Received: May 25, 2023. Revised: July 4, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Improved Sunflower Optimization Algorithm Based Encryption with Public Auditing Scheme in Secure Cloud Computing

M. Mageshwari[1] **R. Naresh**[2]*

[1]*Department of Computer Science and Engineering, SRM Institute of Science and Technology,*
Kattankulathur, Chengalpattu, Chennai, Tamilnadu, 603 203, India
[2]*Department of Networking and Communications, SRM Institute of Science and Technology,*
Kattankulathur, Chengalpattu, Chennai, Tamilnadu, 603 203, India
*Corresponding author's Email: nareshr@srmist.edu.in

Abstract: Cloud computing (CC) is a pivotal technology in the entire universe. Cloud platforms allow management applications or administrators with privileged accounts to remotely do privileged activities for particular tasks like eliminating virtual hosts. If private accounts can be leaked and perform a dangerous confidential activity, severe security issues are performed in cloud environments. To sort out these issues, researchers focused on auditing the behaviours of private users. But it was found to be tough to audit fine-grained privileged behaviours automatically for the graphical operating system. Also, it is difficult to prevent users from avoiding the audit mechanism or preventing hackers from attacking the audit method. Therefore, this study presents a new improved sunflower optimization algorithm based encryption with public auditing scheme (ISFOAE-PAS) in the secure cloud environment. The major intention of the ISFOAE-PAS technique lies in the accomplishment of data security, integrity, and auditing in the cloud environment. In addition, the ISFOAE-PAS technique designs a new secret image encryption using the homomorphic encryption (SIE-HE) technique to encrypt the data. Moreover, the ISFO algorithm is derived for optimally choosing the keys related to the SIE-HE technique. Furthermore, the public auditing scheme is designed to improve security in the cloud environment. Finally, the DDoS attack detection process is performed by a deep convolutional autoencoder (DCAE). For demonstrating the greater efficiency of the ISFOAE-PAS technique, a series of simulations were involved. The experimental values inferred that the ISFOAE-PAS technique reaches maximum accuracy of 99.42%.

Keywords: Auditing, Cloud computing, Security, Encryption technique, Sunflower optimization algorithm.

1. Introduction

CC brings great ease by allowing applications and users to access diverse services remotely [1]. In addition to general users communicating with cloud storage (CS), the administrator's applications with private accounts frequently accomplish private activity to do particular tasks like downloading database files and deleting virtual hosts [2]. Cloud data are widely dispersed by cloud storage providers (CSP) on a cloud network. Cloud users can share their desired data within the group by sharing the data services. This mitigated the complexity of data storage [3]. Also, the users could not able to control the storage capacity manually. Further, certain faults can imperil the data reliability because of human intervention errors and hardware or software [4]. To tackle these issues, CS is imperative while sharing on a cloud network. CC combines different technologies and processes to protect cloud user data. Hence, there occurs competition on the security system providers. Also, various security-wise ambiguities exist which make entities hesitant to completely use CC.

As the number of cloud users are increasing, data sharing increases and data auditing is vital and hence diverse public key (PBK) structure-related models are adopted that results in certificate management problem [4]. Though a certificate-shared auditing method was not efficient in managing dynamic data and preserving data privacy, the verifier is unable to access the data and assure its integrity. Storage services are rendered without the interaction of humans with the increasing CSs. Hence, ensuring data integrity becomes essential. If a group members upload a file, others in the group could modify and access it. The integrity of saved data uses RDPC methods to produce an authentication tag for all blocks. With the tag correctness, the data status can be verified. In block upgrading, the regeneration of the tag becomes another challenge. Authentication tag generated during auditing rises the checking complexities. Also, the group can be dynamic in such a way the user revocation should be solved. Those revoking all their PVK or PBK are invalid. CC benefitted the user concerning cost, ease of access, and scalability. A huge CSP is identifying difficulty in managing malicious aggressors. Metaheuristics are presently preferrable like guided pelican algorithm (GPA) [5], stochastic komodo algorithm (SKA) [6], extended stochastic coati optimizer (ESCO) [7], attack-leave optimizer (ALO) [8], quad tournament optimizer (QTO) [9], multiple interaction optimizer (MIO) [10], etc.

This study introduces a new improved sunflower optimization algorithm-based encryption with public auditing scheme (ISFOAE-PAS) in the secure cloud environment. The major intention of the ISFOAE-PAS technique lies in the accomplishment of data security, integrity, and auditing in the cloud environment. In addition, the ISFOAE-PAS technique designs a new secret image encryption using the homomorphic encryption (SIE-HE) technique to encrypt the data. Moreover, the ISFO algorithm is derived for optimally choosing the keys related to the SIE-HE technique. Furthermore, the public auditing scheme is designed to improve security in the cloud environment. Finally, the DDoS attack detection process is performed by a deep convolutional autoencoder (DCAE). For demonstrating the greater result of the ISFOAE-PAS technique, a series of simulations were involved.

The remaining sections of the article is arranged as. Section 2 and 3 offers the literature review and the proposed method. Section 4 elaborates the results evaluation and Section 5 completes the work.

2. Related works

Song et al. [11] introduce a novel method that combines integrity auditing and safe de-duplication in encoded CS. This prevents the CSP and protected the ownership privacy in forging the auditing outcomes for low-entropy datasets. Further, the author devised a BC-based system that minimizes the locally stored key cost and helps to assure key recoverability. Wang et al. [12] devised an arbitrable data auditing method related to the BC. In this, clients should conduct public and private audits by triggering smart contract if authentication failed in private auditing. This fusion auditing model enabled clients to receive compensation by saving audit fees automatically in a prompt manner if the CSP corrupts the outsourced dataset. Tian et al. [13] devised a BC-related safe de-duplication and shared auditing method in decentralized storing. This method uses a new de-duplication protocol to attain potential space saving while safeguarding operators from data loss under fake attacks and single points of failure. Further, it might reduce the storage and computational cost of metadata by presenting an update protocol and lightweight authenticator generation method.

