Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:648
doi: 10.56294/sctconf2024648

Category: STEM (Science, Technology, Engineering and Mathematics)

ORIGINAL

A Novel Autoencoder based Federated Deep Transfer Learning and Weighted k-Subspace Network clustering for Intelligent Intrusion Detection for the Internet of Things

Un nuevo autocodificador basado en el aprendizaje de transferencia profundo federado y la agrupación de redes de subespacio k ponderado para la detección inteligente de intrusiones en el Internet de las cosas

V. S. Lavanya[1] ✉, R. Anushiya[1] ✉

[1]Department of Computer Science. P.K.R. Arts College for Women. Gobichettipalayam. India

Cite as: Lavanya VS, Anushiya R. A Novel Autoencoder based Federated Deep Transfer Learning and Weighted k-Subspace Network clustering for Intelligent Intrusion Detection for the Internet of Things. Salud, Ciencia y Tecnología - Serie de Conferencias 2024; 3:648. https://doi.org/10.56294/sctconf2024648

Submitted: 21-12-2023 **Revised:** 02-02-2024 **Accepted:** 22-03-2024 **Published:** 23-03-2024

Editor: Dr. William Castillo-González

ABSTRACT

Federated Learning (FL) has established as a potentially effective practice for cyberattack identification in the last decade, particularly for Internet-of-Things (IoT) structures. FL can increase learning effectiveness, lower transmission overheads, and enhance intrusion detection system (IDS) privacy by spreading the learning process amongst IoT gateways. The absence of labeled data and the distinction of data features for training pose significant obstacles to the deployment of FL in IoT networks. In this research, suggest an Autoencoder based Deep Federated Transfer Learning (ADFTL) to conquer these obstacles. Specifically, Create an ADFTL model utilizing two AutoEncoders (AEs) as the basis. Initially the supervised mode is employed to train the first AE (AE1) on the source datasets while the unsupervised mode is employed to train the second AE (AE2) on the target datasets without label information. The bottleneck layer, or latent representation, of AE2 is forced via the transfer learning method in an effort to resemble the latent representation of AE1. Subsequently, assaults in the input in the target domain are identified employing the latent representation of AE2. Particularly, Weighted k-Subspace Network (WkSNC) clustering is proposed for clustering the dataset and Boosted Sine Cos method (BSCM) is used for feature selection. The requirement that the network datasets utilized in current studies have identical properties is significant since it restricts the effectiveness, adaptability, and scalability of IDS. Nonetheless, the suggested structure can tackle these issues by sharing the “knowledge” of learning among distinct deep learning (DL) simulations, even in cases when their datasets possess dissimilar features. Comprehensive tests on current BoT-IoT datasets demonstrate that the suggested structure can outperform the most advanced DL-based methods by more than 6 %.

Keywords: Federated Learning; Transfer Learning; Internet-of-Things; AutoEncoders; Clustering; Feature Selection and Intrusion Detection Systems.

RESUMEN

El aprendizaje federado (FL) se ha establecido como una práctica potencialmente eficaz para la identificación de ciberataques en la última década, en particular para las estructuras de Internet de las Cosas (IoT). El FL puede aumentar la eficacia del aprendizaje, reducir los gastos generales de transmisión y mejorar la privacidad del sistema de detección de intrusiones (IDS) mediante la difusión del proceso de aprendizaje entre las pasarelas IoT. La ausencia de datos etiquetados y la distinción de las características de los datos

para el entrenamiento suponen obstáculos significativos para el despliegue de FL en las redes IoT. En esta investigación, sugerimos un Aprendizaje de Transferencia Profundo Federado basado en Autoencoder (ADFTL) para superar estos obstáculos. En concreto, se crea un modelo ADFTL utilizando dos Autoencoders (AEs) como base. Inicialmente, el modo supervisado se emplea para entrenar el primer AE (AE1) en los conjuntos de datos de origen, mientras que el modo no supervisado se emplea para entrenar el segundo AE (AE2) en los conjuntos de datos de destino sin información de etiquetas. La capa cuello de botella, o representación latente, de AE2 se fuerza mediante el método de aprendizaje por transferencia en un esfuerzo por parecerse a la representación latente de AE1. Posteriormente, las agresiones en la entrada en el dominio objetivo se identifican empleando la representación latente de AE2. En particular, se propone la agrupación en redes de subespacios k ponderados (WkSNC) para agrupar el conjunto de datos y se utiliza el método Boosted Sine Cos (BSCM) para la selección de características. El requisito de que los conjuntos de datos de red utilizados en los estudios actuales tengan propiedades idénticas es significativo, ya que restringe la eficacia, adaptabilidad y escalabilidad de los IDS. No obstante, la estructura sugerida puede abordar estos problemas compartiendo el "conocimiento" del aprendizaje entre distintas simulaciones de aprendizaje profundo (deep learning, DL), incluso en los casos en que sus conjuntos de datos posean características disímiles. Pruebas exhaustivas en conjuntos de datos actuales de BoT-IoT demuestran que la estructura sugerida puede superar a los métodos más avanzados basados en DL en más de un 6 %.

Palabras clave: Aprendizaje Federado; Aprendizaje de Transferencia; Internet de las Cosas; AutoEncoders; Clustering; Selección de Características y Sistemas de Detección de Intrusos.

INTRODUCTION

Smart transit systems, innovative farming, medical care, and enterprises focused on enhancing economic and social progress are just a few of the domains where the IoT has seen immense expansion in recent times.[1] These IoT structures are made up of several network-enabled devices, actuators, and interconnected sensors.[2] They exchange various kinds of data over both private networks and the Internet infrastructures. By 2025, there will be 75.3 billion actively linked IoT devices on average, according to the Cisco research team.[3] IoT technology differs from conventional internet protocols in that human intervention is not required for data flow across systems. The requirement for more data network bandwidth has increased with the expansion of IoT framework. The majority of IoT framework have limited resources, which makes it difficult to use the conventional security techniques for system defense against cyberattacks. When handling sensitive data is required, serious questions about the IoT device come up. In order to solve the resource-constraint issues in IoT networks, it is imperative to deploy the MEC framework[4], which enables IoTs to offload highly computationally heavy jobs to the proximate edge server.

Cybersecurity should be taken seriously because the IoT is now the engine driving the present technological advancement and the system for gathering real-time dependant data.[5] In order to safeguard the IoT network and the systems that are developed on it, a Network Intrusion Detection System (NIDS) that is proficient of identifying both present and potential threats is required. By observing network traffic, the IDS ascertains whether any dangers are present on the network due to attacks. It is accessible 24/7 to produce data about the system's condition, keep an eye on user activity, and send findings to a monitoring station. IDS is characterized as host-based, network-based, and hybrid-based.[6] Data utilized for recognizing hacking attempts is classified based on its type and source. IDS is missing a standard definition, which is because they view it as any system breach; nonetheless, this also fails to appropriately disclose the problems. To detect and stop assaults on both host-based and network-based structures, enterprises, entrepreneurs, government agencies, the health sector, and even individual users require IDS. The operation has a set of guidelines and procedures to detect any threats, attacks, or incursions that could allow someone to obtain data without authorization or intercept a package en route to its intended destination. Direct Internet connections allow IoT gadgets to be readily exploited and exposed to a variety of risks. While several methods were employed to safeguard such environments, such as firewalls, safe setup, and current updating, none of them are simple to execute and cannot guarantee that the infrastructure will be protected from various threats.[1] IDS offers protection by keeping an eye out for harmful activities or policy infractions on networks or systems. Comparable to a "guard," an IDS, observes the network and offers superior security over other methods. IoT IDS were enhanced in recent years by advances in AI. It is currently necessary to perform a full, current taxonomy and critical evaluation of this latest work. Several ML and DL approaches were utilized in multiple relevant investigations utilizing diverse datasets for verifying the creation of IoT IDS. However, the best dataset, ML method, or DL strategy for creating a successful IoT IDS remains unresolved.[8,9] Second, even though it is essential to the success of "online" IDSs, the time spent developing and testing IoT IDS is not taken into account when evaluating certain IDSs methodologies.

https://doi.org/10.56294/sctconf2024648

By analyzing the current IDSs in usage in this industry, this study suggest a DL-based IDS solution for IoT environments that can improve safeguards, encompassing both host-based and network-based. The following succinctly describes the key findings of this study:

- Here presents a unique framework for mutual learning utilized for recognizing intrusions in decentralized IoT platforms. When compared to traditional DL-based IDS, the suggested structure can increase learning effectiveness and intrusion detection accuracy by fusing the capabilities of FL and TL.
- This study suggests a successful transfer learning strategy that can enable the rich-data network's DL framework to impart valuable knowledge to the low-data network, despite the latter's disparate attributes for IoT network intrusion identification. Also propose effective feature selection and clustering method.
- Finally, conduct in-depth tests on current real-world datasets, such as UNSW and BoT-IoT, to assess where the suggested collaborative learning system performs. According to the findings, the suggested method can outperform the unsupervised learning strategy by up to 6 %.

