International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

An Efficient Iot Network Intrusion Detection And Prevention System JARVIS – Just A Rather Very Intelligent System.

Dr. Shanthakumar H. C.[1*], Dr. Doddegowda B. J.[2]

Submitted: 04/05/2024 **Revised**: 17/06/2024 **Accepted**: 24/06/2024

Abstract: Given the race to find the best technique that suits and protects all Internet of Things (IoT) wireless devices, all around the world are in a quest to develop Intrusion Detection And Prevention Systems (IDPS). This has been led by a huge change from the traditional world shifting to the smart and intelligent world empowered and made possible by IoT devices and Artificial Intelligence and Machine Learning techniques (ML). The scope of security is much a relevant need but is challenged and limited by the computation memory and processing hardware which are typically small or micro in most heterogeneous IoT devices. Hence Machine Learning (ML) algorithms come into play while constructing an effective IDPS that treats every threat by detecting and preventing it from attacking the IoT devices and their network. In the proposed paper we show how the Intrusion Detection System (IDS) can be developed from both supervised and unsupervised machine learning techniques which addresses both static and dynamic intrusion attacks by using the KDD-CUP dataset and prevent them using the different cryptographic techniques that can perform well in small processing environments. Afterward in the results, it has been shown that among the algorithms of ML Support Vector Machine (SVM), Random Forest (RF), Linear Discriminant Analysis (LDA), Classification and Regression Trees (CART), RF gives the best values for the F1 score, recall, accuracy, and other evaluation metrics. Then using the Java Springs framework work we have built the IDPS which is integrated with the smart IDS thus forming an IDPS that safeguards the network and devices from the generic attacks which are known and unknown intrusions assuming the intruder is based on the server.

Keywords: *Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Intrusion Detection And Prevention System (IDPS), Intrusion Detection System (IDS), Intrusion Prevention System (IPS).*

I. INTRODUCTION

As almost all the attacks and threats to the wireless IoT come under the big umbrella of Intrusions, it becomes a basic requirement for every network of IoT devices to have an inbuilt IDPS that protects it from all security breaches. The rising usage of new and different IoT devices has posed a problem in solving adversary attacks and saving the network from catastrophic failures. IoT as a field of science is converging towards becoming a new lifestyle among the nuance population of the world which is driving the complete activities to be automated and powered by these technologies. Under these situations, researchers and engineers all around the world have come together to propose and implement a safe environment through the ML Algorithms and platforms which ensure the development and deployment is done in a proper way [1].

Intrusions can be done from remote attackers to IoT networks which ultimately make the system malfunction in no time. The intruder primarily uses his/her technique by exploiting the vulnerabilities either of the network or the device to breach into the system by various attacks.

All the attacks are from a superset which is the main intrusion attack. Thus, to prevent it from happening, there must be a detection technique or subsystem that alerts the IoT devices whenever such unfavourable attacks or intrusions are about to take place. Hence the system must adopt an optimized and effective prevention system to take a suitable course of action or perform some operations using the cryptographic models to save the IoT system from such intrusive attacks.

The basic way of classifying the intrusions are of 3 types namely: i) Signature based intrusion attacks ii) Anomaly based intrusion attacks and combination of two i.e. iii) Hybrid intrusion attacks. These are considered to be the possible superset of attacks in which each of them contains various subclasses or sub attacks. They are depicted in the figure 1 below. Now a days they are multiple types of IDS have been evolved other than classic Network based IDS(NIDS) and Host based IDS(HIDS) [2].

[1*] *Associate Professor, Dept. of CSE, SJB Institute of Technology, Bengaluru, India*

[2] *Associate Professor Dept. of CSE, AMC Engineering College, Bengaluru, India.*