Zhang et al. [14] modelled a BC-related multi-cloud stored data audit method to safeguard data veracity and precisely adjudicate service conflicts. The author not just presents the BC to register the correlations amongst organizers, users, and CSP as evidence in data auditing, but also use the smart contract for finding service dispute for enforcing the untrusted organizers to identify malicious CSPs. Homomorphic verifiable tags and BC are utilized to attain low-cost batch verification without a third-party auditor (TPA). Li et al. [15] presented a model that uses BC approach to verify CS data reliability. In this, two pre-defined entities that could not trust are indulged, and 3rd party auditor for auditing data was eliminated out of 3 participated entities.

Xie et al. [16] presented a novel BC-based proxy-oriented public audit (BBPO-PA) and BB model for low-achieving terminal gadgets. Firstly, a trusted proxy that could upload and process DO's encoded file is presented. Then, BC can be used for smart contracts rather than non-trusted TPA to enhance the stability and integrity of audit outputs. Next, index tables are used to assure dynamic data functions. Bandaru and Visalakshi [17] developed a unique BC-aided audit with the optimum multi-key homomorphic encryption (BEA-OMKHE) approach for public cloud settings. This intends to ensure auditing, data integrity, and CS safety. Also, this approach was abstracted to achieve data integration into the cloud atmosphere by modelling end-wise technique.

3. The proposed model

In this manuscript, a novel ISFOAE-PAS approach for effectually securing the cloud environment using encryption and auditing schemes is presented. The article intends to accomplish data security, integrity, and auditing in the cloud environment. It involves four major processes namely the SIE-HE, ISFO-based optimal key selection, auditing, and DCAE-based DDoS attack detection. Fig. 1 represents the overall procedure of the ISFOAE-PAS system.

3.1 Design of SIE-HE technique

In this article, the SIE-HE model is enforced to encrypt the data in the cloud environment. This model is employed to effectively encrypt the secret data [18]. This model is a cryptosystem that allows to estimate an arithmetical circuit on ciphertext, possibly diverse key encryption. Where $\mathcal{M}$ remains the message space with the arithmetical model. This method takes 5 PPT models (Setup, Eval, KeyGen, Dec, and Enc). Consider that each contributing party has an index to its open and private keys (PVKs). A multi-key cipher text implicitly has arranged set $T = \{id_1, \dots, id_k\}$ of linked reference.

For instance, a new ciphertext $ct \leftarrow$ SIE-HE. $Enc(\mu, pk_{id})$ matches to single-component set $T = \{id\}$ however the dimension of reference achieved better than the computation amongst ciphertext in party development.

- Setup: $pp \leftarrow$SIE-HE. $Setup(1^{\lambda})$. Proceed the secure variable as input and returned the public parameterization. Consider each other method implicitly attains pp as input.
- Key Generation: $(sk, pk) \leftarrow$ SIE-HE. KeyGen (pp). Resulting in a pair of private and PBKs.
- Encrypted: $\leftarrow < KHE.Enc(\mu, pk)$. Encrypt a plaintext $\mu \in M$ and resultant a ciphertext $ct \in \{0,1\}^*$.
- Decrypted: $\mu \leftarrow$ SIE-HE. $Dec(\overline{ct}; \{sk_{id}\}_{id\in T})$. To offer a ciphertext $\overline{ct}$ with the corresponding sequence of a PVK, the outcome is a plaintext μ. The Homomorphic estimation can be defined by Eq. (16):

$$\overline{ct} \leftarrow MKHE.Eva1(C, (\overline{ct}, \dots, \overline{ct}_1), \{pk_{id}\}_{id\in T}) \quad (1)$$

To give a circuit C, the corresponding set of PBKs $\{pk_{id}\}_{id\in T}$ and a tuple of multi-key cipher-text $(\overline{ct}, \dots, \overline{ct}_1)$, resulting in a ciphertext $\overline{ct}$. It mentions that the set is union $T = T_1 \cup \cdots \cup T_\ell$ of reference set T_j of input ciphertext $\overline{ct}_j$ for $1 \le j \le \ell$.

Semantic safety for any 2 communications $\mu_0, \mu_1 \in \mathcal{M}$, the distribution {SIE-HE. $Enc\ (\mu_i; pk)$} for $i = 0,1$ is computationally identical where $pp \leftarrow$SIE-HE. Setup (1^{λ}) and $(sk, pk) \leftarrow$SIE-HE. $KeyGen\ (pp)$. Compactness and correctness. This model has been compressed if the dimensional of ciphertext related to k parties was limited by poly (λ, k) to set a polynomial poly $(\because)$.For $1 \le j \le \ell$, consider ct_j to be ciphertext (with the reference set T_j) such that SIE-HE. $Dec(\overline{ct}, \{sk_{id}\}_{id\in T_j}) = \mu_j$ Consider $C: \mathcal{M}^{\ell} \to \mathcal{M}$ be circuit and $\overline{ct} \leftarrow$ SIE-HE. $Eval(C, (\overline{ct}, \dots, \overline{ct}), \{pk_{id}\}_{id\in T})$ for $T = T_1 \cup \cdots \cup T_\ell$. Then,

$$SIE - HE.Dec(\overline{ct}, \{sk_{id}\}_{id\in T}) = C(\mu_1, \dots, \mu_\ell) \quad (2)$$

3.2 Optimal key selection using ISFO algorithm

The ISFO algorithm is used for optimal key selection. The life process of sunflowers can be probable with the clock point, it can develop and accompany the sun every day [19]. It can be developed in the conflicting direction during night-time, until the subsequent day. Hence, the heat quantity Q_i engaged by every plant is evaluated as:

$$Q_i = \frac{P}{4\pi r_i^2} \quad (3)$$

whereas P and r_i implies the sources energy and the distance between the present optimum and plant i. The sunflower's route toward the sun is stated as:

$$\overrightarrow{S_i} = \frac{X^* - X_i}{\|X^* - X_i\|}, i = 1,2, \dots, n_p \quad (4)$$

The sunflower's stride from the way $\overrightarrow{S_i}$ is defined as:

$$d_i = \lambda \times P_i(\|X_i - X_{i-1}\|) \times \|X_i - X_{i-1}\| \quad (5)$$

Λ refers to the perpetual value which defines the plant's "inertial" movement, and $P_i(X_i - X_{i-1})$ signifies the likelihood of fertilization.

The maximal step can determine in the subsequent approach:

$$d_{\max} = \frac{\|X_{\max} - X_{\min}\|}{2 \times N_{pop}} \quad (6)$$

whereas $X_{\max}$ and $X_{\min}$ represent the maximal and minimal values correspondingly, and N_{pop} demonstrates the entire plant counts.

