Research article

# Hough Transform Based Deep Belief Network and Improved Homomorphic Encryption for Cloud Security Based Intrusion Discovery

Sivakumar Ramu, Master[1], Ramakrishnan Ramamoorthy[1], Rameshkumar Ranganathan[1]

[1] Computer Science and Engineering, Yanbu Industrial College

Keywords: Cloud security, Intrusion Analysis, Adaptive white shark optimization, Hough transform based deep belief network, Improved homomorphic encryption

https://doi.org/10.53370/001c.92142

Yanbu Journal of Engineering and Science

Vol. 20, Issue 2, 2023 Submitted: 05 OCT 2023 Revised: 13 NOV 2023 Accepted: 26 NOV 2023

The enlarge development in information technology is cloud computing, which offers minimized infrastructure cost, lower maintenance, greater flexibility and scalability. Nowadays, the network security plays vital role in enterprises and organizations. The influence vulnerabilities were occurred due to attackers based on network configuration. Because of cloud and IoT growth, enlarge amount of data obtained from IoT sensor and devices are transmitted to cloud data centers. Several security issues like focused web servers in the cloud and information collection mishandling are faced by storage and cloud-based computing when offering us considerable convenience. For that reason, this article proposes a deep learning-based cloud security oriented intrusion discovery. Primarily, the input dataset is pre-processed by using normalization techniques followed by the features are selected using an Adaptive White Shark Optimization (AWSO) algorithm. The normal and intrusion data is classified by using Hough Transform based Deep Belief Network (HT-DBN) after that the sensitive data are secured with the help of an Improved Homomorphic Encryption (IHE) model. The simulation tool of MATLAB is been used to simulate the proposed implementation part and the experimental results outperformed the detection accuracy of 97% than other previous approaches.

## 1. INTRODUCTION

Cloud security,[1] often referred to as web-based protection, is a group of safety features intended to safeguard data, programs, and facilities that are hosted in the cloud. These steps provide information and capacity authorization, client and connection identification, and knowledge confidentiality. It also assists with the conformity of statutory documents, in cloud settings, safety precautions are used to guard against malware, criminals, distributed denial attacks, and unauthorized user entry and exploitation. Since the supplier takes care of everything, a business fails to have to manually set up objects to access the public web, independent online vendors deploy publicly accessible clouds. Public clouds[2] must include safety amenities like authorization, administration of identities, and certification, users often use mobile devices to navigate the supplier's internet services.

Since private clouds tend to be assigned to an individual band or person and depend on that organization's or individual's router, the latter are frequently more safeguarded than shared clouds. Since only one organization is allowed to use these cloud-based services, this separation aids in keeping them safe from external dangers. Nevertheless, some risks, such as psychological manipulation and compromises, continue to pose safety hazards. In hybrid clouds, better control assets provided by encrypted clouds are combined with the flexibility of cloud computing.[3] These databases link several settings that can grow more readily dependent on request, such as an individual and a cloud that is publicly accessible. Users can connect to all of the settings through an individual consolidated administration interface in productive cloud configurations. Given that the majority of businesses currently use online computing in some capacity, safeguarding it is essential.

Safeguarding sensitive firm information, such as requests from clients, top-secret development documents, and accounting data, is a key aspect of on-demand privacy.[4] Sustaining client confidence and safeguarding the resources that enhance with more information differentiation depends on managing breaches and knowledge loss. For every business moving to cloud storage, safety in the cloud is essential due to its capacity to protect both records and other resources. With numerous endpoints and systems needing protection, online computing[5] provides organizations with a centralized place for information and software. To guarantee the entire process is secure, cloud-based protection[6] simultaneously handles all of the devices, apps, and information.

The centralized platform makes it simpler for secure cloud firms to carry out duties like putting backup strategies in place, simplifying system event surveillance, and improving online screening. It requires a rapid, safe method of accessing this information, the Information files and applications are accessible to authorized users thanks to cloud security. It will always have a dependable means for obtaining cloud-based apps and data,[7] enabling businesses to address any possible security concerns right away. With the ability to adapt to meet evolving needs, a cloud-based system gives access to additional software and information capacity whatever it's necessary.

The centralized structure of cloud security enables organizations to quickly incorporate fresh programs and other capabilities without compromising the protection of information as requirements arise. To improve a cloud method safety features[8] can increase throughout times of significant usage and stretch downwards during times of minimal usage. Additionally, there remains a chance that an individual can access critical data regardless of all the precautions taken to safeguard networks in the cloud, the risk of an information breach exists with stored-in-the-cloud safety measures. Below sentences pointed out the major contribution this work.