***Corresponding Author:** Dr. Shanthakumar H C*

**Associate Professor, Dept. of CSE, SJB Institute of Technology, Bengaluru, India*

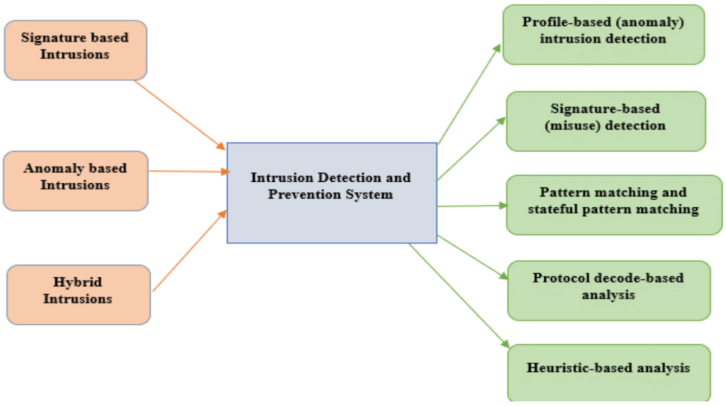
Signature based Intrusions
Anomaly based Intrusions
Hybrid Intrusions
Intrusion Detection and Prevention System
Profile-based (anomaly) intrusion detection
Signature-based (misuse) detection
Pattern matching and stateful pattern matching
Protocol decode-based analysis
Heuristic-based analysis

Fig 1. Hybrid Intrusion Detection System

Some of the IDPS are listed b based on their location of deployment and their purpose. Protocol-based Intrusion Detection System (PIDS), Application Protocol-based Intrusion Detection System (APIDS), Hybrid Intrusion Detection System summarized by fig 1.

The detection techniques deployed in such IDS include the following detection and analysis, here's a brief description of each:

1. Profile-based (anomaly) intrusion detection: This method involves monitoring system activity and classifying it as either normal or anomalous. It's good at detecting zero-day and unknown attacks and has low dependency on resources. However, it may have poor accuracy due to changes in observations.
2. Signature-based (misuse) detection: Also known as misuse detection, this approach involves comparing the code in a program to the code of known virus types that have already been encountered, analysed, and recorded in a database. It's simple to capture known intrusions2, but it may be poor in detecting unknown variants.
3. Pattern matching and stateful pattern matching: Pattern matching involves searching for a specific pattern or sequence of elements within a given data structure. Proactive pattern matching adds to pattern-matching by searching for unique sequences that might be distributed across several packets within a stream.
4. Protocol decode-based analysis: This method involves decoding all protocol or client-server conversations. The elements of the protocol are identified and analyzed while looking for an infringement.
5. Heuristic-based analysis: Heuristic analysis is a method of detecting viruses by examining code for suspicious properties. It involves examining patterns and characteristics of a file or program to determine whether it is malicious or not, without relying on known signatures of known viruses.

Proposed Work: This work provides a solution to such problems by considering ML and cryptographic techniques for detection and prevention measures in order to save IoT devices and networks through a Network based IDPS which mainly targets on all 3 classes of the intrusion attacks by ML based supervised learning which analyses the incoming data flow by profile and misuse based detection analysis. In this regard we also compare the most trending yet basic algorithms of ML which approach efficiently to give a feasible and working IDPS. The proposed work uses feature extraction and selection methods on the pre-processed data.

Mainly this propounded work of research serves as a lightweight IDPS involving very less overhead both on network and devices in an IoT ecosystem. The contributions of the proposed system are as follows:

• We have used the accurate models and ML techniques to design the IDPS which is accurate in detecting the

intrusions and maintain reliability of the whole network.

• We have made use of the supervised and unsupervised algorithms for detection no attacks cannot be ignored as

each packet is treated through both IDS and IPS by using KDD CUP dataset.

- The performance results of the propounded IDPS are evaluated and compared.

II. Literature Survey

There are many works already done that exploit either the data or techniques to yield the best Intrusion detection and prevention system. Many authors have proposed their work which explores more in feature space to ensure the perfect development of the IDPS.

Kabir *et al.*, in their work [3] utilized a hybrid approach to achieve a lightweight IDS based on clustering algorithms and signature rules but were only able to build anomaly-based IDS and the results were measured through accuracy and real time prediction which gave decent output values, but the techniques deployed could not properly detect the generic attacks in sensory networks.

Alkahtani *et al.,* have [4] used the deep learning models to develop IDS which could only able to fit the current data into its model, with the best results with accuracy of 88%and optimal F1 score for the model. But could not bear the overhead data as it could only predict and detect time series of attacks.

Abhale *et al.* in their work[5] could not construct a Prevention system as they achieved a very good IDS that used various ML algorithms like Naïve Bayes, Ada Boost, etc to detect the attacks that were anomaly-based and were too specific in kind they suggested NB classifier as it gave the best results and accuracy score and detection rate.

Seo *et al.,* have [6] showed how to develop a bi-level model to classify the packets using deep packet inspection. With the satisfactory results achieving an accuracy of 90%. This improved the prevention of the threatful packets but did not detect or foresee the potential intrusion by an IDS as they were not efficient to deploy on the heavy IPS model already present.

