JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

Enhancing Database Security through AI-Based Intrusion Detection System

Rafeeq Ahmad[1], Humayun Salahuddin[2], Attique Ur Rehman[1], Abdul Rehman[2], Muhammad Umar Shafiq[3], M Asif Tahir[2], and Muhammad Sohail Afzal[1]

[1]Department of Computer Science, National College of Business Administration & Economics (Sub Campus) Multan, Pakistan.
[2]Department of Computer Science, Riphah International University Sahiwal Campus, Sahiwal, Pakistan.
[3]College of Arts and Sciences, The University of Alabama at Birmingham, Birmingham, Alabama, USA.
[*]Corresponding Author: Humayun Salahuddin. Email: humayun.salahuddin@riphahsahiwal.edu.pk

Received: March 21, 2024 **Accepted:** August 09, 2024 **Published:** September 01, 2024

Abstract: Cybersecurity attacks on network database systems are becoming widespread, causing many problems for individuals and organizations. In order to improve access to the search system for database security, this study proposes the use of cognitive-based models. Artificial intelligence algorithms are used as the first step in determining the most important parts of network data. Database security is improved by using advanced technology. Four classification algorithms are used for intrusion detection: K nearest neighbor (KNN), support vector machine (SVM), decision tree (DT), and a combination of neural network (CNN). The performance of the penetration testing model is demonstrated and analyzed using the test model and NSL-KDD datasets. According to the empirical results, the deployment method improves the access. The conclusion is that the proposed model is better than the original model. This study uses four classification algorithms to identify four types of network attacks, such as DoS attacks, U2R attacks, R2L attacks, and packet sniffing attacks, but the accuracy of the CNN classifier is higher than other classifications with 98.4% accuracy.

Keywords: Database Security; Convolutional Neural Network; Intrusion Detection System; Machine Learning.

1. Introduction

A significant part of the Internet network is the Internet Protocol. Enter the basic settings required for a database "intrusion detection system (IDS)" designed to detect malicious activity in large databases. A solid foundation in a database management system (DBMS) is required. To do this, you need to understand database models, data structures (such as relational models and NoSQL), queries (such as SQL), and database security techniques. This includes anomaly- and signature-based hybrid methods and search methods that support access to search terms, methods, and procedures. Although the system does not perform well on large-sized data, it always uses machine learning (ML) techniques to correctly classify two real-world data with up to 99.40% accuracy [1].

This includes model selection based on engineering techniques and evaluation techniques, as well as supervised, unsupervised, and semi-structured learning techniques. Understanding encryption techniques and security techniques is essential to protect information during transmission and storage [2]. A stealthy attack that manipulates, cleans, and executes special operations to avoid detection. Attackers use simple services to prevent malicious orders from being recognized as normal packets, and the attack is spread over multiple sessions and a long period of time to avoid discovery. According to the research, convolutional neural networks outperform other machine learning algorithms [3].This is an important skill to have at speed in a dynamic environment. This article explores the use of AI and machine learning in e-commerce, business management, and finance [4] [5].

This is used to detect and identify suspicious attacks in the network. Since the attack is weak, the evaluation of the test data is also very important. The size of the network is reduced by removing the

unnecessary part of the attack for accurate calculations. First, the advantage of using deep techniques is that the need for a convolutional neural network (CNN) model to reduce features is reduced. This function uses the KDD Cup 99' dataset to calculate accuracy. Simulations were run in MATLAB environment and results were compared with the most popular machine learning methods. Predictive models perform better in terms of accuracy. For comparison, use deep neural network (DNN), random forest (RF), support vector machine (SVM), etc. An accuracy of 96% was achieved through simulation [6]. Predictive models perform better in terms of accuracy. For comparison, use (DNN), (RF) and (SVM). An accuracy of 96.6% was achieved through simulation [7].

The main Objectives of this paper are:

- To study the cause and effect of Enhanced Security Infrastructure.
- To strengthen malware detection based on state-of-the-art machine learning algorithms.
- To provide recommendations for improving database security policies and procedures based on the findings and insights from the research.
- Early detection of malware attacks.

1.1. Author's Contribution

The author's contribution highlights to detect the fourth type of cyber-attack named as packet sniffing attack discussed in the methodology and result section by implementing Convolutional Neural Network (CNN) with the accuracy of 98.4% and early detection of malware attack which is enough for securing database system for an organization or individual.