In the plant population, the state-of-the-art planting could be:

$$\vec{X}_{i+1} = \vec{X}_i + d_i \times \vec{s}_i \quad (7)$$

This technique starts with creating an even or

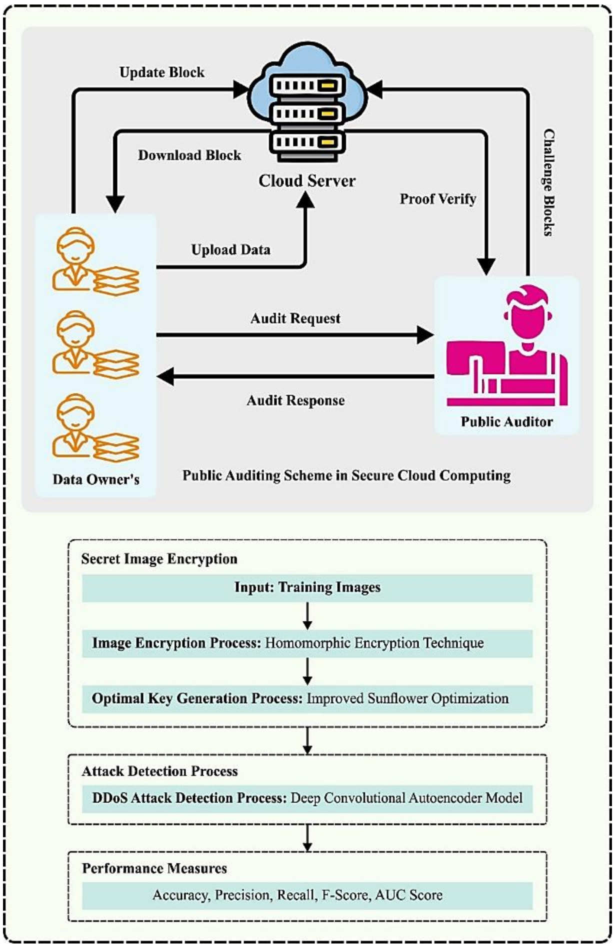

Update Block
Download Block
Cloud Server
Challenge Blocks
Proof Verify
Upload Data
Audit Request
Audit Response
Public Auditor
Data Owner's
Public Auditing Scheme in Secure Cloud Computing
Secret Image Encryption
Input: Training Images
Image Encryption Process: Homomorphic Encryption Technique
Optimal Key Generation Process: Improved Sunflower Optimization
Attack Detection Process
DDoS Attack Detection Process: Deep Convolutional Autoencoder Model
Performance Measures
Accuracy, Precision, Recall, F-Score, AUC Score

Figure. 1 Overall procedure of ISFOAE-PAS system

arbitrary individual populace. The evaluation of every individual allows one to choose that one be transformed as the sun. But it can be planned to contain the possibility to function with many suns in a later version, this study can be projected controlled to one. Next, related to sunflowers, every novel species is become associated with sun and migrate in an arbitrarily controlled fashion.

In the ISFO algorithm, opposition-based learning (OBL) was integrated, which is an optimizer algorithm which enhances the capability of intelligent algorithms to escape from local optimum [20]. Random OBL (ROBL) is an upgraded form of OBL.

$$\hat{x}_j = l_j + u_j - rand \ \times xj, j = 1,2,\cdots,n \quad (8)$$

In Eq. (8) Ld_j and Ud_j denote the lower and upper boundaries of the j - th solution space's dimension), $\hat{x}_j$ symbolizes the outcome of stochastic backward learning, and $rand$ indicates the randomly generated value in zero and one. Meanwhile, the movement of individual flamingos in the FSA model can be inclined mainly by the optimum individual, once it could not escape from the local optima, the value of the last solutions is frequently not ideal, and the inverse outcome is evaluated using the above-mentioned formula is further stochastic than the novel OBL-derived inverse solution that could assist the model to decrease the possibility of getting trapped as local optima.

Meanwhile, the movement of individual flamingos among populations from the searching space can be inclined mainly by the elite individual, thus, the greedy choice of elite individual flamingo might improve the population diversity but speed up the convergence rate. The value of fitness of the newest location of the elite individual at all the iterations is related to the novel location, and when the value of fitness of the newest location is superior to the original location, then the elite individual location can be exchanged with the newest location. Or else, the individual location remains the same.

$$x_i^{t+1} = \begin{cases} x_i^{new}, & if \ f_i^{new} < f_i^{old} \\ x_i^{old}, & if \ f_i^{new} \geq f_i^{old} \end{cases} \quad (9)$$

In Eq. (9), f_i^{new} and f_i^{old} denote the fitness value of elite individual flamingos in novel and new locations, correspondingly. $x_i^{new}\ and\ x_i^{old}$ shows the new and default location of $i\text{-}th$ individuals, and x_i^{t+1} signifies the location of $i\text{-}th$ individual at the $t+1th$ iteration.

3.3 Public auditing scheme

For addressing the integrity problem in CS, the model of data reliability auditing was presented that permits the data owner (DO) for verifying the reliability of outsourced information saved on the CS server (CSS) lack of every download action [21]. For realizing the scale economies from CC, this case utilizes a TPA-related public audit procedure that decreases the DO computational rate and gained any ideal features like batch auditing and dynamic data upgrade. To ensure the DO data integrity, CSS receives the TPA audit and creates an equivalent proof based on the audit task presented by TPA. The CSS is a semi-trusted entity that carries out the equivalent functions based on this procedure among them assumes for providing DOs with the reliability proof without the saved DO novel data intact. Based on DO delegation, TPA shows an integrity audit task to CSS. Once the obtaining of the equivalent proof created by CSS is, TPA defines the medicinal data's integrity by examining the legitimacy of proofs and responds to the audit outcome to DO.

