Research Article

*International Journal of Advanced Technology and Engineering Exploration, Vol 9(89)*
*ISSN (Print): 2394-5443 ISSN (Online): 2394-7454*
*http://dx.doi.org/10.19101/IJATEE.2021.875064*

# Improved sun flow optimization (I-SFO) algorithm based de-centralized information flow control for multi-tenant cloud virtual machines

**Yogesh B. Gurav[*] and Bankat M. Patil**
Department of Computer Science and IT, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad (MS), India

Received: 20-October-2021; Revised: 01-April-2022; Accepted: 02-April-2022

## Abstract

***A novel multi-tenant decentralized information flow control (MT-DIFC) model is introduced in this research work. In cloud computing, the MT-DIFC allows a larger pool of resources to be shared among a larger number of people without compromising privacy and security. Initially, the sensitive data is isolated from the rest on the basis of the security level. Then, these sensitive data are subjected to encryption via an improved signcryption algorithm. At the receiver end, the decryption takes place based on the computed two-level trust model. Interestingly, here the direct, as well as indirect trust, is computed for the ones who request for access privileges to the data owners. Based on the computed trust level, the access privilege is provided to the user's request; and here the level of document readability and downloading capability will be decided by the data owner. Based on the computed trust level, the decryption of the data (only the permitted data-level access provided by the owner) is accomplished. Furthermore, the improved sun flow optimization algorithm (I-SFO) has been introduced for optimal key generation. This I-SFO model is validated by varying its weight function W from 100, 150 and 200, respectively. In addition, a non-parametric analysis has been carried out to validate the efficiency of I-SFO. Accordingly, the outcomes reveal that the proposed work has attained the least cost function, while fixing W=100, 150 and 200, respectively.***

## Keywords

***Cloud computing, Multi-tenant virtual machine, I-SFO, Non-parametric analysis.***

## 1.Introduction

The cloud computing has been utilized in different aspects like business, information technology (IT), educational institutions [1−4]. The major reason behind the expanding demand for cloud computing is owing towards its low-cost and practical, on-demand services. In the cloud computing platform, the multi-tenant architecture is being the most basic feature that refers to the model of sharing the program components or the system components multi-user environment. In the multi-tenant architecture, there is a need for mutual information isolation amongst the tenants for physical resource sharing [5−9]. Therefore, in the multi-tenant architecture, the tenant data security isolation is exhibited to be the key, and it's been the major aspect of ensuring the security of the tenant's sensitive data [10, 11].

The label-based information flow control (IFC) system in the cloud architecture is providing a secured data sharing facility by preventing data leakage. In IFC, a user with a certain class of clearance level would only be able to access the data labeled with that clearance level. Mostly, these systems are preferred for military or academic purposes, wherein data confidentiality is being a high-priority issue [12−15]. Later in decentralized information flow control (DIFC) systems, the classes in the IFC model were replaced with security labels having multiple tags specifying the authorized data readers [16−20]. Recently, the DIFC model has been highly investigated among the research community to provide security to the user's sensitive data during the information flow [21−25]. The DIFC policies aid in providing the information flow along with the application components [26−29].

Security concerns are frequently regarded as a difficult to cloud computing adoption. IFC is a well-known mechanism for mandatory access control.

[*]Author for correspondence

Although the first IFC models focused on security in a centralized setting, decentralized IFC has been devised and implemented, generally as part of the university research initiative. As a result, decentralized IFC has the potential to provide greater cloud security than currently offered. The sun flow optimization algorithm (SFO) algorithm is inspired by nature and is assessed as an iterative, population-based, meta-heuristic optimization technique. The proposed improved sun flow optimization algorithm (I-SFO) algorithm has can find global optimal solutions without getting stuck in local optimal solutions. The I-SFO algorithm has the advantage of not using derivatives while assessing the objective function.

### 1.1Objectives

The main objective of this work is as follows:

- The aim of the research strategy is to attain the critical break time.
- For this, there is a need for an improved optimization algorithm.

The major contribution of this research work is:

- Analyzing the efficiency of I-SFO by varying the weight function W from 100, 150, and 200, respectively.

The rest of this paper is organized as: section 2 addresses the recent works on DIFC and IFC. The decentralized ciphertext IFC for multi-tenant sensitive information flow has been discussed in section 3. In addition, an illustration of the proposed secured multi-tenant DIFC is manifested also in section 3. The results acquired by varying the weight function are manifested in section 4. Discussion in section 5. This paper is concluded in section 6.

## 2.Literature review

In 2016, Elsayed and Zulkernine [1] have introduced a new "information flow control as a service (IFCaaS)" model based on inspiration acquired from the security as a service (SecaaS). The cloud-delivered IFC-based security analysis and monitoring services have been provided by the IFCaaS. In addition, the vulnerabilities within the software as a service (SaaS) framework have been identified during the information flow. Therefore, the projected model has been suggested as a solution for protecting data integrity as well as confidentiality during the information flow.

In 2014, Bacon et al. [2] have projected DIFC for solving the security issues in the SaaS level of the cloud. The proposed DIFC being the mandatory access control method was said to provide higher security of the data. Moreover, here proper labeling and validation mechanisms have been available, and they together monitored the information flow by satisfying the rules and regulations.

In 2015, Xi et al. [3] have projected a distributed approach for securing the IFC. Initially, the authors have validated each service component using model checking. Subsequently, they have accomplished the compositional verification procedure to secure the safety of the data during its flow. As a consequence, the proposed work was found to be a global verification approach with minimized cost consumption for verification.

In 2018, Xi et al. [4] have introduced a secure information flow verification theorem for multiple clouds to boost the security constraints on every component. On a regular information flow as well as encrypted information flow, the data security is validated via distributed IFC framework and algorithm. The suggested model has been identified to be much more appropriate for multiple clouds improved security-based IFC.

In 2019, Khurshid et al. [5] have introduced a dynamic control method for sensitive IFC, the proposed work was based upon virtual boundary recognition. The tenant's feature vectors corresponding to their behavior have been identified by analyzing the operation log and behavior of the tenants. Moreover, the dynamic spiking neural network has been utilized for identifying the virtual boundary of the tenant automatically.

In 2020, Moussaid and Azhari [30] have improved security attributes by dynamically forming them by analyzing entity behaviour and associating it with a trust level and security class. They created a template for this purpose and developed a security strategy to ensure the security attributes. Finally, the findings demonstrate the efficacy of the suggested strategy in terms of classification and real-time detection rate.

In 2021, Zhang et al. [31] presented a tenant-led ciphertext IFC technique for virtual machines of the cloud. The IFC strategies of taint infection, secret-level reduction, and ability propagation is realized in ciphertext form through the design of a DIFC security policy, a secret-domain key management scheme, and a multi-ID-based threshold encryption scheme, which can effectively prevent malicious users inside and outside the system from illegally reading private data. Security proof and an experiment are used to verify the method's effectiveness.

In 2022, Li [32] have presented a big data IFC mechanism based on semantic features. The big data information flow is hierarchically managed and dynamically corrected. The load of each sub-flow is balanced, and real-time control of big data, information flow is obtained, by setting the network bandwidth occupancy ratio parameter of big data information flow. The outcomes demonstrate that the big data IFC approach based on semantic characteristics can not only minimize the noise content of big data, information flow, but also increase the control speed as well as control performance in the cloud computing environment.

In 2022, Lu et al. [33] have presented decentralized information flow control (DIFC) approach, for protecting both the confidentiality and integrity of shared cloud data. Also, a privilege protection policy for DIFCS is presented, allowing it to prevent malicious users from changing privilege. Moreover, the findings of the analysis show that DIFCS holds. The experimental results further demonstrate the high efficiency of DIFC in terms of security, integrity, privilege and authenticity.

In 2022, Gurav and Patil [34] have introduced a novel DIFC framework that employs a hybrid advanced encryption standard-elliptic curve cryptography (AES-ECC) encryption model. The introduced two-fold improved poor rich optimization (TF-IPRO) algorithm was used to perform optimal key selection within the hybrid AES-ECC encryption model. Here, an algorithmic evaluation was performed, to validate the efficiency of the proposed TF-IPRO, which was used for optimal key selection during the DIFC for cloud virtual machines.

Numerous methods have been focused in the field of DIFC for cloud virtual machines. But, still there exist a common problem such as high energy consumption, high execution time, secures in-cloud data flow alone, no guarantee end-to-end security, may violate the standard noninterference and complex structures. Hence there is a need for a new multi-tenant DIFC assisted with an optimization algorithm for optimal key generation to overcome the above-mentioned issues.

# 3.Methods

## 3.1Decentralized ciphertext information flow control for multi-tenant sensitive information flow

***Overall methodology and system model***

Based on the multi-tenant sensitive information flow, this research work provides a distinctive decentralized ciphertext IFC system. Three major components make up an effective cloud computing environment: (a) cloud service provider (CSP), (b) data store (DS), and (c) consumer. *Figure 1* depicts the planned project's overall architecture.

CSP houses our contribution, which encompasses (1) the central authority (CA), (2) the encryption proxy (EP), (3) the cloud server (CS), and (4) the cloud tenant virtual machines. The hardware resources (including central processing unit (CPU), memory, network, and storage, among others) are wrapped within the CSP's management centre using virtualization technology. These resources are then distributed across multiple virtual computers. The CA, being both a key management centre and a labeling management centre, has always been in charge of both labeling management and key distribution. In addition, the EP is in charge of executing security policies and conducting storage EP activities for authorized cloud tenants inside this virtual machine hypervisor. The CS is an online storage server with such a substantial quantity of storage capability and processing capabilities. All virtual machines within that cloud tenancy communicate with CS through the EP to periodically access information (read, create, and change). Based on the suggested signcryption algorithm, EP implements security policies. Every tenant submits an application of CA to generate a new secret-domain label and to provide trusted tenant capabilities to virtual machines. Because the CA and EP are both expected to be trustworthy in this study, the security labels and generated keys will be scrupulously preserved by the CA for any and all tenants. The data records are indeed saved as metadata inside the DS including associated relevant integrity as well as security tags DS. The people who consume the cloud are indeed the people who are using the cloud.

The suggested work is divided into three sections: (a) sensitive information classification, (b) trust assessment, as well as (c) optimum key-based cipher-text information flow security. Initially from the original data, the sensitive information has been identified depending on the security value.

The encryption procedure would therefore commence when this determination of has been made. EP authentically implements the ciphertext information flow security method for based on the suggested trust assessment. The suggested improved signcryption technique decrypts the user's data, and the best key is created using the newly proposed improved sun flow optimization algorithm (I-SFO). This I-SFO is an enhancement on the traditional SFO algorithm from a conceptual standpoint SFO. Finally, users will be given the decryption key based on the suggested trust rating. Direct and indirect trust has both been taken into account. The degree of access privileges for the concerned files (portions) would be assessed based on the determined trust model. Existing users who have been granted access permissions are generally known as direct users, whilst newcomers are known as indirect users.