The effectiveness of data-driven intelligent decision making in cyber security systems and services is attributed to machine learning approaches. It is driven by the growing importance of machine learning and cyber security technology. Its effect on security data has also been talked about, in terms of data analysis and gaining understanding of security occurrences. The primary subjects of conversation were the developments in machine learning and the difficulties with IoT security intrusion detection systems [8] [9]. The development of artificial intelligence skills to meet the demands of service innovation performance an urgent need to survive in a volatile environment is explained in this paper [10].

This work offers conceptual insights to improve the research stream. The paper presents a novel deep learning (DL) approach that is managed by software-defined networking (SDN) to create an intelligent intrusion detection system (IDS) for a smart network. Topics such as supervised learning, un-supervised learning, and reinforcement learning discussed [11].

This method presents SDN architecture as a potential solution that can manage the dispersed architecture of smart CE networks and allow reconfiguration over static network infrastructure by separating the control and data planes [12].

This research advances network security in higher education institutions and helps them better safeguard their valuable assets and sensitive data from cyber-attacks by understanding how data quality affects intrusion detection system (IDS) performance and putting into practice efficient deployment strategies [13]. Three classification methods were used in this study's intrusion detection system: "Naive Bayes (NB), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN)" [13].

This article describes various IoT host interference scenarios at the interface level, as well as effective methods and techniques to protect the host from the outside. We recommend that you take security measures to reduce the risks that may affect the host in particular. Fuzzy recommendation systems such as MORA, TOPSIS, VIKOR, and WASPAS are used to evaluate the algorithms and provide ratings. The team of machine learning algorithms Random Forest, Lite Gradient Boost, Decision Tree, and Extra Gradient Boost improve the accuracy, recall, and F1 scores, while increasing the true value (about 99%) and proving its effectiveness in reaching performance. Network communication [14].

This study aims to support physical knowledge by explaining these attacks in detail, providing solutions for determining the effects in the network, and proposing a common system that combines three different learning algorithms. Remote-to-local (R2L) attack detection is most accurate when only machine learning is used to analyze network data. On the other hand, the overall detection efficiency of R2L attacks of the cluster group is 99.8% [15]. This study aims to increase the body's knowledge by explaining these attacks in detail, providing solutions to detect network outages, and offering solution suggestions by combining three different learning algorithms. The detection of remote-to-local (R2L) attacks gives the

most accurate result when the same machine learning model is used to analyze network data. On the other hand, the overall detection efficiency of R2L attacks of the cluster group is 99.8% [16].

In this study, we use "Gaussian Naive Bayes (GNB) and Stochastic Gradient Descent (SGD)" machine learning algorithms. We found that experts agree that content-aware addition yields better results. In order to minimize the work of the machine, we first perform the main analysis points and the destruction results of the original data. Based on the WSN-DS dataset, the proposed SG-IDS model achieves 98% accuracy, 96% recall, and 97% F1 index [17]. Indicate the data used to evaluate the IDS model. This paper includes "CIC-IDS-2017 and CSE-CIC-IDS-2018" and provides an overview of ML and DL algorithms for IDS. These are up-to-date information on new and potential cyber-attacks. This work presents the recent developments in IDS data that can be used as a guide by different research groups to develop ML-based IDS using new IDS data [18]. SVM algorithm is combined with genetic algorithm to identify network components. The combination of training and testing using KDD Cup99 data resulted in a decrease from 42 to 29. It also achieved a false positive rate of 0.012 and a true positive rate of 0.9987 [19].

Considering the problems related to global water scarcity, the proposed data-centric IoT approach represents a major leap forward in agricultural water management and holds good promise for proper and stable water supply [20]. ML based on ANN is an effective and promising method for monitoring air pollution based on the Internet of Things, which can solve the limitations in monitoring ordinary pollution. The strategic approach paves the way for proactive pollution strategies by enabling intelligent and pollution monitoring system decision-making by utilizing the potential of artificial neural networks. This scheme has the ability to change air pollution monitoring through its solutions, based on the effort to show an accuracy of 91.3% compared to previous methods [21]. Sample detection can predict whether food contains allergens. These standards help doctors and nutritionists create food lists that reduce the risk of food allergies by promoting non-allergenic foods. The rating model identifies the food and evaluates its distribution. The training and recognition accuracies of random forest, support vector machine and k-many neighbor models are 96.8%, 93.54% and 95.16%, respectively. Decision tree achieves the highest testing accuracy of 98.4%. This demonstrates a way to understand the nature of food allergies. In-depth analysis of allergen prevalence can provide insight into the occurrence of different allergens in various foods. This system can provide personalized recommendations to people with dietary restrictions or allergies, improving their decision-making and ability to choose healthy foods [22].