3.4 DDoS attack detection

At the final stage, the DDoS attack detection process is performed by the DCAE model. DCAE integrates the advantages of convolution filtering CNN with unsupervised pre-trained of AEs [22]. Compared to the topology for AEs, but, rather than the fully connected (FC) layer, the encoded comprise convolution layers, and decoded comprises deconvolution layers. Deconvolution filters can be transposed forms of convolution filters; otherwise, as is complete in this case, it can be learned from scratch. Fig. 2 illustrates the infrastructure of DCAE. Furthermore, an un-pooling layer follows all the deconvolution layers. The un-pooling function can be executed by storing the places of maximal values under the pooling, maintaining the values of these places in the un-pooling, and zeroing the remaining. Spatial locality can be retained by integrating a convolutional function at every neuron. Therefore, to provide input matrix P, the encoded calculates as:

$$e_i = \sigma(P * F^n + b) \tag{10}$$

whereas σ implies the activation function, $*$denotes the 2-D convolutional, F^n represents the nth 2-D convolution filters and b indicates the encoded bias. For retaining spatial resolution, zero padding can be executed to input matrix P. Afterward, the rebuilding was attained as:

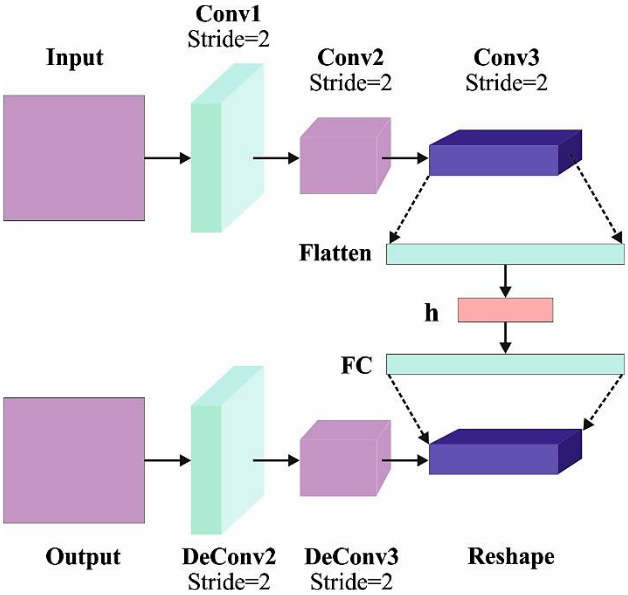


Figure. 2 Structure of DCAE

$$z_i = \sigma\left(e_i * \tilde{F}^n + \tilde{b}\right). \tag{11}$$

At this point, z_i implies the reconstruction of ith input, Fen refers to the nth 2-D convolution filters from decoded and $\tilde{b}$ denotes the bias of decoding. Unsupervised pre-trained was carried out to the network to minimize the subsequent formula:

$$E(\theta) = \sum_{i=1}^{m}(x_i - z_i)^2 \tag{12}$$

Next unsupervised pre-trained the un-pooling and deconvolution layers, the network's decoded portion can be eliminated and FC layers and softmax classifier can be supplemented within the network.

4. Results and discussion

In this segment, the security achievement of the ISFOAE-PAS model in the cloud environment is assessed in detail. In Table 1 and Fig. 3, an overall comparative Encryption Time (ET) result of the ISFOAE-PAS technique with recent models is given. The results identified that the ISFOAE-PAS technique reaches the least ET values under large and small datasets.

For instance, on a large dataset, the ISFOAE-PAS technique attains decreasing ET of 0.5632s while the AES, DES, RSA, BEA-OMKHE, and Blowfish approaches obtain increasing ET of 1.0353s, 1.5936s,

Table 1. ET analysis of ISFOAE-PAS approach with the recent system under two datasets

Encryption Time (sec)						
Test Dataset	DES	RSA	Blowfish	AES	BEA-OMKHE	ISFOAE-PAS
Large Dataset						
TS1	1.1068	1.5840	2.0792	0.5315	1.2015	0.8622
TS2	1.2585	1.3473	1.1127	0.3464	0.8741	0.2141
TS3	0.4450	1.1521	0.1013	2.7858	0.1913	0.5103
TS4	0.9006	1.3115	0.0191	1.8367	0.4491	0.3059
TS5	1.4655	2.5733	1.7681	1.9077	0.6264	0.9236
Average	1.0353	1.5936	1.0161	1.4816	0.6685	0.5632
Small Dataset						
TS6	0.0142	0.0184	0.009	0.0081	0.0123	0.0072
TS7	0.007	0.0036	0.0083	0.0185	0.0035	0.0045
TS8	0.0064	0.0028	0.0032	0.0068	0.0002	0.0003
TS9	0.0112	0.0072	0.0146	0.0082	0.0073	0.0072
TS10	0.014	0.0123	0.0319	0.0114	0.0028	0.0027
Average	0.01056	0.00886	0.0134	0.0106	0.00522	0.00438

