An IoT Based advanced deep study on Network Intrusion Detection Systems (IDSs)

Mr. J.N.S.S Janardhana Naidu
Research Scholar,Dept of CSE
Vels Institute of Science Technology and Advanced Studies,Chennai,India
jnss.janardhana@gmail.com
Dr.E.N.Ganesh
Professor, Dean School of Engineering VISTAS
Vels Institute of Science Technology and Advanced Studies, Chennai,India
dean.se@velsuniv.ac.in
Mr. D.Shankar
Assistant Professor,Dept of CSE
Vishnu Institute of Technology,Bhimavaram,India
shankar.d@vishnu.edu.in

Abstract:

The current technology is moving in a rapid way through big data, cloud computing, data mining, and IoT platforms. These all networks are facing issues like security, attacks, virus, DDoS, and trojans, the following issues are cannot crossover to existing technologies such GA, PSO, RFO, and X-boosting conventional models. Therefore, effective deep learning or machine learning-based Network Intrusion Detection Systems (IDSs) method is required. The computer systems and network hostiles are continually analyzing information and sometimes these are misused by attackers. The attackers are concentrating on the huge network, lite password-authenticated low maintenance servers. In this research work, advanced Network IDSs and their limitations are discussed. The application's robustness such as accuracy, sensitivity, Recall, F measure, intrusion based on the signature, anomaly IDSs scores has been calculated. This survey is finding problem statements and objectives of future study of Network intrusion detection with deep intelligence methods.

Keywords: IDSs, Network security, machine intelligence, deep intelligence.
DOINumber: 10.14704/NQ.2022.20.12.NQ77173 **NeuroQuantology2022;20(12): 1991-2005**

Introduction:

The emerging technology of the Internet of Things (IoT) is constantly evolving and being exploited in the last couple of years, enabling communications and interactions among several devices via a network; thus, it is propelling new technology of business process. Subsequently, several challenges in many aspects, such as financially, in proving credibility, in the enforcement, and in business operations, have come to the fore resulting from the exponential growth of cybersecurity attacks. Cloud computing is normally used as an IoT data storage, which is formulated as a model that supplies various resources and services to the customer on-demand. Typically, cloud computing minimizes the human intervention between users and providers. Due to its impressive features, it has received serious attention from organizations and users. However, to transit from the current platform to the cloud computing platform, several struggling issues can be faced related to the operation mechanism and security. There has been a massive increase in data generated by today's networks due to the rapid development

of new network technologies like 5G, cloud computing, and the Internet of Things (IoT). An essential part of Intrusion Detection (ID) is being able to accurately identify and classify unauthorized network access attempts. Take the information features of the existing attack data and compare them to the information on the host or network by analyzing network information. Misuse detection is the name of the game here. In order to link the network data to the sample database's typical behavior trajectory features, step 2. Anyone who deviates from the norm is considered an intrusion. To combat malware and DDoS attacks from networks, a broad range of ML (Machine Learning) methods has been investigated during the last decades. Malware detection in machine learning is an iterative process that includes obtaining available data, cleaning and preparing the data, constructing models, verifying and putting into production.

The analysis of network traffic is less time consuming than working directly with the base system since it is easier to extract characteristics that offer an abstract picture of the virus activities. Based on expert knowledge of the subject, the machine learning algorithms depend mostly on manually constructed features. Feature engineering has traditionally been seen as a labor-intensive step in machine learning workflows. Detection of malware using machine learning has begun to move towards deep learning models, following current advancements in the field. In lieu of the previously specified machine learning feature engineering method, several new approaches have taken their place.

Cyber security is an essential study area because of the growing significance of networks in contemporary life. Anti-virus software, firewalls, and Intrusion Detection Systems (IDSs) are the most common strategy used in network security (IDSs). These techniques protect networking against both internal and external attacks. Intrusion Detection Systems (IDS) is a critical component of any network's defense against external threats. In 1980, the initial idea for an intrusion detection system was put out. Since then, there have been a number of mature IDS products. IDSs still have a high false alarm rate, which increases the strain on security analysts, and may result in a significant attack being unnoticed because of the large number of false alarms. Because of this, a number of academics have concentrated on designing IDSs through higher detecting efficiency & lower fake fear levels. Accessible IDSs also have the limitation of not being able to identify unknown threats. Because of the rapid evolution of network infrastructures, new attack variations and new assaults are continually being developed. Consequently, IDSs that can identify unknown attacks are a must.

Computer scientists are now developing IDSs utilizing ML techniques in an effort to address the issues outlined above. Machine learning is a technique used in artificial intelligence (AI) to uncover new information from massive datasets on the fly [2]. The detection capabilities of machine learning-based IDSs may be greatly improved if sufficient training data and generalizable models are made accessible. Machine learning-based IDSs are very simple to construct and build since they don't rely on domain knowledge. Using deep learning, machine learning may reach remarkable results. DL models are good at coping through large amounts of information than typical ML approaches. Deep learning methods may be used to produce conclusions after feature representations have been built from raw data. The deep structure of deep learning is one of its most noteworthy characteristics. To the contrary, the SVM (Support Vector Machine) and k-NN (k-Nearest Neighbor) are classic

machine learning models with just one hidden layer. Because of this, classic machine learning models are referred to as shallow models.