The research process of this study refers to the significant selection of the best methods to analyze and classify electrocardiogram (ECG) data, determine research objectives, select algorithms, information, and study plans. This study analyzed the heart disease electrocardiogram image dataset, focusing on data preprocessing steps including image resizing, grayscale conversion, and dataset partitioning for training and testing [23].

The main problems encountered in accessing the dataset are privacy and confidentiality issues related to sharing medical information. In medical image analysis (MIA), the division of labor between centralized networks (CNN) and government strategies for protecting private information is exciting. Our results show that CNN can achieve 0.90 accuracy. We present a mobile application for skin disease classification using CNN and federal learning techniques. Analysis of human skin using this mobile application is highly effective in ensuring data security [24].

2. Proposed System and Methodology

The aim of this study is to achieve the research goal by providing solutions to information security problems discussed in various international topics and to solve the problems more effectively and efficiently than thinking and solving them in the past. In this study, the original KDD Cup 99 dataset is replaced with the Network Security Laboratory Database Knowledge Discovery (NSL-KDD) dataset, which provides a better understanding of the access behavior. The methods used in this study include six methods: data collection, preliminary data, feature evaluation, feature selection, design and verification. The malware attack group is called "0=Normal, 1=DoS, 2=R2L, 3=U2R, 4=Packet Sniffing". Each attack dataset goes through all different classification algorithms before producing the result. This data is based on different methods like "Decision Tree (DT), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Convolutional Neural Network (CNN) classifiers". This is also done to evaluate whether the truth is better compared to testing and training all the methods to classify the material.

The author's contribution highlights to detect the fourth type of cyber-attack named as packet sniffing attack discussed in the methodology and result section by implementing Convolutional Neural Network (CNN) with the accuracy of 98.4% and early detection of malware attack which is enough for securing database system for an organization or individual.

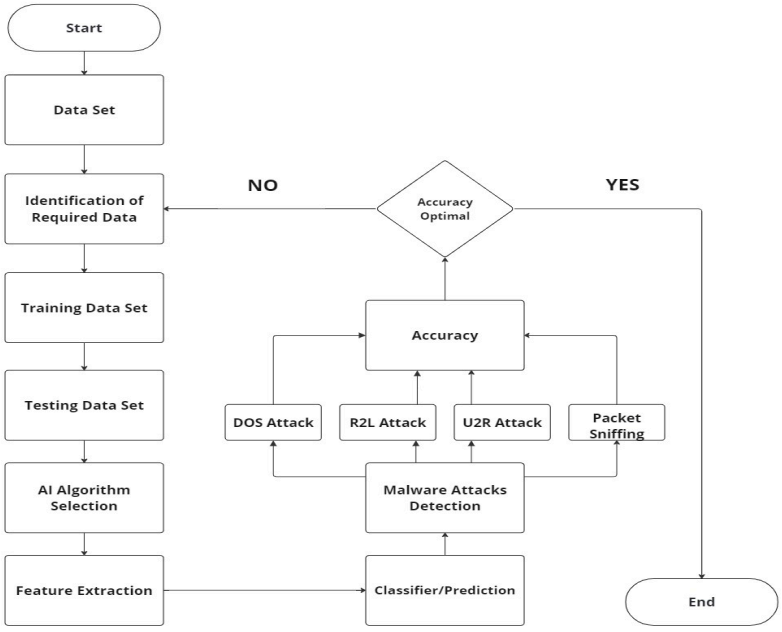

Figure 1. Proposed System for Malware Attacks detection

3. Results of Proposed System

The application of the machine learning methods is covered in this section. It also describes the widely used assessment metrics for machine learning techniques for intrusion detection systems. Table 1 displays the general confusion matrix, which is used to show how well our supervised learning algorithms work.

