I. J. Computer Network and Information Security, **2023, 6, 40-51**
Published Online on December 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.06.04

A Cryptographic based I^{2}ADO-DNN Security Framework for Intrusion Detection in Cloud Systems

M. Nafees Muneera*
Department of Computer Science and Engineering, Sathyabama institute of science and technology, Chennai, Tamilnadu, India
E-mail: nafeeshabib2005@gmail.com
ORCID iD: https://orcid.org/0000-0002-9541-0576
*Corresponding author

G. Anbu Selvi
Department of Computer Science and Engineering, Sathyabama institute of science and technology, Chennai, Tamilnadu, India
E-mail: anbuselvi.cse@sathyabama.ac.in
ORCID iD: https://orcid.org/0009-0007-7199-8284

V. Vaissnave
Department of Computer Science and Engineering, Sathyabama institute of science and technology, Chennai, Tamilnadu, India
E-mail: vaissnave.cse@sathyabama.ac.in
ORCID iD: https://orcid.org/0000-0001-7333-531X

Gopal Lal Rajora
Institute for research in technology, Universidad Pontificia, Madrid, Spain
E-mail: glrajora@comillas.edu

Received: 08 January 2023; Revised: 30 March 2023; Accepted: 12 May 2023; Published: 08 December 2023

Abstract: Cloud computing's popularity and success are directly related to improvements in the use of Information and Communication Technologies (ICT). The adoption of cloud implementation and services has become crucial due to security and privacy concerns raised by outsourcing data and business applications to the cloud or a third party. To protect the confidentiality and security of cloud networks, a variety of Intrusion Detection System (IDS) frameworks have been developed in the conventional works. However, the main issues with the current works are their lengthy nature, difficulty in intrusion detection, over-fitting, high error rate, and false alarm rates. As a result, the proposed study attempts to create a compact IDS architecture based on cryptography for cloud security. Here, the balanced and normalized dataset is produced using the z-score preprocessing procedure. The best attributes for enhancing intrusion detection accuracy are then selected using an Intelligent Adorn Dragonfly Optimization (IADO). In addition, the trained features are used to classify the normal and attacking data using an Intermittent Deep Neural Network (IDNN) classification model. Finally, the Searchable Encryption (SE) mechanism is applied to ensure the security of cloud data against intruders. In this study, a thorough analysis has been conducted utilizing various parameters to validate the intrusion detection performance of the proposed I2ADO-DNN model.

Index Terms: Cloud Computing, Security, Intrusion Detection System (IDS), Z-Score Normalization, Intelligent Adorn Dragonfly Optimization (IADO), Intermittent Deep Neural Network (IDNN) Classification, and Searchable Encryption.

1. Introduction

In recent days, the cloud is one of the fastest growing technologies in the Information Technology (IT) sector. The term "cloud computing" [1, 2] refers to Internet-based computing where software, platforms, infrastructure, policies, and a variety of resources are virtually provided via shared servers, or data centers. There are numerous ways to define a cloud data center [3], but the three most common definitions are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Likewise, the four cloud computing deployment models are public, private, community, and hybrid clouds [4]. A business group is tasked with managing and encouraging the use of public clouds. A private cloud is set up for a certain association with many users and is run by that specific association [5, 6]. Community clouds are created for a specific user base from businesses with similar objectives. Any association within that group or an outside user may manage it. Two or more separate cloud infrastructures make up a hybrid cloud. Security and privacy issues [7, 8] are the key barriers to the general adoption of the cloud environment around the world, despite the great technical and economic benefits. When selecting a cloud service, special attention should be paid to security. Security is one of the most important factor need to be addressed in the cloud system, since the different types of vulnerabilities/intrusions [9, 10] can disrupt the performance of cloud. For instance, the most common attacks affect the cloud are Denial of Service (DoS), Distributed Denial of Service (DDoS), packet spoofing, man-in-middle, port scanning, and etc. So, an Intrusion Detection System (IDS) is developed to ensure the security, privacy, and confidentiality of cloud.

Typically, the IDS [11, 12] may consist of hardware, software, or a combination of both. Data from the network under investigation is collected, and the network manager is notified via email or a log entry of the intrusion incident. The incorporation of an IDS can be crucial for identifying attacks or other activities that may be seen as suspicious or illegal in light of these security considerations. IDS [13] solutions currently in use were created by traditional networks and systems, but they are difficult to modify for a fast - changing environment like cloud computing. Therefore, it is essential to provide a flexible, secure solution that can be adjusted to the complicated, ever-changing cloud environment. IDS components cannot comprehend all of the massive reports generated, despite the fact that IDS models have been suggested in the scientific literature [14]. Due to their isolation, these suggested solutions continue to have limitations because they cannot cooperate or work together. As a result, their detection results are isolated and cannot be systematically gathered and examined. In order to efficiently detect assaults and respond to intrusions by shortening response times, IDS solutions based on the notions of cooperation, solidarity, independence, and mobility are essential. Traditional methods of detection and prevention are ineffective for coping with those threats and a high data flow at the same time. Machine learning (ML) [15, 16] approaches are highly useful for detecting attacks, whether they be classic or zero-day assaults. A number of algorithms used in machine learning may recognize patterns in data and make predictions based on those patterns.