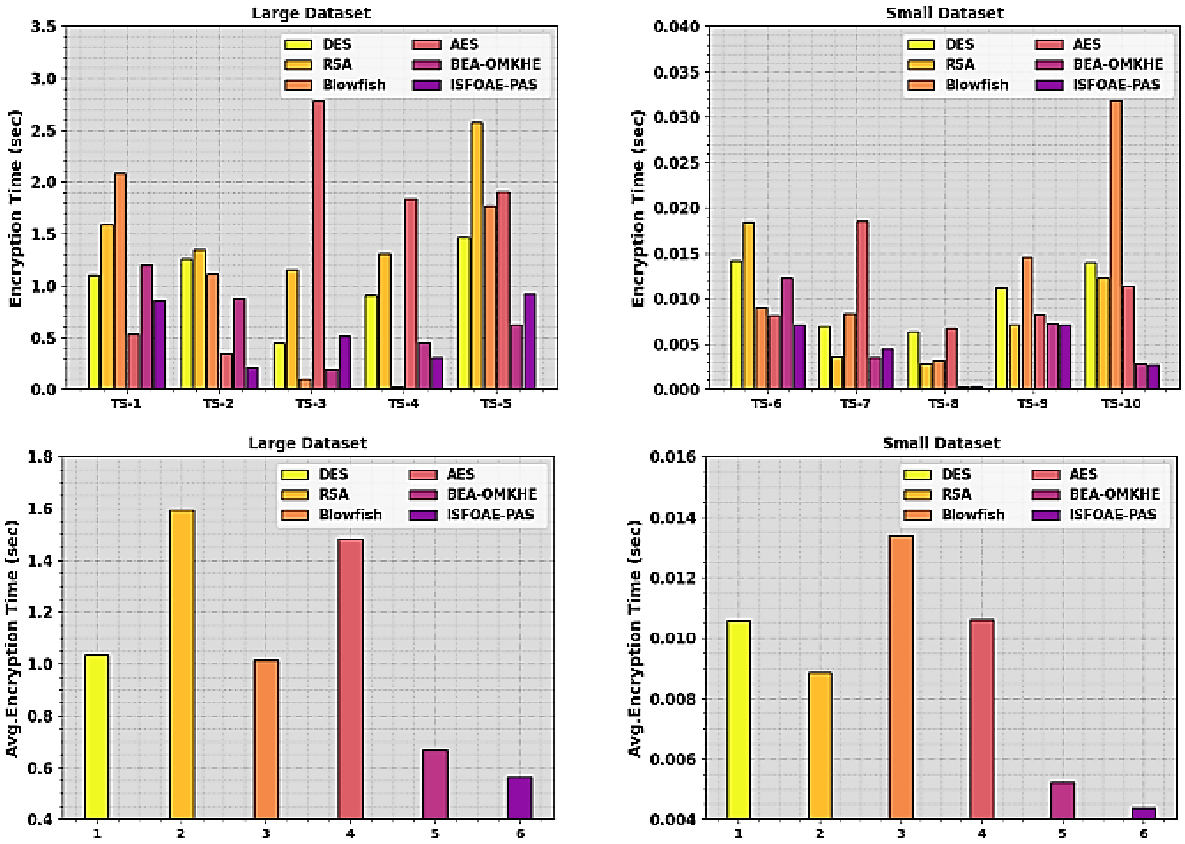


Figure. 3 Large dataset ET and average ET and small dataset ET and average ET

Table 2. DT evaluation of the ISFOAE-PAS model with the current system under two datasets [17]

Decryption Time (sec)						
Test Dataset	DES	RSA	Blowfish	AES	BEA-OMKHE	ISFOAE-PAS
Large Dataset						
TS1	2.0024	1.8874	0.2358	2.2432	1.3580	1.2742
TS2	0.7768	2.6773	0.3113	2.1995	1.7352	1.6913
TS3	0.0423	2.0750	0.5928	0.2307	0.5961	0.2223
TS4	1.1198	0.3535	2.1924	1.3129	0.2555	0.0065
TS5	1.2669	3.2478	1.2249	2.5141	0.9080	0.1180
Average	1.0416	2.0482	0.9114	1.7001	0.9706	0.6625
Small Dataset						
TS6	0.0037	0.0088	0.0127	0.0096	0.0087	0.0035
TS7	0.0099	0.0071	0.0086	0.0083	0.0028	0.0027
TS8	0.0126	0.0035	0.0123	0.0100	0.0069	0.0036
TS9	0.0191	0.0067	0.0043	0.0022	0.0139	0.0023
TS10	0.0039	0.0290	0.0105	0.0139	0.0069	0.0038
Average	0.0098	0.0110	0.0097	0.0088	0.0078	0.0032

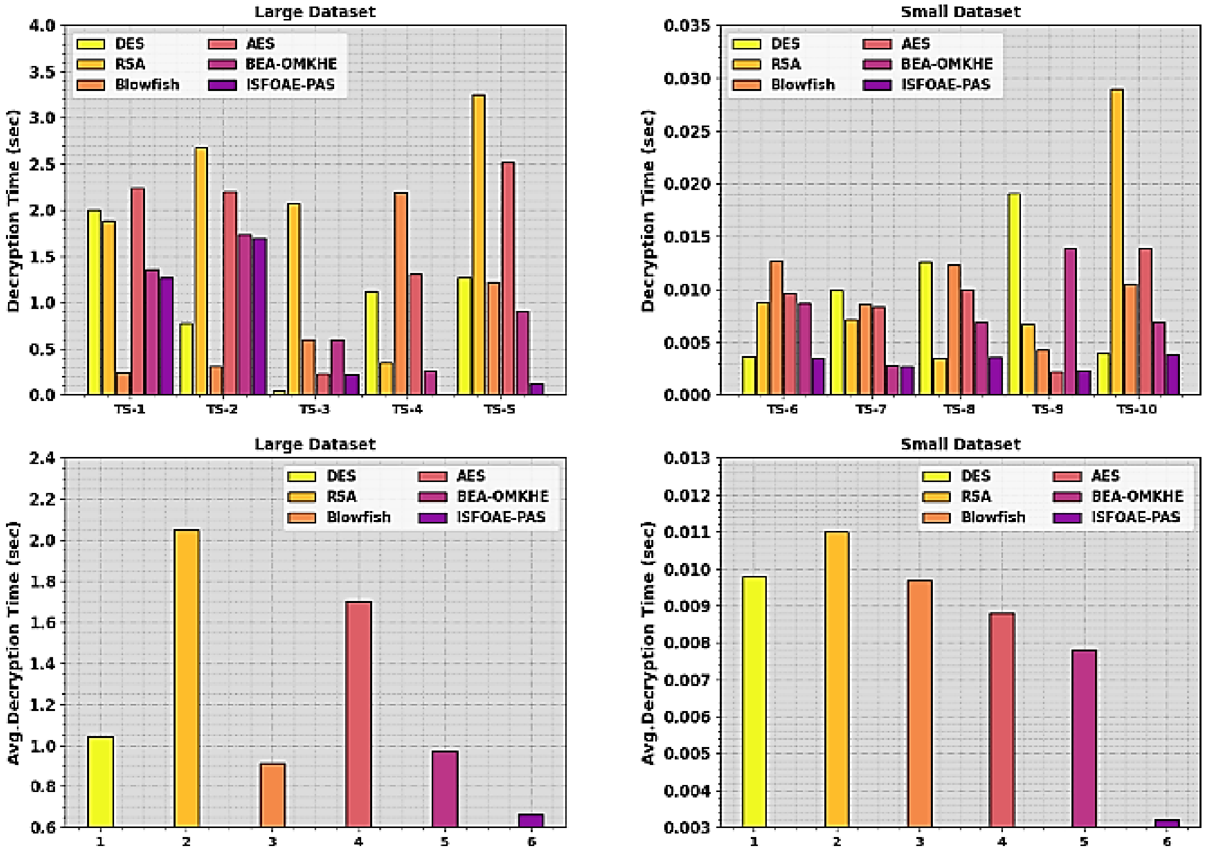


Figure. 4 Large dataset DT and average DT and small dataset DT and average DT

Table 3. Throughput efficient of ISFOAE-PAS model with other models [17]