This is the format for the remainder of the research. In Section II, go over similar works. Next, in Section III, suggest the federated transfer learning approach to detecting intrusions. Section IV then discusses the simulation conditions and outcomes. In Section V, conclude the report by discussing further research.

Related work

Sharma et al.[10] introduced an anomaly-based IDS for IoT. Specifically, a filter-based DNN algorithm for feature selection was provided, in which features with high correlation are eliminated. The framework is also fine-tuned using a variety of variables and hyperparameters. This is carried out utilizing the UNSW-NB15 dataset, which consists of four assault classes. The accuracy of the suggested model was 84 %. GANs were employed to create synthetic data of smaller attacks to solve class imbalance. With a balanced class dataset, they reached 91 % accuracy. A model with insufficient complexity may result in an underfit model and exhibit poor performance on training data. A framework with excessive complexity may result in an overfitting issue that can be resolved by the application of different regularization strategies.

Deep neural network technology along with SI techniques to create an effective IDS for IoT-cloud scenarios can be used.[11] To extract the best properties from the IoT IDS data, deep neural networks are initially employed. Next, an effective feature selection method is suggested, which depends on the newly developed CapSA SI optimizer. Four IoT-Cloud datasets are used to evaluate the CNN-CapSA algorithm's efficiency: NSL-KDD, BoT-IoT, KDD99, and CIC2017. Further, consideration in-depth empirical comparisons utilizing many categorization metrics with alternative optimization strategies. The results confirmed that the devised method performs competitively throughout the entire dataset. Many datasets containing superfluous and useless information are available to address IDS. Thus, this strategy has an extremely high computational expense. Techniques for feature selection employed to overcome this obstacle.

An IDS for Internet of Things smart homes that relies on regression and correlation was presented.[12] The method of clustering was applied to enhance the outcomes. The true and false positive rate were applied to assess the results. The findings demonstrate a 99% true positive rate when comparing the most advanced methods. Although this approach has demonstrated notable efficiency, it is only effective with very large datasets. As a result, different approaches are required to be appropriate for every dataset.

An IDS-SIoEL is a revolutionary IDS for IoT-based smart settings with EL was presented.[13] The structure suggested an ideal anomaly recognition system that combines various feature selection methods with AdaBoost. Employing the GPU, the optional approach was measured on the BoT-IoT, IoT-23, and Edge-IIoT datasets. With 99,9 % record detection rate and 33,68 sec computation times and 0,02156 sec for recognition, this method outperforms current IDS of ACC, recall, and precision. Nevertheless, a few rules are required to fully address the problem of damaged hubs. It was suggested that a model-diminished defect identification technique is required.

The dataset was developed in the UNSW Canberra Cyber in a realistic network setting. The amalgamation of attack and regular traffic data is included in the traffic data. For IoT networks, a highly scalable DNN is created that can aggressively identify IoT botnet attacks. According to the assessment, the DNN operates quite more accurately and precisely than the current methods. Because of the network's diverse components and resource limitations, it is challenging to implement the suggested advanced safety safety measures in IoT frameworks.[14]

An DL-based explainable IDS that enhances the resilience and openness of IoT frameworks were suggested.[15] The structure utilizes a SHAP approach to explain DL-based IDS judgments to professionals so they can guarantee the security of IoT networks and create better cyber-resilient devices. Employing the ToN_IoT dataset, the suggested structure was verified and contrasted with other strong methods. With a 98,83 % F1 score and a 99,15 % accuracy, the testing findings demonstrate the outstanding efficacy of the suggested structure and its capacity to defend IoV networks from advanced cyberattacks. Although even professionals find it difficult to understand the reasoning behind the projections made by this kind of ML approach, it has a high

https://doi.org/10.56294/sctconf2024648

false-positive rate. Understanding or being able to comprehend the reasoning driving an IDS's blocking decision a certain packet assists cybersecurity specialists in confirming its acquiring and developing other cyber-resilient technologies.

An IoT NID procedure relying on the LNN were proposed.[15] Use the PCA method to minimise the features dimensionality to avert high-dimensional raw traffic data that could result in an elaborate model. In order to perform efficient feature extraction at a low computational expense, the classifier makes use of the compression and expansion framework, the inverse residual framework, and the channel shuffle process. In order to address the issue of unequal sample distribution in the multiclassification position, substitute the usual cross-entropy loss with the NID loss, which functions as an improved loss function. Studies on two NID data sets determine that this technique is acceptable for sorting IoT traffic in normal and attack circumstances, with accuracy for sorting at low level of difficulty and modest model size. The real implementation of DL-based high-complexity algorithms is hampered by the constrained computation and storage capacities of IoT gadgets.

A PSO-LightGBM for the intrusion detection was introduced.[16] The characteristics of the data are extracted utilizing PSO-LightGBM, which then feeds the features into OCSVM to identify and classify harmful data. The IDS is validated employing the UNSW-NB15 dataset. The outcomes demonstrate that the framework provide can identify a variety of harmful or benign data, particularly tiny sample data like worms, backdoors, and shellcode. The low detection rate and limited scalability of this suggested IDS prevent it from adjusting to the intricate and dynamic IoT environment.

IDS built on DBN and GA[17] is a layer's optimal quantity of neurons and hidden layers are generated adaptively in response to various kinds of attacks over repeated GA iterations, enabling the IDS centered DBN to accomplish a high detection rate with an efficient layout. The framework was evaluated and simulated utilizing the NSL-KDD dataset. The findings demonstrate that the enhanced IDS in conjunction with DBN effectively raise the intrusion attack detection rate while lowering the intricacy of the neural network architecture. When it comes to the suggested IDS, a model of a neural network might detect one type of attack with great accuracy, but it might not detect other types of attacks effectively. Designing a self-adaptive framework to modify the network architecture for various attack is thus urgently needed.

Inference: In contrast, there are several real-world difficulties that DL-based cyberattack detection mechanisms has to conquer. Especially, large amounts of data are typically needed for outstanding results in conventional DL algorithms. Transmitting such a substantial quantity of data over the network adds to the communication load in addition to privacy considerations. As a result, these restrictions have made it more difficult for DL approaches to be useful in cyberattack detection devices. The application of FL has shown to be a very successful solution for these issues. Traditional DL methods gather data and train the global archetypal at a central server; in contrast, FL allows learning to happen amongst all devices. Nevertheless, it could be expensive and time-consuming to obtain enough labeled data. Even when the data are accessible, the user data that gets involved in typically has distinct feature sets.[19,20]

This makes FL's process of aggregating the global representation challenging or perhaps error-prone. As such, they might not be appropriate for FL's rigorous training regimen. Transfer learning (TL) has emerged as a possible method to overcome these restrictions, particularly in situations with diverse training data. In contrast to DL and FL methods, which are trained exclusively for certain issues, TL can leverage “knowledge” from rich resource data to improve the ML algorithms’ effectiveness and training processes. TL explicitly address the paucity of labeled data by transferring “knowledge” from comparable situations with abundant high-quality data. Suggest a hybrid learning architecture to succeed the obstacles of traditional DL-based IDS by leveraging the advantages of both TL and FL.[21,22,23,24,25]

Proposed Methodology

The network architecture that employs ADFTL for IoT threat detection is shown in Figure 3. Initially, all IoT device data is gathered by the data collection function, WkSNC is proposed for clustering the dataset and BSCM is used for feature selection. There are labeled and unlabeled data in the training set. Certain IoT devices that are optimized for data labeling are the source of the labeled data.[26,27,28,29] Second, the ADFTL algorithm receives the gathered data and uses it for training. The training procedure makes an effort to translate the knowledge data acquired from labeled data to unlabeled data. The disparity among latent representations of the target and source data is minimized to accomplish this. Following training, the detection system employs the trained ADFTL framework to identify incoming traffic from every IoT device as either attack or regular data. The next section explains a thorough explanation of the ADFTL paradigm.[30,31,32,33,34,35]

Input Data collection and feature extraction

The raw network traffic needs to be gathered in the first stage. Utilize the BoTNeTIoT-L01[19,36,37,38,39] publicly accessible dataset and UNSW-NB15[20,40,41,42,43] as the sources of raw traffic in this study. Attacks are denoted by 0 in the dataset class label and normal samples by 1. The next step involves obtaining packet-level labels

from the raw network traffic and extracting pertinent fields (each field corresponding to a feature) from these packets. A method utilizing aggregated packet data, the features employed on header field data from individual packets. Broad traffic features might be tracked instead of producing attack-specific data which was useful in recognizing specific threat activities. After that, the 344 PCAP files were analyzed utilizing the TShark application to extract the header fields of individual packets. The packets were labeled and saved as CSV files. Here, the PCAP files were limited to IP packets, and a 29 packet header fields were extracted. Since ARP packets are needed to convert IP addresses to MAC addresses and are unrelated to the attacks that are suggested in the dataset, they were eliminated.