To improve prediction, the ML approaches combine statistics and computer science. Also, it includes three basic learning paradigms [17]: semi-supervised, unsupervised, and supervised. For instance, K-Nearest Neighbor (KNN), Naïve Bayes (NB), Random Forest (RF), K-Means, and etc are the commonly used ML approaches in the cloud security application systems. Multi-layered computing models with Deep Learning (DL) can learn data representations with different levels of abstraction [18]. Applications including text categorization, natural language processing, and computer vision have all made significant strides. But the traditional ML/DL-based IDS frameworks [19, 20] are struggling with issues including high time complexity, ineffective data handling, high false positives, lack of dependability, and low detection accuracy. As a result, the proposed effort aims to create an innovative and efficient IDS system that includes an encryption mechanism for cloud security. The following are this paper's main contributions and goals:

- The z-score normalization based preprocessing methodology is used to remove the missing values, duplicate elements, and duplicated instances.
- An Intelligent Adorn Dragonfly Optimization (IADO) technique is used to extract the key characteristics from the normalized traffic data that are highly connected to the incursions.
- A computationally effective Intermittent Deep Neural Network (IDNN) classification model is used to classify the normal and attacking traffic data.
- A lightweight Searchable Encryption (SE) technology is utilized to guarantee the strong security of data for storage.
- During analysis, a number of parameters are utilized to evaluate the proposed framework's security performance and outcomes.

The remaining sections of this work are divided into the following categories: The comprehensive literature assessment of the IDS approaches currently in use for cloud security is provided in Section 2. Additionally, it addresses their advantages, drawbacks, and difficulties in light of its detecting procedures. The suggested I^2ADO-DNN based IDS framework is presented in Section 3 with a thorough explanation of how it works. The outcomes of the suggested security model are validated and compared in Section 4 using various parameters. In Section 5, the overall work is

described together with its implications, conclusions, and future scope.

2. Related Works

The literature review of the current IDS and encryption approaches used to ensure the security of cloud systems is presented in this part. In addition, it addresses the effectiveness and operations of intrusion detection as well as the benefits, drawbacks, and challenges of conventional works.

Nassif, et al [21] conducted a comprehensive review to validate the different types of machine learning techniques used for ensuring the security of cloud systems. The original purpose of this work was to protect the cloud against vulnerabilities like Denial of Service (DoS), zombie attack, phishing attack, and man-in-the-middle. Based on the study, it was analyzed that the data protection mechanism guarantees the security and privacy of the cloud system. *Guezzaz, et al* [22] discussed about the different types of attacks that degrade the security of cloud networks. Here, the cloud based honeypots are used to ensure the high security and privacy of cloud systems. Typically, the honeypots are treated as the most suitable and successful technology widely used in many security applications. Honeypots are created specifically to not only intentionally attract and trick hackers but also to spot improper online activity and can be considered a successful way to monitor hacker behaviors. A honeypot is a system or asset that is used to catch, monitor, and identify erroneous requests that are present in a network. Moreover, the honeypots are categorized into the following types: low interaction honeypots and high interaction honeypots. An IDS is used to establish the detective control mechanism in this instance. The network traffic data that is used to construct the IDS using a machine-learning algorithm has a significant impact on the IDS's detection accuracy. Here, the network traffic data has been preprocessed by using the cuckoo optimization algorithm, which also helps to improve the detection accuracy of IDS. In this framework, the network flow data is first gathered and prepared as a data set. Following that, the COFS is used to remove redundant and irrelevant features from the data set. The Naive Bayes (NB) classification approach is then used to construct the intrusion-detection model using the pertinent features. Depending on the source of the data used to create and learn the model, this model is then deployed in the network or on a cloud host. The intrusion detection model detects anomaly or intruder packets, and an alarm signal such as attack or normal is delivered depending on the packet that enters the network. Based on the alert message the IDS generated, the intrusion prevention system then takes preventive action. However, the accuracy of NB classifier is not up to the mark, which degrades the detection performance of IDS.

Ahsan, et al [23] provided a detailed overview about the different types of bio-inspired optimization algorithms used for improving the security of cloud systems. Typically, big data management problems, system integrity, and threat protection are the goals of security management for distributed computing. Big data security places a strong emphasis on dynamic real-time security observations to spot any potential threats, vulnerabilities, or simply strange behaviors. There is always a chance of private information leaks even while maintaining the data access speed at a manageable level. Moreover, the different class of algorithms used in this study are evolutionary-based, swarm-based, immune-based, and neural models. As social media material begins to rule cloud computing, trust management (TM) is becoming more and more crucial. But despite this, there isn't enough study being done in this area. Some of the trust models in cloud security include service level agreements, recommenders, and reputation-based approaches. *Meryem, et al* [24] developed a machine learning based hybrid IDS framework for strengthening the security and privacy of cloud systems. In this model, both the rule based and anomaly based mechanisms are deployed for accurately labelling the behaviors. *Almiani, et al* [25] used a deep recurrent neural network algorithm for developing an IDS to protect IoT systems. The purpose of this work is to develop an artificial fully automated IDS model for the detection of cyberattacks from fog.

3. Proposed Methodology

The suggested I^2ADO-DNN based IDS framework for ensuring the security and privacy of cloud systems is clearly described in this section. The unique contribution of this work is the creation of a novel DL-based security model combined with a simple encryption scheme to defend cloud systems from attackers.

Fig. 1 depicts the suggested framework's workflow, which encompasses the following operations:

- Preprocessing using z-score normalization
- IADO based feature selection
- IDNN based intrusion classification
- SE based data security

The IDS network traffic datasets are used in this instance as the processing's input. The dataset is first preprocessed using the z-score normalization approach to remove redundant instances, duplicate fields, and missing values. Following that, an IADO algorithm is used to best choose the features from the normalized dataset to increase the classifier's prediction accuracy. In order to accurately classify the normal and attacking instances in accordance with the optimum set of features, an IDNN classification technique is constructed. Finally, the SE mechanism is used to guarantee the privacy preservation of data saved in the cloud by preventing attackers from using the data. The main

benefits of employing this framework are its ease of deployment, high accuracy, guarantee of privacy, and enhanced intrusion detection.