Throughput Effectiveness (Mbps / Sec)		
Methods	Encryption	Decryption
DES	16.913	14.170
RSA	09.267	04.836
Blowfish	12.830	10.967
AES	05.224	04.836
BEA-OMKHE	27.961	27.622
ISFOAE-PAS	29.868	28.576

Table 4. Dataset details

Class	No. of Samples
Benign	500
DDoS	500
DoS	500
Brute Force	500
Bot	500
Infiltration	500
Web	500
Total Number of Samples	3500

1.0161s, 1.4816s, and 0.6685s respectively. On the other hand, on a small dataset, the ISFOAE-PAS approach reaches a lower ET of 0.00438s while the DES, RSA, Blowfish, AES, and BEA-OMKHE systems gain higher ET of 0.01056s, 0.00886s, 0.0134s, 0.0106s, and 0.00522s correspondingly.

In Table 2 and Fig. 4, an overall comparative Decryption Time (DT) outcome of the ISFOAE-PAS approach with recent algorithms is given.

The outcomes identified that the ISFOAE-PAS technique reaches minimal DT values under large and small datasets. For instance, on a large dataset, the ISFOAE-PAS technique attains decreasing DT of 0.6625s while the DES, RSA, Blowfish, AES, and BEA-OMKHE approach reach a maximum DT of 1.0416s, 2.0482s, 0.9114s, 1.7001s, and 0.99706s correspondingly. Followed by, on a small dataset, the ISFOAE-PAS approach attains decreased DT of 0.0032s while the DES, RSA, Blowfish, AES, and BEA-OMKHE systems attain higher DT of 0.0098s, 0.0110s, 0.0097s, 0.0088s, and 0.0078s correspondingly.

The throughput efficiency of the ISFOAE-PAS model with other encryption models under the encryption and decryption process is reported in Table 3.

Table 6. Comparative outcome of ISFOAE-PAS approach with other algorithms [24]

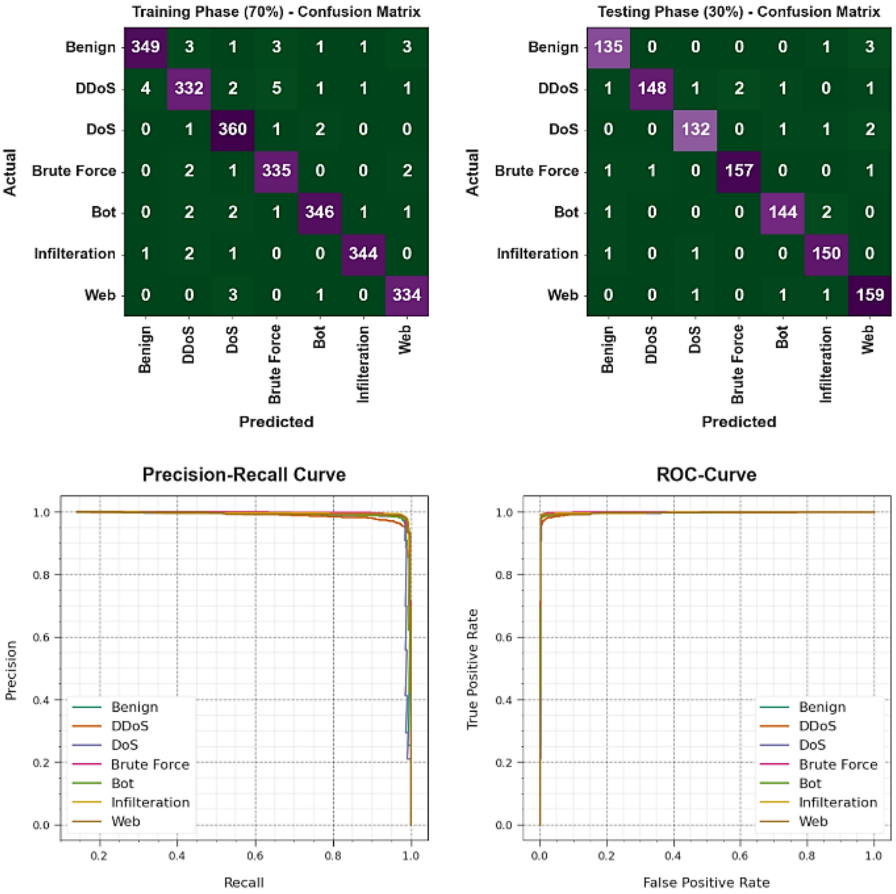
Model	Accuracy	Precision	Recall	F1-Score
Semi-self-taught NIDS	97.90	96.00	96.00	96.00
DVM-NID	98.38	96.79	97.04	97.06
PCA-DNN	97.93	95.97	97.12	96.68
MLP-PSO	96.25	96.75	96.80	97.16
MLP-BP	98.97	96.98	96.80	96.38
ISFOAE-PAS	99.42	97.96	97.96	97.96

The outcomes stated that the ISFOAE-PAS technique reaches increased throughput values under both processes. In the encryption process, this technique gains higher throughput efficiency of 29.868Mbps/s while the existing DES, RSA, Blowfish, AES, and BEA-OMKHE approach obtain lower throughput efficiency values. In the decryption process, the ISFOAE-PAS approach reaches superior throughput efficiency of 28.576Mbps/s while the existing DES, RSA, Blowfish, AES, and BEA-OMKHE algorithms gain lesser throughput efficiency values.

The DDoS attack identification achievement of the ISFOAE-PAS approach is validated on the CSE-CIC-IDS2018 dataset [23], which contains 3500 instances under seven classes as given in Table 4.

Fig. 5 portrays the classifier outcomes of the ISFOAE-PAS approach under the test database. Figs. 5a-5b shows the confusion matrix of the approach on 70 and 30 percent of TRP/TSP. The figure indicated that the ISFOAE-PAS method precisely identified and classified all 7 class labels. Likewise, Fig. 5c shows the PR evaluation of the ISFOAE-PAS method. The figures stated that the ISFOAE-PAS approach had maximal PR achievement under 7 classes. Eventually, Fig. 5d shows the ROC study of the ISFOAE-PAS approach. The figure exhibited that the ISFOAE-PAS technique has productive outcomes with higher ROC values under 7 class labels.