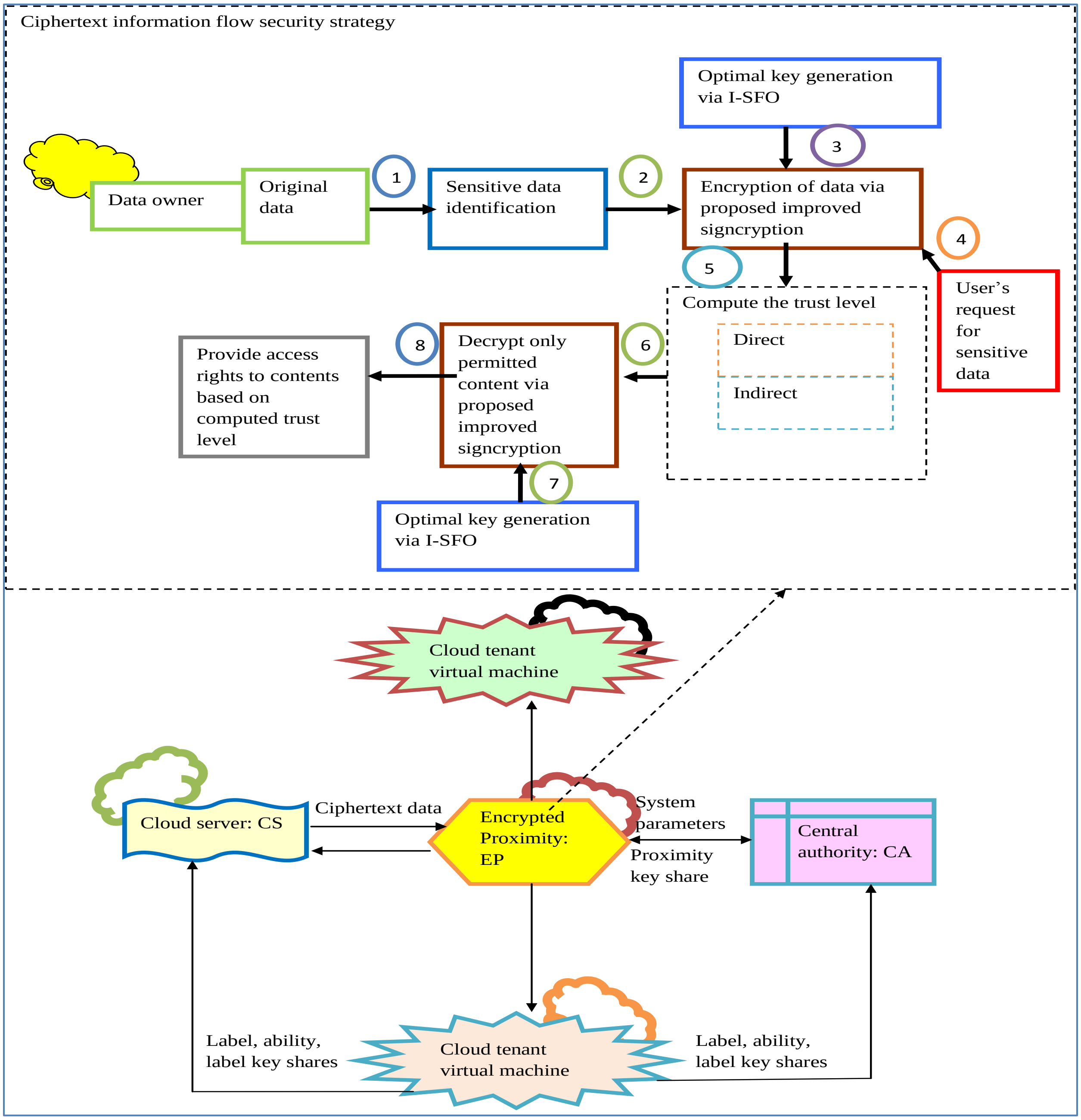

Ciphertext information flow security strategy
Optimal key generation via I-SFO
3
Data owner
Original data
1
Sensitive data identification
2
Encryption of data via proposed improved signcryption
4
5
User's request for sensitive data
Compute the trust level
Direct
Indirect
8
Decrypt only permitted content via proposed improved signcryption
6
Provide access rights to contents based on computed trust level
7
Optimal key generation via I-SFO
Cloud tenant virtual machine
Cloud server: CS
Ciphertext data
Encrypted Proximity: EP
System parameters
Proximity key share
Central authority: CA
Label, ability, label key shares
Cloud tenant virtual machine
Label, ability, label key shares

**Figure 1** Overall architecture of the projected DIFC model in cloud

***Objective function and solution encoding***

The main goal of this research strategy is to create critical break time $Time_{keybreak}$. The objective function is expressed mathematically as Equation 1.

$$\boldsymbol{Obj = Min\left(\frac{1}{Time_{keybreak}}\right)} \quad (1)$$

## 3.2Illustration of the proposed secured multi-tenant DIFC

***An Illustration***

Let's say there are six tenant virtual machines (multi-tenant): $Owner$ (data owner), $Tenant_2$ (doctors),$Tenant_3$ (researchers), $Tenant_4$ (friends or family members of patients), and $Tenant_5$ (health insurance company representatives). As the data owner, the patient uploads his or her encrypted sensitive data to the cloud. Within $File_1$, there are two files: $File_1$ and $File_2$. The level of security of $File_1$is configured to be relatively low, but the level of security of the file $File_2$ is set to be substantially larger. Since, the level of security of $File_1$is lower, all the users who've requested read access rights will be provided, On the other hand, when a user needs to modify $File_1$, then his/her trust level is computed, and based on the computed trust level the access rights are provided to users. In this case, the owners decide the quantity of data that can be given to the user for modification, and based on the owner's response, only the particular part of the data will be decrypted with I-SFO. On the other hand, the security level of $File_2$is said to be larger, therefore it is said to encapsulate a huge count of most sensitive data. When user's (say $Tenant_2$ (doctors),$Tenant_3$ (researchers)) request for data readability to$Owner$, the $Owner$ computes the trust level of $Tenant_2$ (doctors), $Tenant_3$ (researchers) and provides the level of readability of $File_2$. On the other hand, when $Tenant_2$ (doctors),$Tenant_3$ (researchers) requests for downloading the $Owner$'s data. Now $Owner$ again computes the trust level based on the previous access history, and then provides the write privilege rights based on his/her preference and not based on the requests. The complete decision-making of information flow and security resides within the data owner, and hence the process is said to be highly secured.

***System initialization***

1. The public key $P_{key}(N, E)$ and the private key $S_{key}(N, D)$ are both generated by the CA.
2. Mostly on basis of the total method, CA allocates a recognizing $tid$ to every one of the labels.
3. The label t is put into consideration, and CA generates the tenant key share $sk_{tid-user}$ and customer proximity share $sk_{tid-ep}$ using the key generation technique $keygenerate(P_{key}, tid, S_{key})$. The proxy key is also obtained over the encrypted channel by the EA. Furthermore, each one of the secret-domain tags is individually initialized.
4. For every confidential data secret domain, CA establishes a secret-domain secret-level label key$SCK_{key1}$, $SCK_{key2}$, $SCK_{key3}$and $SCK_{key4}$ that denotes the Secret-domain *key* highly confidential key, secret-domain $key$ confidential key, secret-domain $key$ private key, and secret-domain $key$ public key are the secret-domain $key$ top-secret key, secret-domain K confidential key, secret-domain $key$ secret key, and secret-domain $key$ public key, respectively.
5. CA receives a security label and virtual machine capabilities whenever a virtual machine has been established. As a result, the tenant key shares $sk_{tid-user}$ that correspond to the label have been assigned.

***Label management***

The label management for accessing the $File_2$by the highly trusted tenant $Tenant_2$is manifested in this section.

The data owner tenant virtual machine would seek the CA to establish the private information secret-domain label$Q$, and indeed the CA would grant the permission to run $Q$'s key initialization operation. The tenant virtual machine subsequently transmits the tenant key private key share $sk_{tid-user}$ and proxy key shares$sk_{tep-ep}$towards the tenant virtual machine. The renters' capability set has indeed been expanded to include the $Q^+, Q^-, Q^\pm$.

Tenant$Owner$'s virtual system required the CA in terms of giving tenant $Tenant_2$'s vm with the ability $Q^+_{key-p}$ (i.e., *Owner* 's vm can append labels $(Q_k.p)$to one's own security label). CA additionally looked as to whether the label $Q^\pm_k$ was present in the ability set of the$Owner$vm. The CA of the $Tenant_2$tenant vm adds capacity set $t^+_{key-p}$ if the obvious response to such a query is yes.

The label $(t_k.SC_k)$has been added to $Tenant_2$ 's vm about the capability according to a requirement from CA. CA additionally validates if the tenant vm has label $Q^+_{key-SC_k}$ capabilities. The tenant vm has received the tenant key shares$sk_{tid-user}$depending on its own availability, as well as the label $(Q_k.SC_k)$has indeed been applied to the tenant vm independently depending upon $Q^{+}_{key-SC_k}$.

The tenant vm $Owner$requests that perhaps the CA withdraw the t tenant's label $(Q_k.SC_k)$or $Q_k^+$or$Q_k^-$ ability. The capability set $Q_k^{\pm}$ of the $Tenant_2$ vm is validated by CA. The $Owner$ tenant virtual machine's label $(Q_k.SC_k)$ or$Q_k^+$or$Q_k^-$ability is lost once the ability set $Q_k^{\pm}$ appears available inside the $Tenant_2$ vm.

The tenant vm $Owner$ has requested that the CA provide the ability $Q_k^{\pm}$ to the tenant vm $Tenant_2$, and the CA had also confirmed the presence of label $Q_k^{\pm}$within the $Owner$ vm. Whenever label $Q_k^{\pm}$ is present in $Owner$ virtual machine, the ability set is introduced to $Tenant_2$ .

***Communication between*** $\boldsymbol{Owner}$***and*** $\boldsymbol{Tenant_2}$

File $File_2$ is sent from $Owner$ vm to $Tenant_2$ vm. A validation of the information policy rule was done to run the DIFC module within the hypervisor vm of $Tenant_2$ and $Owner$. While the rule has been in effect, the tenant vm $Tenant_2$'s confidentiality label gets highly contaminated, and $File_2$ may now be viewable by $Tenant_2$.

***Information flow between*** $\boldsymbol{Owner}$***and*** $\boldsymbol{Tenant_2}$

The data file $File_2$ was transferred from the $Owner$ vm to the $Tenant_2$ vm. The entity of $Owner$ with the flow of information to entity $Tenant_2$ commences whenever the constraints are satisfied. This model is shown in: $Owner \rightarrow bifLabel_{Owner} - Ability^{-}_{Owner} \subseteq Label_{Tenant_2} + Ability^{-}_{Tenant_2}$Whenever information is received by vm $Tenant_2$, $Tenant_2$'s security signature is compromised, causing the associated changes. This is represented as: $Label'_{Tenant_2} \leftarrow Label_{Tenant_2} \cup (Label_{Owner} - Ability^{-}_{Owner})$ The information outflow entity $Owner$'s transmitting ability and the information inflow entity $Owner$'s receiving ability, as well as the implementation of label propagation, all must be properly considered periodically to identify that low-security information streams to the secret domain's high-security level.