Using classification and summarization, as well as abstracting the key notions of applying machine learning to security domain issues, the main theme of the study is to analyze existing obstacles & potential future improvements in machine learning-based IDSs. In order to conduct this survey, we focused on publications published between 2015 and 2019. Machine learning methods have been used to classify research efforts in prior studies [3–5]. In order to aid machine learning researchers, these surveys are largely aimed at introducing various machine learning techniques used in IDSs. The difficulty is that this sort of taxonomy system focuses on particular implementation technologies, rather than cyber security domain concerns. Thus, these surveys do not explicitly address how machine learning may be used to tackle IDS domain concerns. It is for this reason that the results of this study suggest a new IDS classification based on data, along with the related studies.

In IDS, information objects are at the very foundation. Data objects have properties that are associated with attacks. According to various data pieces, the most suited machine learning models also vary in terms of their feature types and extraction methodologies. As a result of this investigation, IDSs are classified according to the data sources they handle. This taxonomy provides readers with an easy way to locate research ideas for certain domain issues by presenting a process including data–feature–attack behavior–detection. For example, the following issues may be resolved with this taxonomic system: What distinguishes one assault from another, and how can this be determined? When it comes to recognising specific threats, what kind of data is most appropriate? Is there a certain data format for which machine learning techniques are most appropriate? (4) In what ways are IDSs improved by machine learning methods? Cyber security researchers are interested in these issues. Finally, current sample research are summarized to address the problems and future development of IDS machine learning approaches.

The following are the study's most significant contributions:

1). A hybrid machine learning approach based on anomaly detection is proposed in order to identify DDoS assault behaviours. Observable traffic flow patterns are regarded performance attributes for detecting attacks when network functions are executed in virtual machines.

2). In order to increase the detection rate of attacks, a metaheuristic optimization search technique based on metaheuristic optimization should be developed.

3). It is possible to improve detection rates while reducing detection time by using a deep learning model to learn network traffic flow characteristics automatically.

Traditional intrusion detection systems (IDSs) have a high false alarm rate, a poor detection accuracy, and a limited ability to identify innovative threats. As a result, effective IDS must be designed to boost detection accuracy, reduce false alarms, and raise the pace at which new kinds of threats are discovered. ML approaches have been extensively studied in order to develop IDSs that are capable of working optimally in order to meet network security needs. Computational algorithms that mimic human intelligence are being developed in the subject of Deep Learning (DL).

A powerful ePIA (improved Packet Inspection) technique is developed in our study to analyse every packet delivered by cloud network routers. Analysis of the packet count, trust levels and flows, as well as the arrival time of the packets, is performed before assigning the

request to the cloud virtual machines. In order to distinguish malicious traffic from legitimate, the Shannon entropy is calculated based on the flow features.

Improving bald eagle search, or IBES, is used in the initial part of the intrusion detection process to choose the most supported characteristics. The IBES is a brand-new optimization for intrusion detection that hasn't yet been put into practise in terms of featureselection. The IBES algorithm utilises a powerful fitness function to eliminate characteristics that are both redundant and unimportant. Machine learning techniques based on prediction accuracy are used to verify the effectiveness of IBES in terms of determining feature selection efficiency.

This approach combines RNN (Recurrent Neural Network) with EKNN in a second phase to better forecast assaults, notably DDoS ones, on the cloud (Enhanced K-nearest Neighbour). Euclidean distance is used in the KNN method to determine the similarity between neighbours. Kernel-Based similarity Measure is used instead of Euclidean distance measure to improve the performance of the KNN.

To build the model, we'll leverage the NSL-KDD 99,UNSW-NB15 dataset and go through many stages, including data collection and feature selection.

IDS Taxonomy and Concepts:

Intrusion detection systems (IDS) define an intrusion as an illegal or unauthorised attempt to gain access to or damage computer systems or data.. Computer security tools such as an IDS, for example, are designed to detect a wide range of security breaches, from outsiders trying break-in to within system penetrations and abuse. Systems that use intrusion detection software (IDS) keep an eye on the computers and networks they are connected to, look for unusual behaviour, and provide alerts when anything is amiss. Monitoring hosts and networks linked to one another is one of the primary functions of IDSs, which is why they are often placed near secure network components (e.g., the switches in major network segments).

There are detection-based and data source-based IDS classification options to choose from. There are two subcategories of IDS' detection-based methodologies: misuse and anomaly detections. Depending on the data source, IDS may be categorised as either host-based or network-based [7]. The data source is the primary classification factor in this study, and the detection technique is treated as a supplementary classification element. Figure 1 depicts the suggested taxonomy. The study focuses on machine learning approaches when it comes to detecting anomalies. We go into great depth about how machine learning may be used to IDS and other kinds of data.