Table 1. Confusion Matrix

Actual Class	**Predicted Class**	
	Attack	Normal
Attack	True_Positive	False_Negative
Normal	False_Positive	True_Negative

3.1. DoS Attack

Tables 2 and 3 display the outcomes of using the DT, SVM, KNN, and CNN classifier on our DoS attack dataset. Table 3 displays additional metrics that the classifiers looked for, whereas Table 2 displays the confusion matrix for DoS assaults that were categorized using the four previously mentioned classifiers algorithms. Metrics including F-measure, accuracy, recall, and precision.

Table 2. Confusion matrix for four classifiers on DoS attack

DoS Attack		**Predicted Attacks**	**Classifier**
Actual Attacks	0	1	DT
0	9602	109	
1	2625	485	
	0	1	SVM
0	9677	34	
1	3578	3882	
	0	1	KNN
0	9653	58	
1	2645	4815	
	0	1	CNN

0	9715	62
1	3165	5223

Table 3. Evaluation metrics for four classifiers on DoS attack

Metrics	Precision	Recall	F-Measure	Support	Classifiers
0	0.79	0.99	0.88	9711	DT
1	0.98	0.65	0.78	7460	
Accuracy	-	-	0.84	17171	
Macro avg	0.88	0.82	0.83	17171	
Weighted avg	0.87	0.84	0.83	17171	
0	0.73	1	0.84	9711	SVM
1	0.99	0.52	0.68	7460	
Accuracy	-	-	0.79	17171	
Macro avg	0.86	0.76	0.76	17171	
Weighted avg	0.84	0.79	0.77	17171	
0	0.78	0.99	0.88	9711	KNN
1	0.99	0.65	0.78	7460	
Accuracy	-	-	0.84	17171	
Macro avg	0.89	0.82	0.83	17171	
Weighted avg	0.87	0.84	0.83	17171	
0	0.77	0.99	0.87	9711	CNN
1	0.99	0.64	0.77	7460	
Accuracy	-	-	0.984	17171	
Macro avg	0.88	0.83	0.89	17171	
Weighted avg	0.86	0.85	0.89	17171	

Out of 12,821 applications, 9,602 were classified as adversaries. Out of 3,110 models included in the evaluation, the vendor is estimated to have only 485 models. Table 2 shows this. This study shows that decentralized decision trees provide better performance to network operations. The accuracy of this method is 0.84 but could be better. CNN and reconnaissance mission will prove it. After some training using decisions on DoS_attack_dataset, SVM classifier uses metric to calculate the accuracy of the classification algorithm and the result is 0.79. A simple method called KNN classifier is used to collect patterns and classify them according to similarity measures such as distance function. Compared to decision trees, product confusion matrices provide the ability to prevent network behavior and strong DoS attacks against predictions. The accuracy of this classification is the same as decision tree which is 0.84. The CNN classifier produces DoS events with an accuracy of 0.984. Figure 2 is a graph comparing four CNN models. A full measure of DoS is shown in Figure 2. This may be due to the development of deep neural networks in the CNN model, unlike other machine learning algorithms that only send the dataset to the category once.

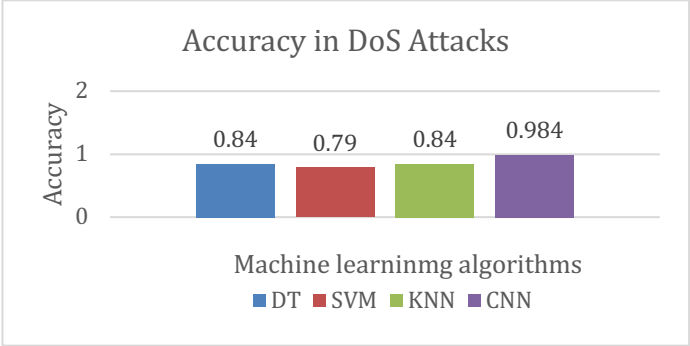

Figure 2. Accuracy in DoS Attack

3.2. There is R2L Attack

The situation where a remote user tries to send a packet to gain unauthorized access is represented by the R2L attack type. Table 4 shows the confusion matrix showing the effectiveness of the decision tree classification in identifying these R2L attacks in the context of our research. This matrix shows the effectiveness of the decision tree model in detecting and blocking access points by showing the bad predictions.