- To use min-max normalization to pre-process the data and employ AWSO algorithm to select best feature sets.
- To apply Hough Transform based Deep Belief Network to detect both intrusion and non-intrusion data from the relevant set of selected features and enhancing the accuracy of detection.
- To utilize Improved Homomorphic Encryption model to secure intrusion data to cloud and the encryption and decryption time performance is computed.

Rest of the paper work is arranged like; Section 2 summarizes the related works with respect to the cloud intrusion identification. Section 3 proposed a novel Hough transform based deep belief network and improved homomorphic encryption framework. The simulation outcomes are explained in Section 4 and Section 5 concludes the overall work.

## 2. LITERATURE SURVEY

Samy et al.[9] have presented a fog-based attack detection framework assaults are detected extremely quickly, and there is a more rapid reaction than with cloud-based surveillance. It is categorized by the way it detects used on the cloud nodes to find assaults. To ensure its distributive, expansion, and speed, the identification mechanism is managed by an online platform. The initial stage seeks to train the DL model and tweak the hyper parameters to attain the best reliability. It identifies numerous assaults with an elevated rate of identification and correctness levels. However, it could be challenging to identify the data gathered at the edge level.

Abirami et al.[10] have described crypto-deep neural network cloud security (CDNNCS)as superior to an encrypted proportional mathematical solution technique for increasing the degree of credibility amongst cloud consumers. The suggested paradigm improves connectivity while presenting node-level information. The crucial aspect of enhancing network safety is the training element. Cloud security increases confidence in the on-demand domain, transmission loss has been decreased by 10% while the reaction period has risen by 5%. Therefore, the cloud setup is a multifaceted problem that has to be resolved.

Gao. Et al.[11] developed a Bidirectional Long Short Term Memory (Bi-LSTM) failure prediction to locate failed tasks and jobs in the cloud. To modify the proportions of the proximity and distance input characteristics, users begin by entering the information into reversed and forward-facing states. To achieve excellent forecasting preciseness, more input characteristics are required. Due to the modest false positive rate of the projection approach Bi-LSTM, pre-emptive loss mitigation centred on forecasting findings might additionally grow more successful. Thus, it is not suitable to evaluate our approaches' functionality in a real-time data centre.

Sudhakar et al.[12] have implemented a cancellable biometric system that a variety of consumers can utilize as an offering. The method of arbitrary extension has been used to safeguard personal data stored on the public web. The security of the unique information throughout the event that an attacker gets both the individual's identity and the cancellable pattern. A cloud environment enabled simultaneous processing, which made it statistically quicker than independent systems yet preserved reliability. Therefore, it is not well integrated into the current networks and infrastructures.

Alzubi et al.[13] have evaluated the Hashed Needham Schroeder Cost Optimized Deep Machine Learning (HNS-CODML) method to provide commercial Internet of Things security has been suggested for safe automotive IoT information transfers through cloud environments. Because only authorized cloud customers (CU) have the right to send information and communications through an encrypted link and may be educated, the speed of computation has been lowered. Given the average project completion duration, transmission expenses, and transmission overhead, the process's efficacy is assessed, facilitating modification. Hence, the communication cost was shown to be more extensive.

Nguyen et al.[14] have evaluated deep-learning techniques to give a thorough understanding of the construction of an automated component for preventative system surveillance and processing system mitigation. Superior materials model efficiency in volatile and quickly evolving circumstances is ensured by the right integration of flexible information pre-treatment and DL simulation. For feature productivity at dimension, the information pre-treatment component makes use of massive data collection technology. The shortage of actual labels for data with recognized patterns in actual manufacturing is a limitation of exploitation identification.

Yin et al.[15] suggested a secure federated data collaboration framework (FDC) may achieve safe multi-party information handling cooperation under the presumption that the knowledge is not required to be transported outside of its information centre. The handling of information, storage enrollment, and information administration are the purview of the confidential information center. For multi-party encrypted calculations, a common storage facility is utilized. Reliable utilization of information and transfers are ensured by the distributed ledger notion. The efficiency of the suggested design is examined using a real-world online technology situation. Thus, it is unable to examine and verify the transactions.

Wang et al.[16] highlighted a stacked contractive auto-encoder (SCAE) offered for obtaining characteristics without supervision. From unprocessed information about networks, the SCAE approach may determine crucial and reliable low-dimensional characteristics and feed those characteristics to a superficial Support Vector Machine predictor. Utilizing the advantages of basic and extensive training methods separately together may significantly enhance the ability to detect. Hence, it cannot recognize various network threats.

