*electronics*

MDPI

*Article*

# A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology

**Yedida Venkata Rama Subramanya Viswanadham * and Kayalvizhi Jayavel**

Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai 603203, Tamil Nadu, India
* Correspondence: yvrsvish@gmail.com

**Abstract:** Blockchain is a recently developed advanced technology. It has been assisted by a lot of interest in a decentralized and distributed public ledger system integrated as a peer-to-peer network. A tamper-proof digital framework is created for sharing and storing data, where the linked block structure is utilized to verify and store the data. A trusted consensus method has been adopted to synchronize the changes in the original data. However, it is challenging for Ethereum to maintain security at all blockchain levels. As such, "public–private key cryptography" can be utilized to provide privacy over Ethereum networks. Several privacy issues make it difficult to use blockchain approaches over various applications. Another issue is that the existing blockchain systems operate poorly over large-scale data. Owing to these issues, a novel blockchain framework in the Ethereum network with soft computing is proposed. The major intent of the proposed technology is to preserve the data for transmission purposes. This new model is enhanced with the help of a new hybrid algorithm: Adaptive Border Collie Rain Optimization Algorithm (ABC-ROA). This hybrid algorithm generates the optimal key for data restoration and sanitization. Optimal key generation is followed by deriving the multi objective constraints. Here, some of the noteworthy objectives, such as information preservation (IP) rate, degree of modification (DM), false rule (FR) generation, and hiding failure (HF) rate are considered. Finally, the proposed method is successfully implemented, and its results are validated through various measures. The recommended module ensures a higher security level for data sharing.

**Keywords:** data privacy preservation system; Ethereum blockchain technology; adaptive border collie rain optimization; supply chain network; data sanitization and restoration



**Citation:** Viswanadham, Y.V.R.S.; Jayavel, K. A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology. *Electronics* **2023**, *12*, 1404. https://doi.org/10.3390/electronics12061404

Academic Editor: Akshya Swain

Received: 12 January 2023
Revised: 7 March 2023
Accepted: 8 March 2023
Published: 15 March 2023



## 1. Introduction

Developers can create many distributed apps based on smart contracts over the Ethereum programming platform. For example, voting, financial transactions, business administration, and contract signing are the applications used in the Ethereum platform [1]. During data sharing, the protection of privacy is very important. If shared data fall into the wrong hands, the data could be misused and accessed by intruders, the denial of loans and health insurance, and victimization of a person by financial fraud [2]. However, if the data can be shared with the right users, then there is no information to be stolen and misused by unauthorized entities [3]. The newly developed privacy-preserving data publishing (PPDP) and privacy-preserving data mining (PPDM) approaches are utilized to reduce privacy issues [4]. Data analysis contains commodity data, and mining turns it into economic value [5]. The digital world increases the possibility of losing control over all of one's own intellectual, emotional, and situational knowledge, breaking the informational privacy area and losing one's autonomy [6]. The primary problem in this situation is that control of privacy leakage by every individual requires high freedom in the flow of information the technology enables, the connections it facilitates, and the advantage supplied by the

information source [7]. Government organizations also create legislative guidelines to protect personal data, including what purposes the particular data is used for, how it is gathered, and how it should be preserved. Corporate privacy issues are also solved by these guidelines [8].

Ethereum is a programming environment that makes it possible to provide privacy preservation with the help of blockchain by building over distributed applications [9]. With "smartcontract", the contract may be carried out without needing a centralized authority after it has been installed. The smart contract executes intent in a perfect world, and it produces reliable results [10]. Blockchain is a new technology that has gained popularity due to the rise of cryptocurrency such as Ethereum and Bitcoin [11]. It may be considered a distributed ledger with cryptography, and accurately records the results of every transaction. A transaction recorded on the blockchain cannot be changed beyond that point, and everyone can see it [12]. Every network member will reach a consensus on the blockchain, ensuring that all valid transactions are recorded [13]. Secondly, every network member will reach a consensus on the blockchain, ensuring that no invalid transactions are recorded. Thirdly, all transactions recorded on the blockchain are auditable by network members and cannot be tampered with by other issues. Smart contracts are being deployed alongside the advancement of blockchain technology such as Ethereum and Hyperledger to increase the potentiality of blockchain [14]. Addressing a transaction for a certain smart contract's address will cause it to be activated [15]. When a smart contract is activated, it can run the predefined program independently through a centralized authority.

The challenges of the existing supply chain are shown below. Rival actors can be found in the same supply chain, which makes data sharing very difficult [16]. Due to these challenges, research on and implementation of traceability are growing slowly. Although there has been work to create supply chain traceability, it is not practical in the actual world. The work demonstrates several procedures in a centralized system's data structures and transparent framework. Researchers' interest in blockchain technology and its application to the supply chain has grown over the last few years [17]. Some limitations of the existing research and their techniques are depicted here. The supply chains' global character makes it challenging to achieve the desired traceability. Several methods are implemented to provide better privacy-preserved data transfer in the supply chain network. However, these methods fail to address issues with certificate verifiability and raise concerns about the existence of privacy-sensitive information. A hash network links the blockchain in chronological order. For each node, it has a copy of a ledger, and few mutually distrusting nodes often maintain this hash network. This system provides better confidentiality and non-repudiation over the Ethereum networks, but the cost requirement is high and the system's feasibility low. To overcome these challenges, a novel blockchain-based privacy preservation model is implemented in the Ethereum network to provide better privacy preservation.

The contributions of the designed Ethereum-based privacy preservation model are listed below.

- To design a blockchain-based data privacy preservation model with a hybrid meta-heuristic algorithm over the supply chain network to secure information exchange and guarantee the privacy of data access in the Ethereum platform. Here, the performance improvement of the proposed model is applicable to different applications regarding cryptocurrency, food supply chains, and sealed-bid auctions.
- To generate the key with the help of developed ABC-ROA for exchanging the secured data in the supply chain framework using data restoration and data sanitization procedures in the Ethereum environment. The developed ABC-ROA algorithm is utilized to restore the data from the receiver side. Consequently, it helps to access the original data that can be generated from the original key.
- To implement the hybrid meta-heuristic algorithm known as ABC-ROA for choosing the best optimal key to maximize the performance of the developed blockchain-based

privacy preservation model. Here, the designed ABC-ROA algorithm improves the system's robustness. It is also used to solve complex issues.

- To compare the developed ABC-ROA-based privacy preservation system with existing meta-heuristic algorithms using a variety of metrics to verify the performance of the developed model.

This paper is split into the following sections. The merits and demerits of recent privacy preservation in the Ethereum network model based on blockchain are described in Section 2. The suggested dataset for the blockchain-based privacy preservation system in Ethereum and the model explanation offered are covered in Section 3. The procedures used to create the privacy preservation model, such as data restoration and sanitization in the supply chain method, are shown in Section 4. The Ethereum privacy preservation model with the ABC-ROA algorithm, optimal key details, and objective function details are described in Section 5. The acquired outcomes of the recommended method are summarized in Section 6. The paper is concluded in Section 7.

## 2. Literature Survey

### *2.1. Related Works*

In 2021, Lin et al. [18] introduced privacy-preserving blockchain architecture (PPChain), and PPChain's design has been changed in Ethereum. PPChain's architecture allowed regulation to provide security. They specifically incorporated cryptographic primitives such as broadcast encryption and group signature into a workable byzantine fault tolerance consensus protocol with a separation mechanism to remove the transaction fee and mine for a reward instead of using the existing mining model. They offered in-depth security and privacy analysis and a performance study to demonstrate the usefulness of PPChain. Examples from the food supply chain, sealed-bid auctions, and cryptocurrency described how the PPChain might be used in regulation applications. In 2022, Rahmadika et al. [19] implemented an efficient architecture for secure misbehavior detection in lightweight IoMT tools in the "artificial pancreas" model (APS). The suggested method used deep learning, which protected privacy, and boosted security by integrating blockchain technology built on the Ethereum smart contract ecosystem. The efficacy of the developed system has been empirically tested for commensurate incentive schemes, exhaustiveness with compact findings, and an untraceable characteristic from a different neural deep learning technique. Consequently, the model has a high recall rate, demonstrating that it is almost completely capable of identifying harmful events in the case being studied.

In 2022, Xiong et al. [20] designed a secure privacy preservation authentication mechanism for inter-constellation collaboration. They created both permanent and transient identities for each satellite to protect privacy. The permanent identity was used for inter-constellation collaboration, whereas the temporary identity was utilized for communication inside the constellation. For information exchange among cooperative satellite constellations, a consortium blockchain was introduced. A replica storage node mechanism has been suggested to enable effective authentication with minimal resources, where well-resourced satellites cache the duplicated data exchanged across the blockchain. A branch-and-bound approach has been used to address the integer programming issue of choosing the replica storage node. According to a security study, the suggested authentication technique was secure against various possible attacks, which included formal analysis using informal verification and BAN Logic. The suggested system provided efficiency in communication overheads, signaling, and processing with greater performance, based on a comparison between it and other privacy preservation schemes. Evaluations showed that the suggested onboard caching approach achieved minimal storage costs and communication delay.

In 2022, Singh et al. [21] implemented a privacy preservation model in smart healthcare using a blockchain-based federated learning method for preserving privacy, which used IoT cloud platforms to provide privacy and security. Scalable machine learning applications such as health-care use federated learning technologies. Users could also utilize a well-trained deep learning system without putting their private information in the

cloud. Additionally, it covered the uses of federated learning in a smart city's distributed secure environment. In 2020, Guo et al. [22] implemented a blockchain-based privacy preservation system in the Ethereum network to provide better privacy preservation data. In that model, they used various mechanisms in the blockchain. Privacy protection and analyzing anonymity methods were used in digital currency. The aim of the encryption mechanism was focused on the privacy protection scheme.

In 2022, Mohan et al. [23] designed the proof of authority (PoA) consensus process, which required little computational power, and it has been implemented on a Raspberry Pi network. The elliptic integrated encryption process used a double-encryption process to protect the secrecy of data. With a speed of at least 25 transactions per second, it has been reported to perform well in contrast to previous systems. It was also readily expandable to accommodate various health-care workers. A new range of real-time health monitoring tools with excellent security and data privacy might come from further work on this concept, potentially leading to significant innovation in the IoMT sector. In 2018, Elisa et al. [24] developed a model for a decentralized deep learning e-government system utilizing a blockchain framework that guaranteed data confidentiality and privacy and boosted public sector confidence. A prototype of the suggested system was also provided, supported by a theoretical and in-depth examination of the system's security and privacy consequences.

In 2022, Dewangan et al. [25] suggested a system that used tokens to create pupils' identities and saved them in a file system. The suggested model used SHA-256 for cryptographic hashing, Edwards-curve digital signature algorithm (EdDSA), and IPFS for digital signature and verification. The results of this suggested method show the transaction speed, the time needed for validating and signing a transaction, and the time needed for each transaction. They evaluated the privacy, transaction costs, huge file storage, blockchain registration, and implementation costs of this system to those of the already built solutions.

### 2.2. Statement of Problem

Personal information is stolen by many hackers and intruders, so privacy preservation is much needed nowadays. Personal data information theft, virus threats, and spamming are illegal activities. However, limited hardware resources in IoT applications, including network bandwidth, computing power, and storage pose unique challenges to the blockchain. Therefore, various researchers have developed efficient technique to secure the data along with the blockchain technology. Some of the disadvantages and advantages of the existing blockchain-based privacy preservation techniques are listed in Table 1. PPChain [18] provides qualitative security and efficient privacy over personal data. Additionally, it ignores the correlation between variables to enhance training performance. However, it is not sufficiently developed to achieve conflicting properties, such as regulation, transparency, anonymity, and confidentiality, and is computationally expensive. Bi-LSTM [19] significantly increases the storage cost. Additionally, it achieves higher prediction accuracy, precision, and f1 score, yet it requires more time for training and is slow compared to other convolutional techniques and does not contain expensive hardware to perform complex mathematical calculations. Signs [20] indicate a high percentage of false positives. Additionally, the board caching method achieves low storage costs and communication latency. However, it does not access the service anywhere and does not provide any security system for communication and privacy protection, so it suffers slightly from the security perspective. Federated learning [21] achieves efficiency in computation, communication overheads, and low signaling with more functionality. Additionally, it achieves high authentication with replica storage and limited resources, yet the efficiency is low when compressing the massive number of devices in the security system and it is very expensive. Data encryption [22] efficiently achieves strict rights management, mainly used for several functions. Additionally, it increases the integrity of the data, and it is very cheap to implement. However, it provides less computation for compatibility and the scalability is very low. For the Raspberry Pi network [23], the implementation cost is low. Additionally, the implementation cost is low, yet to handle a large amount of data,

more storage is needed in this network, and it does not provide a proper balance between connectivity and storage requirements. Peer-to-peer technology [24] improves computation rationality and identity anonymity. Additionally, it is easy to set up the client data and does not need any special knowledge. However, the data confidentiality is very poor, and the file resources do not centrally organize, so it takes more time. EdDSA [25] improves the immutability and transparency to enhance the privacy system. Additionally, it reduces the computational complexity of the decentralization algorithms, yet while using the enormous data, the private key is sometimes leaked and does not support merging complex data. Therefore, these challenges motivated us to develop an efficient privacy-preserving system with blockchain technology.