Table 4. Confusion matrix for four classifiers on R2L attack

R2L Attack		Predicted Attacks	Classifier
Actual Attacks	0	3	DT
0	9649	62	
1	2560	325	
	0		SVM
0	9711	0	
3	2885	0	
	0	3	KNN
0	9710	0	
3	2885	1	
	0	1	CNN
0	9635	72	
3	3091	445	

Table 5 shows that the accuracy of the decision tree and SVM methods is 84%. Since this accuracy is not very high in terms of network security, we will use various classifications to select the models with the highest accuracy. Since these accuracy levels are not sufficient for cybersecurity needs, KNN and additional classification are used to determine the accuracy. Although the accuracy of the classification algorithm reaches 77%, it still cannot guarantee the overall security of the network. So far, we have found that machine learning methods cannot achieve R2L even with good predictions. The output of the CNN classifier is 0.984. This fact is useful for predictive models in cybersecurity. Figure 3 shows the graphical representation of various distributions used to define R2L profiles.

Table 5. Evaluation metrics for four classifiers on R2L attack

Metrics	Precision	Recall	F-Measure	Support	Classifiers
0	0.79	0.99	0.88	9711	DT
1	0.84	0.11	0.2	7460	
Accuracy	-	-	0.84	17171	
Macro avg	0.82	0.55	0.54	17171	
Weighted avg	0.8	0.79	0.72	17171	
0	0.79	0.99	0.88	9711	SVM
1	0.84	0.11	0.2	7460	
Accuracy	-	-	0.84	17171	
Macro avg	0.82	0.55	0.54	17171	
Weighted avg	0.8	0.79	0.72	17171	
0	0.77	1	0.87	9711	KNN
1	0	0	0	7460	
Accuracy	-	-	0.77	17171	
Macro avg	0.39	0.5	0.44	17171	
Weighted avg	0.59	0.77	0.67	17171	
0	0.78	0.96	0.89	9711	CNN
1	0.98	0.66	0.78	7460	
Accuracy	-	-	0.984	17171	
Macro avg	0.88	0.83	0.88	17171	

Weighted avg	0.87	0.85	0.89	17171

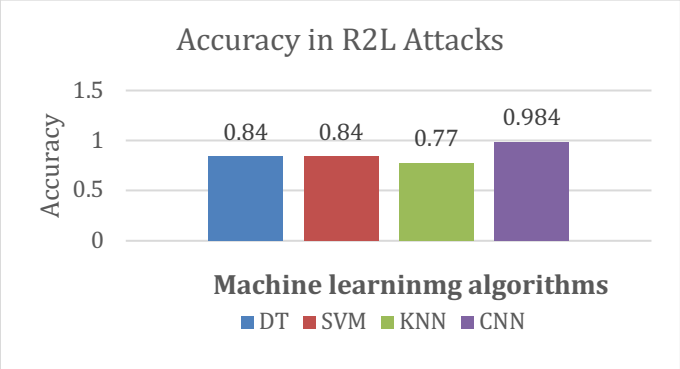

Figure 3. Accuracy in R2L Attack

3.3. U2R Attack

User-to-root (U2R) attack occurs when a local user who is authorized to access the primary network but not the backend network is granted access to the root cause. Table 6 shows the true positive, negative, negative, and negative values for the four tests in this study. Table 7 provides additional indicators. The output accuracy of this classification test is 98.4%, indicating that it is effective and suitable for predicting cyber-attacks. Figure 4 shows the accuracy of 91% for the U2R attack using the SVM classifier. This means that the SVM classifier can predict the future U2R attacks of the network. Also, the accuracy of this KNN product is only 85%, which shows that the search accessibility needs to be further improved. The estimated delivery rate of CNN classification results is 98.4%.

Table 6. Confusion matrix for four classifiers on U2R attacks

U2R Attack		Predicted Attacks	Classifier
Actual Attacks	0	5	DT
0	9706	5	
4	52	15	
	0	4	SVM
0	9711	0	
4	67	0	
	0	4	KNN
0	9709	2	
4	60	7	
	0	6	CNN
0	9788	8	
4	71	11	

Table 7. Evaluation metrics for four classifiers on U2R attack

Metrics	Precision	Recall	F-Measure	Support	Classifiers
0	0.99	1	1	9711	DT
1	0.75	0.22	0.34	7460	
Accuracy	-	-	0.88	17171	
Macro avg	0.87	0.61	0.67	17171	
Weighted avg	0.99	0.99	0.99	17171	
0	0.99	1	1	9711	SVM
1	0	0	0	7460	
Accuracy	-	-	0.91	17171	
Macro avg	0.5	0.5	0.5	17171	
Weighted avg	0.9	0.99	0.99	17171	