## 3. PROPOSED METHODOLOGY

Figure 1 shows the overall of proposed work structure. It includes different core phases. Few specific ranges with data normalization is handled via the normalization of Min–Max technique during pre-processing. Subsequently, AWSO algorithm choose most appropriate features and both intrusion and non-intrusion data is classified using HT-DBN. From this, the sensitive information in cloud is secured based on IHE algorithm.

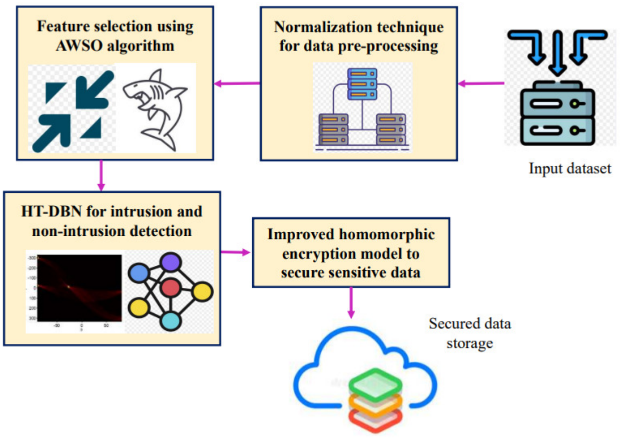

Feature selection using AWSO algorithm
Normalization technique for data pre-processing
Input dataset
HT-DBN for intrusion and non-intrusion detection
Improved homomorphic encryption model to secure sensitive data
Secured data storage

**Fig. 1. Proposed Work Structure**

### 3.1. DATA PRE-PROCESSING

Prepare the input dataset and process the technique of normalization. To the finite numeric ranges, the bigger numeric values with the important dominating attributes are changed. Under linear transformation principle, perform the normalization of min-max.[17] Where, $[\max(p), \min(p)]$ to $[\min_{New}(p), \max_{New}(p)]$ to is the attribute value ranges for mapping.

$$\overset{\wedge}{X}_k = \frac{[x_k - \min(p)] \times [\max_{New}(p) - \min_{New}(p)]}{[\max(p) - \min(p)]} + Min_{New}(p) \tag{1}$$

Based on the dataset, the maximum and minimum attribute values are max $(p)$ and min$(p)$ that describes the input as $x_k$ .The minimum and maximum specified ranges are symbolized as $\min_{New}(p)$ and $\max_{New}(p)$.The effect of scale difference are eliminated by the normalized pre-processed output is described as $\overset{\wedge}{X}_k$. According to the original dataset, retrieve the new data to every tuples next to pre-processing model is performed.

### 3.2. SELECTING FEATURES

Some of them are least significant and the remaining few values are few vector values among transformed features. This research suggests an Adaptive White Shark Optimization (AWSO) algorithm to select better feature sets also reducing the dimensionality of features thereby enhancing the intrusion detection performance. The foraging and white navigating smell and hear sensing of white shark's feature characteristics demonstrates the White Shark Optimization (WSO) algorithm.[9] The white shark to the prey speed and the direction predict the feature vectors. Following formula update the location of each features.

$$X_k(T+1) = U\ [X_k(T) + G_4 V_{10}\,(R_{H_A}(T) - R_k(T)) + H_5 K_{11}(R_{Ak}(T) - R_k(T))] \tag{2}$$

Where, $X$ and $M$ are the speed and population of white shark. From this, $R_A$and $R_{H_A}$are the best solution of selecting features and higher strategic standing vector. The ranges for [0, 1] to the random numbers $K_{10}$and $K_{11}$.

$$G_4 = \underset{G}{\max} + (\underset{G}{\max} - \underset{G}{\min})\exp(-(4T/t)^2) \tag{3}$$

$$G_5 = \underset{G}{\max} - (\underset{G}{\max} - \underset{G}{\min})\exp(-(4T/t)^2) \tag{4}$$

$$U = \frac{2}{\left|2 - \vartheta - \sqrt{\vartheta^2 - 4\vartheta}\right|}\ and\ \vartheta = 4.125 \tag{5}$$

The prey moving to white shark fragrance location. Below expression update the location and the fragrance happen to similar position of feature vectors.

$$R_k(T+1) = \begin{cases} R_k(T) - \oplus R_0 + high.\,z + low.\,y; Ran < m \\ R_k(T) + X_k(T)/freq; Ran \geq T \end{cases} \tag{6}$$

Where, $y$ and $z$ are the one-dimensional binary vectors and freq is the frequency of sea wave movement. Where, *low* and *high* are the search area's upper and lower boundaries. Here, $z_0$ and $z_1$ are constant values.