The work by Araujo *et al.,* [7] designed a complete architecture of the IDPS which mostly works on electronic systems but only were able to binary classify the attack without remembering the previous intrusions which would be less reliable. This work showed an correct prediction rate around half of the predictions made which were less below the average for a good IDPS.

Park *et al.,* have [8] found a session management plan for determining the overall security in their standalone network, with the decent values of accuracy and precision but this was not efficient to solve the other vulnerabilities involved in internal and external attacks on the session.

Many authors in [9], [10], [11] have proposed SVM techniques to tackle the problem of finding an effective solution for IDPS and IDS, but these works tend to overfit and may result in overlapping boundaries in the feature space which ultimately lead to the wrong detection. Though it gave best classification values for the valuation metrics like detection rate, F1- score, etc.

Some other works such as [12],[13] have proposed other gradient-based methods which very well perform the job of detection and prevention but these models converge into vulnerabilities due to network constraints. These gradient based models gave decent Mean values for Mean Square Error, Root Mean Square Error, precision etc.

In other works, concerning to the data instrumentation in regard with the development of IDPS considered only the feature extraction as the sole basis for the intrusion detection in the works [14], [15]the authors found that the features which play a critical role in providing security must be efficiently obfuscated in order to save IoT networks and devices. These data based models mainly used Feature Analysis and Principle Component Analysis algorithms and relied on Random Forest Tree for ML based intrusion detection, which gave a result of 82% accuracy rate with average F1-score which signified the importance of features while implementing any IDPS for IoT networks and their access points.

The further part of the proposed paper consists of Implementation and Results which is then rounded off by a reiterative conclusion that overviews the future prospects of the research work.

III. Methodology

In this part of the paper, we discuss the entire process that led to the development of an IDPS by considering the KDD-CUP dataset. And implementation of IDPS using python IDE and Java spring boot tools along with their built in libraries functions.

Dataset:

The KDD Cup 1999 dataset [16] is a well-known dataset used in the field of machine learning and data mining. This dataset was used for The Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with KDD-99, The Fifth International Conference on Knowledge Discovery and Data Mining. The competition task was to build a network intrusion detector, a predictive model capable of distinguishing between "bad" connections, called intrusions or attacks, and "good" normal connections. The dataset contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment. It is available in full as well as a 10% subset. The KDD Cup 1999 dataset continues to be a valuable resource for researchers and practitioners in the field to benchmark their methods. The KDD Cup 1999 dataset consists a total of 23 different output classes. These classes are based on different types of network intrusions or attacks. Here are some of the classes: Neptune, Multihop, Warezmaster, Portsweep, Smurf, Land, Teardrop, Nmap, Guess_Passwd, Normal, Perl, Spy, Satan, Ftp_Write, Loadmodule, Pod, Back, Buffer_Overflow, Phf, Rootkit, Warezclient, Imap, Ipsweep. Each of these classes represents a specific type of network intrusion. Note that this is not an exhaustive list and the actual dataset may contain more classes. The class “normal” represents the good connections, whereas the remaining 22 classes represent different types of bad connections.

Implementation:

1. ***Dataset Pre-processing:***

As the dataset itself contains redundancy and noise along with outliers we refine it using the various preprocessing methods. Firstly, we focus on pre-processing the data which has 4,94,021 rows with some empty cells and 42 features or attributes. We used mean-filling and redundancy remover tools to clean the noisy data and remove sparsity from the primary dataset. We considered the most significant 10,000 rows for developing and training the IDPS shortlisted through label encoding. The following processes were done in the Anaconda framework using Python version 3.6 as the language for development. It comes along with rich machine learning libraries facilitating the course of implementation. Next in the process of converting the qualitative values to quantitative values we used the Term Frequency–Inverse Document Frequency Transformer from the sci-kit library in Python which gives the more important and frequently appearing numerical values of data attributes which are the major the important attributes.