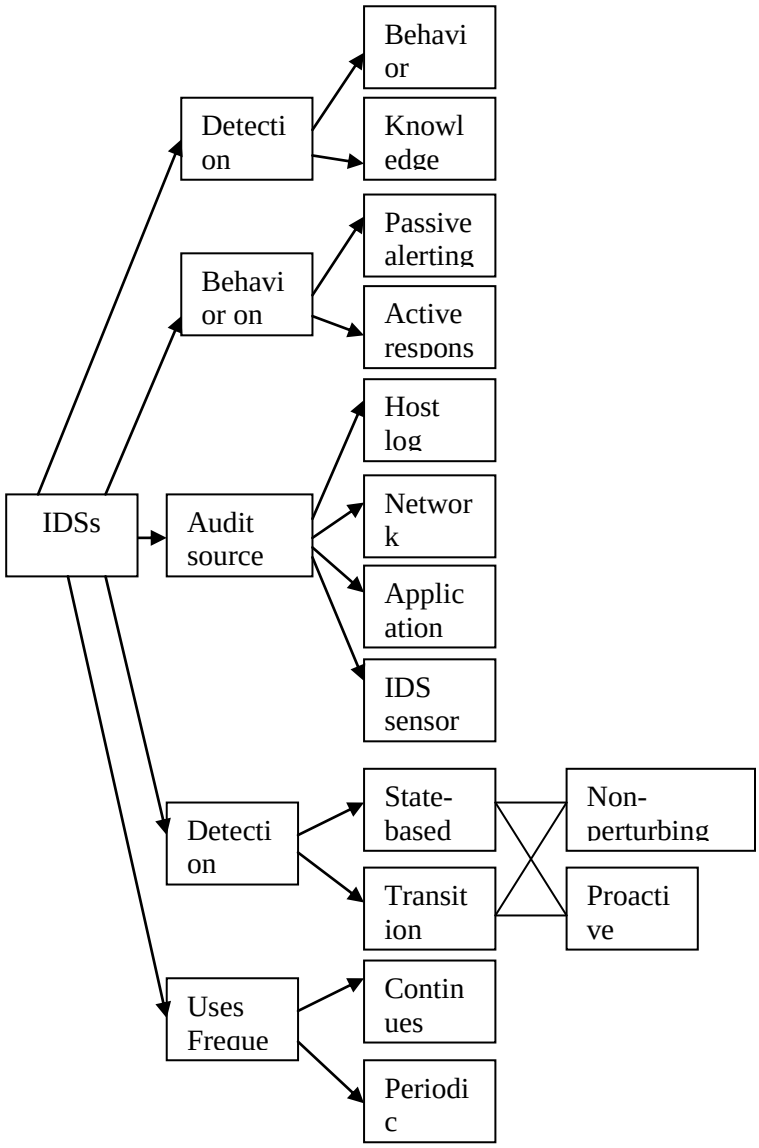


Figure 1. Taxonomy system of IDS.

Literature Survey:

Zhang, J.,etal [2008] It is unreasonable to expect that current security systems will be able to prevent all security breaches. Intrusion detection is essential for maintaining a secure network. Numerous intrusion detection systems (IDSs) rely on rule-based algorithms to detect anomalous activity. However, encoding rules is a time-consuming operation that significantly depends on the information of previously found intruders to work properly. Random forests are a data mining method often used to identify abuse, anomaly, and hybrid-network-based intrusion detection systems (IDSs). The random forests technique is used to build intrusion detection patterns based on training data. After that, network activity may be compared to the patterns to identify intrusions. New incursions are discovered through the random forests algorithm's outlier detection technique. The random forests technique is used to generate network service patterns, and an outlier detection algorithm is used to identify outliers. Hybrid detection systems include both the benefits of abuse detection and anomaly detection. Analyzing the KDDpsila99 dataset,

eISSN 1303-5150

we compare and contrast our various methods. There is a greater detection rate for the proposed anomalous detection technique when the false-positive rate is minimal, and results demonstrate that our suggested misuse strategy outperforms KDDpsila99 in terms of overall performance in comparison to unsupervised learning.[1]

Tarter, A. [2017] Because of its strong ties to individuals' everyday lives, Community Policing (CP) might be just as vulnerable to cyber attacks as the people it is designed to protect. In addition, CP activities might include countering or dealing with the fallout from cybercrime in any form. So it's crucial to know the fundamentals of cyber security, as well as the current and upcoming dangers it faces. From hacking to ransomware to the dark web to cryptocurrency, the concepts and practises in this chapter are explained in a way that is understandable to the general public. Furthermore, the chapter explains why criminals have embraced these tools, how they utilise them, and how enforcement law—especially Community Policing—can realistically investigate and function in this new century.[2]

Murakami, M.,et al [2007] Ink drop spread (IDS) is a modelling methodology that mimics the human brain's ability to digest information. A novel approach to soft computing has been presented using this concept. Using simple pattern information rather than complicated mathematics, IDS modelling is able to achieve reliable and rapid convergences. The IDS method's ability to simulate three standard benchmarks is examined in this research. This approach's modelling performance is contrast to that of feed forward NNs, as shown by the results of the experiments. The IDS method can handle a variety of modelling goals, ranging from simple logic processes to complicated nonlinear systems.[3]

Kumar, K.,et al [2022] By combining the concepts of clustering and autocorrelation, we want to develop an intrusion detection system that can handle both series and non-series data in a single architecture. To manage both series and non-series data, a new system must be conceived and implemented. When they combined these two ideas, the writers came up with an effective way to detect intruders. Non-series data is classified using an unsupervised clustering approach, whereas series data is classified using an autocorrelation methodology used by the authors. A single architecture incorporates data from both host-based and network-based intrusion detection systems. Using the elbow technique of clustering, we were able to determine the ideal number of clusters for the hybrid intrusion detection system.[4]