***Cloud network file read and write between*** $\boldsymbol{Owner}$***and*** $\boldsymbol{Tenant_2}$

Tenant Vm $Owner$ writes Document $File_2$ towards the cloud storage server: The network file writing rules that correspond to the data-flow strategy are implemented by the vm hypervisor within the security confidential proxy module. The safety encryption module has been used by the algorithm $Encrypt(S_{key}, tids, P_{key})$ to encrypt $File_2$ based on the secrecy labelling inside of the user's security label. The document security label is altered and further transmitted to the cloud database according to the write rule.

Tenant Vm $Tenant_2$ downloads document $File_2$ from the cloud database: depending upon that tenant vm security mark and file mark, the vm hypervisor inside the DIFC component validates the document reading rule. The $Decrypt(S_{key}, \{sk_{tid-ep}\}tid \in tids, C)$ method has been used to decode the $\{m_{tid-ep}\}tid \in tids$ encrypted fragment employing the proxy key sharing if indeed the files reading criteria are satisfied.

The ciphertext for the file is therefore disseminated, and the decrypted pieces are being sent to the $Tenant_2$tenant vm. The tenant vm $Tenant_2$ surpasses the authority if indeed the file writing rule is not fulfilled. To retrieve the $\{m_{tid-user}\}tid \in tids$ decrypted fragments, the tenant vm $Tenant_2$ must decrypt the document with the security label to use the tenant key sharing implementation method $Decrypt(S_{key}, \{sk_{tid-eA}\}tid \in tids, C)$. The combination algorithm $combine\big(S_{key}\{m_{tid-w}\}tid \in tis, w \in [user, eA], C\big)$with encrypted pieces is used to obtain the plain text of the algorithm. The read process has now been done.

***Trust evaluation***

Two forms of trust have been calculated: direct trust and indirect trust.

**Direct trust**: The tenant (which could be $Tenant_2$, $Tenant_3$, $Tenant_4$, $Tenant_5$ and $Tenant_6$) has already had access to $Owner$'s file. The previous communication and information accessibility have been maintained in the trust table throughout this scenario. For example, in the past, only doctors $Tenant_2$ as well as friends or family members of patients $Tenant_5$ were allowed access rights, thus $Tenant_2$ and $Tenant_5$ may only see $Tenant_1$'s information. Additionally, $Tenant_2$ and $Tenant_5$ could only retrieve a portion of the document, not the whole thing. Just that portion of the information would be encrypted.

**Indirect trust:** Whenever a new person requests access to the information for which he or she has never had authority, the user's interaction experience is calculated. Whenever researchers seek access privileges to $Owner$, for example, his or her prior interactions are authenticated; if $Tenant_1$ seems to have no previous interactions, the accessibility privilege has been refused. $Tenant_1$ grants access to pharmacists $Tenant_4$ who've already communicated with $Owner$ (but doesn't have all-time access privileges like $Tenant_2$ as well as $Tenant_5$). $Tenant_4$ can also only retrieve a portion of a file, not the entire file. Only that portion of the material would be protected using decrypted.

***Improved signcryption algorithm***

A novel improved signcryption method is presented in this research paper. The encryption is done in the EP throughout the suggested architecture. Digital signatures and encryption are both included in the proposed enhanced signcryption method. Here, the prime number set that has been considered for private key generation based on the fitness evaluation (shown in Equation (1)) passes as input to the proposed model. The outcome from the proposed model is the optimally selected private key $S^*_{key}(N,D)$.

**I-SFO:** The I-SFO framework involves inside the $S_{key}(N,D)$ and constructs the best private key $S^*_{key}(N,D)$. *Figure 2*, *Figure 3* and *Figure 4* depict the solution encoding for three different key sizes. This I-SFO paradigm is indeed an enhancement to the regular SFO paradigm.

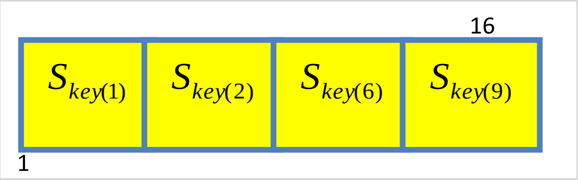


**Figure 2** Solution encoding for key size=16

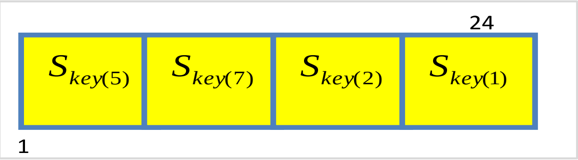


**Figure 3** Solution encoding for key size=24

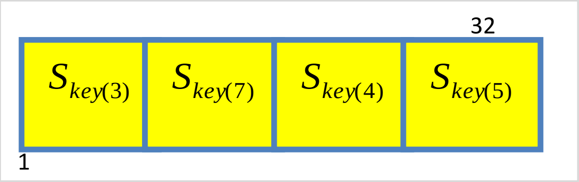


**Figure 4** Solution encoding for key size=32

The encryption is done in the EP, according to the recommended data encryption technique. Rather than adopting the standard advanced encryption standard (AES) paradigm, the enhanced elliptic curve cryptography (ECC) has been implemented. The enhanced ECC receives the original sensitive messages $Sen$ as well as $C_{key}$ and produces $CM$ as a result (ciphertext).

$(Sen, C_{key})$Key generation algorithm→$CM$

During the transfer of information, this encrypted text has been maintained. The encryption of $CM$ is accomplished efficiently utilising the enhanced ECC in the proposed work.

**Improved ECC:**

The private key is generated using Equation 2.

$$P_{key} = S_{key} \times A_c \qquad (2)$$

The private key $S_{key}$ is produced ideally using the I-SFO and $A_c$ is the point on the curve. Equation 3 is used to produce the secret key $C_{key}$.

$$C_{key} = P_{key} + S_{key} + A_c \qquad (3)$$

Two cipher texts are used in the encryption procedure (Equation 4-9).

$$EC(t_1) = \frac{K \times A_c}{C_{key}} \qquad (4)$$

$$EC(t_2) = D_b \times C_{bey} + \frac{(K \times P_{bey})}{C_{bey}} \qquad (5)$$

$EC(t_1)$ and $EC(t_2)$.can be used to compute $D_b$ .

$$EC(t_2) = D_b \times C_{bey} + \frac{K(S_{key} \times A_c)}{C_{key}} \qquad (6)$$

$K$ is a random integer that ranges from 0 to 1.

$$EC(t_2) = D_b \times C_{bey} + EC(t_1) \times S_{key} \qquad (7)$$

$$D_b \times C_{bey} = EC(t_1) - EC(t_2) \times S_{key} \qquad (8)$$

$$D_b = \frac{EC(t_1) - EC(t_2) \times S_{key}}{S_{key}} \qquad (9)$$

**Signcryption**: The $CM$, together with the $S^*_{key}(N,D)$, has been passed into an upgraded ECC. The final outcome is information that has been signed encrypted$(\delta Data)$.

$(CM, S^*_{key}(N,D))$Signcryption→$(\delta Data)$

Unsigncryption process: data signed using the sender's private key $Sender(P_{key})$ and$(\delta Data)$. The signature has been deemed to be authentic if the outcome is 1, else (zan illegal signature) is returned. $(Sender(P_{key}),(\delta Data))$Signature verification→1 or $\perp$ Proposed Decryption: $CM$ (cipher text) and $C_{key}$ are fed into the decryption algorithm (enhanced ECC) to generate the result $Sen\,.\,Sen\,.(CM,C_{key})$ Key generation algorithm→( $Sen$ ).

The steps followed in the I-SFO model are,

Step 1: Initialize population $pop$ of $M$ search agent, current day $Day$ maximal day $\max^{Day}$ .

Step 2: The best solution (sun) is $S^{*}_{key}(N, D)$.

Step 3: All of the plants should face the sun.

Step 4: While ($Day$ <max$^{Day}$ then compute orientation vector$\overrightarrow{J_i}$.

$$\overrightarrow{J_i} = \frac{X_* - X_i}{\|X_* - X_i\|}; i = 1,2,\ldots,n_p \tag{10}$$

Step 5: Calculate the quantities of heat$(Heat)$ absorbed by each plant $i$ .

$$Heat_i = \frac{Power}{4\pi.dist_i} \tag{11}$$

Step 6: plants which are not oriented towards the sunlight have been eradicated.

Step 7: The step has been calculated for each plant. The sunflower's step is calculated in the direction $Q$.

$$d_i = \lambda \times prob_i.(\|X_i + X_{i-1}\|) \times \|X_i + X_{i-1}\| \tag{12}$$

$prob\|X_i + X_{i-1}\|$ is indeed the pollination probability, and $\lambda$ is indeed the plant's "inertial" displacement, which is a constant. The newly derived equation shown below is used to calculate this "inertial" displacement.

$$\lambda = (UL - LB) \times 1 - \left(\frac{day}{max^{Day}}\right) \tag{13}$$

$d_{max}$ is used to calculate the maximum step.

$$d\,\frac{(\|UB - LB\|)}{2 \times N_{pop}}\,{}_{max} \tag{14}$$

The upper and lower limits are denoted by $UB$and $LB$, respectively. $N_{pop}$ also refers to the total number of plants.

Step 8: To assess the additional people, the newly developed mathematical equation presented below is utilized.

$$X_{i+1} = \frac{X_i + d_i \times S_i}{SF} \tag{15}$$

$SF$ is indeed the sinecosine adapted scaling factor, which is calculated according to Equation (8). $W$ also stands for the weight function.

$$SF = \begin{cases} W \times sin\left[\pi \times \left(\frac{day}{max^{day}}\right)\right] & ifr < 0.5 \\ W \times cos\left[\pi \times \left(\frac{day}{max^{day}}\right)\right] & ifr \geq 0.5 \end{cases} \tag{16}$$

Step 9: Update the sun if the new individual seems superior than the previous one.

Step 10: Identify the best solution $S^{*}_{key}(N, D)$.

## 4.Results

### *Experimental setup*

Python was used to implement the suggested task. DIFC with improved signcryption+ I-SFO has been compared to existing models such as DIFC with improved signcryption +WOA, DIFC with improved signcryption + Static single-assignment (SSA), DIFC with improved signcryption +SFO, DIFC with improved signcryption +SFO, DIFC with improved signcryption +LA, DIFC with AES, DIFC with RSA, DIFC with ECC, DIFC with ElGamal, Tenant-Led Ciphertext, DIFC with improved signcryption + DIFC [30]. The evaluation has been made in terms of encryption timer, decryption time, and convergence analysis as well.