$$n = (|z_0 + \exp((T/2 - t)/z_1|)^{-1} \tag{7}$$

The white shark movement phase of WSO algorithm performance is boosted up by maintaining the minimal memory usage of compact strategy[10] and the new model is an adaptive WSO algorithm. The winner and loser-based perturbation iterative is updated as,

$$\gamma^{T+1} = \gamma^T + \frac{1}{M_R}(winner - loser) \tag{8}$$

$$R_k(T+1) = \begin{cases} R_{H_A}(T) + s_1.\,I.\,sgn(s_2 - 0.5); \\ s_3 < Xx\,\gamma^{t+1}; Otherwise \end{cases} \tag{9}$$

From this, $s_1, s_2$, and $s_3$ are the random numbers with the $I$ target distance. The following formula computes the fish school characteristics.

$$R_k(T+1) = \frac{R_k(T) + R_k(T+1)}{2.Ran} \tag{10}$$

Most efficient features among them are determined by the fitness function during the updating procedure of every solutions. Until the maximal accuracy is reached, select the best feature sets in the last phase of AWSO algorithm. Terminate the process once retrieving best feature sets then end up the process else repeat the above steps. Figure 2 displays the flowchart of AWOS algorithm to select best feature set.

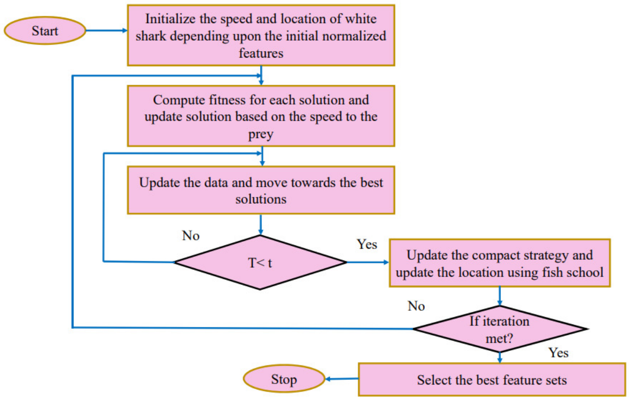

Start
Initialize the speed and location of white shark depending upon the initial normalized features
Compute fitness for each solution and update solution based on the speed to the prey
Update the data and move towards the best solutions
No
T< t
Yes
Update the compact strategy and update the location using fish school
No
If iteration met?
Yes
Stop
Select the best feature sets

**Fig. 2. Flowchart of AWSO algorithm**

### 3.3. DETECT AND CLASSIFY INTRUSION AND NON-INTRUSION DATA

Apply best slected feature vectors to the DBN's input node. The packet information attacked and normal are classified using Hough transform based deep belief network (HT-DBN). The suprivised and unsupervised learning network combintaion is deep belief network (DBN). The downward arrows and upward arrow represnets the generative and detection model.[11] Below expression represent the layer $G$ and the $A$ joint distribution enable the $m$-layer.

$$p(A, G_1, \ldots., G_N) = p(A\,|G_1\,) \prod_{K=1:N-2} p(G_K\,|G_{K-1}\,)p(G_{N-1}\,|G_N) \tag{11}$$

For parameter fine-tuning, the hough transform (HT) with contrastive divergence and the layers of RBM training included in DBN.

The DBN hidden layer performance is improved by using standalone implememnttaion of hough transform (HT). The HT implements the DBN process during attack detction. Pass the polar parameters $(p, \theta)$ with every edge point is $y_j, z_j$.

$$p = y \cos\theta + z \sin\theta \tag{12}$$

In an accumulatary array, increment the pair $(y, z)$ based on varing ranges $\theta$. Store theses line pairs $(p, \theta)$ in the output of hidden layer. Utilize HT and layer approach with unsupervised layer training. Sample $p(G_1\,|A)$ as the distribution and sample $p(A\,|G_1)$ visible variables based on posterior distribution.

Based on the ismilar procedure, effectuate the hidden layers sampling and attain the equilibrium distribution is reached maximum. Continue $G_2$ and repeat the second layer of RBM with input learning is determined by best input vector $A$. The Hough transform based back propagation learning is fine-tuned in DBN parameters. The trained HT-DBN structure are classified once the network attain trained. The cost function of supervised effectuate expected as well as predicted output vector. The proposed HT-DBN classifies the intrusion and non-intrusion data. Figure 3 explains the HT-DBN model for intrusion and non-intrusion detection in cloud.