Sengan, S.,et al [2022] DDoS flooding assaults may be easily carried out using current techniques, which employ static route IDs. Work using machine learning to create a system that can tackle healthcare data issues using Dynamic Secure Aware Routing (DAR-ML). This study proposes an ML-based DoS detection system. To begin, the user must be able to access the permitted process. To compare route information between nodes after user registration, users may utilise the correlation factors between nodes. Then, choose a device that will activate and decrypt the data key automatically. Ultimately, all healthcare data is linked to the DAR-ML module. Users and administrators will be able to discuss their findings in the future module. These are the results of utilising the internet to make it simple. There was an attack detection accuracy of over 98.19 percent across a time span of 21.19 percent of data flow, with a high precision and a high chance of false alarm.[5]

Wang, G et al [2010] There have been several studies that show artificial neural networks

eISSN 1303-5150

(ANNs) outperform conventional approaches in intrusion detection systems (IDS). This does not mean that there is no room for improvement in ANN-based IDS detection accuracy for low-frequency assaults. ANN and fuzzy clustering are used in conjunction with a novel technique called FC-ANN to enable IDS achieve better detection rates, lower false positive rates, and more stability. First, distinct subsets of training data are generated using the fuzzy clustering approach. There are therefore many distinct ANN models that are trained using various training subsets.[6]

Li, J ety al [2019] The KDD 99 benchmark dataset is used to assess two IDSs that employ FLC & ANN, respectively. Based on the results, the main problems and potential in dealing with cyberattacks using artificial intelligence approaches are outlined and further study is proposed.[7]

Cho, S. B. [2002] Industrial applications may be addressed challenging by tough computitions while yet needing a patience for uncertainty and imperfection that can be exploited by soft computing. Hidden Markov models (HMMs) are used to represent normal behaviour and try to identify intrusions by highlighting large departures from the models. Fuzzy logic and neural networks are two of the soft computing approaches included into the system for increased resilience and flexibility.[8]

Prethija, G., et al [2022] A taxonomy for classifying and summarising IDS literature using ML and DL is proposed in this study. This taxonomy system is appropriate for cyber security researchers, according to us. To begin, the survey outlines the meaning and classification of IDSs. This is followed by a discussion of machine learning methods that are widely used in IDSs, metrics, and standard data.. We next use the suggested taxonomic system as a starting point to show how machine learning and deep learning approaches might be used to address important IDS challenges. We then look at a few recent research to see what the future holds for us.[9]

Amiri, F., et al [2011] A mutual information-based feature selection approach is compared to two feature selection algorithms proposed in this work. In order to employ these feature selection techniques, a measure of feature quality is needed. A non-linear correlation coefficient and a linear correlation coefficient are used to choose features. Least Squares Support Vector Machine (LSSVM) intrusion detection technique is also introduced in this paper. It has been shown that our suggested mutual information-based feature selection strategy results in detecting intrusions with greater accuracy, particularly for R2L and U2R assaults.[10]

Lunt, T. F. [1993] The computer security community has been creating automated techniques for analysing audit data on computer systems for questionable user activity for some years now. For the purpose of detecting intrusion into computer systems, such techniques are described in this study, along with a number of potential future technologies.[11]

Alsaadi, H. I. H.,et al [2021] For detecting infiltration, the Information Gain approach was used to prioritise characteristics. In addition, the categorization network data is analysed using the Adaptive Neuro-Fuzzy Inference System (ANFIS). Jang's Neuro-fuzzy and the faster-scaled conjugate gradient are built on the ANFIS technology (SCG). The trials clearly indicate that the proposed system has enhanced its ability to distinguish between normal and assault situations.ing Classification accuracy and processing time have been shown to be superior using current models in experiments. Results demonstrate that the suggested system can efficiently and effectively identify different invasions.[12]

Islam, S.,et al [2022] Network security relies heavily on intrusion detection technologies (IDS). Increasing reliance on social media and cloud computing has resulted in a massive surge in data output. Intrusion assaults are becoming more diverse as a result of increased data output. This article focuses mostly on the use ML for intrusion detection and security purposes. KNN, LR, NB, XGB, DT, and the Light Gradient Boosting Machine are among the six classification methods used (LGBM).[13]

Adhikary, S.,et al [2022] Hardware and neural network architectures are growing at the same pace as computer assaults. Most implementations of network intrusion detection systems (NIDS) still rely on signature-based systems, which cannot detect new assaults despite substantial advances in NIDS technology. Because of its high generalisation capacity, deep learning may assist NIDS in detecting new threats. With regards to model performance, the design of the deep neural network is critical. For the binary classification issue of NID, we offer a GA-based model to conclude the ideal number and number of neurons in each layer of the deep neural network (DNN) architecture. Research reveals that the suggested DNN architecture is superior to traditional machine learning techniques in terms of performance and computational cost.[14]

Mukherjee, S., et al [2012] It is the purpose of this research to identify essential reduced input characteristics for IDS creation that is computationally efficient and effective. We focus on three common feature selection approaches: correlation-based Feature Selection, Information Gain, and Gain Ratio. Feature Vitality Based Reduction Method is a method for deciding which decreased input features are most important to the end result, as seen in this example We employ naive bayes, one of the most effective classifiers, to identify intrusions. Network intrusion detection is more successful if it has a limited collection of features rather than a complete set.[15]

Anderson, J. P. [1980] Real-time intrusion detection expert systems may be modelled here. " Predicated on this premise, security breaches may be detected by monitoring audit data for aberrant behaviour. Additionally, the model includes rules for getting information about the behaviour of people with reference to objects from audit records and for recognising anomalous behaviour. With this method, a general-purpose intrusion-detection expert system that is not reliant on any one system or application environment or vulnerability or kind of intrusion may be developed.[16]