0	0.99	1	1	9711	KNN
1	0.78	0.1	0.18	7460	
Accuracy	-	-	0.85	17171	
Macro avg	0.89	0.55	0.59	17171	
Weighted avg	0.99	0.99	0.99	17171	
0	0.99	1	1	9711	CNN
1	0.98	0.1	0.18	7460	
Accuracy	-	-	0.984	17171	
Macro avg	0.9	0.66	0.69	17171	
Weighted avg	0.89	0.99	0.99	17171	

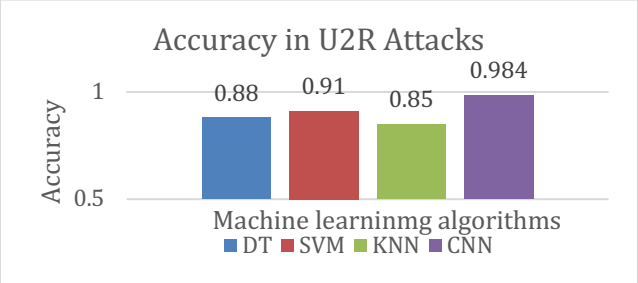

Figure 4. Accuracy in U2R Attack

3.4. Packet Sniffing Attack

These cyber-attacks capture and inspect network packets to obtain private information. Table 8 shows the results of the confusion matrix after processing the data according to CNN, SVM, KNN and decision tree classification. It shows the classification accuracy in predicting the attacks. The results show that the classification accuracy of DT, SVM, KNN and CNN is 88%, 89%, 91% and 98.4% respectively. The most accurate classifier that can detect these attacks is CNN. Table 9 shows the accuracy of the classification algorithm which resulted in 98.4%.

Table 8. Confusion matrix for four classifiers on Packet Sniffing attacks

Packet Sniffing Attack		**Predicted Attacks**	**Classifier**
Actual Attacks	0	7	DT
0	9808	7	
4	65	14	
	0	6	SVM
0	9813	3	
4	77	3	
	0	5	KNN
0	9829	3	
4	80	8	
	0	12	CNN
0	9889	17	
4	81	23	

Table 9. Evaluation metrics for four classifiers on Packet Sniffing attacks

Metrics	**Precision**	**Recall**	**F-Measure**	**Support**	**Classifiers**
0	0.99	1	1	9711	DT
1	0.85	0.22	0.34	7460	
Accuracy	-	-	0.88	17171	
Macro avg	0.89	0.61	0.67	17171	
Weighted avg	0.99	0.99	0.99	17171	

0	0.98	1	1	9711	SVM
1	0	0	0	7460	
Accuracy	-	-	0.89	17171	
Macro avg	0.6	0.5	0.5	17171	
Weighted avg	0.8	0.99	0.99	17171	
0	0.99	1	1	9711	KNN
1	0.77	0.1	0.18	7460	
Accuracy	-	-	0.91	17171	
Macro avg	0.90	0.55	0.59	17171	
Weighted avg	0.98	0.99	0.99	17171	
0	0.99	1	1	9711	CNN
1	0.97	0.1	0.18	7460	
Accuracy	-	-	0.984	17171	
Macro avg	0.9	0.66	0.69	17171	
Weighted avg	0.93	0.99	0.99	17171	

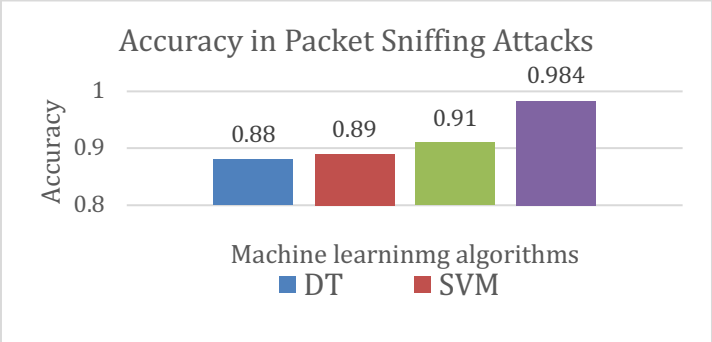

Figure 5. Accuracy in Packet Sniffing Attack

Different tools have been used together to create a cluster classifier before. This information is used to evaluate it to make sure that it identifies the attack. Packet sniffing attacks are used for all distributions. The accuracy of the output of the cluster is as high as 98.4%. From the results shown in Table 9 and Figure 5, it is clear that the CNN classifier produces the most accurate prediction of the attack and the In terms of measurement, the CNN classifier produces results similar to the classification or combination of several machine learning methods.