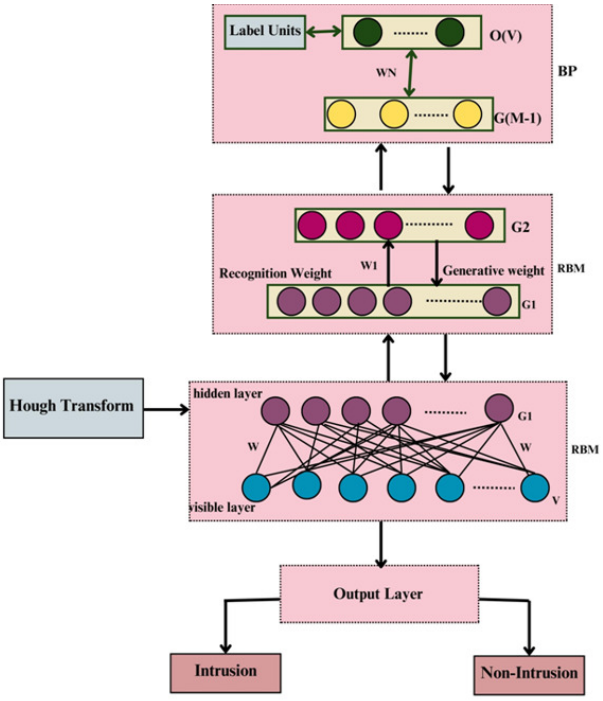


**Fig. 3. HT-DBN model**

### 3.4. INTRUSION DATA SECURTY

To safeguard the information in the cloud system the classified information using the proposed approach are encrypted with the help of an improved homomorphic encryption (IHE).[12] The data are secured using the proposed technique. the phases involved are shown in following eqn.

$$\begin{aligned} IHE = \{ & \text{KeyGeneration } (KG),\ \text{Encryption } (E), \\ & \text{Evaluation } (Ev),\ \text{Decryption } (D)\} \end{aligned} \tag{12}$$

- **KG:** To encrypt the unaffected information, this phase uses two keys known as $PrivateKeyP^K$ and $SecretKeyP^S$based on the needs.
- **E:** The plain text $PT$ from the outcome of proposed classification algorithm are encrypted using the secret key denoted as $EP^S(PT)$ and generated the cipher text $CT$ with respect to the $P^K$.
- **EV:** The calculation of $CT$is effectuated with the additional term 'h' based on the $P^K$as $Cal\left(h\left(P^K\right)\right)$
- **D:** The decryption is commence with the $P^S$ key and decrypted from the Cal $\left(h\left(P^K\right)\right)$ to obtain the source data. The steps followed are enlisted in the Algorithm 1.

The pseudocode in the algorithm 1 explains the IHE and the unaffected inputs are forwarded to the encryption approach by initializing the keys that are generated. For the generated key large prime numbers are assigned and followed by the evaluation of LCM.[13] The value of K is the

**Algorithm 1. IHE pseudocode**

```
Initialize the input and output
Start
KG stage: KG(m,n)
Allot larger prime number for m and n
Calculate $K = mn$ and $\beta = lcm(k-1, l-1)$
Chose the random integer value q in the
Analyse the presence of q with
$\eta = \left(X\left(q^{\beta} modK^{2}\right), K\right) = 1$, here, $X(p) = \frac{p-1}{K}$
The public encryption key $P^{K} = (K, q)$ and $P^{S} = (m, n)$
E: $E(e, P^{K})$
The message to be encrypted is deemed as q which belongs to $e \in CT$
Evaluate the random variable R and $R \in CT$
Evaluate the $CT = q^{e} R^{K} modK^{2}$, here $c \in CT$
D: $E(c, P^{S})$
Decryption of CT is effectuated
Evaluate the PT by $e = \frac{X(c^{\beta} modK^{2})}{X(q^{\beta} modK^{2})} modK$
Return the encrypted data
end
```

product of two prime numbers and the presence of public and secret keys are checked using the calculated $\eta$. The plain text is encrypted to produce the Cipher Text incorporated with the public key. Henceforth decryption process is started to decrypt the plain text. After completing all these processes, the values are stored in the cloud storage to safeguard it for further process. This also averts the attacks and loss of information. The access of data from the cloud should be commences with the request to CSP (Cloud Service Provider). After the security processes have completed the data get accessed by the requested user in all aspects. Thus, the proposed approach enhances the security of the cloud storage.

## 4. SIMULATION ANALYSIS AND DISCUSSION

This section extends the performance analysis of proposed work with the experimental setup and dataset taken. The details are elucidated below subsection. For the experimental study we have taken the system with the specification of Intel R Core 15-3570s processor with the speed of 3.15 GHz. The simulation is carried out in MATLAB simulator.