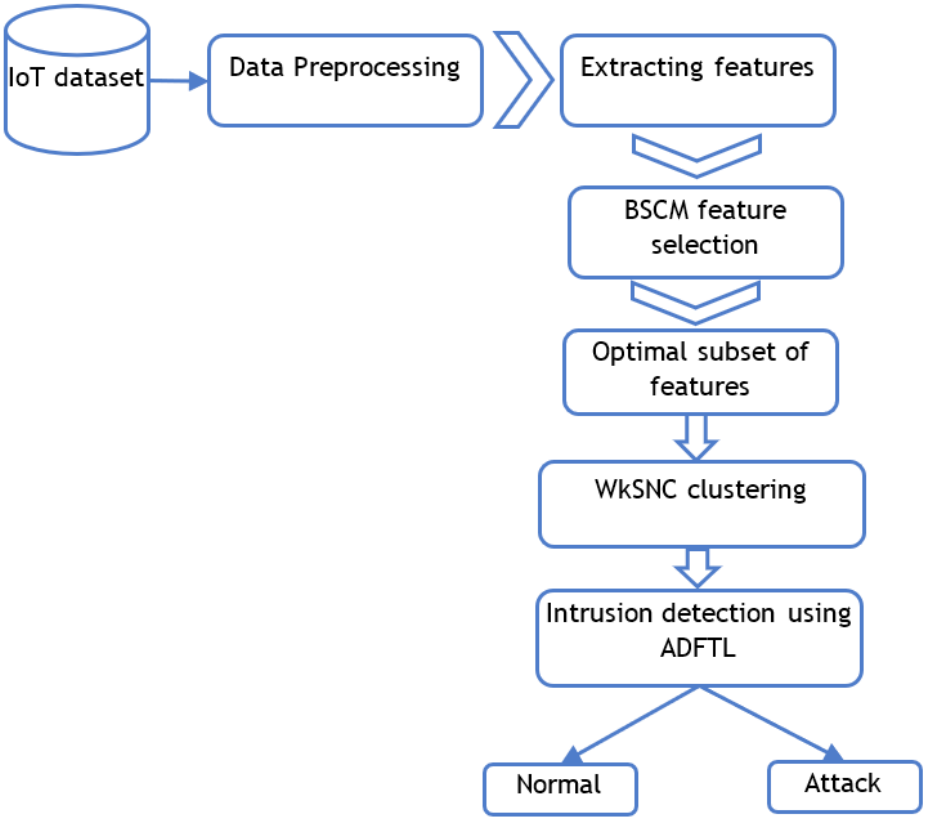


Figure 1. Flow diagram of proposed methodology

Feature selection using BSCM

A crucial step that comes before categorization is feature selection, which aids in eliminating superfluous or undesired features from the whole feature set. FS methods choose the discriminative features by minimizing the feature dimension. This study presents a novel wrapper-based sine-cosine algorithm, the details of which are expounded upon in the next section. The equation of the cosine and sine functions, whose values are determined within a certain range, are utilized by the wrapper-based search method known as the BSCM algorithm.[44,45,46] Algorithm 1 describes the pseudo-code of the BSCM method and the way it operates. Each feature in each dataset is associated with a dimension, and each variable is fixed to fall between [0, 1]. The selection and rejection of features are determined by the search agents' position; that is, if the position value is [0, 5], the feature is assumed to be selected, and if not, it is assumed to be rejected.

The fitness function is employed to gauge the search agents' quality following random initialization. The greatest solutions were successfully found thus far will be considered when evaluating the fitness function of the initial population. This will allow for the evaluation of future solutions. After going through multiple iterations (generations), BSCM arrives at the desired outcome. As the iteration counter rises, the sine and cosine function ranges will be adjusted. Eventually, the method stops itself upon meeting the termination conditions after arriving at the most optimal solution for the particular problem area. The BSCM method's search process first produces a random collection of search agents, each of whose fitness is assessed utilizing a fitness function. This single minimization fitness function FF incorporates the classification error rate and the quantity of features, as shown below:

$$FF=\omega\times Error+(1-\omega)((number\ of\ features\ selected)/(Total\ number\ of\ features)) \quad (1)$$

https://doi.org/10.56294/sctconf2024648

here ω = equalization factor (0.9). When the error rate and feature value are combined into a single fitness function, the relative relevance of the feature value is denoted by a, and the relative importance of the error rate is represented by (1 - ω). The initial population Pop finds an improved solution following the fitness evaluation, and its location will be adjusted. Eq. (2), which is provided below, serves to update location with respect to the destination solution.

$$X_i^{i+1} = \begin{cases} X_i^t + rand_1 x \sin(rand_2) x |rand_3 Pop_i^t - X_i^t| & rand_4 < 0{,}5 \\ X_i^t + rand_1 x \cos(rand_2) x |rand_3 Pop_i^t - X_i^t| & rand_4 \geq 0{,}5 \end{cases} \quad (2)$$

Fitness of the novel population is assessed upon position update utilizing Eq. (2). Subsequently, the revised population position is determined based on two criteria (Criteria I and Criteria II),[47,48,49] which are listed below:

Criteria I: If the fitness of the present population is higher than that of the prior population, the present one will be upgraded.

Criteria II: If the present population's fitness is identical as that of the prior one and its feature count is lower, the present sample will be updated.

In this case, elitism is added to the newly acquired population and iterated, meaning that the two search agents with the lowest fit are swapped out for the two with the highest fit. The algorithm repeats this 20 times until ending on its own after 100 iterations, which is the stopping condition. When BSCM reaches the maximum number of iterations, it finally finds the optimal solution. Due to this alteration, the basic SCA algorithm and BSCM are not the same.[50,51,52,53] This adaptive method of reorganizing the existing population into the optimal solution enhances BSCM's search performance.

Input: Initialize the features of input dataset

Output: Optimal features

- Generate search agent random set and update the best solution
- While (t<max no. of generations)
- Perform elitism concept to boost SCA //proposed BSCM
- Choose $rand_1$, $rand_2$, $rand_3$, $rand_4$ //random numbers between 0 and 1
- Update the position of search agent using
- Evaluate the as in Eq.(1)
- If FF (current)<FF (previous) then
- Update the best solution
- Else if FF (current)=FF (previous)&no.of selected features<no.of selected features(previous) then
- Update the best solution & its position
- End if
- Replace the least optimal search agents with elitism and update the new position
- End while
- Provide back the most effective solution found thus far.

Weighted k-Subspace Network Clustering

Indeed, the k-means technique is generalized by k-subspace clustering. Finding the best k subspaces for a set of samples and placing them in the closest subspace is the aim of k-subspace clustering. This is one way to organize the intuition:

$$\min_{\{SS_k\},\{\alpha_{ik}\}} \sum_{k=1}^{K} \sum_{i=1}^{n} \alpha_{ik} \|x_i - SS_k SS_k^T x_i\|_2^2 \ \alpha_{ik} \in \{0,1\} \quad (3)$$

where $SS_k \in R^{(d \times q)}$, $k \in \{1,2,\ldots,K\}$ is the base of the k-th feature subspace, and α_{ik} denotes the assignment of X_i to SS_k. Generally, the Expectation Maximization (EM) technique is employed by the method to update the subspaces $\{SS_k\}$ and assignments $\{\alpha_{ik}\}$ alternately. To be more precise, given an initialization of k subspaces, the closest subspace receives optimal features by

$$\alpha_{ik} = \begin{cases} 1 & if\ k = \arg \min_{j=\{1,2,\ldots,k\}} \|x_i - SS_k SS_k^T x_i\|_2^2 \\ 0 & otherwise \end{cases} \quad (4)$$

https://doi.org/10.56294/sctconf2024648

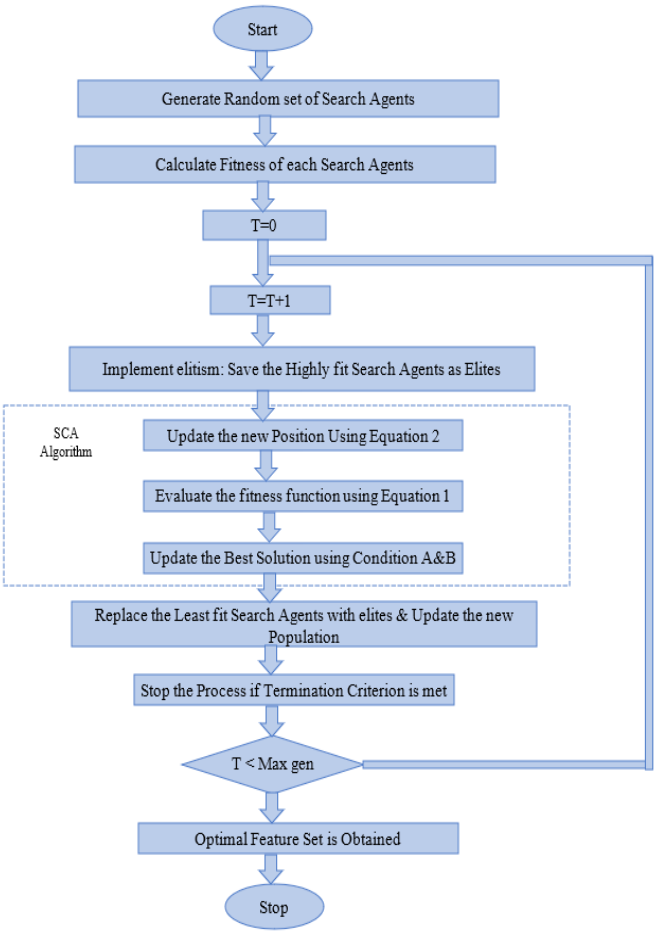


Figure 2. Flowchart of BSCM algorithm

Then Singular Value Decomposition (SVD) is applied to the features that are part of the same cluster in order to update the bases of k subspaces. The object function converges to a local minimum after a number of iterations. DNN is used in the newly suggested kSCN[22] to k-subspace clustering technique, enhancing efficiency while processing large-scale and high-dimensional datasets. Nevertheless, initialization and outlier vulnerability continue to be problems for kSCN. In order to solve this issue, an assignment network computes the membership assignment α_i in this model utilizing soft probability as opposed to hard assignment. The weight ω_i in the assignment network is calculated by