Ahmad, T.,et al [2022] To prevent network assaults before they can do any more harm to the system under attack, we suggest an end-to-end early intrusion detection solution. This prevents unplanned downtime and interruptions. For the purpose of identifying attacks, we make use of a classifier based on a deep neural network. Instead of using a human feature selection procedure as in other comparable techniques, the network is trained under supervision to extract useful characteristics from raw network traffic data. To further assess how early our suggested technique identifies threats, we present a new measure termed earliness. The CICIDS2017 dataset was used to test our method empirically. Our technique functioned well, with an overall balanced accuracy of 0.803, as shown by the data.[17]

Sathesh, A. [2019] The social network's harmful actions may be identified using soft computing technologies. As a result of its cost-effectiveness and resilience, soft computing has become an important study topic. Soft computing technologies are being employed in this study to find security-threatening social

eISSN 1303-5150

network breaches. Fuzzy logic and decision trees are used in conjunction with K means-EM and machine learning in the development of a security strategy that is more successful than classical calculations in recognising abuse in social networks. The KDD-NSL and DARPA datasets are used to measure the security percentage, time utilisation, and cost of the soft computing approach-based intrusion detection system.[18]

Altwaijry, H. [2013] The use of Bayesian probability to identify intrusions is explored in this study. The KDD dataset is used to train the systems before they are built. KDD datasets are used to test the learned classifier. A naïve Bayesian classifier was first employed to design a system for alerting users to impending invasions. An appropriate number of intrusions were detected by this classifier. It was later expanded to include many layers of Bayesian intrusion detection. As a last thought, we offer the idea that the best feasible intrusion detection system is a tiered approach that uses various methodologies at each layer.[19]

Fatani, A.,et al [2022] Building cyber security is an urgent need that is garnering a lot of attention from academic institutions and business organisations throughout the globe. Sustainable computing is essential for the Internet of Things as well (IoT). In order to detect intrusions and identify malicious activity on the Internet of Things, machine learning methods are essential. As a result, in this work, we devise novel feature extraction and assortment techniques for the IDS system that take use of the SI algorithms. Based on standard neural networks, we create a feature extraction method (CNN).[20]

Debar, H.,et al [1999] A classification of IDSs is presented in this work, highlighting the many facets of this field. According on their characteristics, intrusion-detection system families are classified in this taxonomy. Numerous examples from previous and present projects are used to demonstrate this point.[21]

Chaudhary, A.,et al [2016] According to a new technique, neuro-fuzzy classifiers in binary form for mobile ad hoc networks may be used to determine if current activities are normal or unhealthy. Using the Qualnet simulator and the MATLAB toolbox, the attack-based scenarios are illustrated and the performance of the suggested approach is assessed. This soft computing-based approach has been shown to have high positive and low false positive detection rates in mobile ad-hoc networks, according to the findings of the simulations.[22]

Murakami, M.,et al [2008] Rather of relying on complicated algorithms, this approach relies on picture information to represent the data. Soft computing tools are often judged on the basis of their capacity to withstand a wide range of environmental conditions and their ability to be easily implemented. Robustness is measured in terms of its ability to handle noise and faults. The concepts of interpretability and transparency are brought up while discussing tractability. This research shows that the IDS technique is better than artificial neural networks and fuzzy inference systems when it comes to being a soft computing tool.[23]

Guezzaz, A.,et al [2022] For better detection rates on the Internet of Things, this study presents a unique network ID model built on machine learning methods. Using network intrusion detection, the proposed method aims to enhance data categorization. A appropriate classifier has been designed and verified to meet the security task's needs after we explained our technique.[24]

Mukkamala, S.,et al [2003] Problem resolution is increasingly being done with the help of soft computing approaches. Soft computing strategies for intrusion detection are discussed in this study as part of an ensemble approach. Despite the rise in cyberattacks, the

development of reliable intrusion detection systems (IDSs) is still a difficult aim and a significant problem. There are two types of ANNs & SVMs being explored (SVMs). In terms of classification accuracy, we demonstrate that an ensemble of ANN and SVM is superior to individual techniques for intrusion detection.[25]