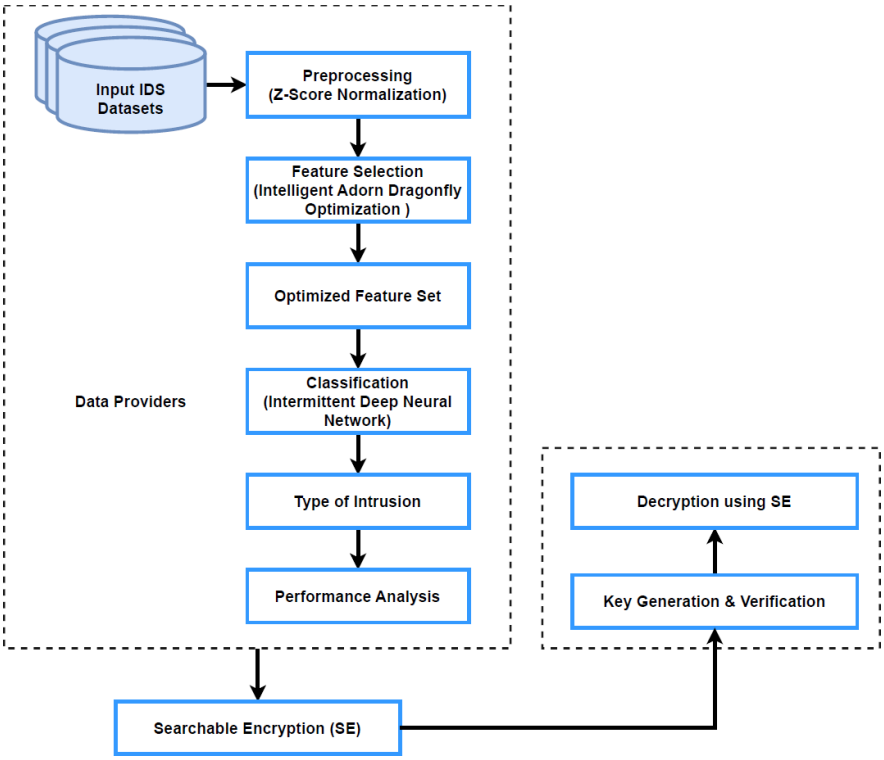

Fig.1. Overall workflow of the proposed work

3.1. Z-Score Normalization based Preprocessing

The input IDS dataset is incomplete and may contain redundant packets and missing values. It is cleaned during preprocessing to get rid of duplicate and redundant instances as well as missing values. Since the network traffic dataset is enormous, sample size reduction techniques must be used. It is necessary to use feature selection techniques to eliminate the unnecessary characteristics from this dataset because it also has a lot of features. Thus, the z-score normalization based preprocessing methodology is used in this work, which generates the complete and balanced data for intrusion detection. The dataset could be standardized during the pre-processing stage, where getting the z-score is the first step in the normalization procedure. After the data have been normalized, the data set can be regulated, which allows the range and data variability to become stable. This procedure should primarily be performed to lessen or completely eradicate data idleness. Following that, the normalized data can be provided as an input for the subsequent processes.

3.2. Intelligent Adorn Dragonfly Optimization (IADO)

The feature selection operation is carried out after normalizing to extract the best features for intrusion detection and classification. Many optimization techniques, including Whale Optimization (WO), Firefly Optimization (FO), Swarm Intelligence (SI), Mayfly Optimization (MO), and others, are employed for feature selection in classical works. The current methodologies, however, have a variety of issues, including low convergence, a need for more iterations to get the best solution, and a lengthy search process. In order to implement a successful IADO optimization algorithm for feature selection, the presented work has this objective.

This algorithm is based on how dragonflies migrate and hunt, which has the similar exploration and exploitation characteristics of the standard optimization process. Below is a list of the three key characteristics that this model emphasizes:

- Separation
- Alignment
- Collaboration

The following model illustrates how the individual particles are separated from their neighbors during separation to prevent collision:

$$G_i = -\sum_{x=1}^{P} H - H_x \quad (1)$$

Where, G_i represents the separation parameter, H and H_x denotes the current position of individual populations, x is the position, and P is the total number of individuals. Then, the mean of velocities is estimated during alignment operation as shown in below:

$$Q_i = \frac{\sum_{x=1}^{P} R_x}{P} \tag{2}$$

Where, Q_i represents the alignment parameter, and R_k indicates the velocity of neighborhood individuals. Then, the cohesiveness is calculated using the attraction of people to the neighborhood's center as shown in below:

$$W_i = \frac{\sum_{x=1}^{P} H_x}{P} - H \tag{3}$$

Where, W_i is the cohesion parameter. Based on the following models, the food source C_i and enemies K_i identified are identified:

$$C_i = H^+ - H \tag{4}$$

$$K_i = H^- - H \tag{5}$$

The following equations are used to describe the factors of step vector and position vector, which are updated in accordance with the movement of dragonflies:

$$\Delta H_{r+1} = (\alpha A_i + \beta B_i + \gamma W_i + \delta K_i + \varepsilon C_i) + \omega \Delta H_r \tag{6}$$

$$\Delta H_{r+1} = H_r + \Delta H_{r+1} \tag{7}$$

Where, $\alpha, \beta, \gamma, \delta, \varepsilon$ are the food vectors, r is the iteration, and ω is the inertia weight factor. The best optimal solution for parameter selection is selected based on the updated position. Fig. 2 depicts the operational flow of the proposed IADO algorithm.