$$\omega_i = \frac{exp^{h_i}}{\sum_{k=1}^{K} exp^{h_{i,k}}}, \text{ where } h_i = h_\varphi(z_i) \quad (5)$$

here $h_\varphi(z_i)$ signifies the transform of fully connected layers. ω_i is initiated by Softmax such that $\omega_{ik} \in [0, 1]$. More complex data can be fitted and the sensitivity to outliers can be better controlled by employing this clsutering to infer the soft clustering assignments. Construct the regularization of soft assignments to effectively mitigate the impact of initialization and avoid some simple solutions:

$$-\sum_{i=1}^{n} \omega_i^T \omega_i + \|\tilde{\omega}\|_2^2, \text{ where } \tilde{\omega} = \frac{1}{n}\sum_{i=1}^{n} \omega_i \quad (6)$$

Given $-\sum_{i=1}^{n} \omega_i^T \omega_i + \|\tilde{\omega}\|_2^2$,

will eventually result in sparse assignment probabilities, allowing each sample to be allocated to a single dominant cluster. Employ the l_2 norm to enforce ω to be uniform to prevent the assignment network from producing the same one-hot vector for every sample, which is known as the trivial minimizer of clustering loss. The probabilities $prob_{ik}$ are obtained by mapping each latent representation z_i retrieved by the encoder to K subspaces utilizing a k-subspace clustering network. In this study, the clustering loss, which is the total of the

https://doi.org/10.56294/sctconf2024648

projection residuals to k subspaces is embedded with soft assignments. The objective function of WkSNC can be written by,

$$OF_c(\vartheta_e, \varphi, \{SS_{ik}\}) = \sum_{k=1}^{K}\sum_{i=1}^{n} \omega_{ik}\|z_i - prob_{ik}\| - \alpha \sum_{i=1}^{n} \omega_i^T \omega_i + \rho\|\tilde{\omega}\|_2^2 \quad (7)$$

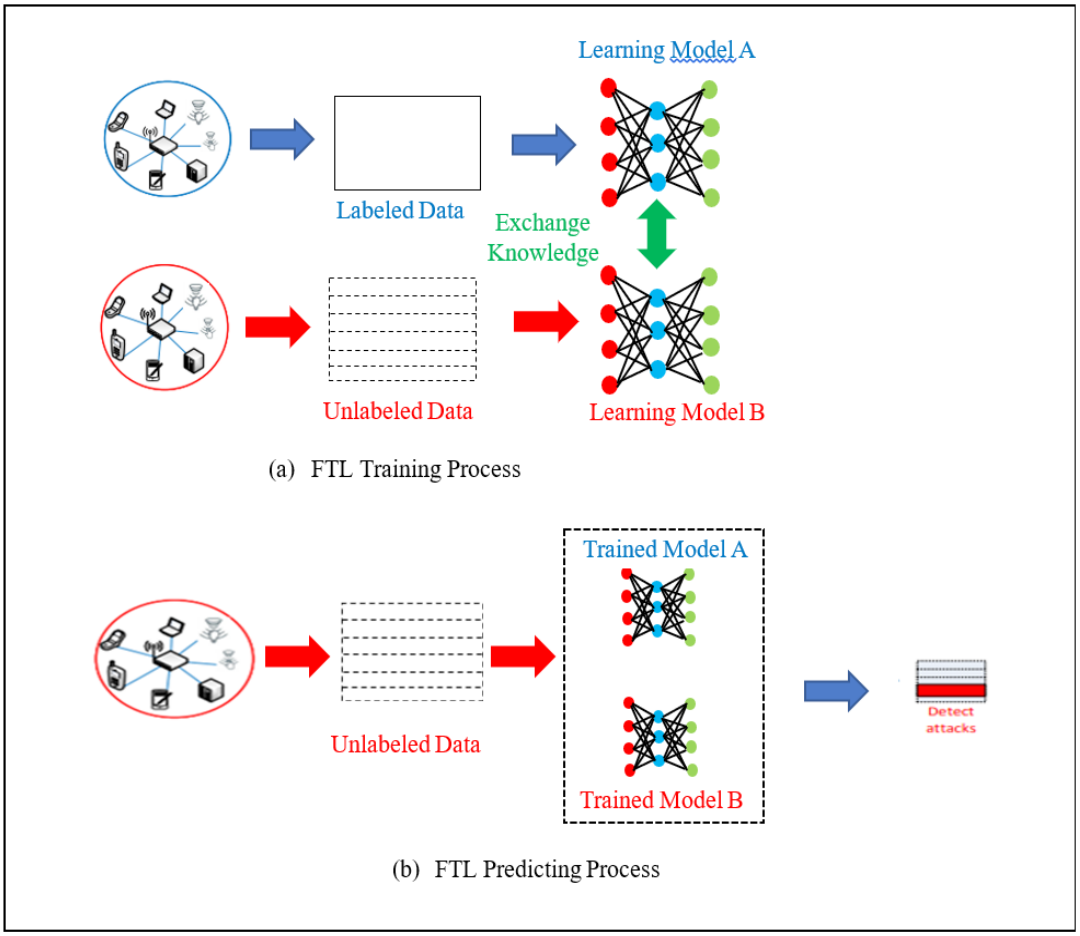
$$\text{Where } prob_{ik} = SS_k SS_k^T z_i$$

where ω_i is learned by Eq. (7), α and ρ are balance parameters. At the same time as grouping the data, reducing the weighted clustering loss will search for the best k subspaces. essentially, one can prevent the unwanted local minima by setting the network's settings utilizing a different fundamental clustering approach. Nevertheless, initializing the bases of the k subspaces is not simple. In order to learn the assignment network, two regularizations must be applied. Ultimately, clustering will be performed well by the right approach for selecting α and ρ. To prevent trivial solutions, it is intuitive to start the training process with somewhat bigger α and ρ. As the training process progresses, α and ρ are subsequently dynamically decreased.

Intrusion detection using ADFTL

Here, a very efficient DFTL model was suggested that can transfer information across many networks, each with its own set of features, and an unlabeled network. Examine an instance where one labeled network is utilized as a source network to assist the unlabeled network to further assess the effects of the suggested technique. It is simple to extend the case with one unlabeled network and several labeled networks, and it can be left for further research. The training and prediction procedures of the DFTL technique, which employ in this instance, are shown in Figure 3. Table I displays the table of notations. As previously mentioned, Network A and Network B, each have a dataset called DS^A, DS^B. Network B has an unlabeled cybersecurity dataset called DS={X, OF} with (X) = $\{x_1, x_2, \ldots, x_N\}$, where N is dataset samples number and OF is the network's optimal feature spaces. Additionally, they have two initialized parameter sets, w^A and w^B. Two neural networks' outputs Y are computed as follows,

$$Z^A = w^A * X^A \text{ and } Z^B = w^B * X^B \quad (8)$$



https://doi.org/10.56294/sctconf2024648

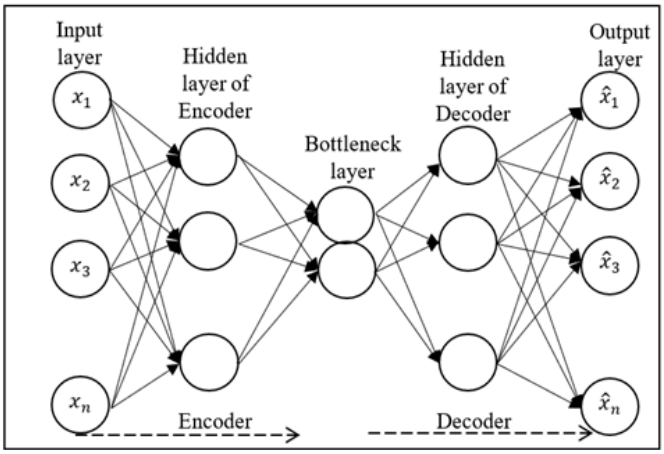


Figure 3. Architecture diagram of DFTL Algorithm

To determine the prediction function (*PF*) needed to forecast Network B's output. In order to identify a high-quality predict function, the labeled dataset has to be utilized first to minimize the loss function (LF) as follows:

$$\arg\min_{\mathbb{w}^A,\mathbb{w}^B} LF^B = \sum_{i=1}^{N_{cl}} LF^B\left(y_i^A, PF(z_i^B)\right) \quad (9)$$