### *Dataset description*

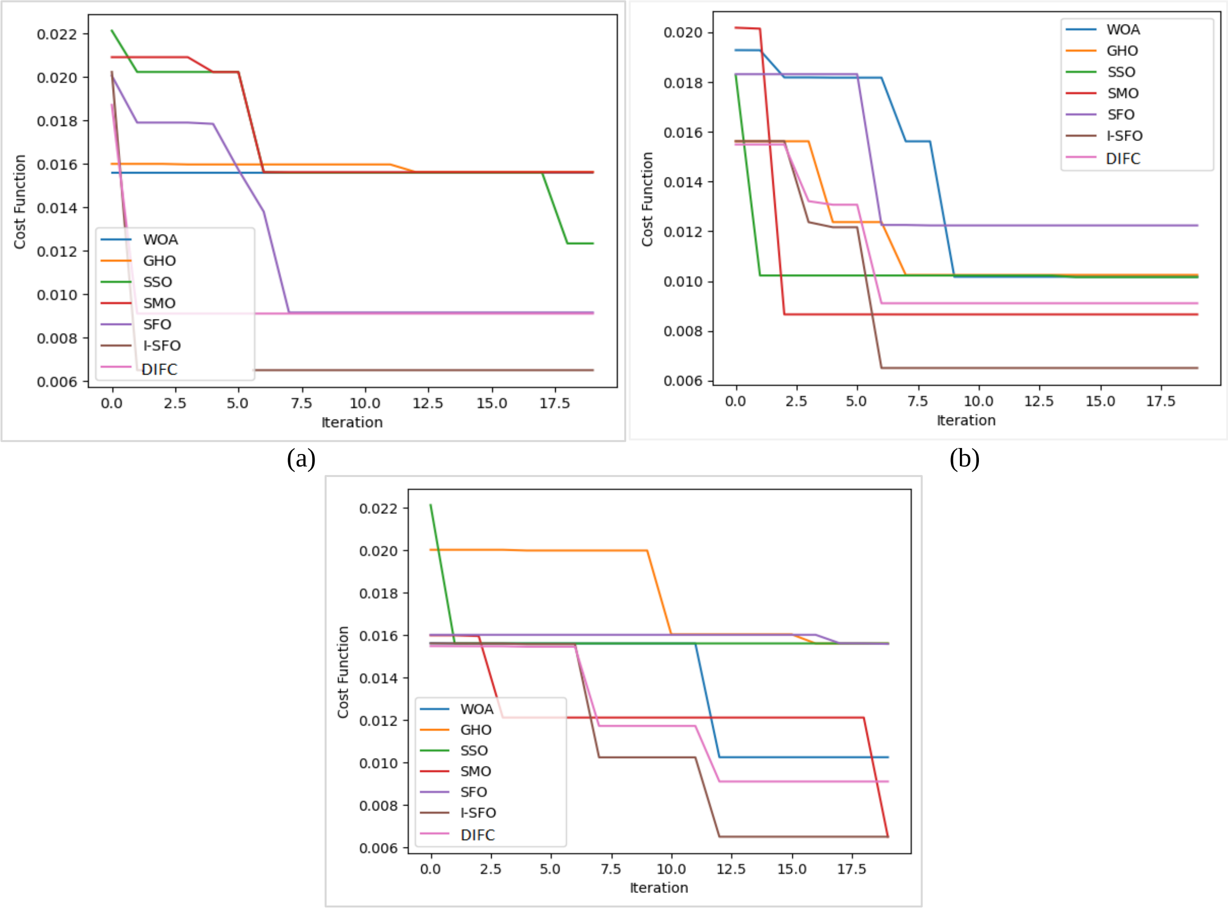
The evaluation was done using 4 datasets: “heart disease dataset: https://www.kaggle.com/ronitf/heart-disease-uci; lung cancer dataset: https://www.kaggle.com/yusufdede/lung-cancer-dataset; breast cancer dataset: https://www.kaggle.com/uciml/breast-cancer-wisconsin-data”, Diabetes dataset: https://archive.ics.uci.edu/ml/datasets/diabetes, respectively.

Although the heart disease dataset has 76 features, all published studies only use a subset of 14 of these. The Cleveland database is the only one that has been used by machine learning researchers to yet. The "goal" field indicates whether or not the patient has the cardiac disease. It has a value of 0 (no presence) to 4 (present). The features in the breast cancer dataset are calculated using a digitized picture of a fine needle aspirate (FNA) of a breast mass. They define the features of the image's cell nuclei.

Automatic electronic recording equipment and paper records were used to acquire diabetes patient records. The automatic device featured an internal clock that was used to timestamp occurrences, whereas the paper records simply contained "logical time" slots (breakfast, lunch, dinner, bedtime). Breakfast (08:00), lunch (12:00), dinner (18:00), and bedtime (18:00) were all allocated regular hours for paper records (22:00). As a result, paper records have false uniform recording times, whereas electronic records have timestamps that are more realistic.

***Convergence analysis***

The convergence analysis is undergone to validate the efficiency of the I-SFO under all the three variables in the weight function W from 100, 150 and 200, respectively. The assessment has been carried out with three different datasets: heart disease dataset, lung cancer dataset and breast cancer dataset. Here, the convergence recorded by the I-SFO is compared over the existing models like whale optimization algorithm (WOA), grasshopper optimization algorithm (GHO), salp swarm optimization algorithm (SSO), spider monkey optimization algorithm (SMO), sun flow optimization (SFO), and DIFC [30] respectively. The result acquired with the proposed work for is manifested heart disease dataset, lung cancer dataset and breast cancer dataset under W =100, W =150 and W =200 is shown *Figure 5*, *Figure 6* and *Figure 7*, respectively. On observing the outcomes, the proposed work has attained the least cost function, while fixing W =100, 150 and 200, respectively. Since, our objective function is the minimization of key break time; the proposed work has attained the minimal cost function even at the highest iteration count.

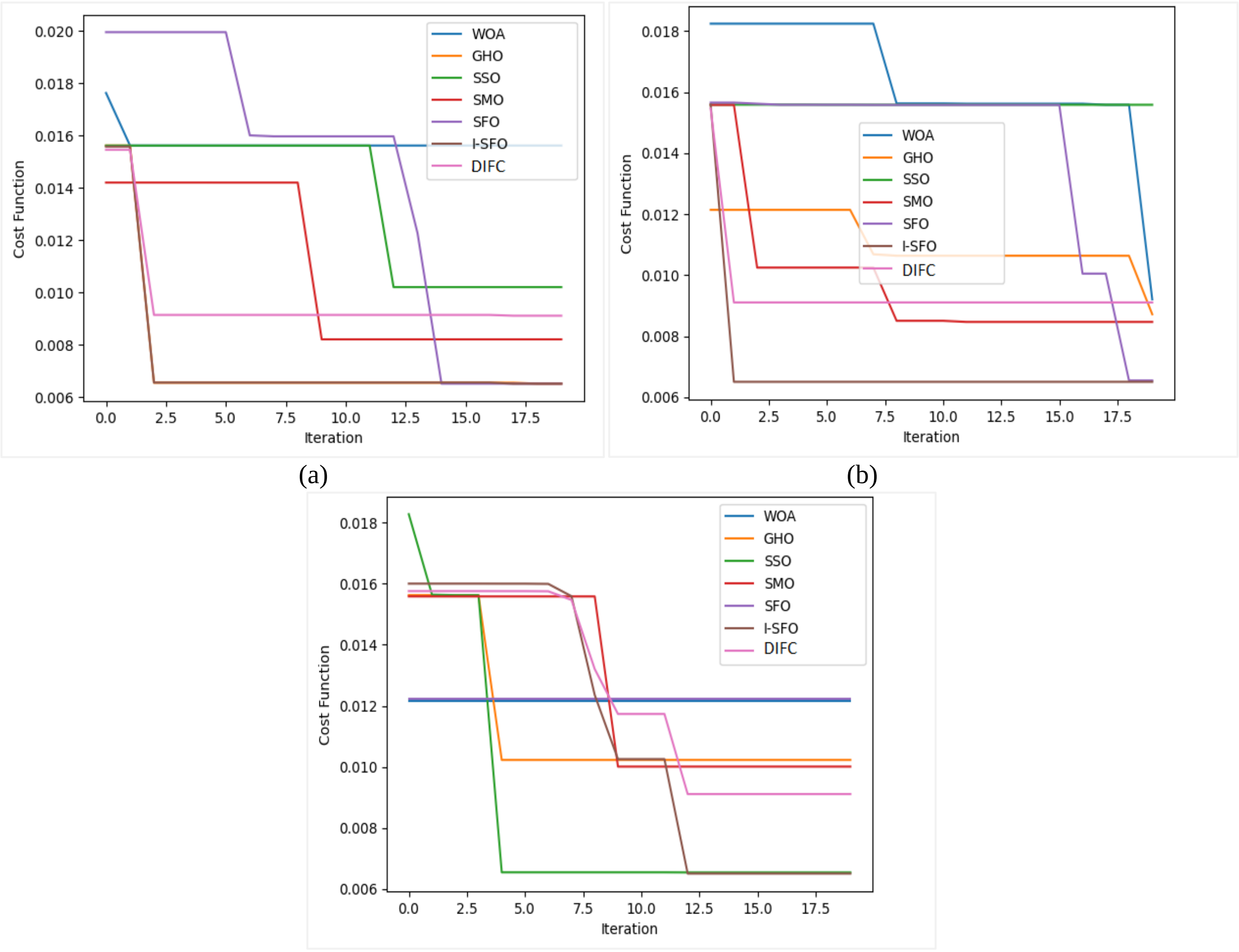


(a)

(b)

(c)

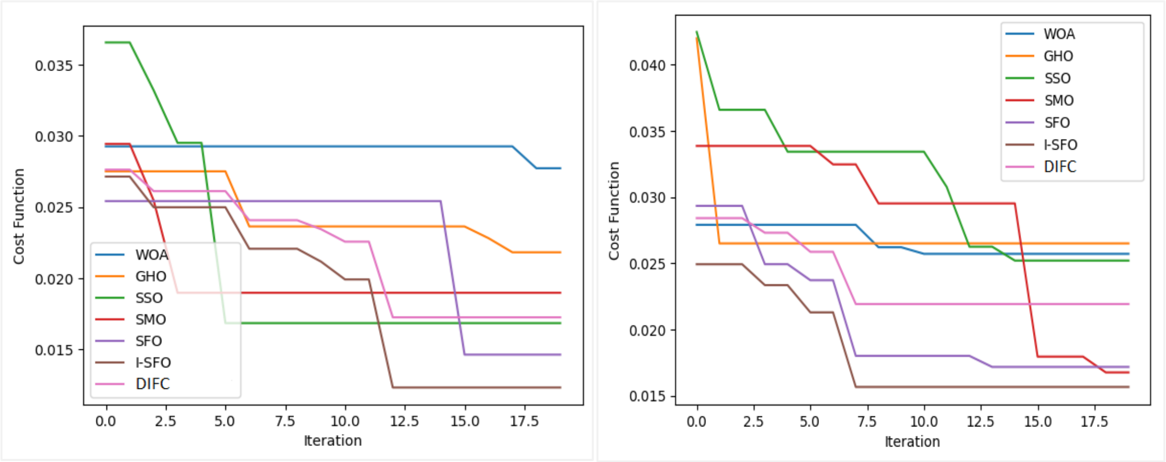
**Figure 5** Convergence Analysis of I-SFO at W =100 for a (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset



