinguished by analyzing each bird's nearest prey.
Step 4	Calculate the new position of fire hawks: In order to set the fire in a particular area, the burning sticks are collected from the main fire by fire hawks.
Step 5	Update new position: The prey finalizes to run way, hide or run towards the fire hawk while dropping the burning sticks by fire hawk which considered these actions to update a new solution by, $W_t^{new} = W_t + \left(x_3 * Z_1 - x_4 * T_1\right), \begin{cases} i = 1,2,\ldots m \\ t = 1,2,\ldots x \end{cases}$ (12) Where, W_t^{new} denotes the new position of t^{th} prey surrounded by i^{th} fire hawk which is indicated as Z_1, T_1, signifies safe place and x_3, x_4 represent random numbers.
Step 6	Evaluate safe place: In essence, it is a place that many animals used to meet in regards to stay safe during risk.
Step 7	Terminate. The steps will be repeated until it attained the exact solution of proposed FHO based OptiBC-SecAuth-DS.

IV. RESULT AND DISCUSSION

The proposed FHO-based OptiBC-SecAuth-DS obtained better outcomes by considering other strategies. The proposed FHO-based OptiBC-SecAuth-DS is done employing the PYTHON tool. The database [16] employed in this work consists of 76 attributes but 14 of them are the most frequently used subset. Specifically, Cleveland is the one that is often employed. The metrics for the analysis employed are revenue, computational cost, and memory usage. Revenue is nothing but the total amount of income constructed by the companies between the shareholders and stakeholders. The memory percentage employed during a sample period is called memory usage. The computational cost is employed to weigh the number of resources in training or interference. FHO-based OptiBC-SecAuth-DS is compared with conventional strategies namely ABE [8], reliable collaboration model [12], and BC-SRDS [13] to show the effectualness of the proposed FHO-based OptiBC-SecAuth-DS. FHO-based OptiBC-SecAuth-DS is computed based on Cleveland and Hungarian datasets by varying block sizes utilizing evaluation metrics.

A. *Assessment based on the Cleveland dataset*

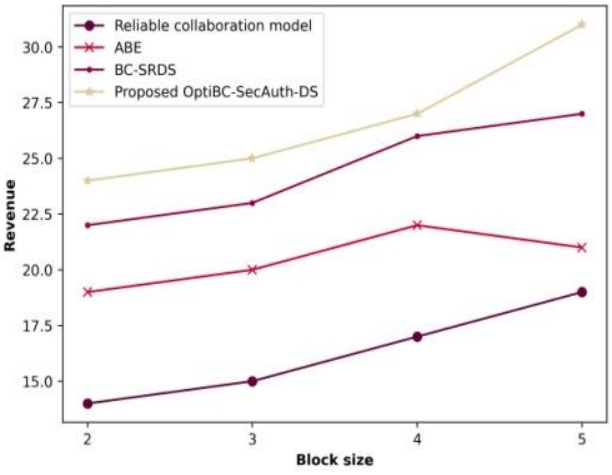
An analysis of FHO-based OptiBC-SecAuth-DS in regards to measures by changing the block size is deliberated in figure 8. Figure 8 a) indicates an assessment of FHO-based OptiBC-SecAuth-DS with revenue is shown. When the block size is 5, the existing techniques namely the reliable collaboration model, ABE, and BC-SRDS attained revenue with 19, 21, and 27; while the proposed FHO-based OptiBC-SecAuth-DS is 31. Figure 8 b) represents memory usage. The traditional methods observed memory usage with 187.726 MB, 130.589 MB, and 122.431 MB while the proposed is 65.295 MB when the block size is 5. Figure 8 c) shows computational cost. When the block size= 5, the techniques obtained the computational cost as 0.951 sec, 0.316 sec, 0.215 sec, and 0.114 sec.

B. *Analysis based on the Hungarian dataset*

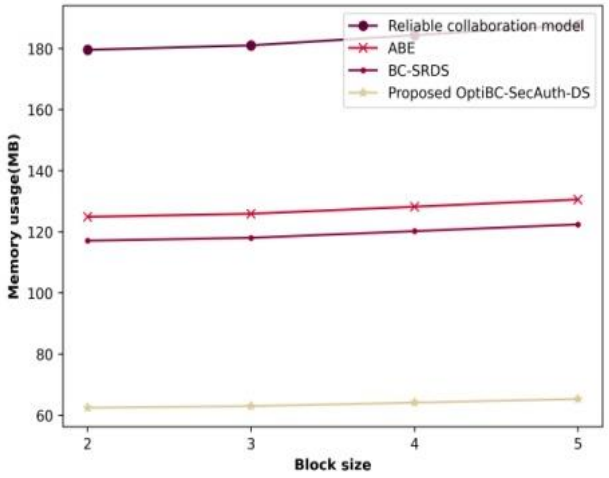
Figure 9 depicts a comparative analysis based on Hungarian. Figure 9 a) presents based OptiBC-SecAuth-DS with revenue. Here, when the block size is 5, the existing methods attained revenue with 19, 26, and 28 while the proposed OptiBC-SecAuth-DS observed 32. Figure 9 b) enumerates memory usage, the conventional techniques obtained memory usage with 188.979 MB, 130.877 MB, and 123.517 MB while the proposed achieved 65.445 MB. Figure 9 c), elucidates computational cost. When the block size is 5, the methods like the reliable collaboration model attained 0.474 sec, ABE observed 0.260 sec, BC-SRDS achieved 0.179 sec and the proposed OptiBC-SecAuth-DS observed 0.058 sec with respect to computational cost.