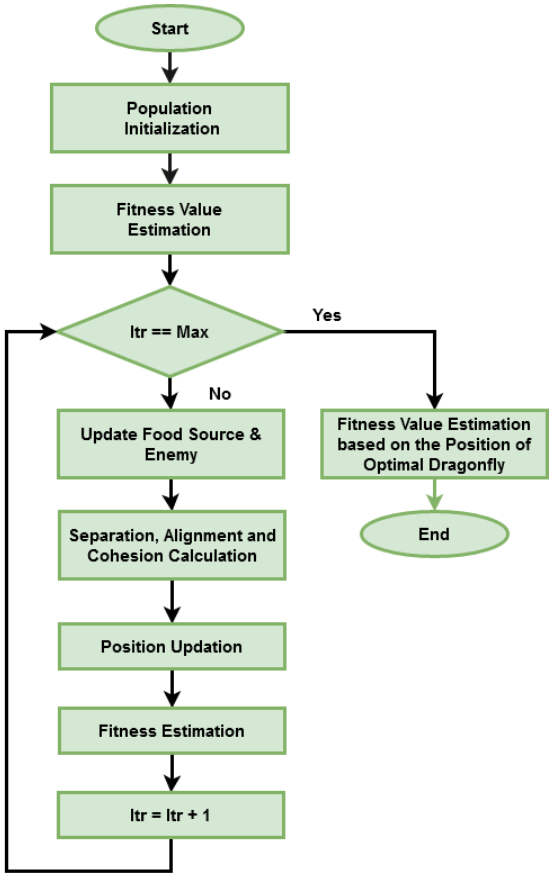

Fig.2. Operational flow of IADO

3.3. Intermittent Deep Neural Network (IDNN)

After feature selection, the trained feature set is used to classify the normal and attacking data using an IDNN algorithm. Various ML/DL approaches, including NB, LR, SVM, KNN, K-means, CNN, LSTM, and others, are applied for IDS applications in the existing works. The setup parameters or hyper parameters in the hidden layers of traditional neural network topologies that are trained using standard backpropagation algorithms suffer from the exploding gradient problem, which can cause the neural network to enter an unstable state. As a result, raising this problem and improving the stability of the neural network response require adding proportional feeding back from the prior state to the present state. However, it has issues related to characteristics such increased overfitting, longer training sessions, complexity, and difficulty implementing. Therefore, the proposed study employs an IDNN algorithm to protect cloud systems against attacks.

Let, consider the feature vector $m^t \in Q^{d*1}$ at time h and dimension d, which may be predicted using the IDNN of order one based on its evenly-spaced prior observations as computed below.

$$m^h = \delta m^{h-1} + x_c + \vartheta^h \tag{8}$$

Where, $\delta \in Q^{d*d}$ is the matrix of the slope coefficients of the model, $x_c \in Q^{d*1}$ is the vector of the regression constants or intercepts, and $\vartheta^h \in Q^{d*1}$ is white noise as the prediction error.

Then, the aforementioned IDNN model can be rewritten as follows:

$$m^{h_n} = \delta(\Delta h_n) m^{h_{n-1}} + x_c(\Delta h_n) + \vartheta^{h_n} \tag{9}$$

Where $\Delta h_n = h_n - h_{n-1}$ is the time gap between the two consecutive data points at time h_n and h_{n-1}, $\delta(.)$ matrix modulated by Δh_n contains the autoregressive effects in the main diagonal and cross- lagged effects in the off-diagonals. Then, the continuous-time autoregressive parameters (drift matrix and bias vector) of $\rho \in Q^{d*d}$ and $\beta \in Q^{d*1}$ i with an exponential solution is defined by using the following model:

$$\frac{dm^h}{dt} = \vartheta y^{h-1} + \beta + \sigma \frac{d\varepsilon^t}{dt} \tag{10}$$

$$m^{h_n} = e^{\vartheta\, \Delta h_n} m^{h_{n-1}} + \vartheta^{-1}(e^{\vartheta\, \Delta h_n} - K_t) + \varepsilon^{h_n} \tag{11}$$

Where, K_t is the identity matrix of size $d \times d$, and $\sigma \in Q^{d*d}$ is the Cholesky triangle of the innovation covariance or diffusion matrix. Here, a power-series expansion can be used to avoid evaluating the matrix exponential function and its derivative as computed in below:

$$e^{\vartheta\, \Delta h_n} = \sum_{y=0}^{\infty} \frac{(\vartheta\, \Delta h_n)^y}{y!} \approx K_t + \vartheta\, \Delta h_n \tag{12}$$

$$m^{h_n} \approx [K_t + \vartheta\, \Delta h_n] m^{h_{n-1}} + \beta\, \Delta h_n + \varepsilon^{h_n} \tag{13}$$

The prior values of the hidden units are stored in recurrent networks for sequence prediction tasks. The final prediction result is produced as follows:

$$OP_{h_n} = \omega_x\, (L_x X_{h_n} + b_x) \tag{14}$$

Where, $X_{h_n} \in Q^{T*T}$ and $OP_{h_n} \in Q^{E*1}$ are the hidden (recurrent) and output layer vectors with T and E nodes, respectively, at an evenly-spaced instant h_n, $L_x \in Q^{T*d}$ and $H_x \in Q^{T*T}$ are the input and hidden weight matrices with K input nodes, $b_x \in Q^{M*1}$ is the hidden bias vector, $L_x \in Q^{T*E}$ and $b_x \in Q^{E*1}$ are the output weight matrix and bias vector, ω_x is hidden layer activation functions. Finally, the output label is predicted as normal or intrusion, which is used to guarantee the security of cloud systems.

3.4. Searchable Encryption (SE)

After classification, the lightweight encryption standard, known as, SE mechanism is employed to ensure the strong security of cloud data. Due to this kind data encryption, the intruders are not able to access the data from cloud. A cryptographic primitive called searchable encryption encrypts data in a way that allows for keyword searches over the encrypted data. The scheme's computational and communication complexity is used to gauge its efficiency. An SE scheme's security has developed through time. There is always a compromise between security at one end of the spectrum and efficiency and query expressiveness at the other end of the spectrum because security is never free. Typically, SE schemes with stronger security also tend to be more complex. The sorts of search queries that are supported, such as the quantity and variety of search keywords and predicates, are determined by the query expressiveness of a SE scheme. The SE provides a technique to effectively access this encrypted database by loosening

the privacy restrictions tiny bit. In particular, SSE leaks data to the server during query execution, which is called leakage. This leakage often comprises both the access pattern, which indicates which files are returned for a query, and the search pattern, which reveals which search queries use the same term. Moreover, it includes the following operations:

- Setup phase – System is modeled with the security parameter and secret key.
- Search – Searching can be enabled according to the requested queries.
- Update – Insertion or deletion of an entry in the database storage.