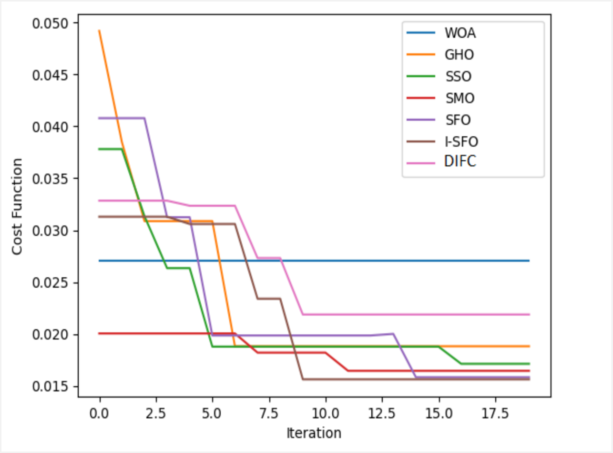
(a) (b)

(c)

**Figure 6** Convergence analysis of I-SFO at W =150 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset



(a) (b)

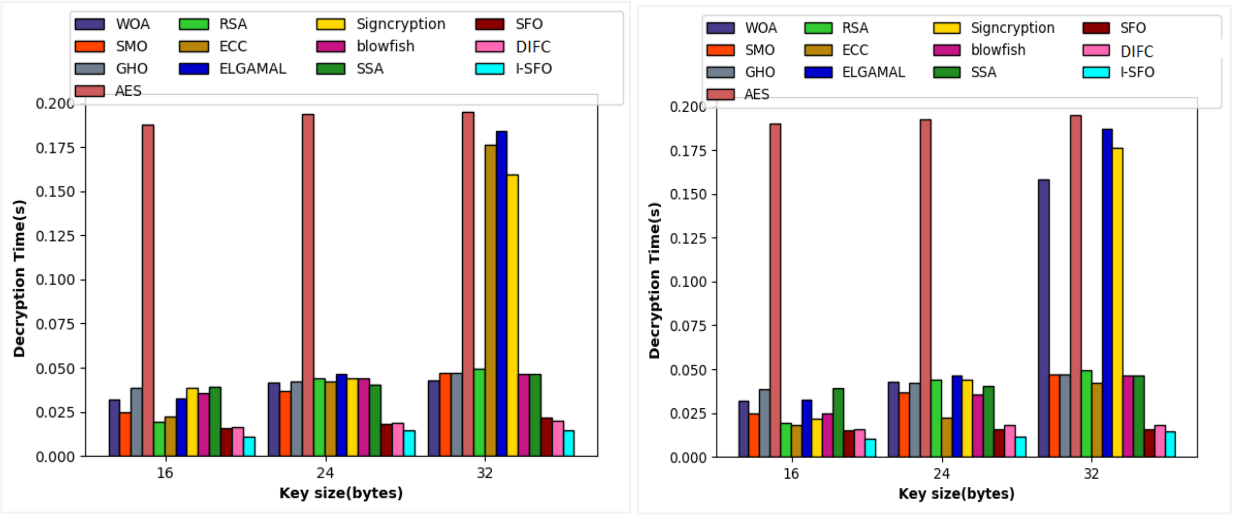


(c)

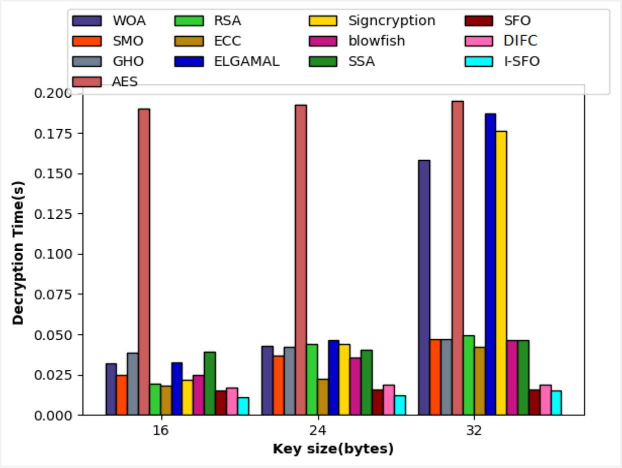
**Figure 7** Convergence analysis of I-SFO at W =200 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset

***Analysis on decryption time***

The time required for decrypting the information for the proposed over the conventional methods is shown in *Figures 8 to 10*. The evaluation has been made for the heart disease dataset, lung cancer dataset and breast cancer dataset by fixing the weight function *W* =100, 150 and 200, respectively. The decryption time analysis for the heart disease dataset, lung cancer dataset and breast cancer dataset at *W* =100, 150 and 200 is shown in *Figure 8*, *Figure 9* and *Figure 10*, respectively. On observing the outcomes, the proposed work has attained the least decryption time for the heart disease dataset, lung cancer dataset and breast cancer dataset under every variation in weight function. This reduction in the decryption time is owing towards the identification of the sensitive data for encryption, rather than encrypting the entire data. Moreover, the optimal key generation-based decryption has been carried out based on the computed trust level, therefore the decryption has been made efficient and less time-consuming. In addition, the improved ECC has been implied rather than the existing AES model, therefore the decryption time has been reduced.

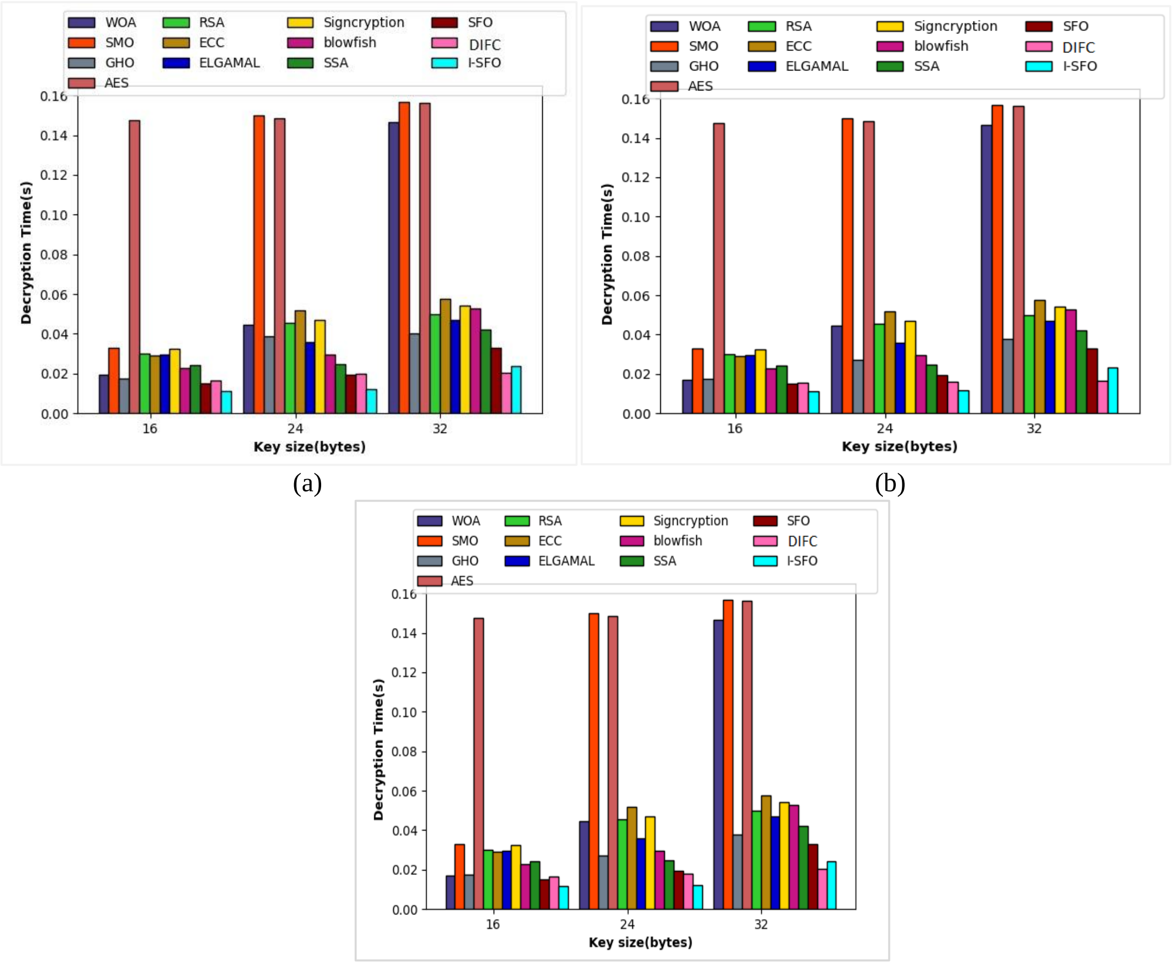


(a) (b)



(c)