**Table 1.** Features and disadvantages of the existing blockchain-based privacy preservation techniques with blockchain technology in Ethereum.

| Study | Techniques | Features | Disadvantages |
| --- | --- | --- | --- |
| Lin et al. [18] | PPChain | • It provides qualitative security and efficient privacy over personal data.<br>• It ignores the correlation between variables to enhance the training performance. | • It is not developed for attaining conflicting parameters such as regulation and confidentiality. Anonymity and transparency.<br>• It is computationally expensive. |
| Rahmadika et al. [19] | BiLSTM | • It significantly increases the storage cost.<br>• It achieves higher prediction accuracy, precision and f1 score. | • It requires more training time and is a slower process than other convolutional techniques.<br>• It does not contain expensive hardware to do complex mathematical calculations. |
| Xiong et al. [20] | SGINs | • It gives a high percentage of false positive rates.<br>• The board caching scheme achieves low storage costs and low communication latency. | • It does not access the service anywhere.<br>• It does not provide any security system for communication and privacy protection, so it suffers slightly from the security issue. |
| Singh et al. [21] | Federated Learning | • It achieves more functionality attributes regarding the efficiency in signaling, communication overheads, and computation.<br>• It achieves efficient authentication with replica storage and limited resources. | • The efficiency is low when compressing the massive number of devices in the security system.<br>• The federated communication system is very expensive. |
| Guo et al. [22] | Data encryption | • It efficiently achieves strict rights management, mainly used for several applications.<br>• It increases the integrity of the data, and it is very cheap to implement. | • It provides less computation for compatibility.<br>• The scalability is very low. |
| Mohan et al. [23] | Raspberry Pi network | • The implementation cost is low.<br>• The model solution is more feasible and reliable. | • To handle a large amount of data, more storage is needed in this network.<br>• It does not provide a proper balance between connectivity and storage requirements. |
| Elisa et al. [24] | peer-to-peer | • It improves computation rationality and identity anonymity.<br>• It is easy to set up the client data and does not need special knowledge. | • The data confidentiality is very poor.<br>• The file resources do not centrally organize, so it takes more time. |
| Dewangan et al. [25] | EdDSA | • It improves the immutability and transparency to enhance the privacy system highly.<br>• It reduces the computational complexity of the decentralization algorithms. | • While using enormous data, the private key is sometimes leaked.<br>• It does not support merging complex data. |

## 3. Privacy Preservation of Supply Chain Management Data: New Meta-Heuristic with Ethereum Blockchain

### *3.1. Data Used for Privacy Preservation*

Client data are protected to establish a privacy preservation system. SCM gathers input data from a dataset called DataCo Smart Supply Chain for Big Data Analysis. It is available at https://www.kaggle.com/shivkp/customer-behaviour (accessed on 10 January 2023). The firm DataCo Global uses these data related to supply networks for their analysis. This dataset comprises registered operations that allow using R software areas and machine learning techniques, such as commercial distribution, sales, production, and supply. It also incorporates the relationship between organized and unstructured data. The gathered data are separated into three subsets: dataset 1, which comprises manufacturer data, dataset 2 counts transmitted data to managers who are present in different nations, and dataset 3 contains data transferred to each firm in each country.

### *3.2. SCM Privacy Preservation Framework*

SCM is one of the best-known commercial organizations due to its capacity for improving the efficiency of the firm. Supply chains and Ethereum blockchains are coupled to improve the security of supply chain networks. Many methods for ensuring the data privacy preservation and security of the Ethereum network with blockchains were introduced, including a VMI mode system, homomorphic encryption, fully observable supply chain management, PBFT algorithm, and consensus-based collaborative management mechanism. These methods help with cost-effective reconciliation, minimizing dispute settlement, increasing security, reducing dwell time, enhancing transparency, decentralizing data distribution, lowering complexity, increasing throughput, and addressing issues with information sharing and data tracking. The architectural representation of the Ethereum blockchain technology developed for privacy preservation is given in Figure 1.

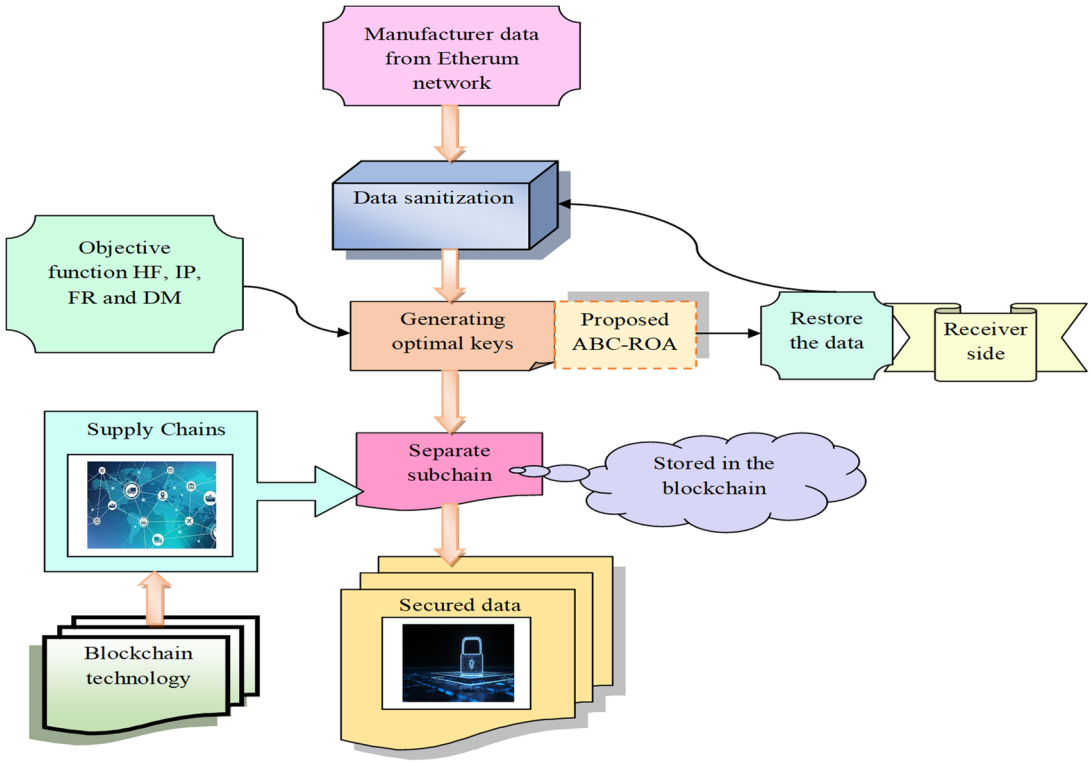



**Figure 1.** Architectural representation of the privacy preservation platform developed in the Ethereum blockchain.

Owing to these issues, higher credibility and dependability of data sharing and keeping security in the Ethereum blockchain technology, a data privacy preservation model using blockchain has been established. Initially, the desired data are gathered from publicly available online databases. Data restoration and data sanitization are the two stages of secured data transfer in the developed model. The initial manufacturer data are cleaned during the sanitization procedure to guarantee the security of the data during transmission. Here, the originally collected data undergo sanitization. Then, the optimal key is generated with the ABC-ROA algorithm, which follows multi objective functions, such as HF, IP, FR, and DM. Then, the sanitized data progress to the restoration process, where they are stored. The restored data are transferred to the supply chain framework, where the blockchain is adapted to preserve the data during transmission. These overall processes are done in an Ethereum environment using blockchain technology. This technique sends the sanitized data over a single blockchain to prevent unauthorized access and delay in data transmission. The performance of this blockchain-based privacy preservation model is verified through various heuristic algorithms regarding key sensitivity, cost function, Euclidean distance, and harmonic mean.

## 4. Supply Chain Network Creation and Privacy Preservation Steps Handled

### *4.1. Supply Chain Networks*

The supply chain network is divided into key levels: level 1 indicates the raw materials, level 2 denotes the supplier, level 3 indicates the manufacturer, level 4 denotes the manager, level 5 indicates the delivery, and level 6 denotes the customer. The network is then incorporated into the blockchain to raise the level of information-sharing security. Here, the manufacturer's data undergo data sanitization to conceal them by employing the "chosen optimal key" created by the ABC-ROA algorithm. Then, in the restoration phase, these cleaned data are restored using the same optimum key through the authenticated users on the receiver end. These actions protect the confidentiality of the data shared in supply chain networks. The proposed data privacy preservation model divides the supply chain network into four main levels: level 1 designates the product's manufacturer, level 2 the management, level 3 the product delivery, and level 4 the vendor. The phenomena that are a part of the supply chain network are further characterized. Manufacturers in various industries create their databases with information on the price, weight, product manager, delivery method, and suppliers of their manufactured goods. The manufacturer's data are concealed or cleaned up using an ideal key. Then, the managers upload their data into the blockchain, dividing it into various subchains to increase security.

Additionally, the data are sent appropriately in their supply chain subchains when transferred from the first management level to the last delivery level. The data restoration then happens at the vendor level. By restoring the actual data, the vendor utilizes the best key to access the private information. Five manufacturers with their required production goods are part of the supply chain network. Pretend these companies produce leather, cosmetics, electronics, paper, and wooden goods. They create a database based on the product information, which contains information such as item price, description, weight (kg), amount, brand, controlled by vendor manager, and shipment mode (delivery). The price, item quality, brand, and item description are understood to be the sensitive fields in this situation, and they must be sanitized using the created EF-HHO algorithm.

The manufacturer's subchains are shown in Equation (1).

$$JM_1^{(1)}, JM_1^{(2)}, JM_1^{(3)}, JM_1^{(4)}, JM_1^{(5)} \tag{1}$$

The terms $JM_1^{(1)}, JM_1^{(2)}, JM_1^{(3)}, JM_1^{(4)}$ and $JM_1^{(5)}$ are the sub-chains and are calculated using Equation (2).

$$\begin{matrix} JM_1^{(1(n));n=1,2}, JM_1^{(2(n));n=1,2}, JM_1^{(3(n));n=1,2}, \\ JM_1^{(4(n));n=1,2,3}, JM_1^{(5(n));n=1,2,3} \end{matrix} \tag{2}$$

The single blockchain $JM_1$ is created by combining these subchains.

These data are then transferred to the manager level. The managers and their corresponding subchains are shown in Equations (3) and (4).

$$FR_1, FR_2, FR_3, FR_4, FR_5 \tag{3}$$

$$JM_2^{(1)}, JM_2^{(2)}, JM_2^{(3)}, JM_2^{(4)}, JM_2^{(5)} \tag{4}$$

The subchains of the manager are given in Equation (5).

$$\begin{matrix} JM_2^{(1(n));n=1,2}, JM_2^{(2(n));n=1,2}, JM_2^{(3(n));n=1,2}, \\ JM_2^{(4(n));n=1,2,3}, JM_2^{(5(n));n=1,2,3} \end{matrix} \tag{5}$$

The vendors and their corresponding subchains are measured by Equation (6) and Equation (7), respectively.

The single blockchain is indicated by $JM_2$.

$$WT_1, WT_2, WT_3, WT_4, WT_5 \tag{6}$$

$$JM_2^{(1)}, JM_2^{(2)}, JM_2^{(3)}, JM_2^{(4)}, JM_2^{(5)} \tag{7}$$

Then, the subchains of the manager are denoted in below Equation (8).

$$\begin{matrix} JM_3^{(1(n));n=1,2}, JM_3^{(2(n));n=1,2}, JM_3^{(3(n));n=1,2}, \\ JM_3^{(4(n));n=1,2,3}, JM_3^{(5(n));n=1,2,3} \end{matrix} \tag{8}$$

Finally, the delivery level is represented in Equation (9).

$$DE_1, DE_2, DE_3, DE_4, DE_5 \tag{9}$$

Here, the term $DE_1$ is a single delivery level. The term $WT_1$ is vendor value in the supply chain.

The representation of the supply chain network with blockchain is given in Figure 2.

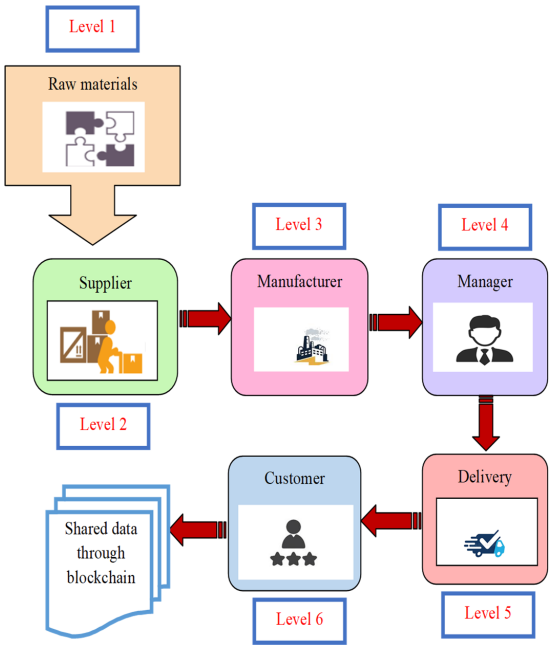



**Figure 2.** Supply chain network with blockchain.

*4.2. Data Sanitization and Data Restoration*

The sanitization and restoration techniques used in this blockchain-based privacy preservation system are described below.