2. ***Feature Selection and Extraction:***

This procedure was implemented using the most popular and effective feature extraction algorithm Principal Component Analysis (PCA) an unsupervised ML algorithm for feature dimensionality reduction. It transformed the correlated features in the dataset to a set of uncorrelated features by orthogonal transformation. As PCA identifies a new set of axes (called principal components) that capture the maximum variance in the data, given a dataset with multiple features. It does this by standardizing the data to to ensure that all features have the same scale (mean = 0, variance = 1). computing the covariance matrix for the standardized data. Then finding the eigenvalues and eigenvectors of the covariance matrix. It sorts the eigenvectors based on their corresponding eigenvalues (in descending order). And chooses the top eigen vectors. Finally projects the original data onto the selected principal components. As PCA reduced the feature count up to 80% by selecting only important and required ones it gave us 12 to 15 features in total of 42 features in the dataset

3. ***Experimentation Analysis:***

After feature selection with 12-15 features, two supervised and unsupervised algorithms were trained using this data and feature set namely SVM, RF LDA, and CART which were implemented using the enriched python libraries which consists of all these algorithms along with their parameters as inputs were passed along with the pre-processed data set which consisted of training and testing dataset in the respective ratio of split in which each algorithm gave different values for different test train split ratio. The best result giving split ratio was selected for each algorithm by seeing their performance at different range of values. And algorithms were turned respectively. By using various train and test split ratios and training the algorithms we got the following performances described below.

Support Vector Machine (SVM) – This ML algorithm is a supervised maximum-margin model that analyses data for classification and regression analysis.

As this algorithm plots the data points and divides them according to the features, the boundary of separation makes the classification decision based on the location of the data point nearest to the non-linear boundary. This algorithm copes with the scaling of the data but the fear of over fitting and misclassification which would lead to failure of this model. The results of this model were decent rounding off results which are pretty good for the size we considered for training as well as testing. After testing the overall performance of this model came around eighty percent. The results are discussed in the following section.

Random Forest (RF) - Random Decision Forests or simple Random Forests is a supervised learning method for regression, classification, and other tasks that constructs a multitude of decision trees at training time.

The RF algorithm is not interpreted by humans, still, the annotations form the decision tree which totally drives the process of classification. The complex and optimal weight nature of this algorithm also overcomes the problem of over fitting and is suitable for large sizes of data. This gave us the best results compared to other algorithms. The testing outcomes were efficient in proving the algorithm to be best suited for an IDS.

Linear Discriminant Analysis (LDA) - Also called Normal Discriminant Analysis or Discriminant Function Analysis, is an unsupervised dimensionality reduction method. This facilitates the modelling of distinctions between groups of more than two classes.

This algorithm used higher dimension feature space for decision making thus making it more complex than any other algorithms thus it proved to give less accuracy due to its low adaptability and assumption of the data space as Gaussian distribution.

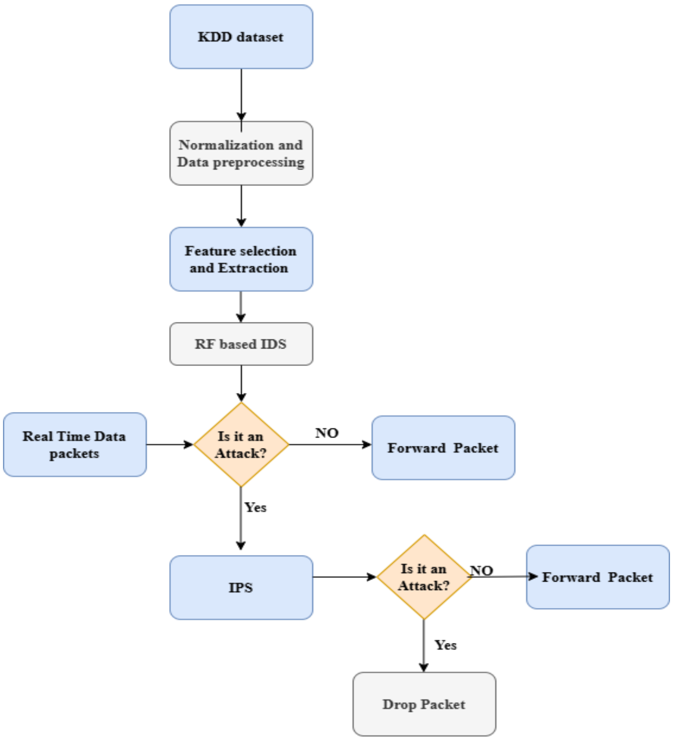

Fig 2. Flow Chart of the Proposed Model.

Classification and Regression Trees (CART) – It is a predictive and unsupervised algorithm used in Machine

learning. It is a decision tree where each fork is split into a predictor variable and each node has a prediction for the target variables.