**Figure 8** Analysis of decryption time of I-SFO at W =100 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset

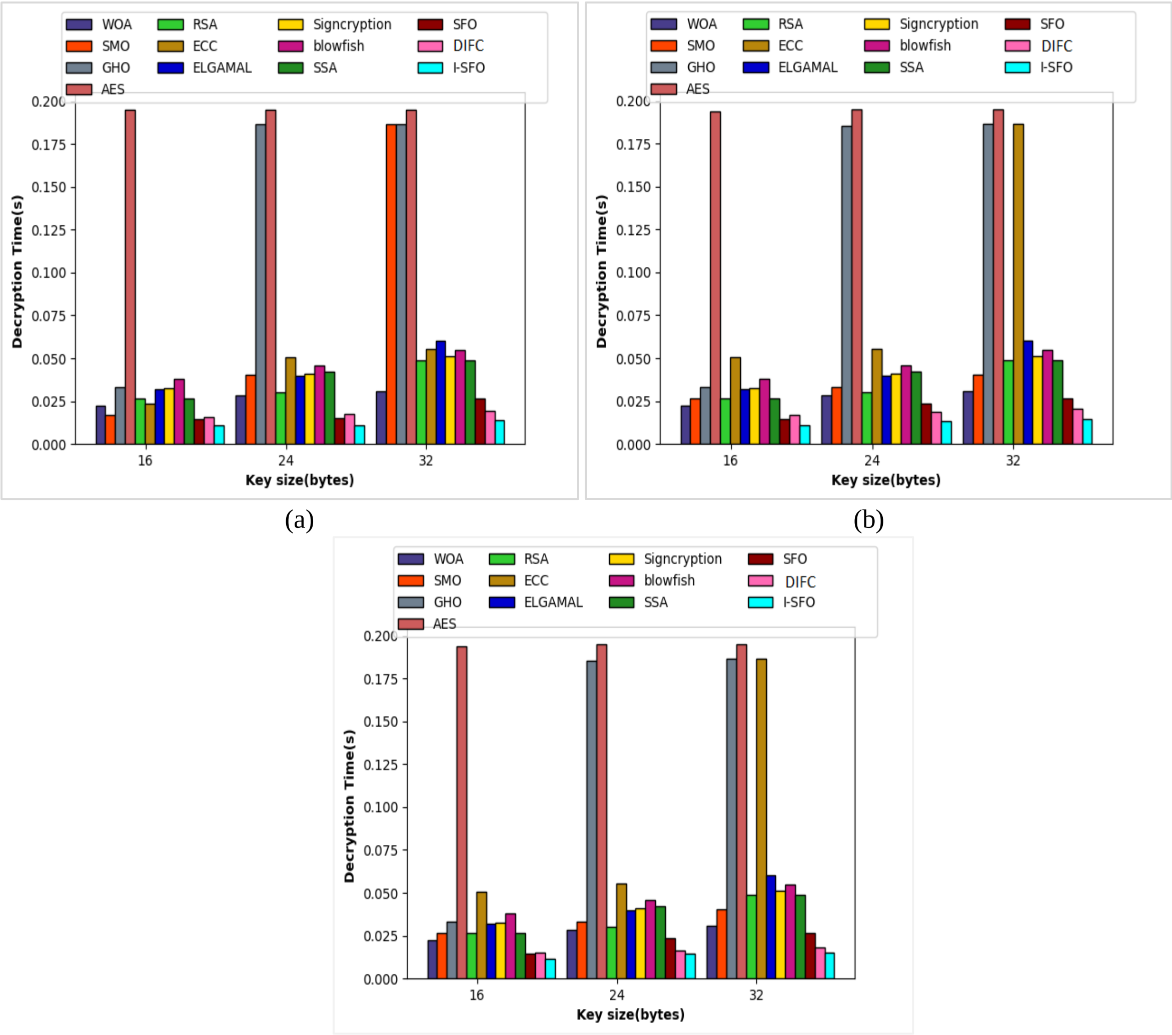


(a)

(b)

(c)

**Figure 9** Analysis of decryption time of I-SFO at W =150 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset



(a)

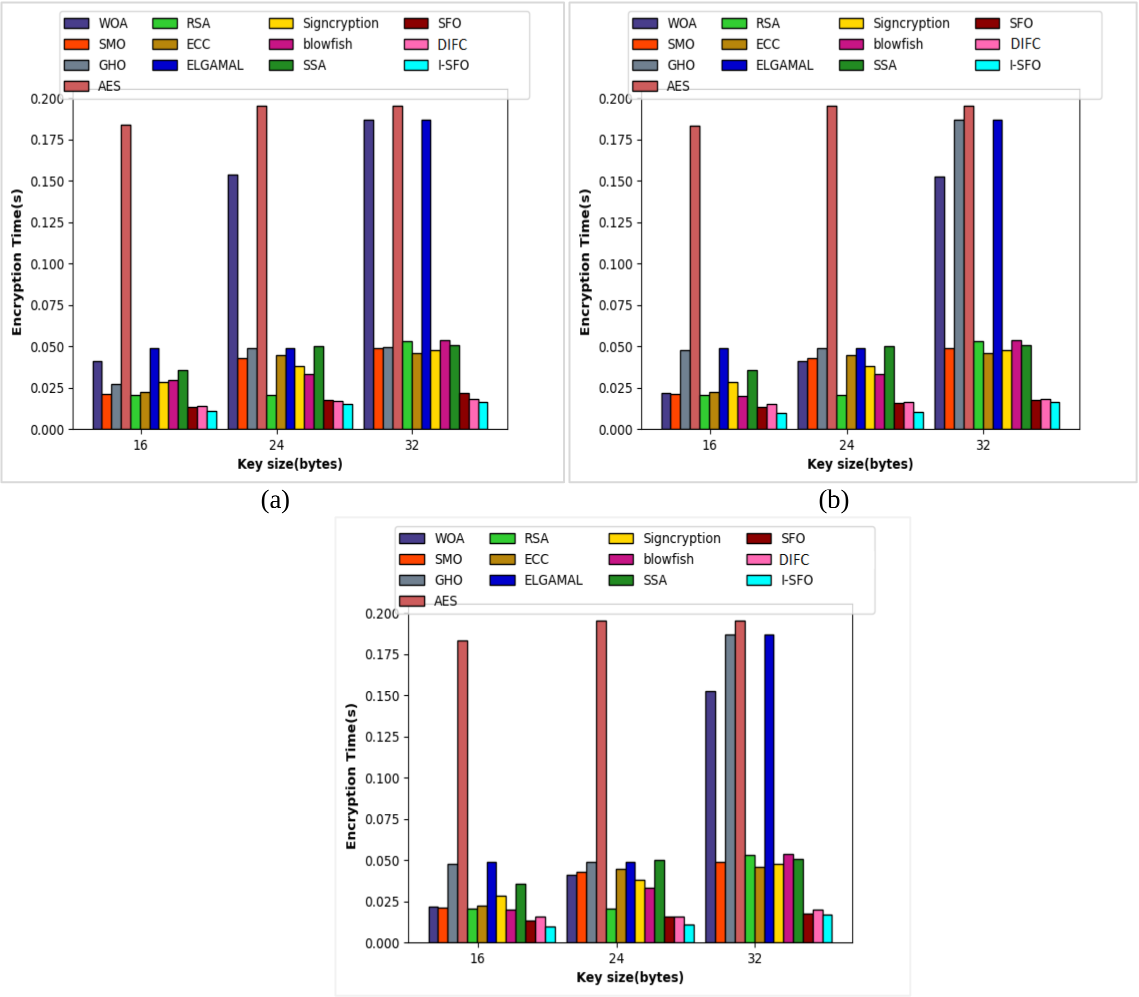
(b)

(c)

**Figure 10** Analysis of decryption time of I-SFO at W=200 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset

***Analysis at encryption time***

The encryption time of the Multi-tenant decentralized information flow control (MT-DIFC)+Improved Signcryption+ I-SFO is evaluated over the existing models like MT-DIFC+Improved Signcryption+ WOA, MT-DIFC+ Improved Signcryption+ SMO, MT-DIFC+ Improved Signcryption+ GHO, MT-DIFC+AES, MT-DIFC+RSA, MT-DIFC+ECC, MT-DIFC+ELGAMAL, MT-DIFC+Signcryption, MT-DIFC+blowfish, MT-DIFC+ Improved Signcryption+ SSA, MT-DIFC+ Improved Signcryption+ SFO, and DIFC with improved signcryption + DIFC [30], respectively. All these evaluations have been carried out by fixing W=100, 150 and 200 in the heart disease dataset, lung cancer dataset and breast cancer dataset. The encryption time analysis of a heart disease dataset, lung cancer dataset and breast cancer dataset at W =100, 150 and 200 is shown in *Figure 11*, *Figure 12* and *Figure 13*, respectively. On observing the outcomes, the encryption time consumed by MT-DIFC+Improved Signcryption+ I-SFO is found to be lower than the other WOA, GHO, SSO, SMO,SFO, and DIFC[30].

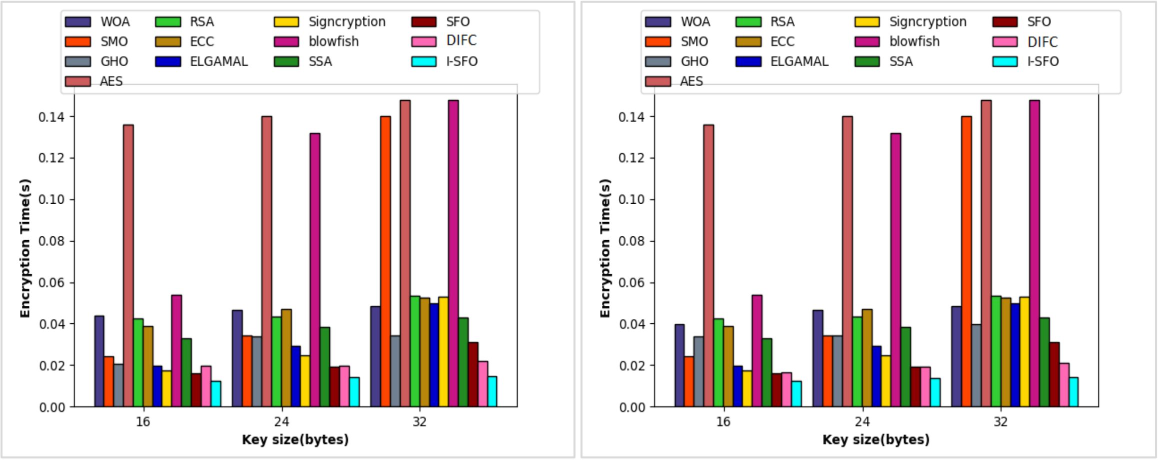


(a)

(b)

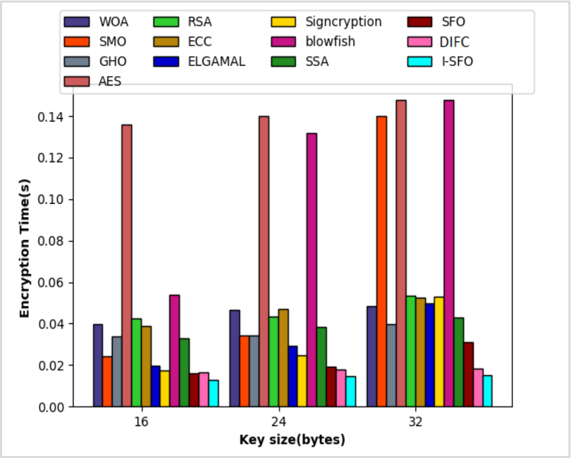
(c)