A SE scheme's functionality also includes any other security or use features it can provide, such as dynamic updates, verifiability, and user revocation, to mention a few. According to the majority of the present methods, the more functionality a SE scheme can accommodate, the more difficult and inefficient its construction will be. As a result, when designing SE schemes, tradeoffs must be made between four different types of factors: functionality versus efficiency, security versus query expressiveness, efficiency versus query expressiveness, and efficiency versus security. Finally, the encryption is carried out using the SE algorithm, in which key creation and verification are carried out in response to user requests. A hash key is generated once a user seeks access to cloud-stored data, and it must be verified by the user in order to serve as authentication. The user can access the data after it has been encrypted if the hash is verified.

4. Results and Discussion

The performance and outcomes of the proposed I^{2}ADO-DNN mechanism are validated in this section using a variety of metrics. To demonstrate the superiority of the suggested approach, the acquired findings are also contrasted with those from more established ML and DL models. Additionally, some of the most well-known and widely-used cyber-threat datasets, such as CSE-CIC-IDS 2018, ISOT, and ISCX, are included in this work for analysis. Fig. 3 and Table 1. shows the comparative analysis among the existing [26] and proposed security methodologies used for protecting cloud networks. One of the most precise metrics scores is accuracy, which measures how well the model performs in terms of producing exact predictions overall. It is necessary to evaluate the model using other performance metric scores, such as recall, precision, and f1-score, in order to have a more complete understanding of how well the model is performing. When all of the actual values are positive and the model receives a very high score from the classifier, recall might be a metric that tells us how well it performs. In addition to being a recognized real value from all of the expected actual values, the proposed IDNN have great precision compared to all other classifiers. It might be a statistic that combines recall and precision by determining its mean value.

Accuracy: The proportion of network packets in the dataset that were successfully identified as attack and benign packets, which is estimated as follows:

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \tag{15}$$

Precision: The proportion of network packets in the dataset that were successfully (or incorrectly) categorized as attack packets out of all attack packets overall.

$$Pre = \frac{TP}{TP+FP} \times 100 \tag{16}$$

Recall: The proportion of attack network packets in the dataset that were successfully classified out of all assault packets, and is computed as follows:

$$Rec = \frac{TP}{TP+FN} \times 100 \tag{17}$$

Error Rate: The proportion of network packets in the dataset that were incorrectly categorized, and is estimated as shown in below:

$$ER = \frac{FP+FN}{TP+FN+FP+TN} \times 100 \tag{18}$$

False Positive Rate (FPR): The proportion of all benign network packets in the dataset that were incorrectly labelled as attack packets, and is computed as follows:

$$FPR = \frac{FP}{FP+TN} \times 100 \tag{19}$$

False Negative Rate (FNR): The proportion of all attack network packets in the sample that were incorrectly labelled as benign packets, and is estimated as follows:

$$FNR = \frac{FN}{TP+FN} \times 100 \tag{20}$$

The total number of network packets that were accurately identified as attack packets is known as a True Positive (TP). The total number of network packets accurately categorized as benign (non-attack) packets is known as a True Negative (TN). The total number of network packets that were incorrectly identified as attack packets is known as a False Positive (FP). The total number of network packets that were incorrectly categorized as benign packets is known as a False Negative (FN). According to the results, it is analyzed that the I^{2}ADO-DNN mechanism provides an improved result, when compared to the other models.

Table 1. Comparative analysis using CSE-CICIDS-2018 dataset

Methods	Accuracy	Precision	Recall	F1-Score
ANN-MLP	99.99	99.96	100	99.9
RF	99.8	99.2	99.8	99.2
KN	99.7	99.8	99.8	99.8
SVM	99.8	90	99.8	99.4
ADA	99.9	99.6	99.8	99.2
NB	99.2	99.2	99.7	99.5
Proposed	99.9	99.9	100	100