Sanitization [26]: The data sanitization phase over the recommended data privacy preservation system in the Ethereum network is described in this section. The collected data from the real databases undergo data sanitization. In most cases, the sanitization process occurs at the manufacturer level, and blockchain sanitization also happens. The sensitive data in the blockchains' subblocks are cleaned after being separated into subblocks. It is not necessary to sanitize the non-sensitive data in the subblocks. The term $JM_1^*$ is a blockchain-sanitized database calculated by Equation (10).

$$JM_1^* = (C_2 \oplus JM_1) + 1 \tag{10}$$

The term $JM_1$ is actual data, and the binarized sanitized data is $JM_1^*$. The term $U_{Y_1^{(1)} \times X}$ is a sensitive field, and the corresponding subchain is represented by $JM_1^{(4(n));n=1,2,3,4}$. The data columns are to be sanitized in the blockchain $JM_1^{(1)}$. The sensitive field is given in the blockchain matrix $JM_1^{(4(n));n=1}$. The blockchain matrix is given in Equation (11).

$$JM_1^{(4(n));n=1} = \begin{bmatrix} M1 & M3 \\ F1 & F3 \\ V1 & V3 \\ KF1 & KF3 \\ Q1 & Q3 \\ D1 & D3 \\ U1 & U3 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 4 & 3 \\ 2 & 2 \\ 3 & 5 \\ 5 & 4 \\ 4 & 1 \\ 2 & 3 \end{bmatrix} \tag{11}$$

The term $U_{Y_1^{(1)} \times X}$ is a sensitive matrix. It is from the blockchain matrix $JM_1^{(4(n));n=1}$ and is given in Equation (12).

$$U_{Y_1^{(1)} \times X} = \begin{bmatrix} KF1 & KF8 \\ Q1 & Q8 \\ D1 & D8 \\ U1 & U8 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 5 & 4 \\ 4 & 1 \\ 2 & 3 \end{bmatrix} \tag{12}$$

Here, the result of the sanitized matrix in the blockchain matrix based on the rule is given. The sensitive data is present in the binarized data $C_2$. The subblock is indicated by $JM_1^{(4(n));n=1}$, and the identity matrix is denoted by $YPS$. In addition, the term $JM_1^{(4(n));n=1}$ and $YPS$ are added to the sanitized data $JM_1^{(*4(n));n=1}$.

Restoration: The restoration process is very efficient for a privacy-preserving system. When employing the ABC-ROA algorithm on the receiver side, the receiver can access the original data using the generated optimal key. The first step is to binarize the blockchain. The key generation methods, the data $C_2$, and the sanitized blockchain $JM_1^*$ are binarized. The sanitized data's binarized form is further altered through the unit phase. To extract the restored data $JM_3$, the binarized key matrix $JM_1^*$ and binarized $YPS$ are subtracted. The data restoration process is measured using Equation (13).

$$JM_3^{(n(n))} = \left( JM_{(n)}^{*(1(n))} - 1 \right) \oplus A_2 \tag{13}$$

Then, the newly designed ABC-ROA algorithm is used to recreate the sanitized key $A_2$. The restored data are denoted by $JM_3$,and hence the lossless function can be performed. The data sanitization and restoration process in the Ethereum blockchain network for the data privacy preservation system is depicted in Figure 3.

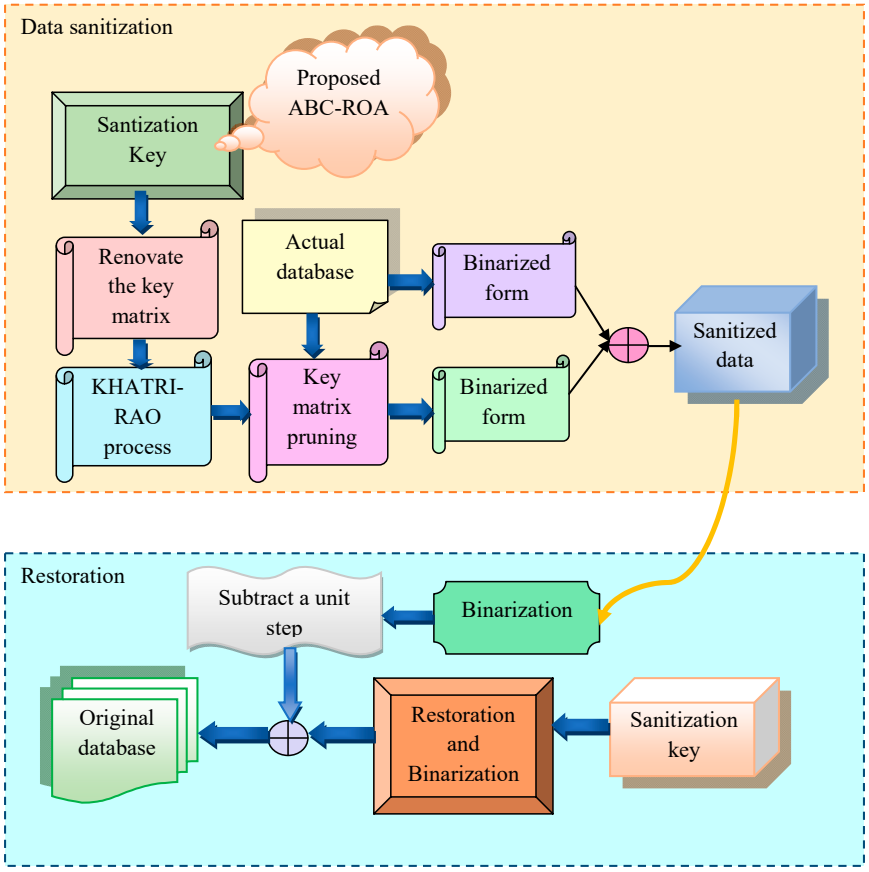



**Figure 3.** Data sanitization and data restoration process in the blockchain-based privacy preservation system.

## 5. Adaptive Border Collie Rain Optimization Algorithm with Ethereum Blockchain for SCM Data Privacy Preservation

### *5.1. Optimal Key Generation*

In the above section, the selected sensitive fields are chosen based on the sanitization process. The ABC-ROA optimization algorithm chooses the optimal key in sensitive fields. The term $A_n$ is an optimal key value. In the key generation phase, the Khatri–Rao product is adapted to transfer the solution. The optimal key is recreated with the matrix dimension and calculated using Equation (14).

$$JM_1^{(*4(n));n=1} = \begin{bmatrix} 5 & 1 \\ 7 & 2 \\ 7 & 3 \\ 6 & 1 \\ 8 & 2 \\ 1 & 4 \\ 2 & 6 \end{bmatrix}, A_1 = 5 \begin{bmatrix} 1 & 1 \\ 4 & 3 \\ 2 & 2 \\ 3 & 5 \\ 5 & 4 \\ 4 & 1 \\ 2 & 3 \end{bmatrix}_{[\sqrt{M_{JM}^n} \times JM_{\max}]} \tag{14}$$

Here, the term $JM_1^*$ is sanitized data. The rule-hiding technique is used in the sanitized database. The ABC-ROA algorithm is adapted to optimize the key values between $A_1$ and $A_n$, respectively. The length of the key value is the same as that of the number of sensitive fields. The key length is determined by using $\sqrt{M_{JM}^n}$. Finally, the optimal key is formed by using the ABC-ROA algorithm.

*5.2. Objective Function*

The ABC-ROA-based privacy preservation system chooses the optimal key in the restoration and sanitization process. These methods are used to solve constraints such $H_1, H_2, H_3 \& H_4$. The objective function of the model is calculated by Equation (15).

$$GG = \underset{\{A_n\}}{\operatorname{argmin}}(H_1 + H_2 + H_3 + H_4) \tag{15}$$

The selected optimal key is denoted by $A_n$. The term $IG$ is normalized data and measured using Equation (16).

$$H_1 = \frac{h_1}{\max(h)\forall iters} \tag{16}$$

$$= \frac{no.of sensitive JM^*}{no.of sensitive JM} \tag{17}$$

The number of sensitive rules is given in Equation (18). The ratio of sensitive rules to the number of sensitive rules is presented below in Equation (19).

$$h_1 = \left|J^1\right| \cap ST \tag{18}$$

$$H_1 = \frac{\left|J^1\right| \cap ST}{ST} \tag{19}$$

The information preservation ratio is calculated using Equation (20).

$$H_2 = \frac{h_2}{\max(h_2)\forall iters} \tag{20}$$

$$= \frac{no.of\ non-sensitive\ wronghiddn JM^*}{no.of\ nonsensitive JM} \tag{21}$$

The information loss is measured using Equation (22).

$$h_2 = 1 - \frac{\left|J - J^1\right|}{|J|} \tag{22}$$

Here, the term $H_3$ is a false rule generation. The false rules generation is calculated by Equation (23).

$$H_3 = \frac{h_3}{\max(h_3)\forall iters} \tag{23}$$

$$= \frac{no.of\ dataoutofbounce JM^*}{total\ no.of\ record JM} \tag{24}$$

$$h_3 = \frac{\left|J - J^1\right|}{|J|} \tag{25}$$

The modified degree is measured in Equation (26).

$$H_4 = \frac{h_4}{\max(h_4)\forall iters} \tag{26}$$

$$h_4 = dist(JM, JM^*) \tag{27}$$

The optimal key is generated in the blockchain-based privacy preservation system. The optimal key selection improves the performance of the model.

### *5.3. Ethereum Blockchain Technology*

A blockchain is a decentralized ledger of data kept by network nodes, and a single entity does not control it. The blockchain data blocks are connected using cryptographic concepts. Everyone on a blockchain is responsible for their actions since the transaction data are immutable and open to the public. A blockchain-based application is transparent and attack-resistant. Ethereum is an open-source blockchain framework for decentralized applications that manage digital wealth. "Smart contracts" refers to the applications that operate on the Ethereum virtual machine (EVM). Two widely used scripting languages for creating smart contracts on Ethereum are Solidity and Vyper. The two types of accounts in Ethereum are contract accounts and externally owned accounts (EOA). Every account type contains a different 20-byte hexadecimal string-based unique address. The data are transmitted with the help of the owner's private key and thus, it controls the EOA, which has an ether balance (i.e., sending data to prompt the initiation of a smart contract). There is no code associated with an EOA. On the other hand, the corresponding code for a contract account with an ether balance is triggered by a transaction or another smart contract. A few benefits of this model's use of Ethereum blockchain technology include restricted access to the consumer's or generator's private data, practical calculation techniques that may be implemented on the smart contract, and complete decentralization, achieving transparent on-chain market clearing. The architecture representation of Ethereum blockchain technology is given in Figure 4.

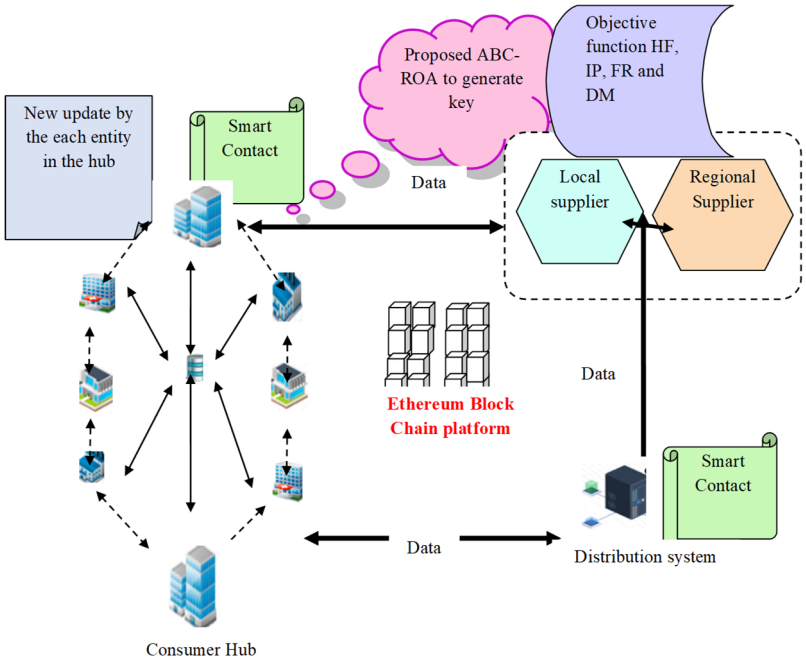



**Figure 4.** Privacy preservation framework in Ethereum blockchain technology.

### *5.4. Proposed ABC-ROA*

The ABC-ROA algorithm is designed to enhance the effectiveness of the developed data privacy preservation system to select the optimal key in the data sanitization and data restoration process in the SCM. The existing algorithms face a few challenges in privacy preservation in Ethereum blockchain technology, where the existing heuristic algorithms have a limited number of resources to store the data. Hence, they face security and scalability challenges. The existing ROA and BCO algorithms are utilized for this work. Here, the BCO algorithm is selected in the developed method to increase the performance and robustness of the model. Additionally, it reduces the errors to increase the effectiveness concerning precision, f1score, and accuracy. The BCO is solving the multi objective combinational optimization problems. However, it gains low scalability and

utility. Due to the issues in the BCO algorithm, the ABC-ROA algorithm is developed by combining the ROA. ROA is chosen in the implemented model since it can perform in parallel computing and is mostly helped for high privacy protection. It is used to improve the user experience. These advantages in both BCO and ROA make the efficient performance in the suggested blockchain-based privacy preservation system by overcoming these conventional issues. The ABC-ROA algorithm is used to improve the performance of the developed blockchain-based data privacy preservation system. The ABC-ROA algorithm is implemented based on the current fitness and average fitness function. The term defines the current fitness $Fit_{cr}$, and the average fitness is denoted by the term $Fit_{avg}$. If $Fit_{cr} < Fit_{avg}$, choose the random parameter $s = 2$ otherwise, select $s = 3$ as the random parameter value. However, in the conventional algorithm, the random parameter $s$ is selected randomly in the interval between $[0, 1]$. If $s == 2$ then, select the ROA algorithm otherwise, select the BCO algorithm. The developed ABC-ROA algorithm increases the fitness function.