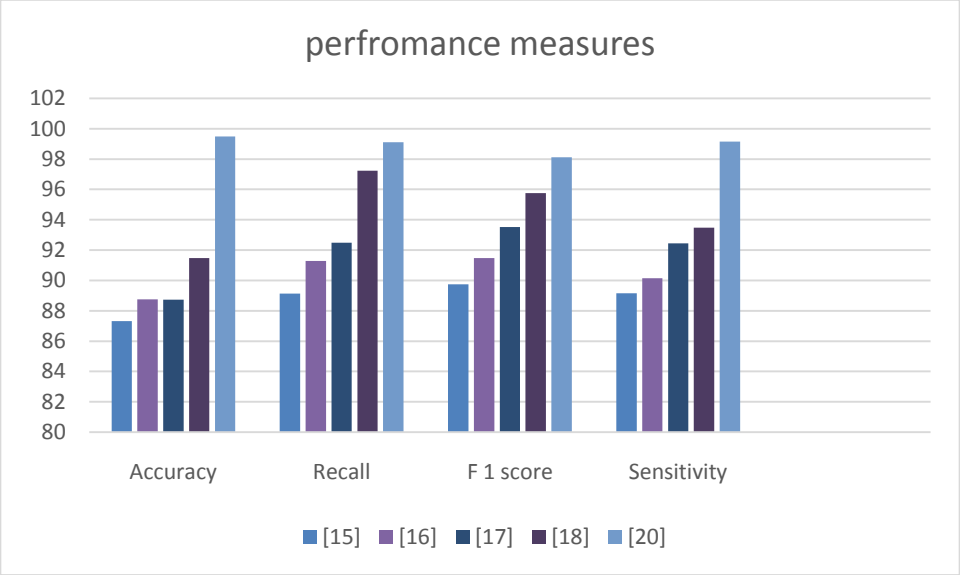
Problem statement

Network security is a very important task to network designers, the attacks like DDoS, anomaly viruses and etc are identified by available algorithms but those are outdated. Moreover, detection time, traffic flow feature, the attack detection rate parameters are cannot that much efficient with conventional models. Therefore deep and machine intelligence-based IDSs are required to cross over the above limitations.

Objectives

1. To Design an anomaly-based hybrid machine intelligence model-based intrusion detection to detect the DDoS attack behaviors'. As network functions run inside virtual machines, the observable traffic flow behaviors' are considered as performance features for attack detection.
2. To Design a metaheuristic optimization-based search strategy for optimal feature selection which supports making an effective hybrid machine learning model which improves the attack detection rate.
3. To apply deep learning model for learning the network traffic flow features automatically which contributes to achieving a high detection rate with less detection time.

parameters	Accuracy	Recall	F 1 score	Sensitivity
[15]	87.32	89.14	89.75	89.15
[16]	88.75	91.28	91.47	90.14
[17]	88.73	92.48	93.52	92.45
[18]	91.48	97.24	95.76	93.47
[20]	99.48	99.12	98.12	99.16



Proposed Model

With this part, the phases of the proposed IoT security are based on extracting the feature from the data using CNN and then selecting the relevant feature using a modified RSA. In general, the IoT security model consists of four stages, as given in Figure 2 and the description of each phase is given as follows.

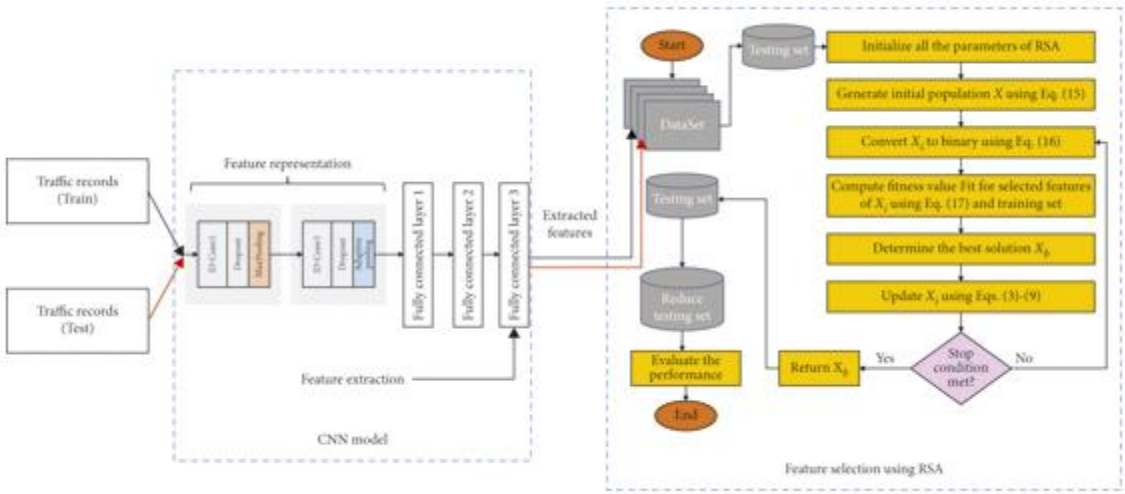


Figure 2_ Steps of the presented IoT security method

First Phase: Prepare IoT Dataset

In this stage, the IoT dataset is prepared to make it suitable for the feature extraction stage (next one). This is achieved by normalizing the dataset using min max approach. For clarity, by considering the collected traffic samples, TS of IoT is represented as

eISSN 1303-5150

$$\mathrm{TS} = \begin{bmatrix} tf_{11} & tf_{12} & \cdots & tf_{1d} \\ tf_{21} & tf_{22} & \cdots & tf_{2d} \\ \cdots & \cdots & \cdots & \cdots \\ tf_{n1} & tf_{n2} & \cdots & tf_{nd} \end{bmatrix}$$

Second Phase: CNN for Feature Extraction

The CNN is a widely used automatic feature extractor in various applications such as image classification, text classification, speech recognition, and others. The core building blocks are convolution layer (Conv), ReLU activation function, fully connected layer (FC), and pooling layer (Pool). The CNN learns complex representations as features from the network traffic samples and classifies them based on their intrusion type. Using a convolution operation, the CNN extracts local and position-invariant patterns while sharing the weights across the layers and channels. In our case, the design of the CNN network was based on the error, and trial method, where the objective is to build a simple yet powerful model that maximizes the classification accuracy on the tackled task. In addition, the best-trained model based on its performance on the test data is used to extract the learned features for the feature selection stage. The proposed CNN is illustrated in Figure 3.