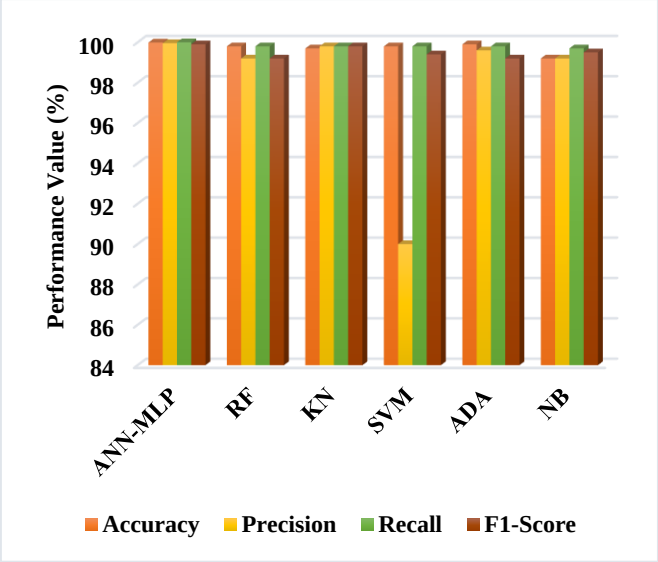

Fig.3. Performance evaluation using CSE-CICIDS-2018 dataset

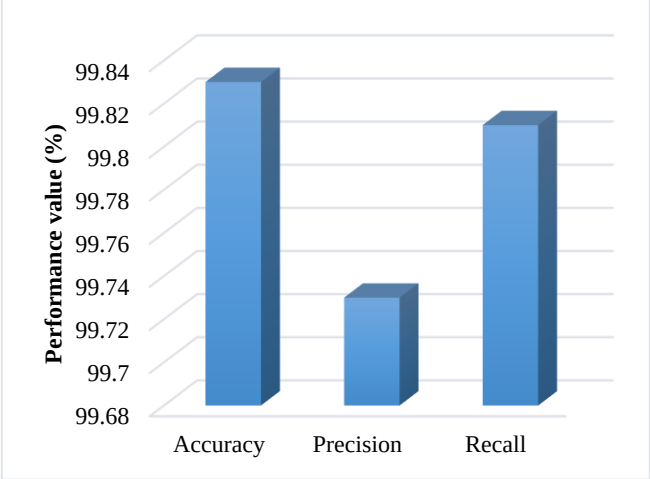

Fig.4. Detection efficiency

Table 2. presents the overall comparative analysis of the proposed I^{2}ADO-DNN mechanism based IDS framework, and its graphical representations are shown in Fig. 4 and Fig. 5 respectively. The estimated results illustrate that the proposed I^{2}ADO-DNN provides an improved results in terms of high accuracy, precision, recall, reduced false and error rate.

Table 2. Overall performance analysis of I2ADO-DNN

Parameters	Performance Value (%)
Classification accuracy	99.83
Precision	99.73
Recall	99.81
Error rate	0.40
FPR	0.42
FNR	0.41

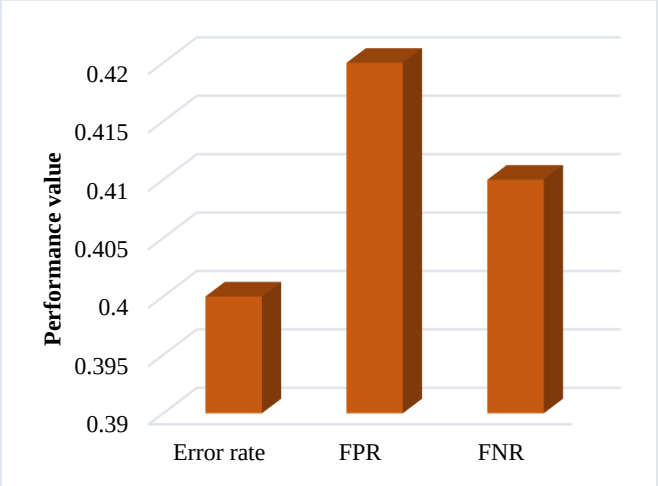

Fig.5. Error and false rate analysis

Fig. 5 and Table 3. compares the intrusion detection rate of existing [27] and proposed feature optimization integrated ML techniques using ISOT dataset. When compared to existing techniques, the proposed I^{2}ADO-DNN model's detection rate is significantly enhanced by using an intelligent feature selection.

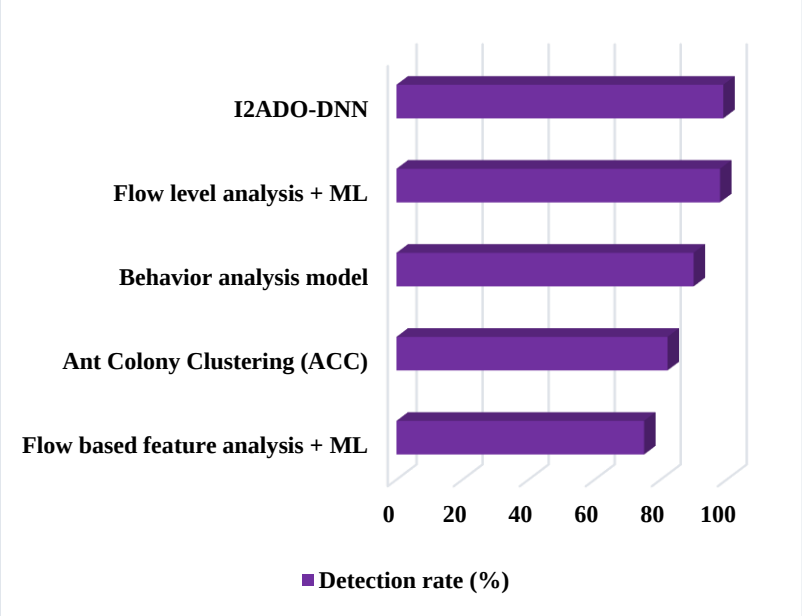

Fig.6. Detection rate

Table 3. Detection rate using ISOT dataset

Techniques	Detection rate (%)
Flow based feature analysis + ML	75
Ant Colony Clustering (ACC)	82.1
Behavior analysis model	90
Flow level analysis + ML	98
I^2ADO-DNN	99

Using the ISCX dataset, Fig. 7 and Table 4 compare the effectiveness of existing [28] and proposed classification approaches in detecting attacks. The proposed I^2ADO-DNN strategy is said to perform better than the current approaches based on the observed findings. The suggested IDS framework has significantly enhanced intrusion detection performance as a result of efficient feature optimization and classification operations.