3.5. Early Detection

The main issue of this study is the accuracy and time of the search, as the results of DT, SVM, KNN and CNN will be discussed. It has been shown that CNN classifier can detect network attacks earlier and better with short detection time compared to other algorithms, as shown in Figure 6.

4. Discussion

This study aims to improve database intrusion detection systems (DIDS) using machine learning methods. The effectiveness of various methods such as data compression and network connectivity analysis should be evaluated to improve database intrusion detection systems (DIDS). In a comparative test, the algorithm and Apache Spark simulator were evaluated to improve data connectivity, connectivity error handling, and security interception. This research aims to manage and control updates in networks by sending fast queries. The studies include the implementation and evaluation of a multi-layered secure relational database management system using AI-based access to a search system that combines content with a secure deductive database management system. These include machine learning techniques that are important for efficiency, optimization, and prevention when using Spark's database intrusion detection system (DIDS).

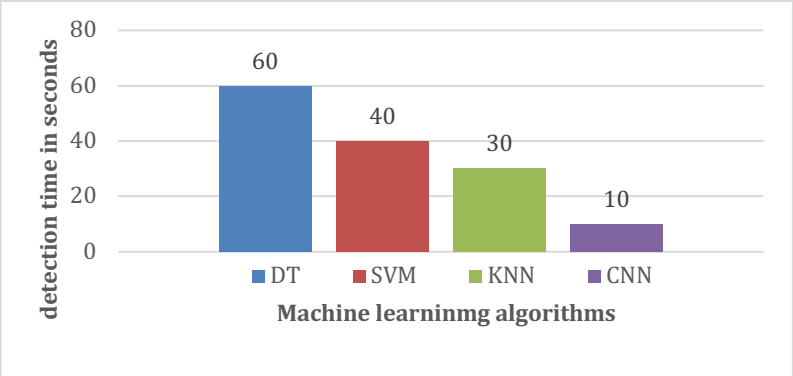

Figure 6. Detection time of machine learning algorithms

5. Conclusion

It is concluded that, this study has evolved the use of machine learning techniques to enhance Database Intrusion Detection Systems (DIDS). The implementation and evaluation of a secure deductive database management system (MLS/DEDBMS) integrated deductive reasoning with a multilevel secure relational database management system, addressing architectural concerns and providing a sample implementation. Machine learning methods for implementing IDS showed promising results in terms of performance, scalability, and preprocessing capabilities, leveraging Spark's distributed processing capabilities to handle massive amounts of network data effectively. Four categories of attacks are detected in this research such as DoS attack, R2L attack, U2R attack and Packet sniffing attack with four classifiers DT, SVM, KNN and CNN. The CNN gives more accurate results with the accuracy rate of 98.4% and the 10 seconds detection time than the other machine learning classifiers to provide environment for improved database security policies, enhanced security infrastructure and malware attacks detection based on state-of-the-art machine learning algorithms.