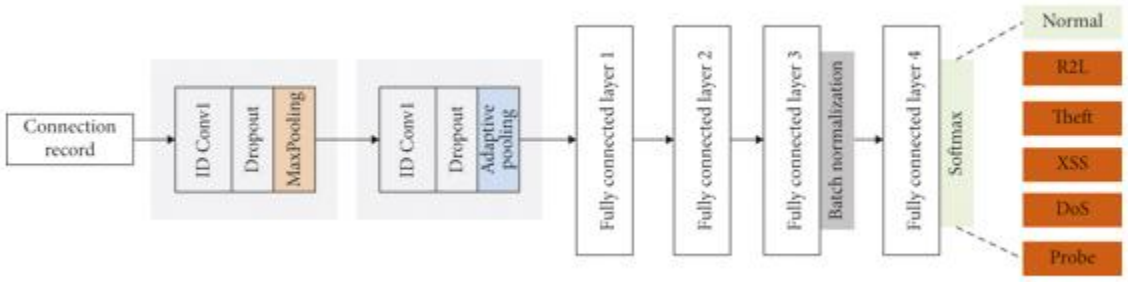


Figure 3 Presented structure of the feature extraction based on CNN

Third Phase: Feature Selection

During this phase, the proposed model selects the relevant features based on their quality. Thus, this process has a significant impact on IDS detection in IoT environments.

The proposed RSA as FS approach (see Figure 4) begins by initializing population, with a number of agents represented by . After that, it converts each agent into its binary version. More so, it reduces the number of features excluding those related to zeros from the binary version. Thereafter, the proposed RSA approach assesses the quality of the chosen features by computing the error classification according to the KNN classifier. Then, the best solutions (agents) are updated till reaching the optimal solutions.

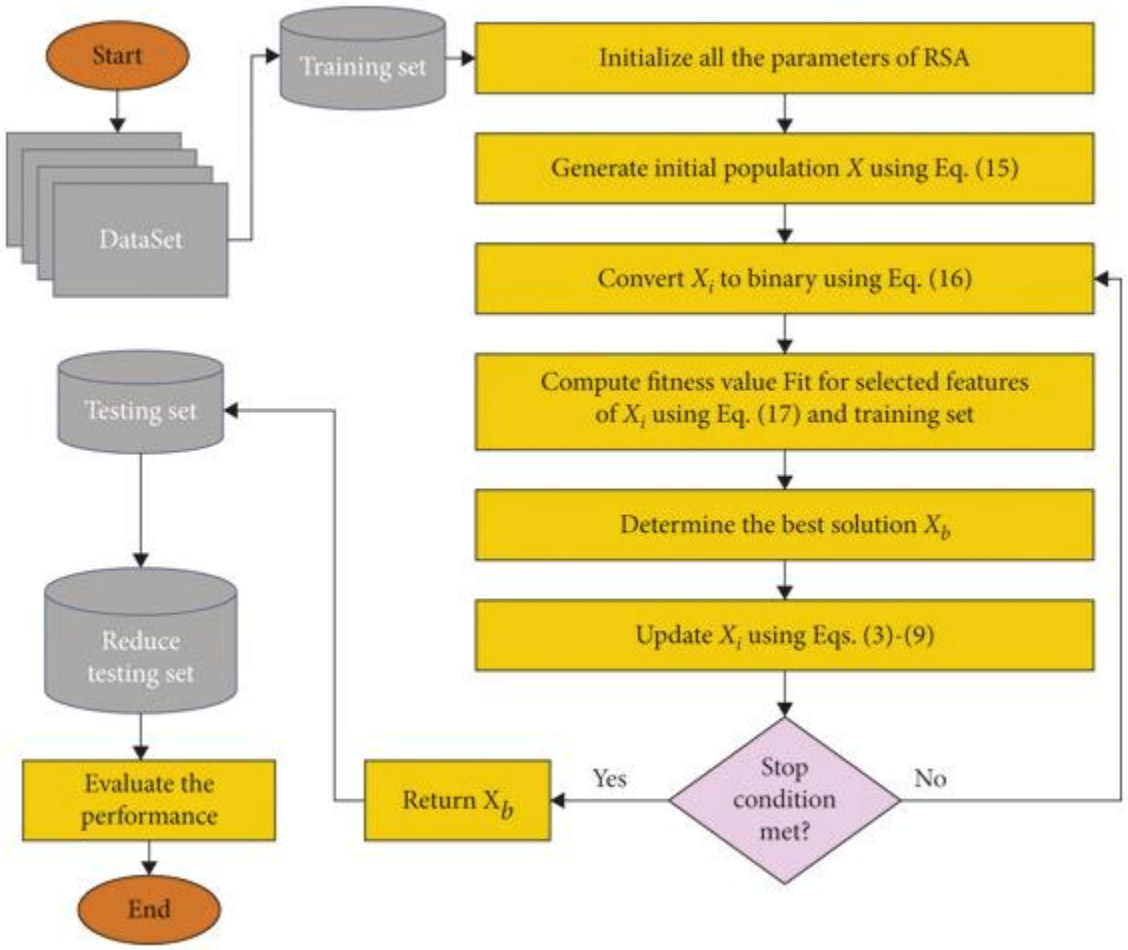


Figure 4_ Steps of the RSA as an FS model for IoT security

Conclusion:

Big data, cloud computing, data mining, and IoT platforms are all examples of how technology is rapidly evolving. These networks are all dealing with concerns like security, assaults, viruses, DDoS, and trojans, and the following problems can't be solved with existing technologies like GA, PSO, RFO, and X-boosting. As a result, effective Network Intrusion Detection Systems (IDSs) based on deep learning or machine learning are necessary. Computer systems and network adversaries are constantly evaluating data, which is sometimes exploited by attackers. The attackers are focusing their efforts on a large network of low-maintenance, lightweight password-authenticated servers. Advanced Network IDSs and their drawbacks are described in this research paper. The application's robustness has been measured, including accuracy, sensitivity, recall, F measure, intrusion based on the signature, and anomaly IDSs scores. The purpose of this survey is to identify issue statements and future study objectives for network intrusion detection using deep intelligence algorithms.