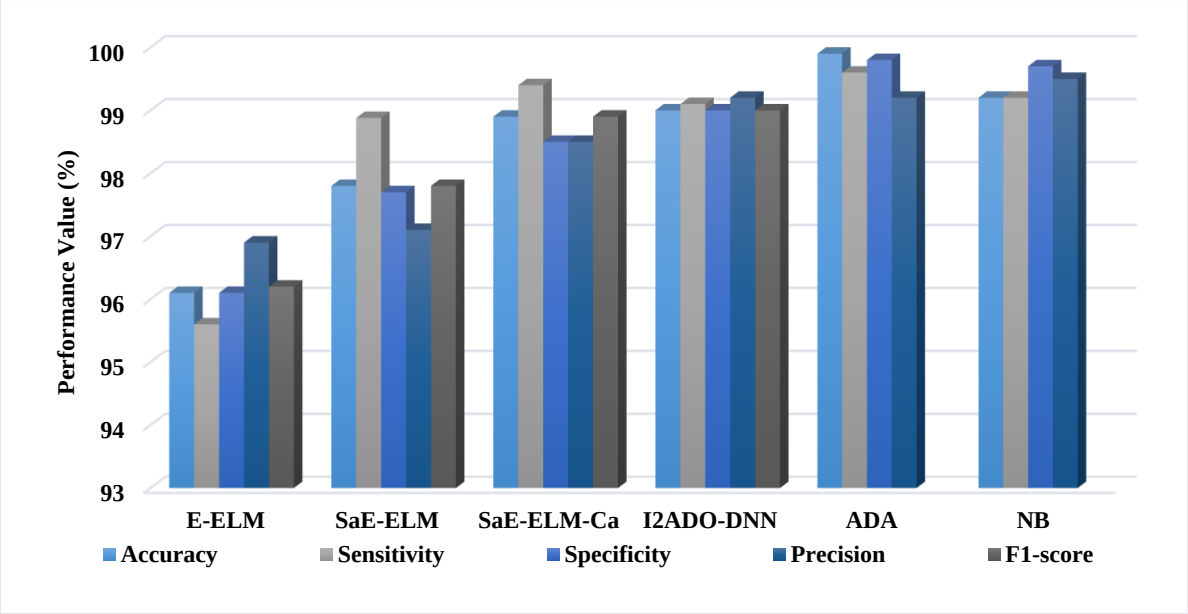

Fig.7. Comparative analysis using ISCX dataset

Table 4. Comparative analysis using ISCX dataset

Methods	Accuracy	Sensitivity	Specificity	Precision	F1-score
E-ELM	96.1	95.6	96.1	96.9	96.2
SaE-ELM	97.8	98.88	97.7	97.1	97.8
SaE-ELM-Ca	98.9	99.4	98.5	98.5	98.9
I^2ADO-DNN	99	99.1	99	99.2	99

5. Conclusions

The security and privacy of cloud systems are ensured by the I2ADO-DNN IDS framework, which is presented in this paper. Popular cyber threats including CSE-CIC-IDS 2018, ISOT, and ISCX datasets have been used in this system. To remove pointless occurrences, redundant fields, and missing values from the dataset, the z-score normalization technique is first used as a preprocessing step. In order to improve the classifier's prediction accuracy, an IADO approach is then utilized to determine which characteristics from the normalized dataset to use. An IDNN classification technique is developed in order to precisely categories the normal and attacking instances in accordance with the ideal set of attributes. By prohibiting attackers from utilizing the data, the SE method is utilized to ensure the privacy preservation of data maintained in the cloud. The exploding gradient problem affects the setup parameters or hyper parameters in the hidden layers of conventional neural network topologies that are trained using conventional backpropagation algorithms, which can result in the neural network entering an unstable state. As a result, in order to address this issue and enhance the stability of the neural network response, proportional feeding back from the prior state to the current state must be added. The primary advantages of using this framework are its simplicity in implementation, high accuracy, privacy guarantee, and improved intrusion detection. For evaluation, the obtained results are also compared with those from older ML and DL models to show the superiority of the proposed approach. It

is obvious that the proposed model provides an increased accuracy up to 99%, while ensuring an increased security to the data. Moreover, the overall attack detection performance is also drastically increased to 99% comparing to the other models. From the overall analysis, it is observed that the detection rate of the proposed I^2ADO-DNN model is greatly improved when compared to previous methods by employing an intelligent feature selection and classification operations.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] V. Chang, L. Golightly, P. Modesti, Q. A. Xu, L. M. T. Doan, K. Hall, *et al.*, "A Survey on Intrusion Detection Systems for Fog and Cloud Computing," *Future Internet*, vol. 14, p. 89, 2022.

[2] Z. Liu, B. Xu, B. Cheng, X. Hu, and M. Darbandi, "Intrusion detection systems in the cloud computing: a comprehensive and deep literature review," *Concurrency and Computation: Practice and Experience*, vol. 34, p. e6646, 2022.

[3] A. Kumar, R. S. Umurzoqovich, N. D. Duong, P. Kanani, A. Kuppusamy, M. Praneesh, *et al.*, "An intrusion identification and prevention for cloud computing: From the perspective of deep learning," *Optik*, vol. 270, p. 170044, 2022.

[4] S. El Kafhali, I. El Mir, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, pp. 223-246, 2022.

[5] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep Generative Learning Models for Cloud Intrusion Detection Systems," *IEEE Transactions on Cybernetics*, 2022.

[6] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A survey of security in cloud, edge, and fog computing," *Sensors*, vol. 22, p. 927, 2022.

[7] P. Ghosh, S. Sinha, R. R. Sharma, and S. Phadikar, "An efficient IDS in cloud environment using feature selection based on DM algorithm," *Journal of Computer Virology and Hacking Techniques*, pp. 1-16, 2022.

[8] S. Naaz, K. Mir, and I. R. Ansari, "Enhancement of Network Security Through Intrusion Detection," in *Soft Computing for Security Applications*, ed: Springer, 2022, pp. 517-527.

[9] M. Almiani, A. Abughazleh, Y. Jararweh, and A. Razaque, "Resilient Back Propagation Neural Network Security Model For Containerized Cloud Computing," *Simulation Modelling Practice and Theory*, vol. 118, p. 102544, 2022.

[10] S. Sobin Soniya and S. Maria Celestin Vigila, "Analysis of Cloud-Based Intrusion Detection System," in *Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, ed: Springer, 2022, pp. 1133-1141.

[11] V. Parganiha, S. P. Shukla, and L. K. Sharma, "Cloud Intrusion Detection Model Based on Deep Belief Network and Grasshopper Optimization," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 13, pp. 1-24, 2022.