The DDoS attack identification results of the ISFOAE-PAS technique are portrayed in Table 5. The results show the effectual results of the ISFOAE-PAS technique under all classes. On 70 and 30 percent of TRP, the ISFOAE-PAS approach gains average $accu_y$, $prec_n$, $reca_l$, F_{score} , and AUC_{score} of 99.42%, 97.96%, 97.96%, 97.96%, and 98.81% and



Training Phase (70%) - Confusion Matrix

Actual \ Predicted	Benign	DDoS	DoS	Brute Force	Bot	Infilteration	Web
Benign	349	3	1	3	1	1	3
DDoS	4	332	2	5	1	1	1
DoS	0	1	360	1	2	0	0
Brute Force	0	2	1	335	0	0	2
Bot	0	2	2	1	346	1	1
Infilteration	1	2	1	0	0	344	0
Web	0	0	3	0	1	0	334

Testing Phase (30%) - Confusion Matrix

Actual \ Predicted	Benign	DDoS	DoS	Brute Force	Bot	Infilteration	Web
Benign	135	0	0	0	0	1	3
DDoS	1	148	1	2	1	0	1
DoS	0	0	132	0	1	1	2
Brute Force	1	1	0	157	0	0	1
Bot	1	0	0	0	144	2	0
Infilteration	1	0	1	0	0	150	0
Web	0	0	1	0	1	1	159

Figure. 5 Classifier result of Confusion matrices, PR-curve, and ROC-curve

Table 5. DDoS attack detection outcome of ISFOAE-PAS algorithm on 70% and 30% of TRP/TSP

Class	$\boldsymbol{Accu_y}$	$\boldsymbol{Prec_n}$	$\boldsymbol{Reca_l}$	$\boldsymbol{F_{Score}}$	$\boldsymbol{AUC_{Score}}$
Training (70%)					
Benign	99.31	98.59	96.68	97.62	98.22
DDoS	99.02	97.08	95.95	96.51	97.74
DoS	99.43	97.30	98.90	98.09	99.21
Brute Force	99.39	97.10	98.53	97.81	99.03
Bot	99.51	98.58	98.02	98.30	98.89
Infiltration	99.71	99.14	98.85	98.99	99.35
Web	99.55	97.95	98.82	98.38	99.24
Average	99.42	97.96	97.96	97.96	98.81
Testing (30%)					
Benign	99.24	97.12	97.12	97.12	98.34
DDoS	99.33	99.33	96.10	97.69	98.00
DoS	99.33	97.78	97.06	97.42	98.37
Brute Force	99.52	98.74	98.12	98.43	98.95
Bot	99.43	97.96	97.96	97.96	98.81
Infiltration	99.33	96.77	98.68	97.72	99.06
Web	99.05	95.78	98.15	96.95	98.68
Average	99.32	97.64	97.60	97.61	98.60

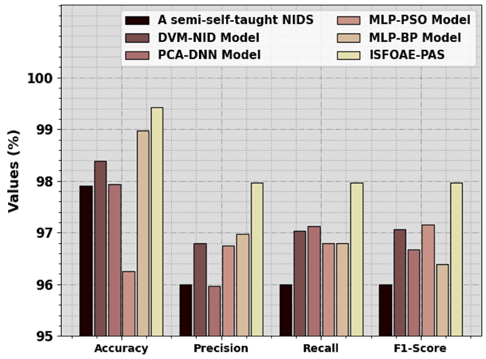


Figure. 6 Comparative outcome of ISFOAE-PAS approach with other algorithms [24]

$accu_y$, $prec_n$, $reca_l$, F_{score}, and AUC_{score} of 99.32%, 97.64%, 97.60%, 97.61%, and 98.60% correspondingly.

In Table 6 and Fig. 6, the overall comparison results of the ISFOAE-PAS technique are provided [17, 24].

The results indicate that the semi-self-taught NIDS, PCA-DNN, and MLP-PSO algorithms have obtained poor performance. Along with that, the DVM-NID and MLP-BP models have reported moderately closer results. However, the ISFOAE-PAS technique showed maximum performance with an $accu_y$ of 99.42%, $prec_n$ of 97.96%, $reca_l$ of 97.96%, and $F1_{score}$ of 97.96%. These results highlighted that the ISFOAE-PAS technique exhibits better results than other models.

5. Conclusion

In this manuscript, we have presented a novel ISFOAE-PAS technique for effectually securing the cloud environment using encryption and auditing schemes. The major intention of the ISFOAE-PAS technique lies in the accomplishment of data security, integrity, and auditing in the cloud environment. It involves four major processes namely the SIE-HE technique, ISFO-based optimal key selection, auditing, and DCAE-based DDoS attack detection. Meanwhile, the ISFOAE-PAS technique designed the SIE-HE technique to encrypt the data. Moreover, the ISFO algorithm is derived for optimally choosing the keys related to the SIE-HE technique. Furthermore, the public auditing scheme is designed to improve security in the cloud environment. At last, the DCAE model is used for the automated DDoS attack detection process. For demonstrating the greater efficiency of the ISFOAE-PAS technique, a series of simulations were involved. The experimental values inferred that the ISFOAE-PAS technique reaches better performance than other models with maximum accuracy of 99.42%.

Conflict of interest

The authors confirm no conflict of interest.

Author contributions:

Conceptualization, Mageshwari; methodology, Mageshwari and Naresh; software, Mageshwari; validation, Mageshwari; formal analysis, Mageshwari and Naresh; investigation, Mageshwari and Naresh; resources, Naresh; data curation, Mageshwari; writing-original draft preparation, Mageshwari; writing-review and editing, Mageshwari; visualization, Naresh; supervision, Naresh; project administration, Mageshwari; funding acquisition, Mageshwari and Naresh. All authors have recited and accepted the final manuscript.

References

[1] P. Goswami, S. De, S. Debnath, N. F. Neetu, and T. C. Tanupriya, "Stub Signature-Based Efficient Public Data Auditing System using Dynamic Procedures in Cloud Computing", 2023, doi: 10.21203/rs.3.rs-2760089/v1.