The CART model splits the whole data based on dividing indices and criteria which leads to overfitting in poor results. As observed CART does not consider outliers and noises the results were also poor compared to other algorithms.

As the RF model suited the best for an ideal IDS, we developed the Intrusion prevention system (IPS) by integrating it using the Java Spring Boot tool. The flow chart of the IDPS model developed is as follows as depicted in fig 2.

Java Spring boot tool enables for rapid application development with the Application interface (API) and micro services features. As the four layers of the spring boot:

• Presentation Layer: Constitutes the front-end processes.

• Data Access Layer: Create, Retrieve, Update, and Delete (CRUD) operations on the underlying databases.

• Service Layer: Consists of service classes and uses services provided by data access layers.

• Integration Layer: It consists of the web and its different web services.

As these layers facilitate the development and simulation of the IPS we also added some cryptographic securitytechniques for the bi-level prevention classifier which include an authentication technique through passkeys and passwords between the two parties involved in communication that is simple and does not overweight the system. This helped to build an overall communication environment among the sender and receiver with the server and Intermediate adversaries. We were successfully able to simulate the normal interactions and intrusions over this architecture. And were able to record the results of various malicious attacks done in the simulating environment.

IV. RESULTS

The performance metrics used for evaluation are described below:

Accuracy: It measures the proportion of correct predictions made by a model out of the total predictions done.

Precision: This metric quantifies the number of positive class predictions that actually belong to the positive class.

Recall or Sensitivity: It denotes the number of positive class predictions made out of all positive examples in the

dataset. F1-Score: This metric provides a single score that balances both precision and recall in one number.

The best accuracy 99.2% is given by the RF model which has descent values for other metrics like recall and F-Score

While SVM and CART have better F measure and recall they do not perform well predicting the accurate predictions.

Thus, LDA stands at last as the least performing model which does not render better results. It can be clearly distinguished that the supervised models give good performance in the ideal IDS model.

They also contribute well and to along well with the IPS thus forming an efficient IDPS, as depicted by Table 1.

Table 1. The evaluation metrics of Algorithms

Method	Accuracy	Precision	F1-Score	Recall
RF	99.2	82.5	90.88	96.13
SVM	83.0	80.10	73.4	68.6
CART	82.55	78.35	72.9	68.7
LDA	68.15	17.93	14.7	13.7

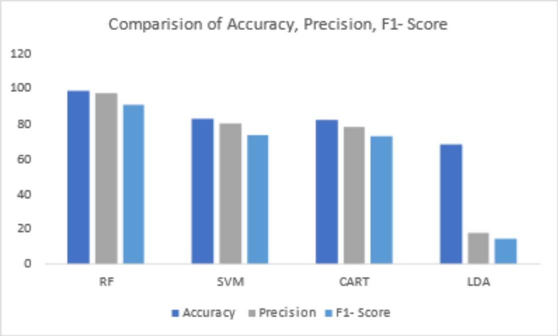

Fig 3: Comparison

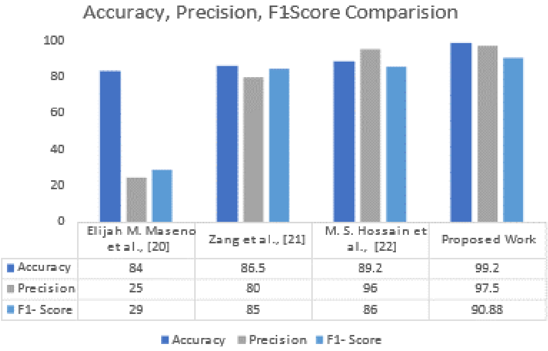

Fig 4: Comparison

The above figures 3 and 4 clearly shows the distinction in performance between the different supervised learning

algorithms and the unsupervised learning algorithms based on accuracy and evaluation metrics. The simulation results also block the malicious packets from the intermediate intruder node thus successfully performing in the simulated network. The state-of-the-art techniques give better results taking the additional cost of space and time but the propounded IDPS get the work done in the most minimal way as demonstrated by the results. When we focus on the comparison between supervised and unsupervised learning there is a clear line of distinction that supervised RF algorithm works well for the IDPS due to it ground truth is clear for easy decision tree based RF classification. But the unsupervised learning failed to achieve the better values even though many learning epochs due to their incapacity to understand the data distribution and flow.