Where N_{cl} is predicted labels number, the outputs of model is z and the labels of a dataset is y, and LF^B displays the loss of the logistic loss function, that dependent on the output type has the labelled y and the projected value z: $LF^B(z,y)=\log(1+\exp(-z\times y))$ (10)

Further, there's a chance that datasets and have some overlying samples. In this case, stands for the overlying samples among datasets A and B, and these samples utilized to enhance the loss function. The alignment loss function across A and B needs to be minimized in this case as shown below.

$$\arg\min_{\mathbb{w}^A,\mathbb{w}^B} LF^{AB} = -\sum_i^{N_{AB}} LF^{AB}\left(PF(z_i^A), PF(z_i^B)\right) \quad (11)$$

Where LF^{AB} signifies the alignment loss function and the common alignment loss function denoted in modulus $LF^{AB}= \|z_i^A - z_i^B\|^2$ or angle $LF^{AB}= -z_j^A * z_j^B$ add the regularization $LF^A_{Reg}=\sum_l^{layers\ A} \|\varsigma^A_l\|$ and $LF^B_{Reg}=\sum_l^{layers\ B} \|\varsigma^A_l\|$ in which ς is training parameter $layers_A$ and $layers_B$ are the number of layers in Neutron Networks A and B to determine the ultimate loss function that must be reduced:

$$\arg\min_{\mathbb{w}^A,\mathbb{w}} LF = LF^B + \kappa LF^{AB} + \frac{\nu}{2}\left(LF^A_{Reg} + LF^B_{Reg}\right) \quad (12)$$

where and are the weight parameters and the gradient for updating w^A,w are estimated as:

$$\frac{\partial LF}{\partial \mathbb{w}_l^i} = \frac{\partial LF^B}{\partial \mathbb{w}_l^i} + \kappa * \frac{\partial LF^{AB}}{\partial \mathbb{w}_l^i} + \nu * \mathbb{w}_l^i \quad (13)$$

The two AEs (AE1 and AE2) in the suggested ADFTL model share the same structure as Figure 3. The ideal feature samples from the source domain OF^i_{SD} are the input of AE1, while the ideal feature samples from the target domain OF^i_{TD} are the input of AE2. The AE loss function is minimized during the training process. The reconstruction error (RE) term and the supervised (SE) term are the two terms which make this loss function. The final loss function of proposed method is:

$$\arg\min_{\mathbb{w}^A,\mathbb{w}} LF = LF^B + \kappa LF^{AB} + \frac{\nu}{2}\left(LF^A_{Reg} + LF^B_{Reg}\right) + LF_{RE} + LF_{SE} \quad (14)$$

Where $LF_{RE} = LF\left(x^i_{SD} + \hat{x}^i_{SD}\right) + LF\left(x^i_{TD} + \hat{x}^i_{TD}\right)$ and $LF_{SE} = -\sum_{j=1}^{cl} y^{i,j}_{SD} * \log\left(z^{i,j}_{SD}\right)$

For instance, identical cyberattack types target various networks' value of IoT devices. Network A utilizes the packet header, timeslot, and IP address to extract attack data, whereas Network B utilizes the error packets, MAC address, and frame header. The method of learning across two networks is firmly backed by the quantity of mutual samples, which is a significant variable. Next, use Eq. (14) to determine the gradient and final loss function (LF). In the end, the gradient and loss functions are utilized by Networks A and B to modify their system's variables. In order to reduce the final loss function, this method is repeated continuously until

https://doi.org/10.56294/sctconf2024648

the framework converges its extreme iterations quantity. After training is finished, the unlabeled dataset DS's ultimate outcome is predicted utilizing the procedure outlined in Algorithm 2. Each Network A and Network B have trained models for that procedure. Z^B is initially calculated by the dataset DS using the trained model of Network B, same like in the training procedure. Next, in order to preserve the transfer learning knowledge from Network A's trained model, Network B sends Z^B to Network A. In order to categorize the attack and the network's typical actions, Network A forecasts the outcomes and provides them back to Network B.

Algorithm 1. The pseudocode of proposed ADFTL for intrusion detection

Detection process:

Input: The learning rate lr, the weight parameter k and v, the maximum iteration iter, the tolerance tl and Network A and Network B set model parameters W^A and W^B.

Output: The trained model parameter W^A and W^B;

- Initially iteration = 0
- while iteration ≤ iter do
- Network A performs: $Z^A_i = W^A_i * X^A_i$
- Send { Z^A_i, Y^A, X_{SD} } to Network B;
- Put Network A as X_{SD} to the input of AE1.
- Lk (X_{SD}) is the representation of X_{SD} at the layer k of AE1
- Z_{SD} is the representation of X_{SD} at the bottleneck layer of AE1
- Network B performs: $Z^B_i = W^B_i * X^B_i$
- Put Network B as X_{TD} to the input of AE2
- Lk (X_{TD}) is the representation of X_{TD} at the layer k of AE2
- Send { Z^B_i, X_{TD} } to Network A;
- Training the ADFTL model by minimizing the loss function in (14)
- X_{TD}=softmax (Z_{TD})
- Network A performs: Calculate $\partial LF / (\partial w^A_l)$ and LF^A, forward to Network B and Update $w^A_l = w^A_l - lr * (\partial LF / (\partial w^A_l))$
- Network B performs: Calculate $\partial LF / (\partial w^B_l)$ and LF^B, forward to Network A and copue Update $w^B_l = w^B_l - lr * (\partial LF / (\partial w^B_l))$
- If LF_{prev} - LF ≤ tl then
- Send stop signal to Network B;
- Break the connection.
- else
- LF_{prev} = LF then do iteration = iter + 1;
- continue;
- end if
- end while

Prediction Process:

- Initialize the model parameters W^A and W^B and dataset X_{DS};
- Network B performs: $Z^A_i = W^B_i * X^B_i$
- Send {$Z^B_i = X_{TD}$} to Network A;
- Network A performs:
- Compute Probability (Z^B_i) = $W^A[Z^B_i]$ and send it to Network B.
- Return Y_{TD}
- END.

The Bot-IoT and UNSW-NB15 data sets are united to create a single customized data set, which utilized by the suggested IIDS framework to train the CSRvNN utilizing 26 features. Both binary and multi-class classifications have an average classification accuracy that is higher than 96%. The findings demonstrate the relevance of the suggested technique in IoT settings and its improved accuracy in detecting various forms of intrusions through the use of flow and TCP features. Each object in the study is described by 41 attributes that come together to form a vector. Be aware that not all features are nominal and that some are continuous. These nominal values must be initially transformed to continuous values since the clustering and classification methods need continuous values. The training data should be divided into subsets for the fuzzy clustering module employing the AKM clustering module, and CSRvNN should be utilized for identifying intrusions.

Evaluation Metrics: The efficacy of ML techniques was assessed using a number of measures on the suggested

https://doi.org/10.56294/sctconf2024648

IIoT dataset. Specifically, the efficacy of the chosen approaches such as proposed ADFTL, CSRvNN, GWO-PSO-RF,[23] MOPSO-Lévy-KNN[24] and AAFSA with GA-FR-CNN was statistically assessed using F-score, accuracy, recall, and precision. The fraction of correctly recognized normal and attack observations is the accuracy statistic, which indicates a system's general efficacy. The recall measure displays the ratio of successfully identified assaults to all attack data in the test dataset. The precision measure displays the proportion of accurately identified attack observations relative to all attacks that were detected. The harmonic (equally-weighted) mean of precision and recall is determined by the F-score.

$$\text{Precision}=TP/(TP+FP)\times 100 \quad (15)$$

$$\text{Recall}=TP/(TP+FN)\times 100 \quad (16)$$

$$\text{F-measure}=2*((\text{precision}*\text{recall})/(\text{precision}+\text{recall})) \quad (17)$$

$$\text{Accuracy}=(TP+TN)/(TP+FP+TN+FN)\times 100 \quad (18)$$

False Negative (FN) represents the quantity of actual attack cases which falsely defined as normal, True Positive (TP) signifies the quantity of actual attack records which accurately recognized as attacks, True Negative (TN) signifies the quantity of actual normal data which is properly categorized as normal, and False Positive (FP) signifies the quantity of actual normal events which mistakenly recognized as attacks.