BCO [27]: Three dogs and sheep are considered in the Border collie optimization process. In a real-world scenario, one dog can manage the herd by himself. However, three dogs are considered because the search space for certain optimization issues might be large. When the algorithm is started, a group of three dogs and some lambs are exhibited here. The dogs are in charge of returning the sheep to the farm after they have gone out in different directions for grazing.

Random variables are used to initialize the positions of sheep and dogs. According to their positions, the dogs are designated lead, left, and right. From the front, the lead dog directs the herd. The person with the fitness $Fit_g$ is chosen to be the dog in front of the herd or the lead dog.

The major task of these dogs is to observe and stalk the herd. The terms $Fit_{sj}$ and $Fit_{mf}$ denotes the fitness values. The fitness of the sheep is known as $Fit_t$. The velocity of the lead dog is calculated using Equation (28).

$$W_g(u+1) = \sqrt{W_g(u)^2 + 2 \times NC_g(u) \times P_g(u)} \tag{28}$$

Then, the velocity of the left dog is measured using the given Equation (29).

$$W_{sj}(u+1) = \sqrt{W_{sj}(u)^2 + 2 \times NC_{sj}(u) \times P_{sj}(u)} \tag{29}$$

The term $NC$ is the acceleration of the dog and the term $P$ is the dog's position. The term $W$ indicates the velocity of the dog. The right dog velocity is calculated using Equation (30).

$$W_{mf}(u+1) = \sqrt{W_{mf}(u)^2 + 2 \times NC_{mf}(u) \times P_{mf}(u)} \tag{30}$$

Here, the variables $W_{sj}(u+1)$, $W_{mf}(u+1)$ and $W_g(u+1)$ is denoted by the velocity of time at $(u+1)$ for the right, left, and lead dogs. Moreover, the terms $NC_g(u)$,$NC_{sj}(u)$, and $NC_{mf}(u)$ denotes the acceleration for lead, right, and left dogs. $P_g(u)$,$P_{sj}(u)$, and $P_{mf}(u)$ describes the position of lead, right, and left dogs.

Gathering: In the sheep gathering method, the updated sheep velocity is considered. The approaches of stalking, gathering and eyeing are used in this algorithm. The sheep near the lead dog follow the lead dog's direction. The sheep that is closer to the lead dog is determined using Equation (31). Here, the term $E_h$ determines the positive shows the sheep nearer to the lead dog.

$$E_h = (Fit_g - Fit_t) - \left( \left( \frac{Fit_{mf} - Fit_{sj}}{2} \right) - Fit_t \right) \tag{31}$$

Equation (32) indicates the sheep's velocity. The term $P_g$ is the current sheep location.

$$W_{th}(u+1) = \sqrt{W_g(u+1)^2 + 2 \times NC_g(u) \times P_g(u)} \tag{32}$$

The variable $W_{th}$ is defined as the velocity of the sheep that is influenced by the lead dog.

Stalking: To keep the dogs to guide, they must stalk the sheep closer to the left and right dogs. The stalked sheep velocity is updated using Equations (33) and (34), respectively.

$$W_{sj} = \sqrt{\left(W_{sj}(u+1)\tan(s_1)\right)^2 + 2 \times NC_{sj}(u) \times P_{sj}(u)} \tag{33}$$

$$W_{mf} = \sqrt{\left(W_{mf}(u+1)\tan(s_2)\right)^2 + 2 \times NC_{mf}(u) \times P_{mf}(u)} \tag{34}$$

$$W_{tt}(u+1) = \frac{W_{mf} + W_{sj}}{2} \tag{35}$$

Consequently, the term $W_{tt}$ represents the velocities of left and right dogs. Hence, the traversing angles of $s_1$ and $s_2$ is considered randomly.

Eyeing: In this scenario, it is anticipated that the least fit dog will follow the sheep and give them a close look. The velocity of the left dog is given in Equation (36). The variable $W_{mf}$ and $NC_{mf}$ is described the velocity and acceleration of the left dog. Additionally, the term $W_{sj}$ and $NC_{sj}$ is defined as the velocity and acceleration of the right dog. Hence, the term $P_{sj}$ defines the collection of sheep that are presented in the current location. Additionally, the average time of individual can be represented as $e$.

$$W_{tf}(u+1) = \sqrt{W_{mf}(u+1)^2 - 2 \times NC_{mf}(u) \times P_{mf}(u)} \tag{36}$$

The velocity of the right dog is given in Equation (37).

$$W_{tf}(u+1) = \sqrt{W_{sj}(u+1)^2 - 2 \times NC_{sj}(u) \times P_{sj}(u)} \tag{37}$$

The updated acceleration of the sheep and dog is calculated by Equation (38).

$$NC_j(u+1) = \left(\frac{W_j(u+1) - W_j(u)}{Time_j(u)}\right) \tag{38}$$

The updated time of the sheep and dog is measured by Equation (39).

$$Time_j(u+1) = Avg\sum_{j=1}^{e} \frac{W_j(u+1) - W_j(u)}{NC_j(u+1)} \tag{39}$$

The lead dog's position is updated using Equation (40).

$$\begin{aligned} P_g(u+1) &= W_g(u+1) \times Time_g(u+1) \\ &+\tfrac{1}{2} NC_g(u+1) \times Time_g(u+1)^2 \end{aligned} \tag{40}$$

The left dog's position is updated and calculated by Equation (41).

$$\begin{aligned} P_{mf}(u+1) &= W_{mf}(u+1) \times Time_{mf}(u+1) \\ &+\tfrac{1}{2} NC_{mf}(u+1) \times Time_{mf}(u+1)^2 \end{aligned} \tag{41}$$

The position of the right dog is updated using Equation (42).

$$\begin{aligned} P_{sj}(u+1) &= W_{sj}(u+1) \times Time_{sj}(u+1) \\ &+\tfrac{1}{2} NC_{sj}(u+1) \times Time_{sj}(u+1)^2 \end{aligned} \tag{42}$$

The updated locations of the sheep are determined using Equation (43) and Equation (44), respectively.

$$P_{th}(u+1) = W_{th}(u+1) \times Time_{th}(u+1) + \frac{1}{2}NC_{th}(u+1) \times Time_{th}(u+1)^2 \quad (43)$$

$$P_{tt}(u+1) = W_{tt}(u+1) \times Time_{tt}(u+1) - \frac{1}{2}NC_{tt}(u+1) \times Time_{tt}(u+1)^2 \quad (44)$$

The eyed sheep are updated, and it is determined using below Equation (45).

$$P_{tf}(u+1) = W_{tf}(u+1) \times Time_{tf}(u+1) - \frac{1}{2}NC_{tf}(u+1) \times Time_{tf}(u+1)^2 \quad (45)$$

Then, the sheep go to the track with the help of dog guidance, which is given in Equation (46).

$$P_g(u+1) = W_g(u+1) \times Time_g(u+1) + \frac{1}{2}\frac{\left(W_g(u+1) - W_g(u)\right)}{Time_j(u)}NC_{tf}(u+1) \times Time_{tf}(u+1)^2 \quad (46)$$

The stalking, gathering and eyeing behavior over the sheep by a dog is described. By substituting the value of $NC(u+1)$ in Equations (46) and (47), the population values are attained based on the gathered sheep, left dog, stalked sheep, eyed sheep, and right dog.

ROA [28]: Raindrops fall on the ground randomly. A raindrop can serve as a metaphor for each possible solution. As raindrops fall randomly on the ground, certain places in the solution space can be chosen randomly. Each raindrop's radius is the most distinguishing characteristic. As time passes and a raindrop is joined to other droplets, its radius can decrease time. The radius of each droplet can decrease the time and also increase the connectivity of other droplets within a suitable range after the first population of replies is generated. Every droplet checks its nearest neighborhood based on its size at each cycle. Check for the end of the area that a single droplet has covered if it is still unconnected to any other droplet. Every droplet has variables while we are addressing a problem in n dimensions. Here, the term $S$ is a large drop in radius.

Then, the radius $S_1$ and $S_2$ makes a large form of the raindrop. The term $m$ defines the variables in each droplet and is calculated using Equation (47).

$$S = (S_1^m + S_2^m)^{\frac{1}{m}} \quad (47)$$

Therefore, by increasing the number of iterations, weak droplets disappear, or the droplets create strong droplets.

The initial population will decrease continuously, causing a speed of determining the correct answer.

The term $\gamma$ represents the soil characteristic given in Equation (48).

$$S = (\gamma S_1^m)^{\frac{1}{m}} \quad (48)$$

Here, the variable $s_1$ is the radius that does not move on the properties of the soil, which is depicted as $\gamma$. As a result, the droplet's radius will be used to establish the lower and upper bounds of the variable in the initial stage. Two endpoints of the variable are examined in the next stage, and so on until the last variable. The term $PDp$ is an ordering cost and is measured using Equation (49).

$$PDp = \sum_{j=1}^{M} \frac{ES_j(U)}{R_j} \quad (49)$$

The initial droplet cost would be adjusted at this point. The inventory holding cost is indicated by $IDp_s$, and is given in Equation (50).

$$IDp_s = \sum_{j=1}^{M} \frac{I_j}{2R_j} \left(R_j - T_j\right)^2 \tag{50}$$

The shortage of the cost is denoted by $TDp$ and is shown in Equation (51).

$$TDp = \sum_{j=1}^{M} \frac{M_j}{2R_j} T_j^2 \tag{51}$$

The term $UsDp$ is a transportation cost measured using Equation (52).

$$UsDp = \sum_{j=1}^{M} ES_j TIDp_j \tag{52}$$

The objective of the solution is calculated by Equation (53).

$$UpDp = (EDp + CDp + PDp + IDp_s + TDp + UsDp) \tag{53}$$

Here, the term $UpDp$ denotes the total cost. The total investment is indicated by $InV$, and it is shown in Equation (54).

$$InV = \sum_{k=1}^{M} \sum_{J_{kj=1}}^{J_{kj}} G_{MJ_{jk}} Y_{MJ_{jk}} \tag{54}$$

Here, the term $Y_{MJ_{jk}}$ is an inventory capacity level. The fixed cost is represented by $G_{MJ_{jk}}$. The term $EU$ is total time calculated by Equation (55).

$$EU = \sum_{y=1}^{y} \sum_{k=1}^{m} \sum_{j=1}^{o} \left(U_{MO} + U_{YMO}\right) ES_j \cdot Z_{YMO} \tag{55}$$

The number of raindrops is denoted by $y$ and the number of warehouses is represented by $m$.

For each droplet, this situation would be repeated. Nearby droplets in their route may interact with one another, greatly speeding up the process. A droplet's radius continuously decreased at the lowest point, greatly improving the accuracy of the re-

sponse. The pseudocode of the implemented ABC-ROA is presented in Algorithm 1.

**Algorithm 1**: Developed ABC-ROA

```
Initialize the population and acceleration value
Find the fitness solution
Calculate the velocity Using Equation (29).
  For j = 1 to Maxiter
   For k = 1 to PoP
      If (CurrentFit < avgFit)
                        Assign the value of s = 2
      Else
                        Assign the value of s = 3
      End if

        If (s == 2)
           Select the radius of the raindrop using Equation (50).
            Update the solution with the ROA algorithm using Equation (51).
      Else
           Update the solution with the BCO algorithm using Equation (38).


      Determine the best fitness of the sheep
    Update the velocity of the sheep in the BCO algorithm
      Evaluate the sheep's position
      Update the position of the sheep using Equation (32).
      End if
    End
   End
   Obtain the best position
End
```

## 6. Results and Discussion

### *6.1. Simulation Setting*

The developed ABC-ROA-based privacy preservation model over the Ethereum network by blockchain technology was implemented in the MATLAB environment. In this developed system, the chromosome length was set at five, and the population size was set at 10. The efficiency analysis was conducted over key sensitivity, cost function, Euclidean distance, known-plaintext attack (KPA), harmonic mean, known ciphertext attack (KCA), arithmetic mean, CCA, and CPA. The efficiency of the developed model has been compared through various heuristic algorithms such as Harris hawks optimizer (HHO) [28], entity framework Harris hawks optimizer (EF-HHO) [29], BCO [26], and ROA [27].

### *6.2. Effectiveness Analysis Using Euclidean Distance*

The overall analysis of the recommended ABC-ROA-based privacy preservation model over the Ethereum network with three datasets in terms of Euclidean distance is given in Figure 5. From the analysis, dataset 2 gives a very low Euclidean distance than dataset 1 and 2. While using dataset 2, the developed ABC-ROA-based privacy preservation model gives improved Euclidean distance of 36.03%, 8.62%, 2.54%, and 8.77% over HHO, EF-HHO, BCO, and ROA. In the graph analysis, the developed ABC-ROA method is utilized to show effective performance. Here, the existing EF-HHO algorithm attains second-best performance. While considering all three datasets, the Euclidean distance of the proposed method shows better performance in dataset 2. Thus, the developed ABC-ROA-based data privacy preservation model over the Ethereum network gives higher effectiveness than the other heuristic algorithms.

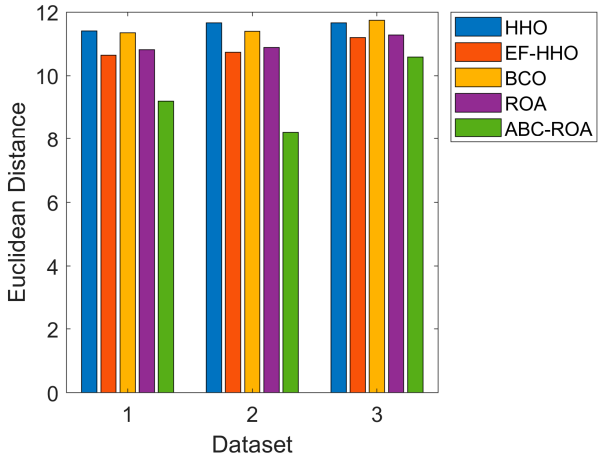



**Figure 5.** Effectiveness analysis on the offered blockchain-based privacy preservation model using Euclidean distance.