### 4.1. DATASET DESCRIPTION

For the study we have taken the publicly available CIC-IDS 2017 dataset. In this 80% of data are taken for training the proposed work and 20% is used for the testing. This dataset includes real-world data with analysed traffic utilizing the CIC Flowmeter. This will label the details such as time stamp, protocols, transmitter and receiver IPs, transmitter and receiver ports, and attacks.

### 4.2. ASSESSMENT BASED ON PERFORMANCE METRICS

This section is used to demonstrate the performance analysis based on the metrics such as security analysis, accuracy, sensitivity, and specificity. For the study we have taken the existing works such as FDC, SCAC, CDNNCS, and BiLSTM. The assessments based on security analysis of the proposed work and existing works such as FDC, SCAC, CDNNCS, and BiLSTM are framed in figure 4. The security analysis eventually shows how our system or other systems protects the data from the attacks and from the figure our approach shows higher security than the existing with the percentage of 98%, and FDC, SCAC, CDNNCS, and BiLSTM show security of 87%, 88%, 93%, and 96% respectively. Thus, the security of the proposed work is higher.

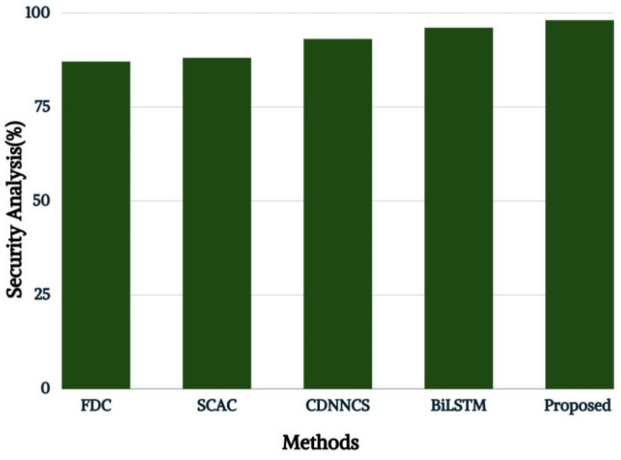


**Fig. 4. Assessment based on the Security analysis**

The assessment based on the accuracy is outlined in figure 5. For analysing the performance metrics we have taken 300 epochs and during the beginning epochs the accuracy of all the works such as proposed and FDC, SCAC, CDNNCS, and BiLSTM showed more or less same accuracy of detection of attacks from the dataset. Meanwhile, the performance of proposed work increases with increasing epochs and attain a stable accuracy around 300 epochs. At 300th epoch our proposed approach attains 97% of detection accuracy and other approaches FDC, SCAC, CDNNCS, and BiLSTM attained accuracy of 89%, 93%, 94%, and 95% respectively.

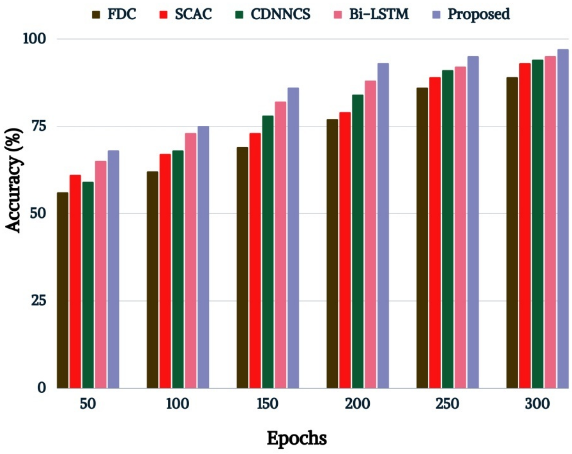


**Fig. 5. Assessment based on the Accuracy**

Figure 6 represents the assessment based on the sensitivity. The proposed work shows better sensitivity than the other existing works such as FDC, SCAC, CDNNCS, and BiLSTM models. At 300th epochs the works attained stable sensitivity values and for our proposed approach the sensitivity at 300th epochs is 98%. Meanwhile, FDC, SCAC, CDNNCS, and BiLSTM have the sensitivity of 89%, 90%, 91%, and 93% correspondingly at 300th epochs.