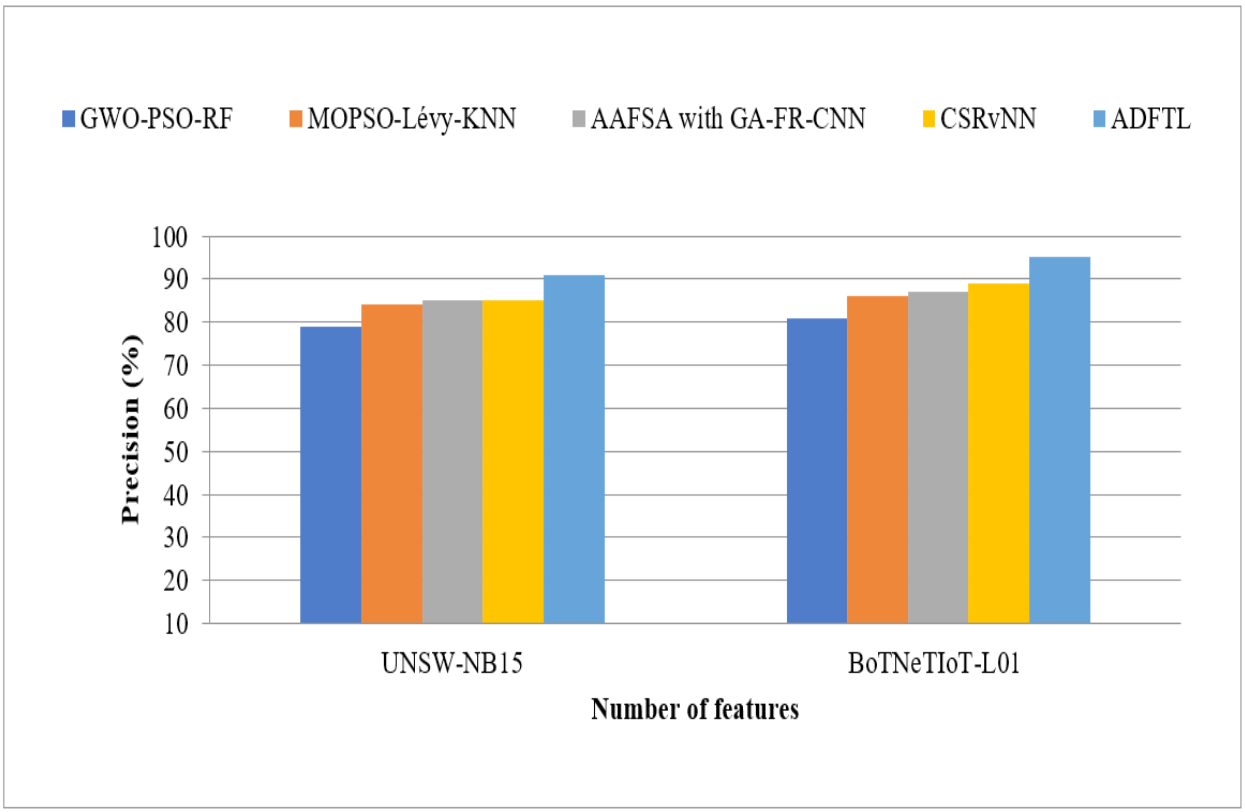


Figure 4. Result of Precision

Figure 4 specifies the precision of suggested and present system for the features quantity in given databases. While quantity of features is increasing, the corresponding precision is exploited. For e.g., UNSW-NB15, the AAFSA with GA-FR-CNN presents a precision of 85 %, proposed CSRvNN provides 85 % and proposed ADFTL attains 91 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. For BoTNeTIoT-L01, the AAFSA with GA-FR-CNN provides a precision of 87 %, proposed CSRvNN provides 89 % and proposed ADFTL attains 95 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. The framework's resistance to multi-type and unbalanced attacks is confirmed by outcomes, which set it apart from other DL frameworks. Overall, it was noted that the proposed classification achieved better results due to introducing WkSNC clustering method, ADFTL's detecting precision can be improved.

https://doi.org/10.56294/sctconf2024648

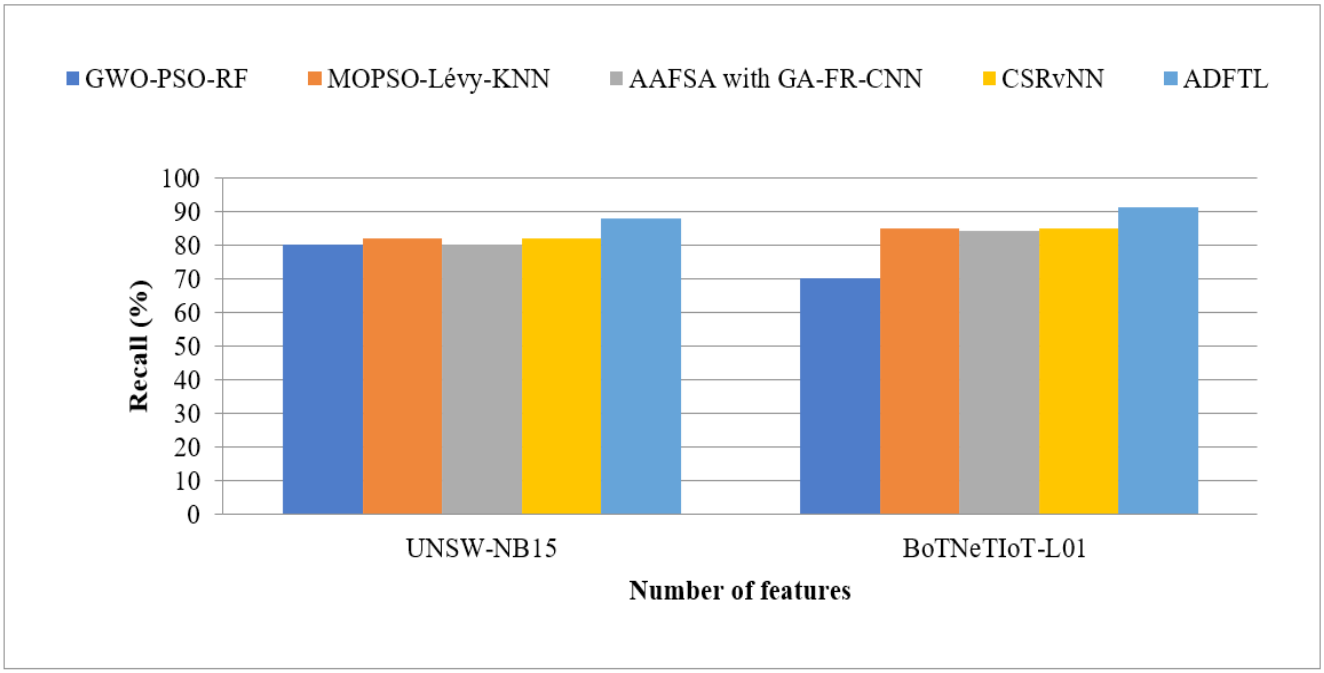


Figure 5. Result of Recall

The recall of optional and present approaches for the number of features in a given database is revealed in Figure 5. Maximizing the amount of features also maximizes the recall. For example, the AAFSA with GA-FR-CNN yields an 80 % recall for UNSW-NB15, proposed CSRvNN provides 82 % and proposed ADFTL attains 88 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. For BoTNeTIoT-L01, the AAFSA with GA-FR-CNN provides a recall of 84 %, proposed CSRvNN provides 85 % and proposed ADFTL attains 91 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. Note that the recall of ADFTL is more because BSCM chosen the optimal features the training time will increase the recall measure.