C. *Comparative discussion*

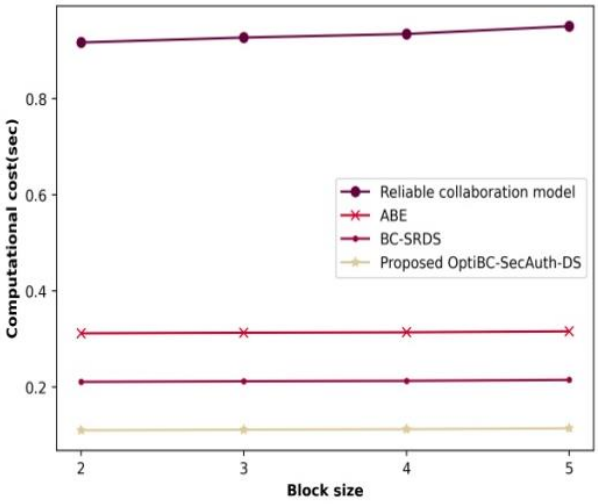
The proposed FHO-based OptiBC-SecAuth-DS observed better outcomes when compared with conventional strategies and the outcome attained are expressed in table 1. This clearly shows that FHO-based OptiBC-SecAuth-DS acquired maximum revenue, minimum memory usage, and minimum computational cost with 31, 65.295 MB, and 0.114sec.



(a)

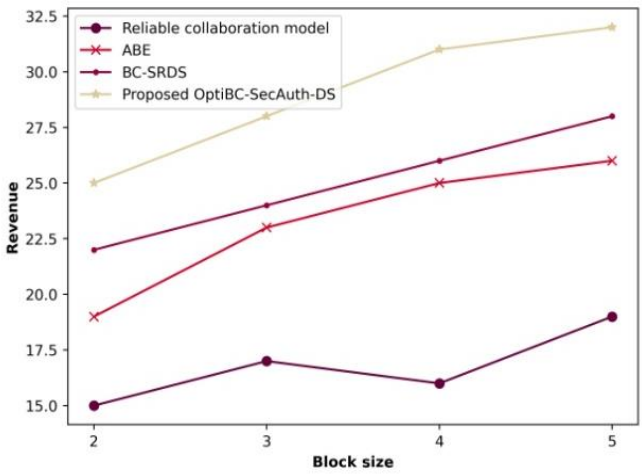


(b)

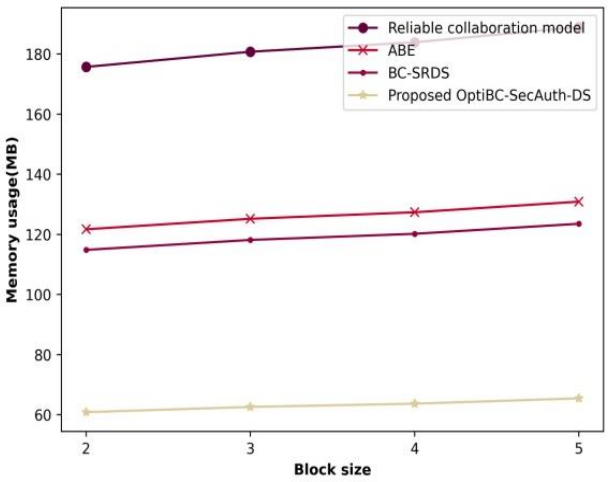


(c)

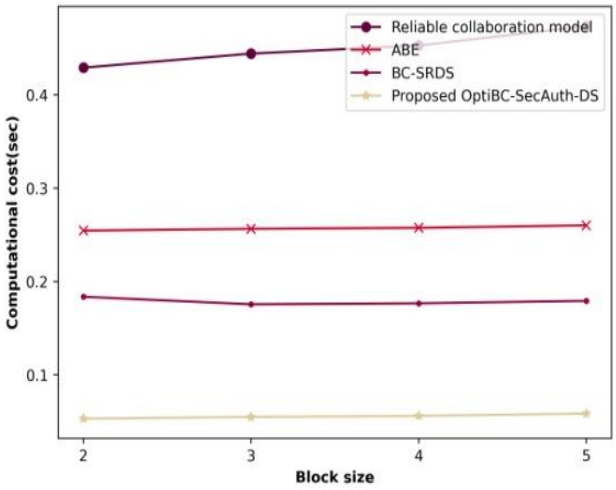
Figure 8. Comparative analysis based upon block size a) Revenue b) Memory usage c) Computation cost



(a)



(b)



(c)