### *6.3. Performance Analysis Using the Harmonic Mean*

The harmonic mean analysis in terms of Euclidean distance, Pearson correlation, and the spearman correlation on the developed privacy preservation system over the Ethereum network among various datasets is given in Figure 6. In dataset 2, the developed ABC-ROA-based privacy preservation system over the Ethereum network provides enhanced harmonic means of25.71%, 27.77%, 35%, and 27.1% than HHO, EF-HHO, BCO, and ROA. From the given graph analysis, the Pearson correlation can be analyzed to measure the strength and direction between the two variables. Here, the Pearson correlation lies in the range of [−1 to 1]. Moreover, the negative correlation is denoted as "−1" as well as the positive correlation can be represented as "1". However, Spearman's correlation can be used to measure the association between the variables. As a result, the analysis of the designed ABC-ROA-based privacy preservation system is superior to the other heuristic approaches.

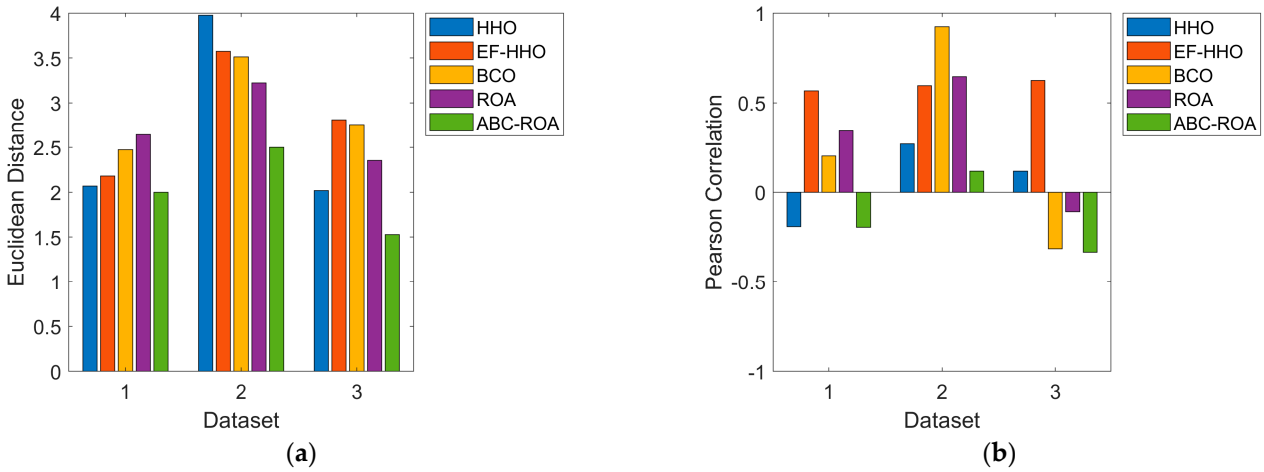
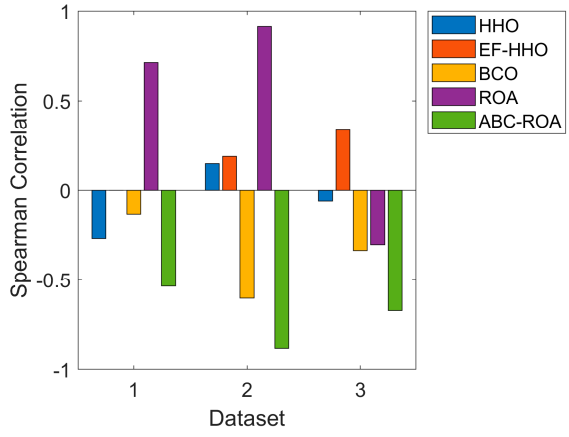



**Figure 6.** *Cont.*

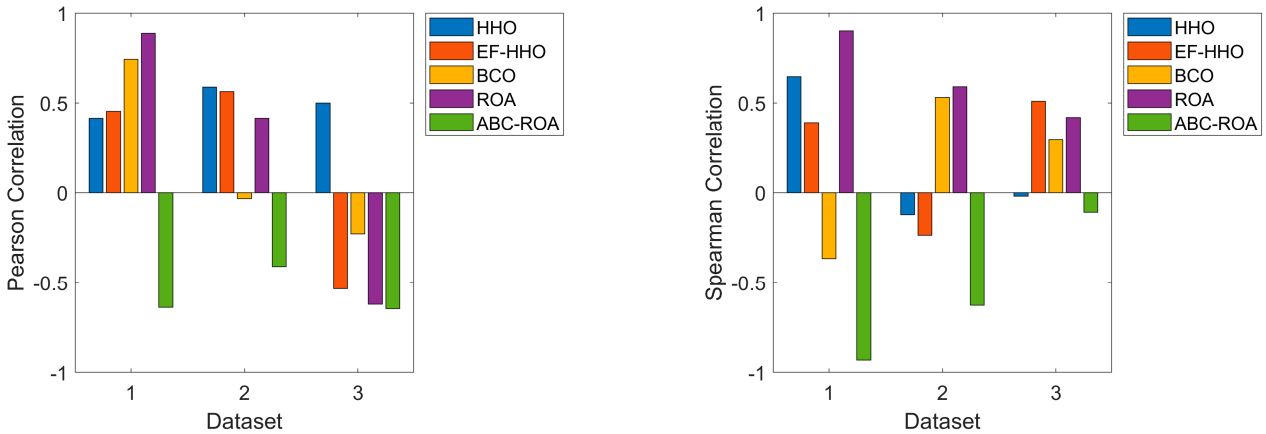



(**c**)

**Figure 6.** Effectiveness analysis of the developed blockchain-based privacy preservation system to (**a**) Euclidean distance, (**b**) Pearson correlation and (**c**) Spearman correlation.

### *6.4. Effectiveness Analysis Using the Arithmetic Mean*

Comparison of the Pearson and Spearman correlations of the designed ABC-ROA-based privacy preservation system among various heuristic algorithms is shown in Figure 7. The sum of the numerical values of each observation divided by the total number of observations is known as the arithmetic mean. From the analysis, the developed ABC-ROA-based privacy preservation achieves secured data transfer when dataset 3 shows a low value. Regarding the spearman correlation value in dataset 2, the developed ABC-ROA-based privacy preservation model has high arithmetic means of 40%, 20%, 20%, and 34.4%, better than HHO, EF-HHO, BCO, and ROA. As a result, the designed ABC-ROA-based privacy preservation system over the Ethereum network shows higher effectiveness than other heuristic algorithms.




(**a**) (**b**)

**Figure 7.** Effectiveness analysis of the designed blockchain-based privacy preservation model in terms of (**a**) Pearson correlation and (**b**) Spearman correlation.

### *6.5. Cost Function Analysis on the Proposed Model*

Comparison of the proposed ABC-ROA-based privacy preservation system convergence rate to existing meta-heuristic algorithms with various datasets is shown in Figure 8. Compared to HHO, EF-HHO, BCO, and ROA, the performance of the ABC-ROA-based privacy preservation system, the cost function is highly improved by 2.98%, 3.07%, 3.56%, and 4.12%, respectively, in dataset 3 at iteration value of 15. If the iteration increases, then the cost function of the designed ABC-ROA method gets decreased. Hence, the graph

analysis shows better performance in the recommended method. The existing EF-HHO algorithm achieves second-best performance. As a result, the developed ABC-ROA-based privacy preservation model using blockchain technology performs more effectively than other algorithms.

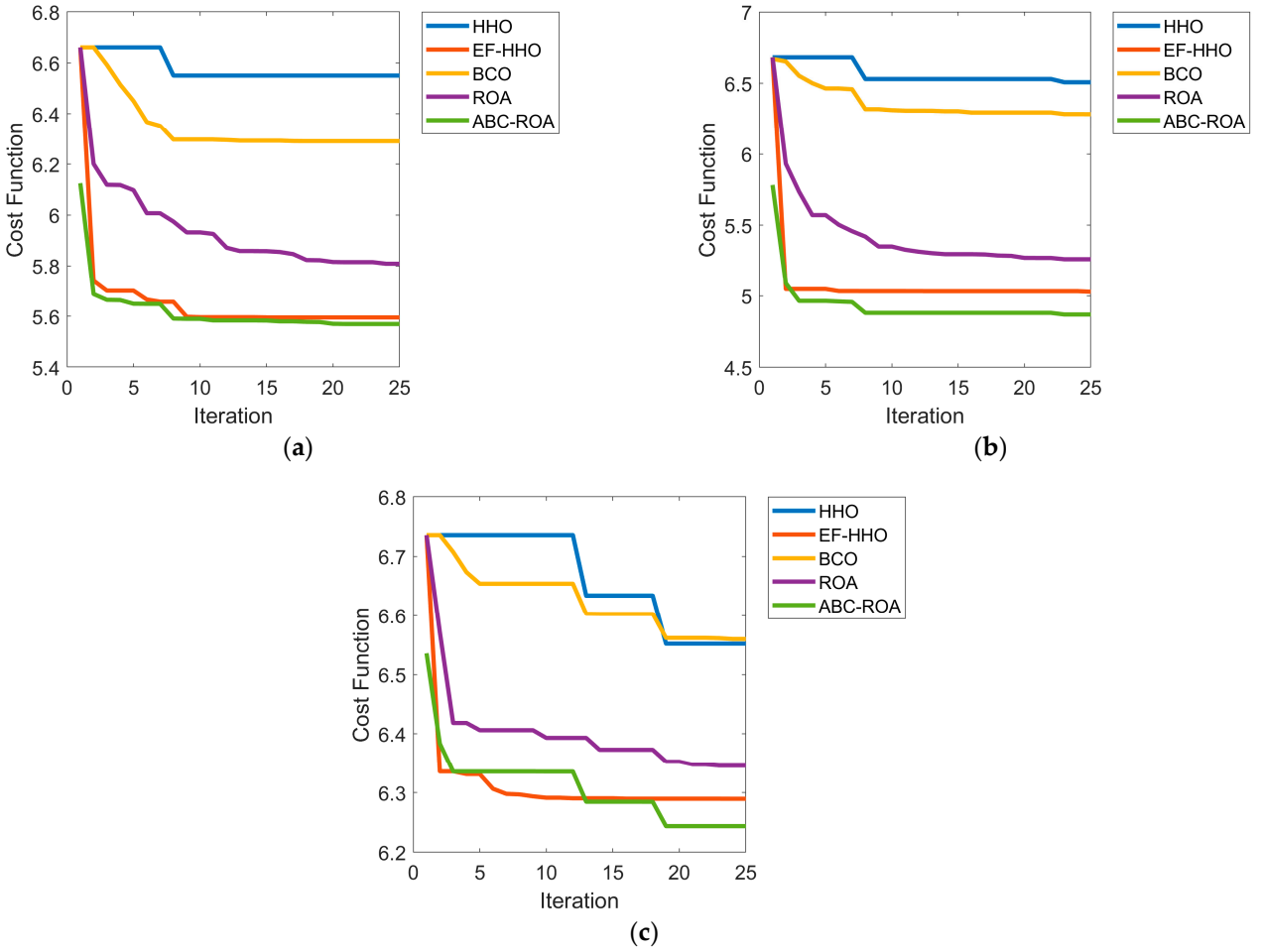



**Figure 8.** Convergence analysis on developed blockchain-based privacy preservation model in terms (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

### *6.6. Effectiveness Analysis Using Key Sensitivity*

The key sensitivity of the obtained optimum key in the ABC-ROA-based privacy preservation system for three datasets with various existing meta-heuristic algorithms at various percentage levels is shown in Figure 9. The key sensitivity of the proposed system is noticed as a lower value while increasing the percentage of the key for all the three datasets. From the analysis, the developed model shows key sensitivity improvements of 11%, 15%, 20%, and 19% to heuristic algorithms such as HHO, EF-HHO, BCO, and ROA, respectively. In the given graph analysis, it shows the equivalence performance. Based on the key sensitivity value, the ROA algorithm is not effective to secure the data in the blockchain. At learning percentage 30, the key sensitivity of the existing EF-HHO algorithm secures second-best performance. As a result, the suggested blockchain-based privacy preservation model executes more effectively than other heuristic algorithms.