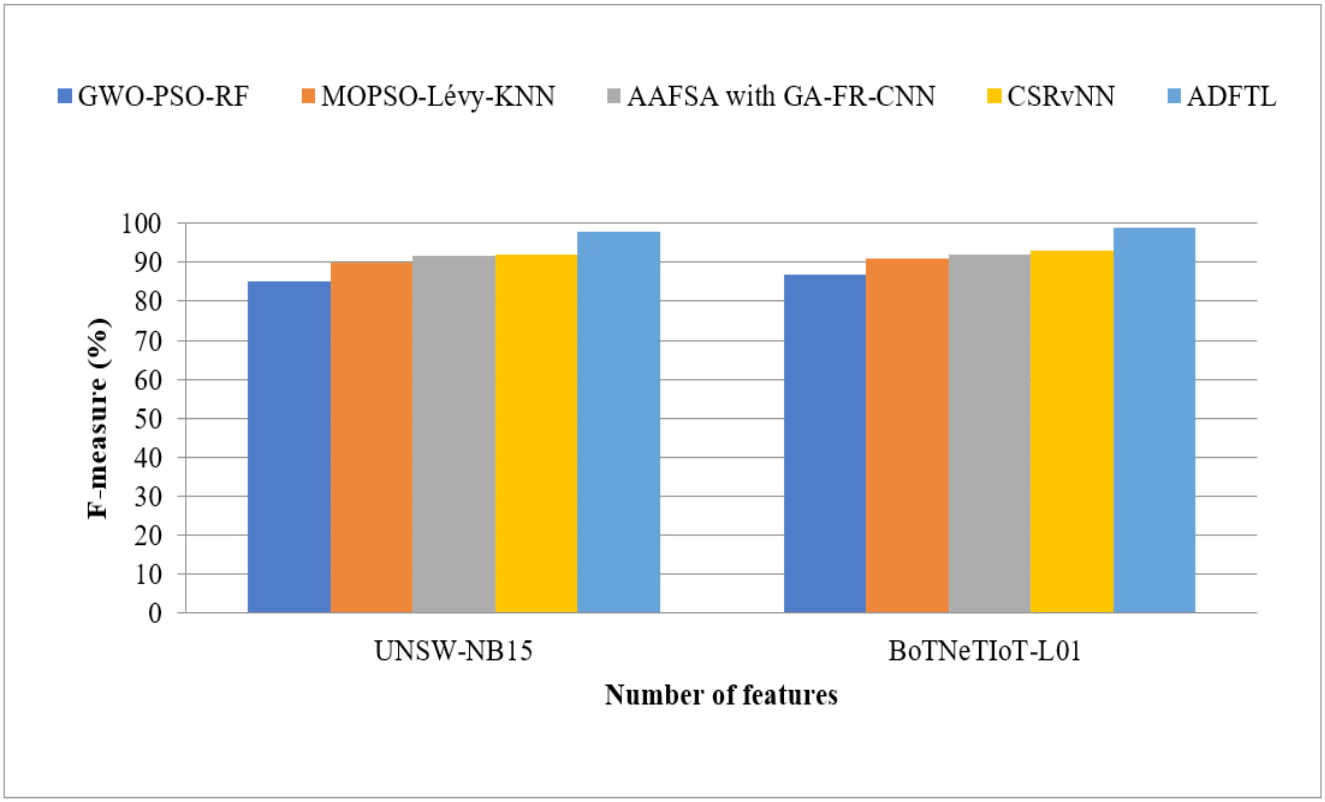


Figure 6. Result of F-measure

https://doi.org/10.56294/sctconf2024648

The f-measure for current and suggested frameworks for the quantity of features in provided databases is revealed in Figure 6. The f-measure is optimized in tandem with feature count maximization. For example, the AAFSA using GA-FR-CNN yields an f-measure of 91,56 % for UNSW-NB15, proposed CSRvNN provides 92 % and proposed ADFTL attains 98 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. For BoTNeTIoT-L01, the AAFSA with GA-FR-CNN provides a f-measure of 92 %, proposed CSRvNN provides 93 % and proposed ADFTL attains 99 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. Furthermore, the efficacy of the transferring operation is enhanced by the suggested ADFTL paradigm, which operates transformation at every level of the AEs' encoding layers. With label data present in the source domain but none in the target domain, the suggested system is relevant. The WkSN clustering segment, which divides a heterogeneous training set into many homogeneous subsets and affects the identification F-measure, is primarily responsible for this enhancement.

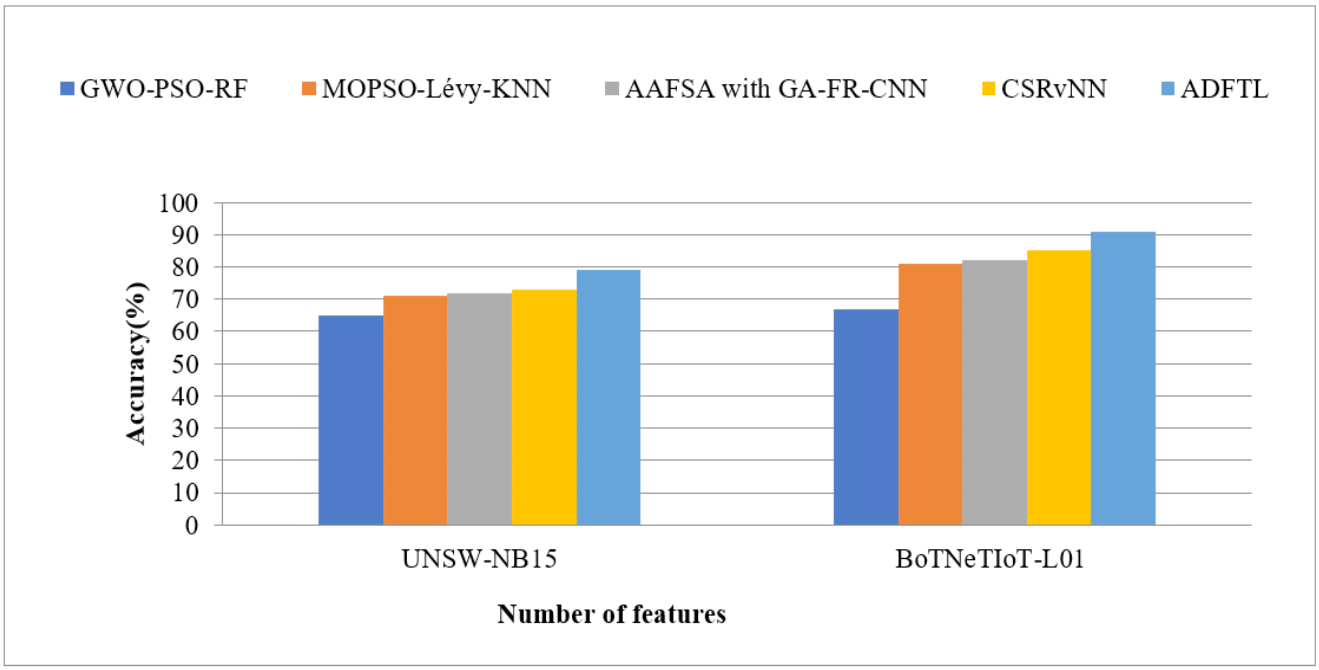


Figure 7. Result of Accuracy

The accuracy of optional and present approaches for the quantity of features in definite databases can be found in Figure 7. The AAFSA with GA-FR-CNN shortens processing times while improving accuracy. For example, the AAFSA with GA-FR-CNN yields a 72 % accuracy for UNSW-NB15, proposed CSRvNN provides 73 % and proposed ADFTL attains 79 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. For BoTNeTIoT-L01, the AAFSA with GA-FR-CNN provides a accuracy of 82 %, proposed CSRvNN provides 85 % and proposed ADFTL attains 91 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. Also, because AE must determine the distance across each encoding layer, the training period of ADFTL is much longer than that of the current approach. Precision, recall, and F-value typically remain steady for high-frequency attacks (such as normal, DoS, and PRB attacks) and increase with increasing k for low-frequency attacks (R2L, U2R). Because of this, ADFTL can achieve higher detection reliability and accuracy.

CONCLUSION AND FUTURE WORK

This research presented an innovative ADFTL-based method for detecting attacks on IoT networks. The suggested method solve the issue of "lack of labeled information" for the training detection system on frequently utilized IoT devices. In particular, two AE models with a similar network framework are fitted to the labeled and unlabeled data. Additionally, information is transferred from the first AE to the second AE utilizing the MMD metric. The structure primarily comprises of a weighted k-subspace network, which is fed data representation into the assignment network to produce soft assignments. These soft assignments indicate the likelihood that the data would cluster in an integrated structure and pertain to the corresponding subspace. A second BSCM utilizing cosine and sine function equations was presented. The highly distinctive characteristics from IoT datasets are found by modifying the optimal solution update process within BSCM by employing the elitism technique. 72 % accuracy is provided by the AAFSA with GA-FR-CNN for UNSW-NB15, proposed CSRvNN provides 73 % and proposed ADFTL attains 79 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. For BoTNeTIoT-L01, the AAFSA with GA-FR-CNN provides a accuracy of 82%, proposed CSRvNN provides 85 % and proposed ADFTL attains 91 % equated to the GWO-PSO-RF and MOPSO-Lévy-KNN. To improve efficiency and stabilize transfer

https://doi.org/10.56294/sctconf2024648

learning procedures in the future, particularly in situations where reciprocal knowledge is scarce, consider for employing more efficient transfer learning strategies. The second will try to expand this framework utilizing neural networks such as Conditional Domain Adversarial Network (CDAN) and Deep Adaptation Network (DAN).

REFERENCES

1. Abd Elaziz, M., Al-qaness, M. A., Dahou, A., Ibrahim, R. A., & Abd El-Latif, A. A. (2023). Intrusion detection approach for cloud and IoT environments using deep learning and Capuchin Search Algorithm. Advances in Engineering Software, 103402.

2. Abdalrahman, G. A., & Varol, H. (2019, June). Defending against cyber-attacks on the internet of things. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

3. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.

4. Amado DPA, Diaz FAC, Pantoja R del PC, Sanchez LMB. Benefits of Artificial Intelligence and its Innovation in Organizations. AG Multidisciplinar 2023;1:15-15. https://doi.org/10.62486/agmu202315.

5. Avros, R., Frenkel, Z., Toledano-Kitai, D., & Volkovich, Z. (2015). An Iterative Projective Clustering Method. Procedia Computer Science, 60, 122-130.

6. Batista-Mariño Y, Gutiérrez-Cristo HG, Díaz-Vidal M, Peña-Marrero Y, Mulet-Labrada S, Díaz LE-R. Behavior of stomatological emergencies of dental origin. Mario Pozo Ochoa Stomatology Clinic. 2022-2023. AG Odontologia 2023;1:6-6. https://doi.org/10.62486/agodonto20236.

7. BoTNeTIoT-L01, link: https://www.kaggle.com/datasets/azalhowaide/iot-dataset-for-intrusion-detection-systems-ids.

8. Caero L, Libertelli J. Relationship between Vigorexia, steroid use, and recreational bodybuilding practice and the effects of the closure of training centers due to the Covid-19 pandemic in young people in Argentina. AG Salud 2023;1:18-18. https://doi.org/10.62486/agsalud202318.