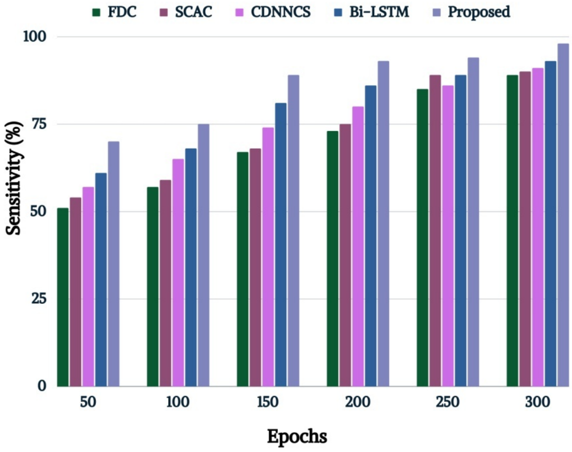


**Fig. 6. Assessment based on the sensitivity**

Figure 7 illustrates the Specificity based performance evaluation. The specificity of proposed approach is higher with the percentage of 97% at the 300th epochs and the other approaches such as FDC, SCAC, CDNNCS, and BiLSTM achieved the specificity of 85%, 89%, 89%, and 92% respectively as shown in figure 8. The betterment of work depends on the selection of techniques and we have utilized appropriate techniques for the feature selection and classification processes. Thus the classification of intrusion as intrusion and normal by our proposed work is accurate than the other existing approaches.

**Table 1. Assessment based on Encryption time**

| Methods | Encryption Time (ms) |
|---|---|
| RSA | 289 |
| AES | 301 |
| T-DES | 238 |
| HE | 213 |
| Proposed IHE | 120 |

**Table 2. Assessment based on Decryption time**

| Methods | Decryption Time (ms) |
|---|---|
| RSA | 249 |
| AES | 284 |
| T-DES | 197 |
| HE | 176 |
| Proposed IHE | 102 |

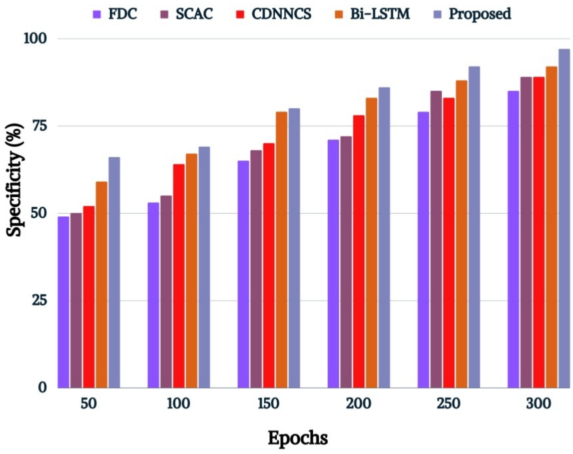


**Fig. 7. Assessment based on the specificity**

### 4.3. PERFORMANCE ANALYSIS FOR SECURITY OF THE CLOUD COMPUTING

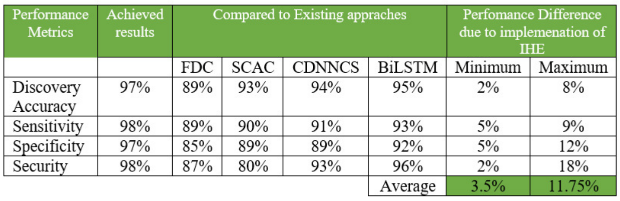
This section is used to present the time taken by the proposed cryptography approaches when compared to the existing approaches such as Rivest Shamir Adlemen (RSA) algorithm,[14] Advance Encryption Standard (AES),[15] Triple Data encryption standard (T-DES),[16] and Homomorphic Encryption algorithm (HE).[17] The encryption time of the proposed and state-of-art cryptographic algorithm are presented in table 1. From this table the proposed IHE shows lesser encryption time than the other approaches with 120ms, whereas, other approaches RSA, AES, T-DES, and HE took encryption time of 289ms, 301 ms, 238ms, and 213 ms respectively.

The assessment based on the decryption time is presented in table 2. The decryption time of proposed work is lower with 102ms. The improved HE has mitigated the decryption time and thus it shows better evaluation. The other approaches RSA, AES, T-DES, and HE showed the decryption time of 249ms, 284ms, 197ms, and 176ms respectively. The reduction of decryption time will improve the overall efficacy of the system to secure the cloud computing and storage.

## 5. CONCLUSION

The work in this article is a nutshell to secure the data in the cloud platform with the accurate discovery of intrusion. To achieve the secured intrusion discovery we have presented an innovative approach known as Hough transform based Deep Belief Neural Network (HT-DBN) to classify/discovered the intrusion from the source. The dataset was pre-processed with normalization technique and forwarded to the proposed novel Adaptive White Shark optimization (AWS) approach for the selection of features from the data in order to discover the intrusion using the proposed approach. The classified non-affected data were secured using the Improved Homomorphic Encryption technique (IHE). Additionally, data set were taken from publicly available CIC-IDS 2017 dataset and the simulations were conducted using the MATLAB simulator. IHE implementation results are astonishing.