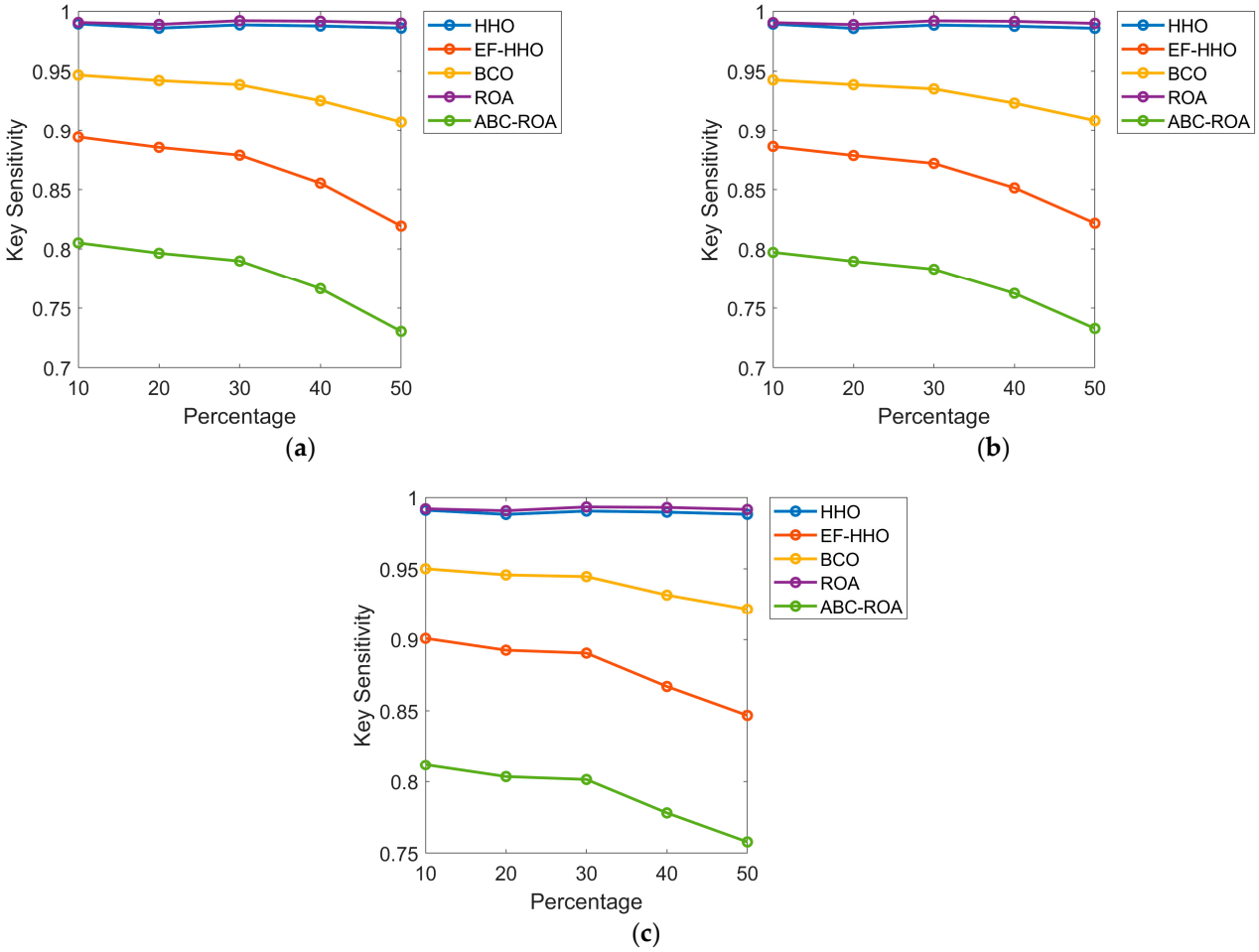



**Figure 9.** Performance analysis of the designed blockchain-based privacy preservation model concerning (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

### *6.7. Performance Analysis Using CPA and CCA*

Comparison of performance analysis of the ABC-ROA-based privacy preservation system over the existing heuristic algorithms in terms of chosen ciphertext attacks (CCA) and chosen plaintext attacks (CPA) with three datasets is given in Tables 2 and 3, respectively. In CPA, the attacker can be used to encrypt the message. Hence, the goal of the CPA attack is to reduce the security of the encryption scheme. Here, symmetric and asymmetric cryptography can be used. However, the CPA is often feasible in the diverse applications. Since the CPA is essential for public key cryptography where the encryption key is public and so attackers can encrypt any plaintext they choose. Moreover, the CCA can able to decrypt the ciphertext message. Here, the CCA can be widely used in cryptanalysis to collect information by obtaining the decryptions of the chosen ciphertext, since it needs to recover the hidden secret key which is used for the decryption. The proposed model has more secure shared data in the transmission while analyzing the results. The CCA value of the developed system is guaranteed with a lower value on raising the proportion of key variations for all three datasets. From the dataset 2 analysis of CPA, the ABC-ROA-based privacy preservation model has high performance of 7.58%, 5.93%, 4.15%, and 7.64% than HHO, EF-HHO, BCO, and ROA for the key variations of 50. The proposed blockchain-based privacy preservation model is more effective than other heuristic algorithms.

**Table 2.** Effectiveness analysis using CCA with three datasets for the developed blockchain-based data privacy preservation system over Ethereum network.

| Key Variations in the Percentage | HHO [29] | EF-HHO [30] | BCO [27] | ROA [28] | ABC-ROA |
|---|---|---|---|---|---|
| | | | Dataset 1 | | |
| 10 | 99.911 | 91.762 | 95.836 | 99.319 | 87.762 |
| 20 | 99.877 | 93.113 | 96.495 | 99.396 | 89.113 |
| 30 | 99.845 | 94.312 | 97.079 | 99.673 | 90.312 |
| 40 | 99.873 | 95.739 | 97.806 | 99.787 | 91.739 |
| 50 | 99.927 | 96.462 | 98.194 | 99.861 | 92.462 |
| | | | Dataset 2 | | |
| 10 | 99.909 | 91.626 | 95.767 | 99.31 | 87.626 |
| 20 | 99.876 | 92.894 | 96.385 | 99.389 | 88.894 |
| 30 | 99.843 | 94.071 | 96.957 | 99.669 | 90.071 |
| 40 | 99.871 | 95.452 | 97.661 | 99.784 | 91.452 |
| 50 | 99.926 | 96.283 | 98.105 | 99.859 | 92.283 |
| | | | Dataset 3 | | |
| 10 | 99.926 | 92.981 | 96.454 | 99.429 | 88.981 |
| 20 | 99.899 | 93.969 | 96.934 | 99.494 | 89.969 |
| 30 | 99.872 | 94.909 | 97.391 | 99.729 | 90.909 |
| 40 | 99.895 | 96.057 | 97.976 | 99.823 | 92.057 |
| 50 | 99.94 | 96.858 | 98.399 | 99.884 | 92.858 |

**Table 3.** Effectiveness analysis using CPA with three datasets for the developed blockchain-based data privacy preservation system over Ethereum network.

| Key Variations in the Percentage | HHO [29] | EF-HHO [30] | BCO [27] | ROA [28] | ABC-ROA |
|---|---|---|---|---|---|
| | | | Dataset 1 | | |
| 10 | 58.784 | 52.465 | 55.624 | 58.236 | 43.465 |
| 20 | 62.388 | 59.351 | 60.87 | 61.866 | 50.351 |
| 30 | 65.623 | 63.651 | 64.637 | 65.13 | 54.651 |
| 40 | 68.534 | 65.454 | 66.994 | 68.075 | 56.454 |
| 50 | 71.114 | 65.723 | 68.418 | 70.684 | 56.723 |
| | | | Dataset 2 | | |
| 10 | 57.875 | 49.222 | 53.548 | 57.313 | 40.222 |
| 20 | 61.469 | 55.313 | 58.391 | 60.935 | 46.313 |
| 30 | 64.722 | 60.534 | 62.628 | 64.219 | 51.534 |
| 40 | 67.695 | 63.39 | 65.542 | 67.223 | 54.39 |
| 50 | 70.332 | 64.698 | 67.515 | 69.891 | 55.698 |
| | | | Dataset 3 | | |
| 10 | 68.646 | 61.093 | 64.87 | 68.191 | 52.093 |
| 20 | 71.919 | 66.26 | 69.089 | 71.501 | 57.26 |
| 30 | 74.772 | 70.154 | 72.463 | 74.389 | 61.154 |
| 40 | 77.269 | 72.702 | 74.986 | 76.918 | 63.702 |
| 50 | 79.448 | 74.553 | 77 | 79.127 | 65.553 |

### *6.8. Statistical Analysis of the Designed Method*

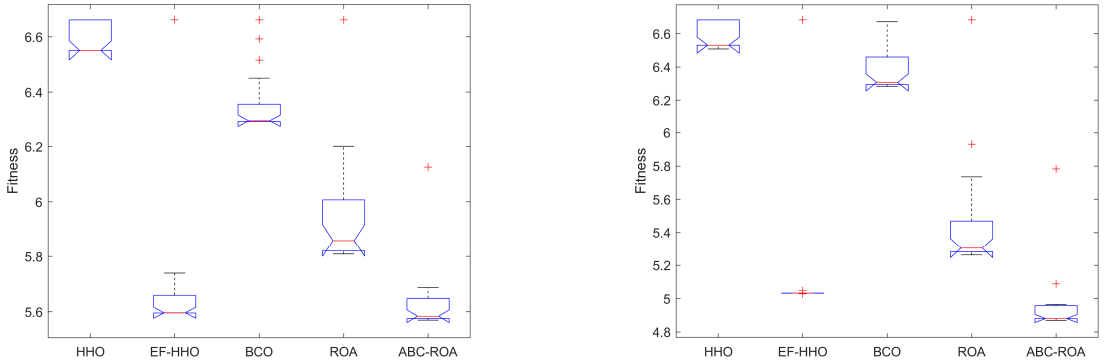
The statistical analysis of the designed blockchain-based data privacy preservation system over the Ethereum network is shown in Table 4. The designed ABC-ROA method attains 14.9%, 0.7%, 11.4%, and 4.1% better performance than HHO, EF-HHO, BCO, and ROA regarding dataset 1. Throughout the analysis, the experimental outcome has attained superior performance when compared to other traditional approaches.

**Table 4.** Statistical analysis on developed data privacy preservation model over the Ethereum network.

| Terms | HHO [29] | EF-HHO [30] | BCO [27] | ROA [28] | ABC-ROA |
|---|---|---|---|---|---|
| Dataset 1 | | | | | |
| Best | 6.5506 | 5.5954 | 6.2903 | 5.8088 | 5.5696 |
| Worst | 6.6609 | 6.6609 | 6.6609 | 6.6609 | 6.125 |
| Mean | 6.5815 | 5.6644 | 6.3546 | 5.9459 | 5.6203 |
| Median | 6.5506 | 5.5963 | 6.2927 | 5.8587 | 5.5836 |
| Standard Deviation | 0.050579 | 0.21239 | 0.12052 | 0.18825 | 0.11126 |
| Dataset 2 | | | | | |
| Best | 6.5078 | 5.0281 | 6.2831 | 5.2618 | 4.8695 |
| Worst | 6.6822 | 6.6822 | 6.6716 | 6.6822 | 5.7822 |
| Mean | 6.5701 | 5.1008 | 6.3662 | 5.4352 | 4.9401 |
| Median | 6.5303 | 5.0323 | 6.3072 | 5.3044 | 4.8807 |
| Standard deviation | 0.071683 | 0.32951 | 0.11869 | 0.3084 | 0.18276 |
| Dataset 3 | | | | | |
| Best | 6.552 | 6.2897 | 6.5597 | 6.3459 | 6.2438 |
| Worst | 6.7356 | 6.7356 | 6.7356 | 6.7356 | 6.5356 |
| Mean | 6.6597 | 6.3163 | 6.625 | 6.4021 | 6.3077 |
| Median | 6.6337 | 6.2905 | 6.6029 | 6.3933 | 6.2847 |
| Standard deviation | 0.080236 | 0.088813 | 0.054733 | 0.082943 | 0.063698 |

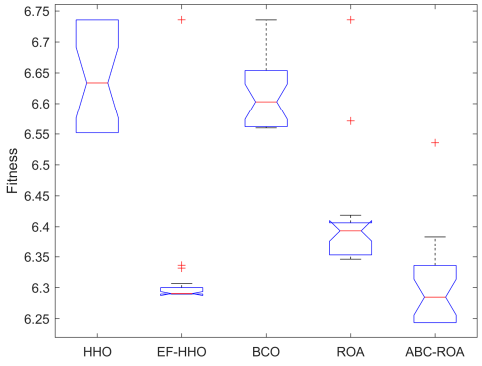
### *6.9. ANOVA Test for the Developed Data Privacy Preservation Model over the Ethereum Network*

The validation of the ANOVA test for the designed ABC-ROA method regarding fitness function is shown in Figure 10. Thus, the experimental result of the developed method attains superior performance compared to other traditional approaches.




(**a**) (**b**)

**Figure 10.** *Cont.*




(**c**)

**Figure 10.** ANOVA of the designed method for privacy preservation over the Ethereum network regarding fitness function (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

### *6.10. Validation of Control for Parameters of Different Algorithms Using the Designed Method*

The validation of control for parameters of different existing algorithms regarding Euclidean distance and Pearson and Spearman correlations is shown in Figure 11. Here, the evaluation of the parameter for the proposed ABC-ROA method is taken as ird = 0.06. Throughout the analysis, the developed method achieves enhanced performance compared to the other existing methods.