9. Cavalcante L de FB. Feminicide from the perspective of the cultural mediation of information. Advanced Notes in Information Science 2023;5:24-48. https://doi.org/10.47909/978-9916-9906-9-8.72.

10. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

11. Chalan SAL, Hinojosa BLA, Claudio BAM, Mendoza OAV. Quality of service and customer satisfaction in the beauty industry in the district of Los Olivos. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:5-5. https://doi.org/10.56294/piii20235.

12. Chávez JJB, Trujillo REO, Hinojosa BLA, Claudio BAM, Mendoza OAV. Influencer marketing and the buying decision of generation «Z» consumers in beauty and personal care companies. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:7-7. https://doi.org/10.56294/piii20237.

13. Choudhary, S., Dey, A., & Kesswani, N. (2021). CRIDS: Correlation and Regression-Based Network Intrusion Detection System for IoT. SN Computer Science, 2, 1-7.

14. Das, S., & Mao, E. (2020). The global energy footprint of information and communication technology electronics in connected Internet-of-Things devices. Sustainable Energy, Grids and Networks, 24, 100408.

15. Diaz DPM. Staff turnover in companies. AG Managment 2023;1:16-16. https://doi.org/10.62486/agma202316.

16. Espinosa JCG, Sánchez LML, Pereira MAF. Benefits of Artificial Intelligence in human talent management. AG Multidisciplinar 2023;1:14-14. https://doi.org/10.62486/agmu202314.

17. Figueredo-Rigores A, Blanco-Romero L, Llevat-Romero D. Systemic view of periodontal diseases. AG Odontologia 2023;1:14-14. https://doi.org/10.62486/agodonto202314.

18. Gonzalez-Argote J, Castillo-González W. Productivity and Impact of the Scientific Production on Human-Computer Interaction in Scopus from 2018 to 2022. AG Multidisciplinar 2023;1:10-10. https://doi.org/10.62486/agmu202310.

19. Gyamfi, E., & Jurcut, A. (2022). Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, ML, and Datasets. Sensors, 22(10), 3744.

20. Gyamfi, E., & Jurcut, A. (2022). Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, ML, and Datasets. Sensors, 22(10), 3744.

21. Habib, M., Aljarah, I., & Faris, H. (2020). A modified multi-objective particle swarm optimizer-based Lévy flight: An approach toward intrusion detection in Internet of Things. Arabian Journal for Science and Engineering, 45(8), 6081-6108.

22. Hazman, C., Guezzaz, A., Benkirane, S., & Azrour, M. (2022). lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning. Cluster Computing, 1-15.

23. Hernández-Flórez N. Breaking stereotypes: "a philosophical reflection on women criminals from a gender perspective". AG Salud 2023;1:17-17. https://doi.org/10.62486/agsalud202317.

24. Hinojosa BLA, Mendoza OAV. Perceptions on the use of Digital Marketing of the micro-entrepreneurs of the textile sector of the Blue Gallery in the emporium of Gamarra. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:9-9. https://doi.org/10.56294/piii20239.

25. Keserwani, P. K., Govil, M. C., Pilli, E. S., & Govil, P. (2021). A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. Journal of Reliable Intelligent Environments, 7(1), 3-21.

26. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), 1-22.

27. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big data, 6(1), 1-21.

28. Lamorú-Pardo AM, Álvarez-Romero Y, Rubio-Díaz D, González-Alvarez A, Pérez-Roque L, Vargas-Labrada LS. Dental caries, nutritional status and oral hygiene in schoolchildren, La Demajagua, 2022. AG Odontologia 2023;1:8-8. https://doi.org/10.62486/agodonto20238.

29. Ledesma-Céspedes N, Leyva-Samue L, Barrios-Ledesma L. Use of radiographs in endodontic treatments in pregnant women. AG Odontologia 2023;1:3-3. https://doi.org/10.62486/agodonto20233.

30. Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access, 9, 38254-38268.

31. Liu, L., Wang, P., Lin, J., & Liu, L. (2020). Intrusion detection of imbalanced network traffic based on ML and DL. IEEE access, 9, 7550-7563.

32. Lopez ACA. Contributions of John Calvin to education. A systematic review. AG Multidisciplinar 2023;1:11-11. https://doi.org/10.62486/agmu202311.

33. Marcillí MI, Fernández AP, Marsillí YI, Drullet DI, Isalgué RF. Older adult victims of violence. Satisfaction with health services in primary care. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:12-12. https://doi.org/10.56294/piii202312.

34. Marcillí MI, Fernández AP, Marsillí YI, Drullet DI, Isalgué VMF. Characterization of legal drug use in older adult caregivers who are victims of violence. SCT Proceedings in Interdisciplinary Insights and Innovations

2023;1:13-13. https://doi.org/10.56294/piii202313.

35. Mirjalili, S. (2016). SCA: a sine cosine algorithm for solving optimization problems. Knowledge-based systems, 96, 120-133.

36. Moraes IB. Critical Analysis of Health Indicators in Primary Health Care: A Brazilian Perspective. AG Salud 2023;1:28-28. https://doi.org/10.62486/agsalud202328.

37. Ogolodom MP, Ochong AD, Egop EB, Jeremiah CU, Madume AK, Nyenke CU, et al. Knowledge and perception of healthcare workers towards the adoption of artificial intelligence in healthcare service delivery in Nigeria. AG Salud 2023;1:16-16. https://doi.org/10.62486/agsalud202316.

38. Oseni, A., Moustafa, N., Creech, G., Sohrabi, N., Strelzoff, A., Tari, Z., & Linkov, I. (2022). An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks. IEEE Transactions on Intelligent Transportation Systems.

39. Peñaloza JEG, Bermúdez L marcela A, Calderón YMA. Perception of representativeness of the Assembly of Huila 2020-2023. AG Multidisciplinar 2023;1:13-13. https://doi.org/10.62486/agmu202313.

40. Pérez DQ, Palomo IQ, Santana YL, Rodríguez AC, Piñera YP. Predictive value of the neutrophil-lymphocyte index as a predictor of severity and death in patients treated for COVID-19. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:14-14. https://doi.org/10.56294/piii202314.

41. Prado JMK do, Sena PMB. Information science based on FEBAB's census of Brazilian library science: postgraduate data. Advanced Notes in Information Science 2023;5:1-23. https://doi.org/10.47909/978-9916-9906-9-8.73.

42. Pupo-Martínez Y, Dalmau-Ramírez E, Meriño-Collazo L, Céspedes-Proenza I, Cruz-Sánchez A, Blanco-Romero L. Occlusal changes in primary dentition after treatment of dental interferences. AG Odontologia 2023;1:10-10. https://doi.org/10.62486/agodonto202310.

43. Quiroz FJR, Oncoy AWE. Resilience and life satisfaction in migrant university students residing in Lima. AG Salud 2023;1:9-9. https://doi.org/10.62486/agsalud20239.

44. Roa BAV, Ortiz MAC, Cano CAG. Analysis of the simple tax regime in Colombia, case of night traders in the city of Florencia, Caquetá. AG Managment 2023;1:14-14. https://doi.org/10.62486/agma202314.

45. Rodríguez AL. Analysis of associative entrepreneurship as a territorial strategy in the municipality of Mesetas, Meta. AG Managment 2023;1:15-15. https://doi.org/10.62486/agma202315.

46. Rodríguez LPM, Sánchez PAS. Social appropriation of knowledge applying the knowledge management methodology. Case study: San Miguel de Sema, Boyacá. AG Managment 2023;1:13-13. https://doi.org/10.62486/agma202313.

47. Serra S, Revez J. As bibliotecas públicas na inclusão social de migrantes forçados na Área Metropolitana de Lisboa. Advanced Notes in Information Science 2023;5:49-99. https://doi.org/10.47909/978-9916-9906-9-8.50.

48. Shareena, J., Ramdas, A., & AP, H. (2021). Intrusion detection system for iot botnet attacks using deep learning. SN Computer Science, 2(3), 205.

49. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. Computers and Electrical Engineering, 107, 108626.

50. Solano AVC, Arboleda LDC, García CCC, Dominguez CDC. Benefits of artificial intelligence in companies. AG Managment 2023;1:17-17. https://doi.org/10.62486/agma202317.

51. UNSW-NB 15 dataset: link: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15?select=UNSW-NB15_1.csv

52. Zhang, Y., Li, P., & Wang, X. (2019). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access, 7, 31711-31722.

53. Zhao, R., Gui, G., Xue, Z., Yin, J., Ohtsuki, T., Adebisi, B., & Gacanin, H. (2021). A novel intrusion detection method based on lightweight neural network for internet of things. IEEE Internet of Things Journal, 9(12), 9960-9972.

FINANCING

The authors did not receive funding for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: V. S. Lavanya, R. Anushiya.
Research: V. S. Lavanya, R. Anushiya.
Writing-original draft: V. S. Lavanya, R. Anushiya.
Writing-review and proof editing: V. S. Lavanya, R. Anushiya.