Additionally, data set were taken from publicly available CIC-IDS 2017 dataset and the simulations were conducted using the MATLAB simulator. IHE implementation results are astonishing and are in adequate heights.



| Performance Metrics | Achieved results | Compared to Existing appraches | | | | Perfomance Difference due to implemenation of IHE | |
|---|---|---|---|---|---|---|---|
| | | FDC | SCAC | CDNNCS | BiLSTM | Minimum | Maximum |
| Discovery Accuracy | 97% | 89% | 93% | 94% | 95% | 2% | 8% |
| Sensitivity | 98% | 89% | 90% | 91% | 93% | 5% | 9% |
| Specificity | 97% | 85% | 89% | 89% | 92% | 5% | 12% |
| Security | 98% | 87% | 80% | 93% | 96% | 2% | 18% |
| | | | | | Average | 3.5% | 11.75% |

As a conclusion the over all output of IHE implemation yeilds explemnperary results with a average of minimum 3.5% and maximum of 11.75%.

# REFERENCES

1. Abirami P, Bhanu SV. Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment. *Soft Comput*. 2020;24(24):18927-18936. doi:10.1007/s00500-020-05122-0

2. Gao J, Wang H, Shen H. Task failure prediction in cloud data centers using deep learning. *IEEE Trans Serv Comput*. 2022;15(3):1411-1422. doi:10.1109/tsc.2020.2993728

3. Sudhakar T, Gavrilova M. Cancelable biometrics using deep learning as a cloud service. *IEEE Access*. 2020;8:112932-112943. doi:10.1109/access.2020.3003869

4. Alzubi JA, Manikandan R, Alzubi OA, et al. Hashed Needham Schroeder industrial IoT based cost optimized deep secured data transmission in cloud. *Measurement*. 2020;150:107077. doi:10.1016/j.measurement.2019.107077

5. Nguyen G, Dlugolinsky S, Tran V, Garcia AL. Deep learning for proactive network monitoring and security protection. *IEEE Access*. 2020;8:19696-19716. doi:10.1109/access.2020.2968718

6. Yin B, Yin H, Wu Y, Jiang Z. FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things. *IEEE Internet Things J*. 2020;7(7):6348-6359. doi:10.1109/jiot.2020.2966778

7. Wang W, Du X, Shan D, Qin R, Wang N. Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. *IEEE Trans Cloud Comput*. 2022;10(3):1634-1646. doi:10.1109/tcc.2020.3001017

8. Agarwal A, Khari M, Singh R. Detection of DDOS attack using deep learning model in cloud storage application. *Wireless Pers Commun*. 2021;127(1):419-439. doi:10.1007/s11277-021-08271-z

9. Braik M, Hammouri A, Atwan J, Al-Betar MA, Awadallah MA. White Shark Optimizer: A novel bio-inspired meta-heuristic algorithm for global optimization problems. *Knowledge-Based Systems*. 2022;243:108457. doi:10.1016/j.knosys.2022.108457

10. Zheng W, Pang S, Liu N, Chai Q, Xu L. A Compact Snake Optimization Algorithm in the Application of WKNN Fingerprint Localization. *Sensors*. 2023;23(14):6282. doi:10.3390/s23146282

11. Abdel-Zaher AM, Eldeib AM. Breast cancer classification using deep belief networks. *Expert Systems with Applications*. 2016;46:139-144. doi:10.1016/j.eswa.2015.10.015

12. Agarwal A, Khari M, Singh R. Detection of DDOS attack using deep learning model in cloud storage application. *Wireless Pers Commun*. 2021;127(1):419-439. doi:10.1007/s11277-021-08271-z

13. Zhao F, Li C, Liu CF. A cloud computing security solution based on fully homomorphic encryption. In: *16th International Conference on Advanced Communication Technology*. IEEE; 2014:485-488. doi:10.1109/icact.2014.6779008

14. Shawkat SA, Tuama BA, Al Barazanchi I. Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen. *IJECE*. 2022;12(6):6496. doi:10.11591/ijece.v12i6.pp6496-6505

15. Dharangan B, Praveen J, Rajagopal S, Jegajothi B. Secure Cloud-based E-Health System using Advanced Encryption Standard. In: *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE; 2022:642-646.

16. Ramachandra MN, Srinivasa Rao M, Lai WC, Parameshachari BD, Ananda Babu J, Hemalatha KL. An efficient and secure big data storage in cloud environment by using triple data encryption standard. *BDCC*. 2022;6(4):101. doi:10.3390/bdcc6040101

17. Kartit A. New Approach Based on Homomorphic Encryption to Secure Medical Images in Cloud Computing. *Trends Sci*. 2022;19(9):3970. doi:10.48048/tis.2022.3970