SVM also gave best results given the condition that the scalability was exploited due to small testing dataset compared to training dataset. Over all the performance of both the ML paradigms were quite unpredicted but the truth is uncovered through true experimentation and implementation of the IDPS in the propounded work of IDS.

Intrusion Prevention system worked well as IDS though it was supported by it at the background, the overall decision making whether to drop the rejected packet by IDS was completely on IPS. We also provided a chance to allow the packet to be if it is falsely qualified as attack by the IDS due to misconceptions of the ML algorithms by the help of cryptographic verification through simple password and other authentication methods, which helped the overall IDPS to work smoothly giving the best results. The comparison of the recent works is as shown in fig 4 along with the same performance evaluation metrics. We have compared and contrasted our proposed work in terms of accuracy, precision, F1-Score along with the works which uses the lightweight approach to develop an IDPS which stands as a comparative reference for our research and implementation done. Hence it is clearly shown from the table in the fig 4 above that the proposed work excels at the evaluation metrics by scoring best result values used and satisfying all the criterion.

V. Conclusion

In a nutshell, this work proposes ML-based IDS followed by IPS which constitutes the integrated IDPS that safeguards the IoT devices and wireless network by detecting and preventing the intrusive packets that are malicious. This system for security uses Random Forest as the decision-driving algorithm which detects the intrusion attacks and the prevention system uses this along with cryptography techniques such as passkeys and passwords which serve as an encryption medium to prevent the attacks by forming a two-layer protection to the IoT devices. We have utilized KDD CUP dataset and this model performs well for both known and unknown attacks on the system causing no overload to the existing IoT devices and networking system. It is found that the supervised learning mechanisms offer a better level of accuracy in predicting intrusion attacks in contrast to the other models of unsupervised learning by the performance and results. The proposed model overcomes the constraints on space, power, and processing providing a better solution to the problem of ensuring zero compromising security. This work satisfies the same by meeting all the requirements of an optimistic IDPS. Further development can be an extra addon to make the IDPS more reliable and sustainable in the dynamic environment of wireless IoT networks.

REFERENCES

[1] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti and T. -H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," in IEEE Access, vol. 10, pp. 121173- 121192, 2022, doi: 10.1109/ACCESS.2022.3220622.

[2] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan and D.Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," in Journal of Communications and Networks, vol. 24, no.2, pp. 264-273, April 2022, doi: 10.23919/JCN.2022.000002.

[3] E. Kabir, J. Hu, H. Wang, and G. Zhuo, “A novel statistical technique for intrusion detection systems,” Future Gener. Comput. Syst., vol. 79,pp. 303–318, 2018.

[4] Hasan Alkahtani and Theyazn H.H. Aldhyani. “Intrusion Detection System to Advanced IOT Infrastructure Based Deep Learning Algorithm”,2021.

[5] B. Abhale and S. S. Manivannan, “Supervised machine learning classification algorithmic approach for finding anomaly type of intrusion detection in wireless sensor network,” Opt. Memory Neural Netw., vol. 29, no. 3, pp. 244–256, 2020.

[6] W. Seo and W. Pak, "Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning," in PF De Araujo-Filho, AJ Pinheiro, G Kaddoum, DR Campelo, FL Soares,” An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost Platform”, IEEE Internet of Things Journal, 2022.

[7] S. Park, S. Kwon, Y. Park, D. Kim and I. You, "Session Management for Security Systems in 5G Standalone Network," in IEEE Access, vol.10, pp. 73421-73436, 2022, doi: 10.1109/ACCESS.2022.3187053.

[8] R. Vijayanand, D. Devaraj, and B. Kannapiran, “Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection,” Comput. Secur., vol. 77, pp. 304–314, 2018.

[9] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” Internet Things, vol. 7, 2019.

[10] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, “Performance analysis of machine learning algorithms in intrusion detection system: A review,” in Procedia Comput. Sci., vol. 171, pp. 1251–1260, 2020.

[11] Omarov, M. Asqar, R. Sadybekov, T. Koishiyeva, A. Bazarbayeva and Y. Uxikbayev, "IoT Network Intrusion Detection: A Brief Review," 2022 International Conference on Smart Information Systems and Technologies (SIST), Nur-Sultan, Kazakhstan, 2022, pp. 1-5.

[12] Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. "An intrusion detection system against DDoS attacks in IoT networks." In 2020 10th annual Computing and Communication Workshop and Conference (CCWC), pp. 0562-0567. IEEE, 2020.