Figure 9. Analysis based on Hungarian a) Revenue b) Memory usage c) computational cost

Table 1. Comparative discussion of FHO based OptiBC-SecAuth-DS

Dataset	Metrics/ Methods	Reliable collaboration model	ABE	BC-SRDS	Proposed FHO based OptiBC-SecAuth-DS
Cleveland	Revenue	19	21	27	31
	Memory usage (MB)	187.726	130.589	122.431	65.295
	Computational cost (sec)	0.951	0.316	0.215	0.114
	Revenue	19	26	28	32
Hungarian	Memory usage (MB)	188.979	130.877	123.517	65.445
	Computational cost (sec)	0.474	0.260	0.179	0.058

V. CONCLUSION

In this research, the data sharing is based on the proposed technique named blockchain based secure authentication and collaborative data sharing in cloud system. The blockchain technology is recently became a basic technology for securing data sharing and storage over decentralized and trustless models. The steps carried out in this research are initialization, registration, authentication, data sharing, revenue sharing and decryption. A data securing phase is done based upon data transformation, XOR operation, encryption and hashing function. In key generation phase, secret key is created utilizing FHO based OptiBC-SecAuth-DS. Initially, the user data was given to the third parties which demands to smart contract. Moreover, it shares the revenue distribution to the cloud and the cloud data was given to the third party through smart contract. The authentication process is done by using FHO. The metrics used here are revenue, memory usage and computational cost. At last, the outcome results that FHO based OptiBC-SecAuth-DS acquired maximum revenue, minimum memory usage and minimum computational cost with 31, 65.295 MB and 0.114secwhen considering Cleveland database. In future, security and privacy related strategies will explore in the generation of blockchain and its application.

REFERENCES

[1] Rashid, A. and Chaturvedi, A., "Cloud computing characteristics and services: a brief review", International Journal of Computer Sciences and Engineering, vol.7, no.2, pp.421-426, 2019.

[2] Pradhan, P., Behera, P.K. and Ray, B.N.B., "Modified round robin algorithm for resource allocation in cloud computing", Procedia Computer Science, vol.85, pp.878-890, 2016.

[3] Mishra, S.K., Sahoo, B. and Parida, P.P., "Load balancing in cloud computing: a big picture", Journal of King Saud University-Computer and Information Sciences, vol.32, no.2, pp.149-158, 2020.

[4] Azizi, M., Talatahari, S. and Gandomi, A.H., "Fire hawk optimizer: A novel metaheuristic algorithm", Artificial Intelligence Review, pp.1-77, 2022.

[5] Tabrizchi, H. and Kuchaki Rafsanjani, M., "A survey on security challenges in cloud computing: issues, threats, and solutions", The journal of supercomputing, vol.76, no.12, pp.9493-9532, 2020.

[6] Wu, Y., He, F. and Yang, Y., "A grid-based secure product data exchange for cloud-based collaborative design", International journal of cooperative information systems, vol.29, pp.2040006, 2020.

[7] Gupta, A., Siddiqui, S.T., Alam, S. and Shuaib, M., "Cloud computing security using blockchain", Journal of Emerging Technologies and Innovative Research (JETIR), vol. 6, no.6, pp.791-794, 2019.

[8] Hong, L., Zhang, K., Gong, J. and Qian, H., "A Practical and Efficient Blockchain-Assisted Attribute-Based Encryption Scheme for Access Control and Data Sharing", Security and Communication Networks, 2022.

[9] Chinnaraj, G. and Antonidoss, A., "A new methodology for secured inventory management by average fitness-based colliding bodies optimization integrated with block chain under cloud", Concurrency and Computation: Practice and Experience, vol.34, no.1, pp.e6540, 2022.

[10] Wang, Y., Su, Z., Zhang, N., Chen, J., Sun, X., Ye, Z. and Zhou, Z., "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain", IEEE Transactions on Industrial Informatics, vol.17, no.11, pp.7688-7699, 2020.

[11] Feng, T., Yang, P., Liu, C., Fang, J. and Ma, R., "Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof", Wireless Communications and Mobile Computing, 2022.

[12] Shen, M., Duan, J., Zhu, L., Zhang, J., Du, X. and Guizani, M., "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds", IEEE Journal on Selected Areas in Communications, vol.38, no.6, pp.1229-1241, 2020.

[13] Yan, B., Dong, A., Chai, B., Han, Y., Zhou, G. and Zhao, F., "Blockchain-assisted collaborative service recommendation scheme with data sharing". IEEE Access, vol.9, pp.40871-40883, 2021.

[14] Deng, H., Zhang, J., Qin, Z., Wu, Q., Yin, H. and Castiglione, A., "Policy-based Broadcast Access Authorization for Flexible Data Sharing in Clouds", IEEE Transactions on Dependable and Secure Computing, 2021.

[15] Wagner, I. and Eckhoff, D., "Technical privacy metrics: a systematic survey", ACM Computing Surveys (CSUR), vol.51, no.3, pp.1-38, 2018.

[16] heart disease database "https://archive.ics.uci.edu/ml/datasets/heart+disease" is assessed on February 2023.