**Figure 11** Analysis of encryption time of I-SFO at W =100 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset



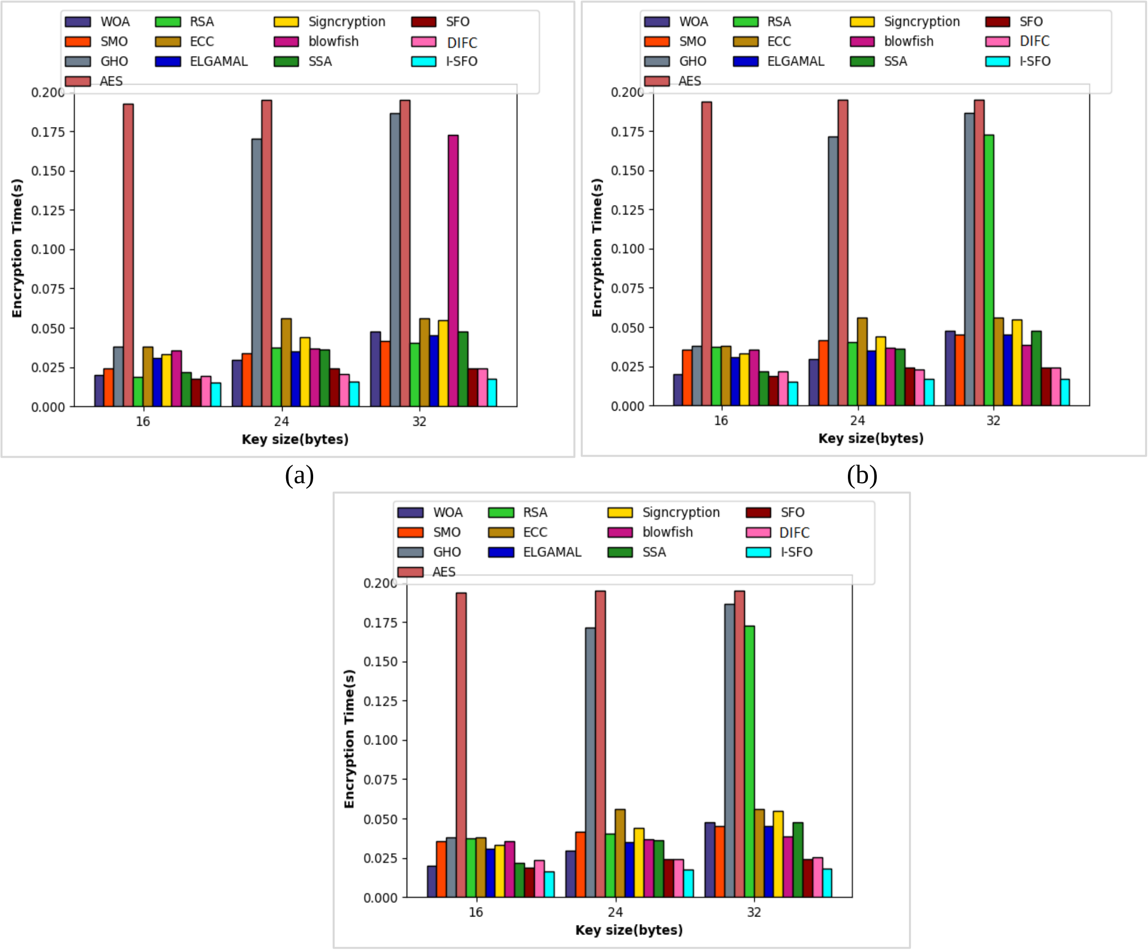
(a)

(b)



(c)

**Figure 12** Analysis of encryption time of I-SFO at W=150 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset



(a)

(b)

(c)

**Figure 13** Analysis of encryption time of I-SFO at W =200 for (a) heart disease dataset (b) breast cancer dataset and (c) lung cancer dataset

### *T-test, P-test and Wilcoxon test analysis*

The T-test Analysis, P-test and Wilcoxon test Analysis of I-SFO is compared over WOA, GHO, SSO, SMO and SFO, respectively. All these evaluations have been made by fixing W =100, 150 and 200 in the heart disease dataset, lung cancer dataset and breast cancer dataset, diabetes dataset, respectively. The results acquired T-test Analysis, P-test and Wilcoxon test for heart disease dataset at W =100, W =150 and W =200 is shown in *Table 1* to *Table 3*, respectively. In addition, results acquired T-test analysis, P-test and Wilcoxon test for breast cancer disease dataset at W =100, W =150 and W =200 is shown in *Table 4* to *Table 6*, respectively. The results acquired T-test analysis, P-test and Wilcoxon test for lung cancer dataset at W =100, W =150 and W =200 is shown in *Table 6* to *Table 9*, respectively. The results acquired T-test analysis, P-test and Wilcoxon test for diabetes dataset at W =100, W =150 and W =200 is shown in *Table 10* to *Table 12*, respectively. A complete list of abbreviations is shown in *Appendix I*.

**Table 1** T-test, P-test and Wilcoxon test analysis of heart disease dataset at W=100

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 2Xe$^{+16}$ | 0 | 2 Xe$^{-06}$ |
| GHO | 1 Xe$^{+02}$ | 7 Xe$^{+-54}$ | 2 Xe$^{-06}$ |
| SSO | 1 Xe$^{+01}$ | 2 Xe$^{-13}$ | 2 Xe$^{-06}$ |
| SMO | 1 Xe$^{+01}$ | 6 Xe$^{+16}$ | 2 Xe$^{-06}$ |
| SFO | 2 | 2 Xe$^{-04}$ | 7 Xe$^{-04}$ |
| PRO | -4 | 4 Xe$^{-02}$ | 6 Xe$^{-01}$ |

**Table 2** T-Test, P-Test and Wilcoxon test analysis of heart disease dataset at W=150

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 4.0424 | 0.0002 | 0.0000 |
| GHO | 3.3697 | 0.0017 | 0.0000 |
| SSO | 1.5110 | 0.1391 | 0.0000 |
| SMO | -0.2364 | 0.1260 | 0.0121 |
| SFO | 6.3626 | 0.0000 | 0.0000 |
| PRO | -1.5643 | 0.8144 | 0.1231 |

**Table 3** T-test, P-Test and Wilcoxon test analysis of heart disease dataset at W=200

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 5.762 | 0.000 | 0.000 |
| GHO | 16.691 | 0.000 | 0.000 |
| SSO | 18.232 | 0.000 | 0.000 |
| SMO | 5.468 | 0.000 | 0.000 |
| SFO | 177.281 | 0.000 | 0.000 |
| PRO | 0.693 | 0.493 | 0.294 |

**Table 4** T-Test, P-Test and Wilcoxon test analysis of lung cancer dataset at W=100

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 56.89418 | 2.18 Xe$^{-38}$ | 1.91 Xe$^{-06}$ |
| GHO | -4.08278 | 0.000221 | 0.012079 |
| SSO | 5.670557 | 1.61 Xe$^{-06}$ | 1.91 Xe$^{-06}$ |
| SMO | 1.318808 | 0.000206 | 0.012079 |
| SFO | 3.356047 | 0.001805 | 0.002325 |
| PRO | -4.10523 | 0.195126 | 0.153646 |

**Table 5** T-test, P-test and Wilcoxon test analysis of lung cancer dataset at W=150

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 13.375 | 0.000 | 0.000 |
| GHO | 5.267 | 0.000 | 0.000 |
| SSO | 13390.147 | 0.000 | 0.000 |
| SMO | -0.576 | 0.000 | 0.001 |
| SFO | 5.969 | 0.000 | 0.000 |
| PRO | -6.694 | 0.568 | 0.097 |

**Table 6** T-test, P-test and Wilcoxon test analysis of lung cancer dataset at W=200

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 7 Xe$^{+15}$ | 0 | 2 Xe$^{-06}$ |
| GHO | 3 | 1Xe$^{-02}$ | 2 Xe$^{-06}$ |
| SSO | 1 | 1 Xe$^{-02}$ | 2 Xe$^{-01}$ |
| SMO | 4 | 3 Xe$^{-04}$ | 2 Xe$^{-06}$ |
| SFO | 7 Xe$^{+15}$ | 0 | 2 Xe$^{-06}$ |
| PRO | -2 | 3 Xe$^{-01}$ | 3 Xe$^{-01}$ |

**Table 7** T-test, P-test and Wilcoxon test analysis of breast cancer dataset at W=100

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 180.788 | 0.000 | 0.000 |
| GHO | 30.426 | 0.000 | 0.000 |
| SSO | 6.795 | 0.000 | 0.000 |
| SMO | 13.503 | 0.000 | 0.000 |
| SFO | 11.876 | 0.000 | 0.000 |
| PRO | 6.604 | 0.000 | 0.000 |

**Table 8** T-test, P-test and Wilcoxon test analysis of breast cancer dataset at W=150

| Method | t-test | p-test | Wilcoxon test |
|---|---|---|---|
| WOA | 69.49 | 0.00 | 0.00 |
| GHO | 22.31 | 0.00 | 0.00 |
| SSO | 18.10 | 0.00 | 0.00 |
| SMO | 12.34 | 0.00 | 0.00 |
| SFO | 10.30 | 0.00 | 0.00 |
| PRO | 9.58 | 0.00 | 0.00 |

**Table 9** T-test, P-test and Wilcoxon test analysis of breast cancer dataset at W=200

| **Method** | **t-test** | **p-test** | **Wilcoxon test** |
|---|---|---|---|
| WOA | 5 Xe$^{+16}$ | 0 | 2 Xe$^{-06}$ |
| GHO | 7 | 2 Xe$^{-08}$ | 2 Xe$^{-06}$ |
| SSO | 8 | 1 Xe$^{-09}$ | 2 Xe$^{-06}$ |
| SMO | 2 Xe$^{+1}$ | 4 Xe$^{-23}$ | 2 Xe$^{-06}$ |
| SFO | 7 | 1 Xe$^{-08}$ | 2 Xe$^{-06}$ |
| PRO | 7 | 1 Xe$^{-07}$ | 2 Xe$^{-06}$ |

**Table 10** T-test, P-test and Wilcoxon test analysis of diabetes dataset at W=100

| **Method** | **t-test** | **p-test** | **Wilcoxon test** |
|---|---|---|---|
| WOA | 175.645 | 0.000 | 0.000 |
| GHO | 28.315 | 0.000 | 0.000 |
| SSO | 5.795 | 0.000 | 0.000 |
| SMO | 12.541 | 0.000 | 0.0112 |
| SFO | 105.563 | 0.000 | 0.0000 |
| PRO | 7.512 | 0.000 | 0.1321 |

**Table 11** T-test, P-test and Wilcoxon test analysis of diabetes dataset at W=150

| **Method** | **t-test** | **p-test** | **Wilcoxon test** |
|---|---|---|---|
| WOA | 70.72 | 0.00 | 0.00 |
| GHO | 19.12 | 0.00 | 0.00 |
| SSO | 18.10 | 0.00 | 0.00 |
| SMO | 11.29 | 0.00 | 0.00 |
| SFO | 11.42 | 0.00 | 0.00 |
| PRO | 10.40 | 0.00 | 0.00 |

**Table 12** T-test, P-test and Wilcoxon test analysis of diabetes dataset at W=200

| **Method** | **t-test** | **p-test** | **Wilcoxon test** |
|---|---|---|---|
| WOA | 4 Xe$^{+14}$ | 1.58 Xe$^{-05}$ | 2 Xe$^{-06}$ |
| GHO | 6 | 1 Xe$^{-08}$ | 2 Xe$^{-06}$ |
| SSO | 7 | 2 Xe$^{-09}$ | 2 Xe$^{-06}$ |
| SMO | 3 Xe$^{+2}$ | 41Xe$^{-21}$ | 2 Xe$^{-06}$ |
| SFO | 6 | 1 Xe$^{-08}$ | 2 Xe$^{-06}$ |
| PRO | 6 | 1 Xe$^{-07}$ | 2 Xe$^{-06}$ |

## 5.Discussion

This paper proposed a new MT-DIFC model using an I-SFO. Here, to analyze the effectiveness of the I-SFO algorithm the weight function is varied from 100, 150, and 200. The proposed MT-DIFC model with improved signcryption+ I-SFO has been compared with traditional models in terms of encryption timer, decryption time, turnaround time, known plain text attack, key sensitivity and convergence analysis. The evaluation was carried out using heart disease, lung cancer, and breast cancer, respectively.