[13] P. Illy, G. Kaddoum, K. Kaur and S. Garg, "ML-Based IDPS Enhancement With Complementary Features for Home IoT Networks," in IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 772-783, June 2022, doi: 10.1109/TNSM.2022.3141942.

[14] Vergütz, B. V. d. Santos, B. Kantarci and M. Nogueira, "Data Instrumentation From IoT Network Traffic as Support for Security Management," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1392-1404, June 2023, doi:

[15] 10.1109/TNSM.2022.3233673. [16] Chaitra, Y.L., Dinesh, R. et al. "Deep-CNNTL: Text Localization from Natural Scene Images Using Deep Convolution Neural Network with Transfer Learning", Arab J Sci Eng, 2022.

[16] Chaitra, Y.L., Dinesh, R. "An Impact of Radon Transforms and Filtering Techniques for Text Localization in Natural Scene Text Images", ICT with Intelligent Applications. Smart Innovation, Systems and Technologies, vol 248. Springer, 2022.

[17] R. Latha and R. M. Bommi, "Hybrid CatBoost Regression model based Intrusion Detection System in IoT-Enabled Networks," 2023 9th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 2023, pp. 264-269.

[18] Ioulianou, Philokypros P., Vassilios G. Vassilakis, and Siamak F.Shahandashti. "A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks." Journal of Cybersecurity and Privacy 2, no. 1 (2022): 124-153.

[19] Elijah M. Maseno, Zenghui Wang and Hongyan Xing "A Systematic Review on Hybrid Intrusion Detection System", Wiely Publictions,2022, https://doi.org/10.1155/2022/9663052IEEE Access, vol. 9, pp. 46386-46397, 2021, doi: 10.1109/ACCESS.2021.3066620.

[20] Zhang, Yunpeng & Gandhi, Yash & Li, Zhixia (Richard) & Xiao, Zhiwen. (2022). Improving the Classification Effectiveness of Network Intrusion Detection Using Ensemble Machine Learning Techniques and Deep Neural Networks. 117-123. 10.1109/IDSTA55301.2022.9923205.

[21] M. S. Hossain et al., "Performance Evaluation of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms," 2023 4th International Conference on Big Data Analytics and Practices (IBDAP), Bangkok, Thailand, 2023, pp. 1-6, doi: 10.1109/IBDAP58581.2023.10271964

[22] Naaz, Sameena. "Detection of phishing in the internet of things using machine learning approach." International Journal of Digital Crime and Forensics (IJDCF) 13, no. 2 (2021): 1-15.

[23] Noman Mazhar; Rosli Salleh; Muhammad Zeeshan; M. Muzaffar Hameed; Nauman Khan, R-IDPS: Real-time SDN based IDPS system for IoT security, 2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET).

[24] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of things," IEEE Access, vol. 7, pp. 42 450–42 471, 2019. [26] F. Zhang, Y. Wang, S. Liu, and H. Wang, "Decision-based evasion attacks on tree ensemble classifiers," World Wide Web, vol. 23, no. 5, pp.2957–2977, 2020.

[25] S. Huang, Y. Lu, W. Wang, and K. Sun, "Multi-scale guided feature extraction and classification algorithm for hyperspectral images," Scientific Reports, vol. 11, no. 1, 2021.

[26] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," in Proc.IEEE ICSPC, 2017.

[27] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," Procedia Comput. Sci., vol. 52, pp. 1047–1052, 2015

[28] S. Sridevi, S. Parthasarathy, and S. Rajaram, "An effective prediction system for time series data using pattern matching algorithms," Int. J. Ind. Eng.: Theory Appl. Pract., vol. 25, no. 2, pp. 123–136, 2018.

[29] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 2009, pp. 1-6, doi: 10.1109/CISDA.2009.5356528.

[30] Bachar, Anouar, Noureddine El Makhfi, and Omar EL Bannay. "Machine learning for network intrusion detection based on SVM binary classification model." Advances in Science, Technology and Engineering Systems Journal 5.4 (2020): 638-644.

[31] M. Belouch, S. El, M. Idhammad, "A Two-Stage Classifier Approach using RepTree Algorithm for Network Intrusion Detection". International Journal of Advanced Computer Science and Applications, 8(6), 2017. doi:10.14569/ijacsa.2017.080651.