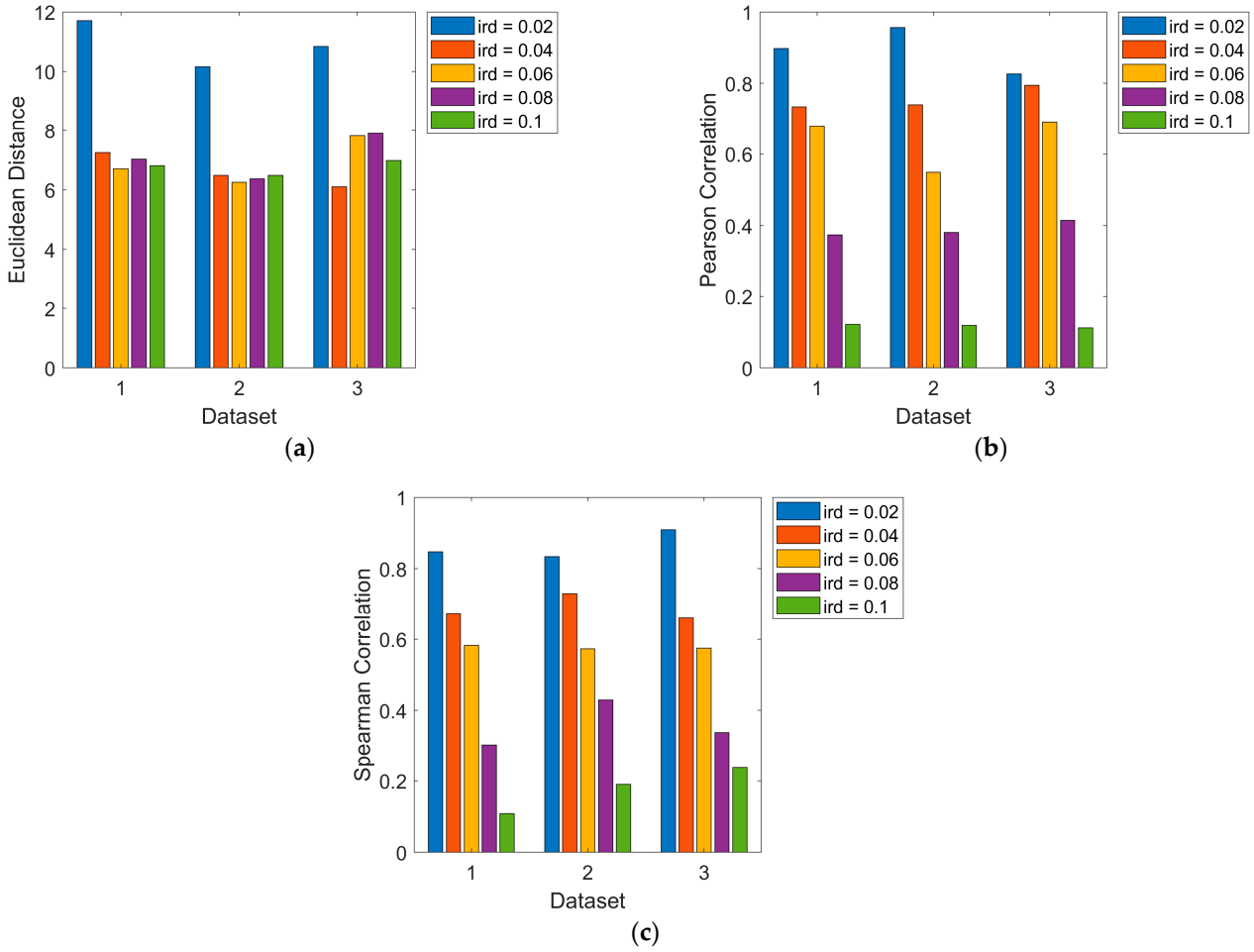



**Figure 11.** Analysis of controlling the parameters of the designed method using (**a**) Euclidean distance, (**b**) Pearson correlation, and (**c**) Spearman correlation.

## 7. Security Analysis

The developed ABC-ROA-based privacy preservation system model is evaluated with various attacks such as KCA, KPA, adaptive chosen-plaintext analysis (ACPA), and Ciphertext-Only Analysis (COA) assessed based on three datasets by comparing with recently used algorithms, as shown in Figures 12–15, respectively. Correlating one original datum with all original data and one sanitized datum with all sanitized data defines KPA analysis. KCA analysis is described as correlating each sanitized data with its data restored data. The ACPA attack is similar to the CPA attack. It selects the plaintext and ciphertext that are learned from past encryptions. In a COA attack, it uses known data collection. In the ABC-ROA-based privacy preservation system, the ACPA, COA, KPA, and KCA analysis shows the lowest value and indicates the minimum error. While analyzing the evaluation of different attacks for the designed ABC-ROA method, it is revealed that the designed ABC-ROA based privacy preservation over the Ethereum network attains effective performance.

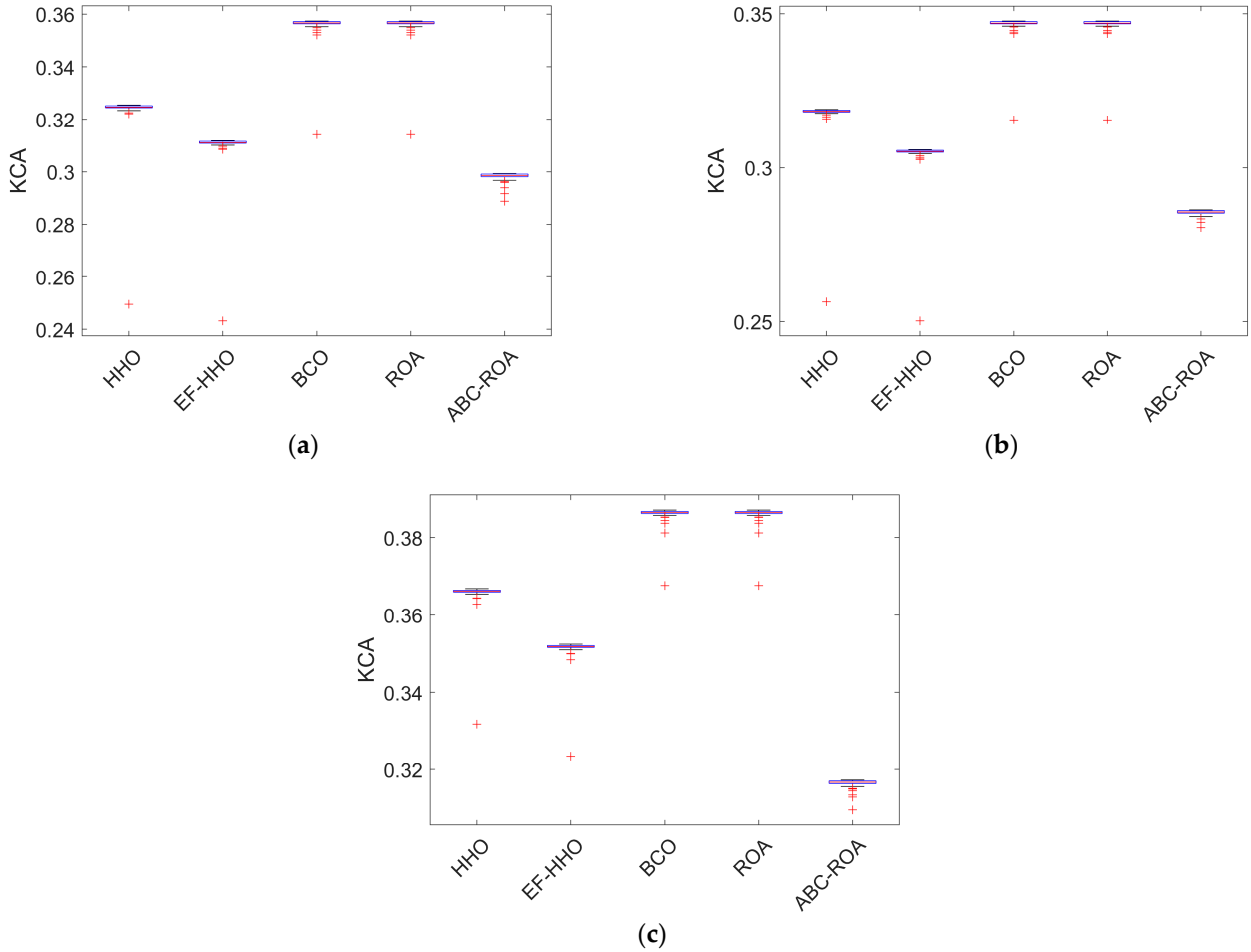



**Figure 12.** Effectiveness analysis of the implemented ABC-ROA based privacy preservation model using KCA in terms of (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

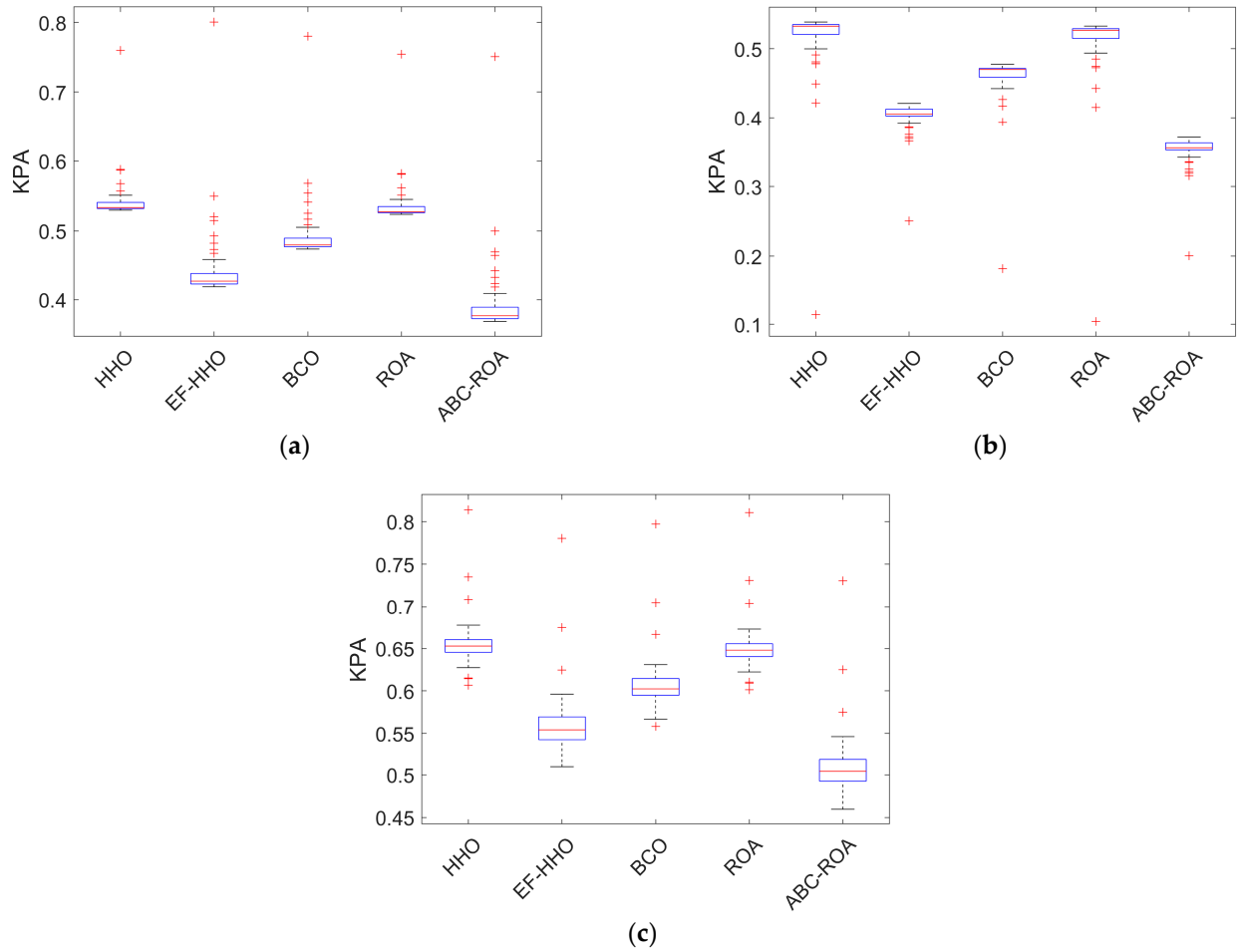



**Figure 13.** Performance analysis of the developed ABC-ROA based privacy preservation model using KPA regarding (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

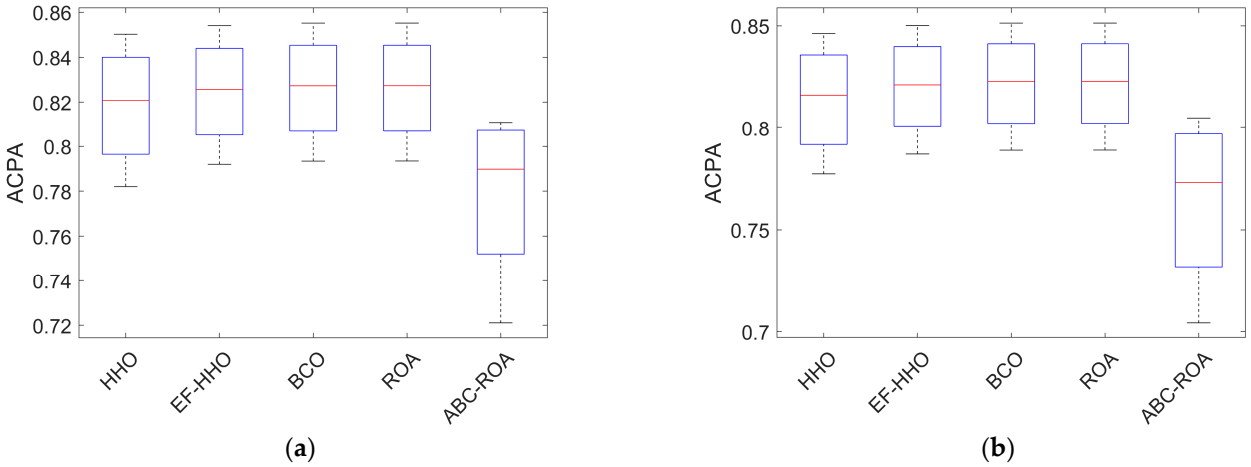
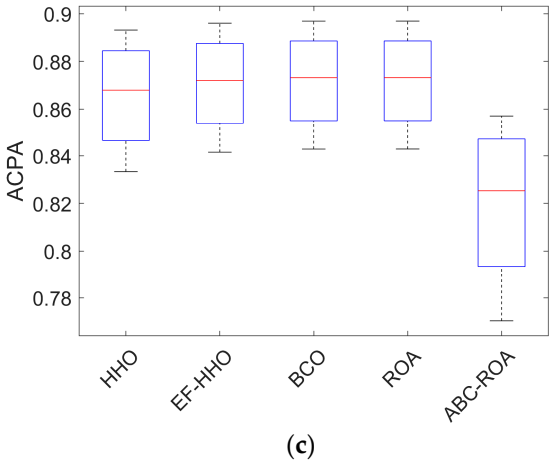