[2] J. Qiu, "Ciphertext Database Audit Technology Under Searchable Encryption Algorith., Blockchain Technology", *Journal of Global Information Management (JGIM)*, Vol. 30, No. 11, pp. 1-17, 2022.

[3] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu et al., "Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment", *Journal of Cloud Computing*, Vol. 12, No. 1, pp. 1-16, 2023.

[4] W. Zhang, Y. Bai, and J. Feng, "Tiia: A blockchain-enabled threat intelligence integrity audit scheme for iiot", *Future Generation Computer Systems*, Vol. 132, pp. 254-265, 2022.

[5] P. D. Kusuma and A. L. Prasasti, "Guided Pelican Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 6, 2022, doi: 10.22266/ijies2022.1231.18.

[6] P. D. Kusuma and M. Kallista, "Stochastic Komodo Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 4, 2022, doi: 10.22266/ijies2022.0831.15.

[7] P. D. Kusuma et al., "Extended Stochastic Coati Optimizer", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 3, 2023, doi: 10.22266/ijies2023.0630.38.

[8] P. D. Kusuma and F. C. Hasibuan, "Attack-Leave Optimizer: A New Metaheuristic that Focuses on The Guided Search and Performs Random Search as Alternative", *International Journal of Intelligent Engineering and Systems*,

Vol. 16, No. 3, 2023, doi: 10.22266/ijies2023.0630.19.

[9] P. D. Kusuma and M. Kallista, “Quad Tournament Optimizer: A Novel Metaheuristic Based on Tournament Among Four Strategies”, *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 2, 2023, doi: 10.22266/ijies2023.0430.22.

[10] P. D. Kusuma and A. Novianty, “Multiple Interaction Optimizer: A Novel Metaheuristic and Its Application to Solve Order Allocation Problem”, *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 2, 2023, doi: 10.22266/ijies2023.0430.35.

[11] M. Song, Z. Hua, Y. Zheng, H. Huang, and X. Jia, “Blockchain-Based Deduplication and Integrity Auditing over Encrypted Cloud Storage”, *IEEE Trans. Dependable and Secure Comput.*, pp. 1–18, 2023, doi: 10.1109/TDSC.2023.3237221.

[12] S. Wang, Y. Zhang, and Y. Guo, "A blockchain-empowered arbitrable multimedia data auditing scheme in IoT cloud computing", *Mathematics*, Vol. 10, No. 6, p. 1005, 2022.

[13] G. Tian, Y. Hu, J. Wei, Z. Liu, and X. Huang et al., "Blockchain-based secure deduplication and shared auditing in decentralized storage", *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 6, pp. 3941-3954, 2021.

[14] C. Zhang, Y. Xu, Y. Hu, J. Wu, and J. Ren et al., "A blockchain-based multi-cloud storage data auditing scheme to locate faults", *IEEE Transactions on Cloud Computing*, Vol. 10, No. 4, pp. 2252-2263, 2021.

[15] J. Li, J. Wu, G. Jiang, and T. Srikanthan, "Blockchain-based public auditing for big data in cloud storage", *Information Processing & Management*, Vol. 57, No. 6, p. 102382, 2020.

[16] M. Xie, Q. Zhao, H. Hong, C. Chen, and J. Yu, "A novel blockchain-based and proxy-oriented public audit scheme for low performance terminal devices", *Journal of Parallel and Distributed Computing*, Vol. 169, pp. 58-71, 2022.

[17] V. N. R. Bandaru and P. Visalakshi, "Block chain enabled auditing with optimal multi-key homomorphic encryption technique for public cloud computing environment", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 22, 2022.

[18] I. Abunadi, H. A. Mengash, S. Alotaibi, M. M. Asiri, and M. A. Hamza et al., “Optimal multikey homomorphic encryption with steganography approach for multimedia security in Internet of everything environment”, *Applied Sciences*, Vol. 12, No. 8, p. 4026. 2022.

[19] D. R. Nayak, N. Padhy, P. K. Mallick, D. K. Bagal, and S. Kumar, "Brain tumour classification using noble deep learning approach with parametric optimization through metaheuristics approaches", *Computers*, Vol. 11, No. 1, p. 10, 2022.

[20] S. Jiang, J. Shang, J. Guo, and Y. Zhang, "Multi-Strategy Improved Flamingo Search Algorithm for Global Optimization", *Applied Sciences*, Vol. 13, No. 9, p. 5612, 2023.

[21] X. Li, S. Liu, R. Lu, M. K. Khan, and K. Gu et al., "An efficient privacy-preserving public auditing protocol for cloud-based medical storage system", *IEEE Journal of Biomedical and Health Informatics*, Vol. 26, No. 5, pp. 2020-2031, 2022.

[22] M. S. Seyfioğlu, A. M. Özbayoğlu, and S. Z. Gürbüz, "Deep convolutional autoencoder for radar-based classification of similar aided and unaided human activities", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 54, No. 4, pp. 1709-1723, 2018.

[23] https://www.unb.ca/cic/datasets/ids-2018.html

[24] S. Alzughaibi and S. E. Khediri, “A Cloud Intrusion Detection Systems Based on DNN Using Backpropagation and PSO on the CSE-CIC-IDS2018 Dataset”, *Applied Sciences*, Vol. 13(4), p. 2276. 2023.

[25] M. Mageshwari and R. Naresh, “Survey on Cloud Auditing by using Integrity Checking Algorithm and Key Validation Mechanism”, *Smart Trends in Computing and Communications: Proceedings of SmartCom*, pp. 437-446. DOI: 978-981-16-9967-2, 2022.

[26] M. Mageshwari and R. Naresh, "Decentralized Data Privacy Protection and Cloud Auditing Security Management", *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, 2022, pp. 103-109, doi: 10.1109/ICCCIS56430.2022.10037676.

[27] S. Sakthipriya and R. Naresh, “Effective Energy Estimation Technique to Classify the Nitroge. Temperature for Crop Yield Based Green House Application”, *Sustain. Comput. Inform. Syst*, Vol. 35, No. 2022.

[28] K. L. Narayanan and R. Naresh, "Improved Security for Cloud Storage Using Elgamal Algorithms Authentication Key Validation", In: *Proc. of 2023 International Conference for Advancement in Technology (ICONAT)*, Goa, India, pp. 1-5, 2023, doi: 10.1109/ICONAT57137.2023.10080619.