References:

1. Zhang, J., Zulkernine, M., & Haque, A. (2008). Random-forests-based network intrusion detection systems. IEEE Transactions on Systems, Man, and

eISSN 1303-5150

Cybernetics, Part C (Applications and Reviews), 38(5), 649-659.

2. Tarter, A. (2017). Importance of cyber security. In Community Policing-A European Perspective (pp. 213-230). Springer, Cham.
3. Murakami, M., & Honda, N. (2007). A study on the modeling ability of the IDS method: A soft computing technique using pattern-based information processing. International journal of approximate reasoning, 45(3), 470-487.
4. Kumar, K., Kumar, A., Kumar, V., & Kumar, S. (2022). A Hybrid Classification Technique for Enhancing the Effectiveness of Intrusion Detection Systems Using Machine Learning. International Journal of Organizational and Collective Intelligence (IJOCI), 12(1), 1-18.
5. Sengan, S., Khalaf, O. I., Sharma, D. K., & Hamad, A. A. (2022). Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach. International Journal of Reliable and Quality E-Healthcare (IJRQEH), 11(3), 1-11.
6. Wang, G., Hao, J., Ma, J., & Huang, L. (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert systems with applications, 37(9), 6225-6232.
7. Li, J., Qu, Y., Chao, F., Shum, H. P., Ho, E. S., & Yang, L. (2019). Machine learning algorithms for network intrusion detection. AI in Cybersecurity, 151-179.
8. Cho, S. B. (2002). Incorporating soft computing techniques into a probabilistic intrusion detection system. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 32(2), 154-160.
9. Prethija, G., & Katiravan, J. (2022). Machine Learning and Deep Learning Approaches for Intrusion Detection: A Comparative Study. In Inventive Communication and Computational Technologies (pp. 75-95). Springer, Singapore.
10. Amiri, F., Yousefi, M. R., Lucas, C., Shakery, A., & Yazdani, N. (2011). Mutual information-based feature selection for intrusion detection systems. Journal of Network and Computer Applications, 34(4), 1184-1199.
11. Lunt, T. F. (1993). A survey of intrusion detection techniques. Computers & Security, 12(4), 405-418.
12. Alsaadi, H. I. H., ALmuttari, R. M., Ucan, O. N., & Bayat, O. (2021). An adapting soft computing model for intrusion detection system. Computational Intelligence.
13. Islam, S., Rouf, M. A., Shahariar Parvez, A. H. M., & Podder, P. (2022). Machine Learning-Driven Algorithms for Network Anomaly Detection. In Inventive Computation and Information Technologies (pp. 493-507). Springer, Singapore.
14. Adhikary, S., Anwar, M. M., Chowdhury, M. J. M., & Sarker, I. H. (2022). Genetic Algorithm-based Optimal Deep Neural Network for Detecting Network Intrusions.
15. Mukherjee, S., & Sharma, N. (2012). Intrusion detection using naive Bayes classifier with feature reduction. Procedia Technology, 4, 119-128.
16. Anderson, J. P. (1980). Computer security threat monitoring and

surveillance. Technical Report, James P. Anderson Company.

17. Ahmad, T., Truscan, D., Vain, J., & Porres, I. (2022). Early Detection of Network Attacks Using Deep Learning. arXiv preprint arXiv:2201.11628.
18. Sathesh, A. (2019). Enhanced soft computing approaches for intrusion detection schemes in social media networks. Journal of Soft Computing Paradigm (JSCP), 1(02), 69-79.
19. Altwaijry, H. (2013). Bayesian based intrusion detection system. In IAENG transactions on engineering technologies (pp. 29-44). Springer, Dordrecht.
20. Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., & Abd Elaziz, M. (2022). Advanced Feature Extraction and Selection Approach Using Deep Learning and Aquila Optimizer for IoT Intrusion Detection System. Sensors, 22(1), 140.
21. Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer networks, 31(8), 805-822.
22. Chaudhary, A., Tiwari, V. N., & Kumar, A. (2016). Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks. International Journal of Soft Computing and Networking, 1(1), 17-34.
23. Murakami, M., & Honda, N. (2008). Performance of the IDS method as a soft computing tool. IEEE Transactions on Fuzzy Systems, 16(6), 1582-1596.
24. Guezzaz, A., Benkirane, S., & Azrour, M. (2022). A Novel Anomaly Network Intrusion Detection System for Internet of Things Security. In IoT and Smart Devices for Sustainable Environment (pp. 129-138). Springer, Cham.
25. Mukkamala, S., Sung, A. H., & Abraham, A. (2003). Intrusion detection using ensemble of soft computing paradigms. In Intelligent systems design and applications (pp. 239-248). Springer, Berlin, Heidelberg.

eISSN 1303-5150