**Figure 14.** *Cont.*




(**c**)

**Figure 14.** Performance analysis of the developed ABC-ROA based privacy preservation model using ACPA regarding (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

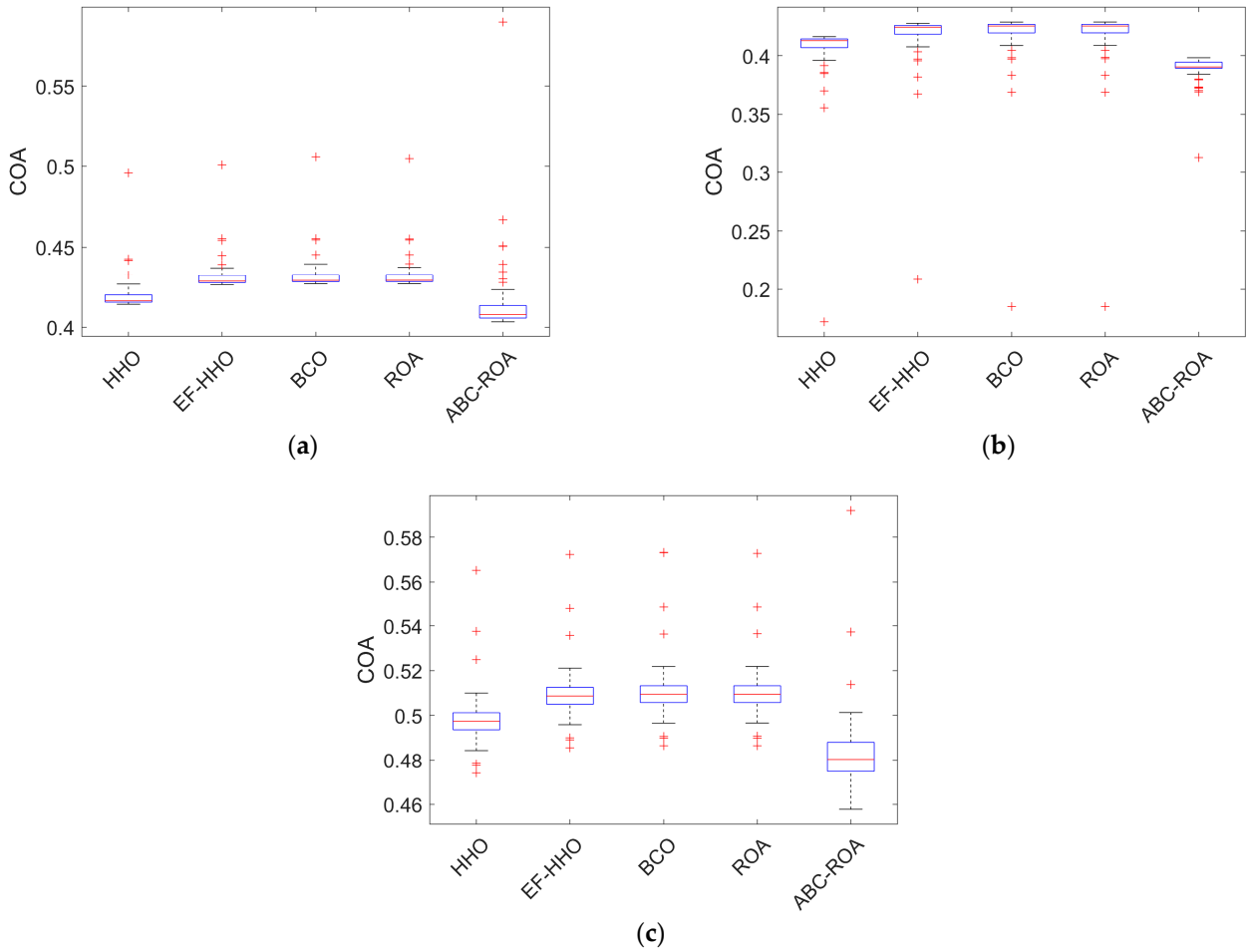



**Figure 15.** Performance analysis of the developed ABC-ROA based privacy preservation model using COA regarding (**a**) dataset 1, (**b**) dataset 2, and (**c**) dataset 3.

## 8. Conclusions

A new blockchain-based privacy preservation model over the Ethereum network was developed for preserving data privacy using blockchain technology. The data were collected from standard databases. Initially, the data were sanitized, and an optimal key developed using the ABC-ROA algorithm. The optimal key generation followed

the objective functions HF rate, IP rate, FR, and DM. The sanitized data progressed to the data restoration process, which restored the data in the database. These data were formed as subchains, known as the supply chain framework. The developed blockchain framework gave better privacy for the data over the supply chain network with the help of the generated optimal key. The effectiveness of the proposed blockchain-based privacy preservation model was compared with the existing privacy preservation models. The proposed ABC-ROA-based privacy preservation model performed 20.2% better than HHO, 17.4% better than EF-HHO, 13.7% better than BCO, and 20.7% better than ROA while considering dataset 2 with the key variation of 50. Therefore, compared to other privacy preservation approaches, the developed ABC-ROA-based privacy preservation model performs better for all key variations than other heuristic algorithms. One of the most important challenges in the existing privacy preservation model over the Ethereum network is scalability. Due to the scalability issues, it cannot provide the optimal solution, and also it generates issues such as inefficiency and limited block size. In this research, the developed ABC-ROA method was utilized to solve these issues. The estimation of convergence and optimization of deep-structure architectures were utilized to resolve the scalability issues. Moreover, implementing standard machine learning and deep learning approaches provides the ability to solve these issues.

**Author Contributions:** Conceptualization, Y.V.R.S.V.; Methodology, Y.V.R.S.V.; Data curation, Y.V.R.S.V.; Writing—Original draft preparation, Y.V.R.S.V.; Visualization, K.J.; Investigation, K.J.; Validation, Y.V.R.S.V.; Reviewing and Editing, K.J. All authors have read and agreed to the published version of the manuscript.
**Funding:** This research did not receive any specific funding.

**Data Availability Statement:** The data underlying this article are available in DataCo Smart Supply Chain for Big Data Analysis database, at https://www.kaggle.com/shivkp/customer-behaviour (accessed on 10 January 2023).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Weng, J.; Weng, J.; Zhang, J.; Li, M.; Zhang, Y.; Luo, W. DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2438–2455. [CrossRef]
2. Tahir, S.; Tahir, H.; Sajjad, A.; Rajarajan, M.; Khan, F. Privacy-preserving COVID-19 contact tracing using blockchain. *J. Commun. Netw.* **2021**, *23*, 360–373. [CrossRef]
3. Huang, C.; Zhao, Y.; Chen, H.; Wang, X.; Zhang, Q.; Chen, Y.; Wang, H.; Lam, K.-Y. ZkRep: A Privacy-Preserving Scheme for Reputation-Based Blockchain System. *IEEE Internet Things J.* **2021**, *9*, 4330–4342. [CrossRef]
4. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1917–1927. [CrossRef] [PubMed]
5. Yang, Y.; Wu, J.; Long, C.; Liang, W.; Lin, Y.-B. Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 9259–9267. [CrossRef]
6. Du, R.; Ma, C.; Li, M. Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains. *Tsinghua Sci. Technol.* **2023**, *28*, 13–26. [CrossRef]
7. Yang, Q.; Wang, H. Privacy-Preserving Transactive Energy Management for IoT-Aided Smart Homes via Blockchain. *IEEE Internet Things J.* **2021**, *8*, 11463–11475. [CrossRef]
8. Tran, Q.N.; Turnbull, B.P.; Wu, H.-T.; de Silva, A.J.S.; Kormusheva, K.; Hu, J. A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture. *IEEE Open J. Comput. Soc.* **2021**, *2*, 72–84. [CrossRef]
9. Yang, Y.; Wei, L.; Wu, J.; Long, C.; Li, B. A Blockchain-Based Multidomain Authentication Scheme for Conditional Privacy Preserving in Vehicular Ad-Hoc Network. *IEEE Internet Things J.* **2021**, *9*, 8078–8090. [CrossRef]
10. Baza, M.; Sherif, A.; Mahmoud, M.M.E.A.; Bakiras, S.; Alasmary, W.; Abdallah, M.; Lin, X. Privacy-Preserving Blockchain-Based Energy Trading Schemes for Electric Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9369–9384. [CrossRef]
11. Zhang, X.; Jiang, S.; Liu, Y.; Jiang, T.; Zhou, Y. Privacy-Preserving Scheme with Account-Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain. *IEEE Trans. Netw. Serv. Manag.* **2021**, *19*, 569–581. [CrossRef]
12. Wu, Y.; Tang, S.; Zhao, B.; Peng, Z. BPTM: Blockchain-Based Privacy-Preserving Task Matching in Crowdsourcing. *IEEE Access* **2019**, *7*, 45605–45617. [CrossRef]
13. Abdelsalam, H.A.; Srivastava, A.K.; Eldosouky, A. Blockchain-Based Privacy Preserving and Energy Saving Mechanism for Electricity Prosumers. *IEEE Trans. Sustain. Energy* **2021**, *13*, 302–314. [CrossRef]

14. Zou, S.; Xi, J.; Xu, G.; Zhang, M.; Lu, Y. CrowdHB: A Decentralized Location Privacy-Preserving Crowdsensing System Based on a Hybrid Blockchain Network. *IEEE Internet Things J.* **2021**, *9*, 14803–14817. [CrossRef]
15. Rahman, M.S.; Khalil, I.; Moustafa, N.; Kalapaaking, A.P.; Bouras, A. A Blockchain-Enabled Privacy-Preserving Verifiable Query Framework for Securing Cloud-Assisted Industrial Internet of Things Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 5007–5017. [CrossRef]
16. Zhang, C.; Zhu, L.; Xu, C.; Sharif, K. PRVB: Achieving Privacy-Preserving and Reliable Vehicular Crowdsensing via Blockchain Oracle. *IEEE Trans. Veh. Technol.* **2020**, *70*, 831–843. [CrossRef]
17. Chulerttiyawong, D.; Jamalipour, A. A Blockchain Assisted Vehicular Pseudonym Issuance and Management System for Conditional Privacy Enhancement. *IEEE Access* **2021**, *9*, 127305–127319. [CrossRef]
18. Lin, C.; He, D.; Huang, X.; Xie, X.; Choo, K.-K.R. PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications. *IEEE Syst. J.* **2021**, *15*, 4367–4378. [CrossRef]
19. Rahmadika, S.; Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Sharma, V.; You, I. Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 710–721. [CrossRef]
20. Xiong, T.; Zhang, R.; Liu, J.; Huang, T.; Liu, Y.; Yu, F.R. A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in Space-Ground Integrated Networks. *Comput. Netw.* **2022**, *206*, 108793. [CrossRef]
21. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Futur. Gener. Comput. Syst.* **2021**, *129*, 380–388. [CrossRef]
22. Guo, L.; Xie, H.; Li, Y. Data encryption based blockchain and privacy preserving mechanisms towards big data. *J. Vis. Commun. Image Represent.* **2019**, *70*, 102741. [CrossRef]
23. Mohan, D.; Alwin, L.; Neeraja, P.; Lawrence, K.D.; Pathari, V. A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. *J. Reliab. Intell. Environ.* **2021**, *8*, 379–396. [CrossRef]
24. Elisa, N.; Yang, L.; Chao, F.; Cao, Y. A framework of blockchain-based secure and privacy-preserving E-government system. *Wirel. Netw.* **2018**, 1–11. [CrossRef]
25. Dewangan, N.K.; Chandrakar, P.; Kumari, S.; Rodrigues, J.J. Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system. *Multimedia Tools Appl.* **2022**, 1–20. [CrossRef]
26. Abidi, M.H.; Alkhalefah, H.; Umer, U.; Mohammed, M.K. Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process. *Int. J. Intell. Syst.* **2020**, *36*, 260–290. [CrossRef]
27. Dutta, T.; Bhattacharyya, S.; Dey, S.; Platos, J. Border Collie Optimization. *IEEE Access* **2020**, *8*, 109177–109197. [CrossRef]
28. Moazzeni, A.R.; Khamehchi, E. Rain optimization algorithm (ROA): A new metaheuristic method for drilling optimization solutions. *J. Pet. Sci. Eng.* **2020**, *195*, 107512. [CrossRef]
29. Elgamal, Z.M.; Yasin, N.B.M.; Tubishat, M.; Alswaitti, M.; Mirjalili, S. An Improved Harris Hawks Optimization Algorithm with Simulated Annealing for Feature Selection in the Medical Field. *IEEE Access* **2020**, *8*, 186638–186652. [CrossRef]
30. Hu, H.; Ao, Y.; Bai, Y.; Cheng, R.; Xu, T. An Improved Harris's Hawks Optimization for SAR Target Recognition and Stock Market Index Prediction. *IEEE Access* **2020**, *8*, 65891–65910. [CrossRef]