- It can be noticed that the presented method has attained less cost when fixing =100, 150 and 200.
- The I-SFO is said to be highly convergent over the existing models, and so it is suggested as an optimal solution for appropriate key generation.
- Thus, the proposed model has obtained the objective function.
- In terms of decryption time, the proposed work has accomplished the least decryption time for the heart disease dataset, lung cancer dataset and breast cancer dataset under every variation in weight function.
- The encryption time the time consumed by the proposed model is found to be lower than the other existing state-of-art models, due to the security level based identification of the sensitive data and encrypting the sensitive data via the optimal key.
- The MT-DIFC+Improved Signcryption+ I-SFO is said to be highly efficient over the existing models.
- On observing the outcomes, the encryption time consumed by MT-DIFC+Improved Signcryption+ I-SFO is found to be lower than the other WOA, GHO, SSO, SMO, SFO, and DIFC[30].
- Our proposed model will be improved in the future in terms of energy efficiency and lesser time consumption. Furthermore, these improvements will facilitate compliance with cloud policies.

## 6.Conclusion and future work

This paper had projected a novel MT-DIFC framework. Initially, the data owner’s sensitive data have been segregated from the original data. These sensitive data have been identified based on the security level. Then, these sensitive data are subjected to encryption via an improved signcryption algorithm. At the receiver end, the decryption takes places based on the computed two-level Trust model. Interestingly, here the direct and indirect trust is computed for the ones who requests for access privileges to the data owners. Based on the computed trust level, the access privilege is provided to the user’s request; and here the level of document readability and downloading capability will be decided by the data owner. Based on the computed trust level, the decryption of the data (only the permitted data-level access provided by the owner) is accomplished. Furthermore, the (I-SFO) has been introduced for optimal key generation. This I-SFO model is validated by varying its weight function from 100, 150 and 200, respectively. In addition, a non-parametric analysis has been carried out to validate the efficiency of I-SFO. Client data can be retained private and secure using the proposed architecture. However, the inability to regulate data, a lack of access into data, and data theft in the cloud are all real limits of this approach. This work will be extended in the future to improve database usability by extending IFC.

## Acknowledgment

None.

## Conflicts of interest

The authors have no conflicts of interest to declare.

## Author's contributions statement

**Yogesh B. Gurav:** Conceptualization, investigation, writing original draft, data collection. **Bankat M. Patil:** Conceptualization, analysis and interpretation of results.

## References

[1] Elsayed M, Zulkernine M. IFCaaS: information flow control as a service for cloud security. In international conference on availability, reliability and security 2016 (pp. 211-6). IEEE.

[2] Bacon J, Eyers D, Pasquier TF, Singh J, Papagiannis I, Pietzuch P. Information flow control for secure cloud computing. IEEE Transactions on Network and Service Management. 2014; 11(1):76-89.

[3] Xi N, Sun C, Ma J, Shen Y. Secure service composition with information flow control in service clouds. Future Generation Computer Systems. 2015; 49:142-8.

[4] Xi N, Ma J, Sun C, Lu D, Shen Y. Information flow control on encrypted data for service composition among multiple clouds. Distributed and Parallel Databases. 2018; 36(3):511-27.

[5] Khurshid A, Khan AN, Khan FG, Ali M, Shuja J, Khan AU. Secure-CamFlow: a device-oriented security model to assist information flow control systems in cloud environments for IoTs. Concurrency and Computation: Practice and Experience. 2019; 31(8).

[6] Phatak A, Kadikar R, Vijayan K, Amutha B. Performance analysis of firewall based on SDN and OpenFlow. In international conference on communication and signal processing 2018 (pp. 0611-5). IEEE.

[7] Candotti D, Steel MD, West AC. Charting the course for Tasmania's energy cloud roadmap. In PES Asia-pacific power and energy engineering conference 2015 (pp. 1-5). IEEE.

[8] Huang G, Chen J, Khojasteh Y. A cyber-physical system deployment based on pull strategies for one-of-a-kind production with limited resources. Journal of Intelligent Manufacturing. 2021; 32(2):579-96.

[9] Bolodurina I, Parfenov D, Shukhman A. Approach to the effective controlling cloud computing resources in data centers for providing multimedia services. In international Siberian conference on control and communications 2015 (pp. 1-6). IEEE.

[10] Li W, Wu J, Cao J, Chen N, Zhang Q, Buyya R. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. Journal of Cloud Computing. 2021; 10(1):1-34.

[11] Xu Z, Zhang Y, Li H, Yang W, Qi Q. Dynamic resource provisioning for cyber-physical systems in cloud-fog-edge computing. Journal of Cloud Computing. 2020; 9(1):1-16.

[12] Pierson JM, Baudic G, Caux S, Celik B, Da CG, Grange L, et al. DATAZERO: datacenter with zero emission and robust management using renewable energy. IEEE Access. 2019; 7:103209-30.

[13] Singh J, Pasquier TF, Bacon J, Eyers D. Integrating messaging middleware and information flow control. In international conference on cloud engineering 2015 (pp. 54-9). IEEE.

[14] Zhou L, Zhang H, Zhang K, Wang B, Shen D, Wang Y. Advances in applying cloud computing techniques for air traffic systems. In 2nd international conference on civil aviation safety and information technology 2020 (pp. 134-9). IEEE.

[15] Nakamura S, Enokido T, Takizawa M. Implementation and evaluation of the information flow control for the internet of things. Concurrency and Computation: Practice and Experience. 2021; 33(19).

[16] Kim N, Yang D. Performance analysis of a centralized burst-mode traffic shaping for distributed parallel queues. IEEE Communications Letters. 2015; 19(3):351-4.

[17] Solanki N, Zhu W, Yen IL, Bastani F, Rezvani E. Multi-tenant access and information flow control for SaaS. In international conference on web services 2016 (pp. 99-106). IEEE.

[18] Enokido T, Takizawa M. A purpose-based synchronization protocol for secure information flow control. International Journal of Computer Systems Science and Engineering. 2010; 25(2):25-32.

[19] Wang C, Chow SS, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers. 2011; 62(2):362-75.

[20] Bauereiß T, Gritti AP, Popescu A, Raimondi F. CoSMeDis: a distributed social media platform with formally verified confidentiality guarantees. In symposium on security and privacy 2017 (pp. 729-48). IEEE.

[21] Pasquier TF, Eyers D. Information flow audit for transparency and compliance in the handling of personal data. In international conference on cloud engineering workshop 2016 (pp. 112-7). IEEE.

[22] Pasquier TF, Powles JE. Expressing and enforcing location requirements in the cloud using information flow control. In international conference on cloud engineering 2015 (pp. 410-5). IEEE.

[23] Pasquier TF, Singh J, Eyers D, Bacon J. CamFlow: managed data-sharing for cloud services. IEEE Transactions on Cloud Computing. 2015; 5(3):472-84.

[24] Pasquier TF, Singh J, Bacon J, Eyers D. Information flow audit for PAAS clouds. In international conference on cloud engineering 2016 (pp. 42-51). IEEE.

[25] Sree TR, Bhanu S. Detection of http flooding attacks in cloud using dynamic entropy method. Arabian Journal for Science and Engineering. 2018; 43(12):6995-7014.

[26] Wang Y, Li J, Wang HH. Cluster and cloud computing framework for scientific metrology in flow control. Cluster Computing. 2019; 22(1):1189-98.

[27] Lu X, Cao L, Du X. Dynamic control method for tenants' sensitive information flow based on virtual boundary recognition. IEEE Access. 2020; 8:162548-68.

[28] Bs R, Nv NK, Shyamasundar RK. Towards unifying RBAC with information flow control. In proceedings of the 26th ACM symposium on access control models and technologies 2021 (pp. 45-54).

[29] Seifermann S, Heinrich R, Werle D, Reussner R. Detecting violations of access control and information flow policies in data flow diagrams. Journal of Systems and Software. 2022.

[30] Moussaid NE, Azhari ME. Enhance the security properties and information flow control. International Journal of Electronic Business. 2020; 15(3):249-74.

[31] Zhang Z, Yang Z, Du X, Li W, Chen X, Sun L. Tenant-led ciphertext information flow control for cloud virtual machines. IEEE Access. 2021; 9:15156-69.

[32] Li L. The control method of big data information flow based on semantic characteristics in cloud computing environment. Journal of Interconnection Networks. 2022.

[33] Lu J, Sun J, Xiao R, Jin S. DIFCS: a secure cloud data sharing approach based on decentralized information flow control. Computers & Security. 2022.

[34] Gurav YB, Patil BM. Two-fold improved poor rich optimization algorithm based de-centralized information flow control for cloud virtual machines: an algorithmic analysis. In international conference on smart systems and inventive technology 2022 (pp. 417-25). IEEE.

**Yogesh B. Gurav** His research activities are currently twofold : while the first research activity is set to explore the Protection and Authentication of Issues in Wireless and ADHOC Networks in Epidemic Conditions ; the second major research theme that he is pursuing is focused on De-Centralized Information Flow Control for Cloud Virtual Machines with Hybrid AES- ECC and Improved Meta-Heuristic Optimization based optimal Key generation.He has also presented various academic as well as research-based papers in several national and international conferences and journals including the " Proceeding of First Doctoral Symposium on Natural Computing Research,2020 Lecture Notes in Networks and Systems 169, under exclusive license to Springer Nature Singapore. His areas of research interest are Cloud Computing and Data Security.

Email: ybgurav1977@gmail.com

**Dr. Bankat M. Patil** received his Ph.D. degree in Computer Science (Data Mining) from Indian Institute of Technology, Roorkee (India) in November 2011. He is currently working as Professor in Computer Science and Engineering in MBES's College of Engineering, Ambajogai. His research interests are generally in the areas of Data Mining, Soft Computing, Decision Support System in Medicine, Computer Networking, Cloud Computing. He has also presented various academic as well as research-based papers in several national and international conferences and journals.

Email: patilbankat@gmail.com

## Appendix I

| S. No. | Abbreviation | Description |
|---|---|---|
| 1 | AES | Advanced Encryption Standard |
| 2 | CA | Central Authority |
| 3 | CPU | Central Processing Unit |
| 4 | CS | Cloud Server |
| 5 | CSP | Cloud Service Provider |
| 6 | DS | Data Store |
| 7 | DIFC | Decentralized Information Flow Control |
| 8 | ECC | Elliptic Curve Cryptosystems |
| 9 | EP | Encryption Proxy |
| 10 | FNA | Fine Needle Aspirate |
| 11 | GHO | Grasshopper Optimization Algorithm |
| 12 | I-SFO | Improved Sun Flow Optimization Algorithm |
| 13 | IFC | Information Flow Control |
| 14 | IFCaaS | Information Flow Control as a Service |
| 15 | IT | Information Technology |
| 16 | MT-DIFC | Multi-Tenant Decentralized Information Flow Control |
| 17 | SecaaS | Security as a Service |
| 18 | SSO | Salp Swarm Optimization Algorithm |
| 19 | SMO | Spider Monkey Optimization Algorithm |
| 20 | SaaS | Software as a Service |
| 21 | SFO | Sun Flow Optimization Algorithm |
| 22 | TF-IPRO | Two-Fold Improved Poor Rich Optimization |
| 23 | WOA | Whale Optimization Algorithm |