References

1. Hang F, XieL, Zhang, Z, Guo, W & Li,H.(2024). Research on the application of network security defence in database security services based on deep learning integrated with big data analytics,International Journal of Intelligent Networks.
2. Azhar S, Yonis N H, & Yosuf H N. (2023). A Review on Big Data Security Issues.
3. Gunjal H, Patel,P, Ebrahimi,D.D&Alzhouri,D.F(2023). A Smart Network Intrusion Detection System for Cyber Security of Industrial IoT.
4. Kumar, P, Sharma, S. K, & Dutot,V. (2022). Artificial intelligence (AI)-enabled CRM capability in healthcare: The impact on service innovation. International Journal of Information Management, 69, 102598.
5. Pallathadka, H, Ramirez-Asis, E. H, Loli-Poma, T. P, Kaliyaperumal, K, Ventayen, R.J. M, & Naved, M (2021). Applications of artificial intelligence in business management, e-commerce and finance.
6. Manikandan, V , Gowsic, K & Prince, T. (2020). DRCNN-IDS Approach for Intelligent Intrusion Detection System.
7. Nugroh, E.P , Djatna, T & Sitagang, I.S. (2020). A Review of Intrusion Detection System in IoT with Machine Learning Approach: Current and Future Research.
8. Sallay, H (2022). An Integrated Multilayered Framework for IoT Security Intrusion Decisions,Intelligent Automation & Soft Computing.
9. Shujaat S, Riaz M, & Jacobs,R. (2022). Synergy between artificial intelligence and precision medicine for computer-assisted oral and maxillofacial surgical planning. Clinical Oral Investigations.
10. Kumar, P, Sharma, S. K, & Dutot,V. (2022). Artificial intelligence (AI)-enabled CRM capability in healthcare: The impact on service innovation. International Journal of Information Management, 69, 102598.
11. Gombolay, G. Y, Gopalan N, Bernasconi, A, Nabbout, R., Megerian, J. T, Siegel, B, &Gombolay M. C (2023). Review of machine learning and artificial intelligence (ML/AI) for the pediatric neurologist. Pediatric neurology,42-51.
12. Javeed,D, Saeed,M.S,Ahmad,I. (2023). An Intelligent Intrusion Detection System for Smart Consumer Electronics Network, Volume 69, No 4.
13. Sindika, D. M, Nicholaus, M. R. & Hamadi, N. B. (2024). Improving Network Security: An Intrusion Detection System (IDS) Dataset from Higher Learning Institutions, Mbeya University of Science and Technology (MUST), Tanzania. East African Journal of Information Technology, 7(1), 23-38.
14. ALSAADI, H.I, ALMUTTAIRI, R.M, BAYAT, O & UCANI, O, N. (2019). Computational Intelligence Algorithms to Handle Dimensionality Reduction for Enhancing Intrusion Detection System.
15. NALLAKARUPPAN1, M. K, SOMAYAJI1, S.R. K, FULADI, S, BENEDETTO, F, ULAGANATHAN1, S. K, AN& YENDURI, G. (2024). Enhancing Security of Host-Based Intrusion Detection Systems for the Internet of Things.
16. Abdulkareem,A, Somefun,T.E, Mutalub,A.L, Adeyinka,A. (2024).Experimental analysis of intrusion detection systems using machine learning algorithms and artificial neural networks, International Journal of Electrical and Computer Engineering (IJECE),Vol. 14,No. 1.
17. Eljialy, A.E.M, Yousuf Uddin.M, &Ahmad,S.(2024). Novel Framework for an Intrusion Detection System Using Multiple Feature Selection Methods Based on Deep Learning, Volume 29, Number 4.
18. SALEH, H.M, MAROUANE, H, &FAKHFAKH, H. (2024). Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning,Volume 12.
19. Thakar, A, Lohiya, R. (2020). A Review of the Advancement in Intrusion Detection Datasets.
20. Salahuddin, H. , Sultan, A. , Shaukat, H. (2023). Resource management in agriculture through IoT and machine learning, Journal of computing and biomedical informatics, ISSN 2710-1606, volume 06, No 1.
21. Salahuddin, H., Kainat. (2024). IoT based intelligent pollution monitoring System using machine learning technique, Journal of computing and biomedical informatics, ISSN 2710-1606, volume 06, No 2.
22. Sultan, A., Shaukat, H., Salahuddin, H. (2024). Enhancing food safety: A machine learning approach for accurate detection and classification of food allergens, Journal of computing and biomedical informatics, ISSN 2710-1606.
23. Salahuddin, H., Abbas, A., (2024). Image enhanced heart disease risk assessment using CNN algorithm, Journal of computing and biomedical informatics, ISSN 2710-1606, volume 07, No 1.
24. Ahmad, G., Saleem, M., Salahuddin, H. (2024). Mobile Application for skin disease classification Using CNN with user privacy, Journal of computing and biomedical informatics, ISSN 2710-1606.
25. Mahmood, T., Li, J., Pei, Y., Akhtar, F., Imran, A., & Rehman, K. U. (2020). A brief survey on breast cancer diagnostic with deep learning schemes using multi-image modalities. IEEE Access, 8, 165779-165809. IEEE.