[12] D. S. David, M. Anam, C. Kaliappan, S. Arun, and D. Sharma, "Cloud security service for identifying unauthorized user behaviour," *CMC-Computers, Materials & Continua*, vol. 70, pp. 2581-2600, 2022.

[13] P. Ghosh, Z. Alam, R. R. Sharma, and S. Phadikar, "An efficient SGM based IDS in cloud environment," *Computing*, vol. 104, pp. 553-576, 2022.

[14] M. Linadinesh, G. Vanathi, L. Sri Vasundhra, and R. K. Shubhakarini, "CLOUD SECURITYUSING MACHINE LEARNING ALGORITHM," *International Journal of Advanced Engineering Science and Information Technology*, vol. 9, pp. 18-24, 2022.

[15] M. Bhandari, V. S. Gutte, and P. Mundhe, "A Survey Paper on Characteristics and Technique Used for Enhancement of Cloud Computıng and Their Security Issues," in *Pervasive Computing and Social Networking*, ed: Springer, 2022, pp. 217-230.

[16] M. Waqas, K. Kumar, A. A. Laghari, U. Saeed, M. M. Rind, A. A. Shaikh, *et al.*, "Botnet attack detection in Internet of Things devices over cloud environment via machine learning," *Concurrency and Computation: Practice and Experience*, vol. 34, p. e6662, 2022.

[17] A. K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, W. Zhang, and S. Balasubramanian, "A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things," *Cluster Computing*, pp. 1-14, 2022.

[18] M. Saran, R. K. Yadav, and U. N. Tripathi, "Machine Learning based Security for Cloud Computing: A Survey," *International Journal of Applied Engineering Research*, vol. 17, pp. 338-344, 2022.

[19] L. Karuppusamy, J. Ravi, M. Dabbu, and S. Lakshmanan, "Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy," *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, vol. 35, p. e2948, 2022.

[20] G. Sreelatha, A. V. Babu, and D. Midhunchakkaravarthy, "Improved security in cloud using sandpiper and extended equilibrium deep transfer learning based intrusion detection," *Cluster Computing*, pp. 1-16, 2022.

[21] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine learning for cloud security: a systematic review," *IEEE Access*, vol. 9, pp. 20717-20735, 2021.

[22] A. Guezzaz, A. Asimi, Y. Asimi, M. Azrour, and S. Benkirane, "A distributed intrusion detection approach based on machine leaning techniques for a cloud security," in *Intelligent Systems in Big Data, Semantic Web and Machine Learning*, ed: Springer, 2021, pp. 85-94.

[23] M. M. Ahsan, K. D. Gupta, A. K. Nag, S. Poudyal, A. Z. Kouzani, and M. P. Mahmud, "Applications and evaluations of bio-inspired approaches in cloud security: A review," *IEEE Access*, vol. 8, pp. 180799-180814, 2020.

[24] A. Meryem and B. E. Ouahidi, "Hybrid intrusion detection system using machine learning," *Network Security*, vol. 2020, pp. 8-19, 2020.

[25] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, p. 102031, 2020.

[26] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *ICT Express*, vol. 7, pp. 366-370,

2021/09/01/ 2021.
[27] R. Faek, M. Al-Fawa'reh, and M. Al-Fayoumi, "Exposing bot attacks using machine learning and flow level analysis," in *International Conference on Data Science, E-learning and Information Systems 2021*, 2021, pp. 99-106.
[28] G. S. Kushwah and V. Ranga, "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," *Computers & Security*, vol. 105, p. 102260, 2021.

Author's Profiles

Dr. M. Nafees Muneera currently working as Assistant Professor in the Department of Computer Science and Engineering at Sathyabama Institute of Science Technnology. She has more than 7 years of teaching experience. She received her Ph.D in Computer Science and Engineering from Saveetha Institute Of Medical and Technical Sciences and M.E in Computer Science and Engineering from Anna University, Chennai. Her research interests include Data Mining, Artificial Intelligence and Machine Learning.

G. Anbu Selvi obtained her Bachelor's degree in CSE from RVS College of Engg., Madurai Kamaraj University. Then she obtained her Master's degree in Computer Science Engg in SRM University, Ramapuram, Chennai and doing her PhD in Computer Science majoring in the field of Machine learning in SRMIST, Kattankulathur, Chennai, India. Currently, she is a assistant professor of Computer Science Engg, Sathyabama Institute of Science and Technology. Her specializations deep learning, Machine learning and Network security.

V. Vaissnave obtained her Bachelor's degree in Information Technology from PSR Engg College, Anna University. Then she obtained her Master's degree in Computer Science Engg in Anand Institute of Higher Technology, Anna University and doing her PhD in Computer Science majoring in the field of Deep learning in Kalasalingam Academy of Research and Technology, India. Currently, she is an assistant professor of Computer Science Engg, Sathyabama Institute of Science and Technology. Her specializations deep learning and Natural Language Processing, Machine Learning.

Gopal Lal Rajora completed his Bachelor's degree in Electronic Instrumentation and Control Technology and Engineering at the Technical University of Rajasthan, India, in 2015. He received a Master of Science in Applied Telecommunications and Engineering Management from the Universitat Politècnica de Catalunya, Spain. In addition, he has a Master of Science in Finance which he received from the University of Siena, Italy. Since November 2020, he has been working as a Predoctoral Researcher and PhD student at the Institute for Technological Research (IIT) of the Comillas Pontifical University, Madrid, Spain. His areas of interest are Intelligent Systems Area, wireless sensor network, predictive maintenance.

How to cite this paper: M. Nafees Muneera, G. Anbu Selvi, V. Vaissnave, Gopal Lal Rajora, "A Cryptographic based I2ADO-DNN Security Framework for Intrusion Detection in Cloud Systems", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.6, pp.40-51, 2023. DOI:10.5815/ijcnis.2023.06.04