AI-Powered Network Intrusion Detection Systems

[1] Vikram A
Associate Professor, Department of Computer Science & Engineering ,
Aditya Engineering College,
Surampalem, India,
vikrama@aec.edu.in

[2] Ammar Hameed Shnain
Department Of Computers Techniques Engineering, College Of Technical Engineering, The Islamic University,
Najaf, Iraq, Department Of Computers Techniques Engineering, College Of Technical Engineering, The Islamic University Of Al Diwaniyah, Al Diwaniyah, Iraq.
ammar.hameed.it@gmail.com

[3] Rubal Jeet
Associate Professor , Department of Computer Science Engineering,
Chandigarh Engineering College,
Chandigarh group of colleges, Jhanjeri, Mohali 140307, Punjab, India ,
Rubal2932.research@cgcjhanjeri.in

[4] C. Vennila
Prince Shri Venkateshwara Padmavathy Engineering College,
Chennai - 127.
vennila.c_maths@psvpec.in

[5] Pooja Sahu
Department of Computer Science & Engineering, IES College of Technology, Bhopal, M.P., India
pooja.research@iesuniversity.ac.in

[6] K. Krishnakumar
Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,
Chennai, Tamilnadu, India.
kkrishnakumar86@gmail.com

2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS) | 979-8-3503-9075-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/IICCCS61609.2024.10763627

***Abstract*—This study aims at analyzing and outlining an AI-based NIDS design and comparing different implementation models to improve the current state of network protection. Current NIDS do not assist organizations against modern cyber threats hence relies on machine learning and deep learning for real-time protections. The detailed plan of work includes the use of signature and anomaly detection techniques in parallel and the use of ensemble technique for increasing the detectors capabilities and decrease the false positive rates. The study employs open datasets for training and benchmarking and establishes that deep learning models, including CNNs and RNNs, elicit improved results compared to more conventional machine learning models. The results show that the ensemble learning model, outperformed the other and thus emphasizes future work should consider the use of this model for detection of network intrusions. This study shows that netsec based on AI-powered NIDS can increase the opportunity to detect threats and effectively respond to incidents in realistic network contexts. Further research by designs will involve handling issues like model interpretability and updates to sustain reliability and scalability.**

***Keywords*— AI-powered NIDS, network security, machine learning, deep learning, intrusion detection**

I. Introduction

This is due to the proliferation and advancement in technology leading to frequent onslaughts from internet vandals globally[1]. Old school security concepts used to be effective against the challenges that existed at that time but these are no longer adequate against the modern challenges that are changing and evolving dynamically. These traditional approaches that rely on set formulas and rigid structures to identify and prevent new types of threats that are more complex and constant in nature cannot easily achieve this goal. Consequently, current conventional security structures are inadequate and must be replaced with more efficient, dynamic, and self-learning systems for protecting cyberspace[2].

The current search for more effective network security measures has seen Artificial Intelligence (AI) as a valuable asset in this regard. Intrusion detection system that combines the architectures of deep learning and machine learning can be highly effective for the detection of threats in real-time[3]. While NIDS unlike traditional ones employ fixed rules and signatures the AI-based systems can more effectively accommodate innovative as well as unprecedented threats. It's for this reason that using machine learning and other AI technologies based systems, results in an NIDS being able to more adequately detect sophisticated as well as zero-day attacks[4].

The functioning of AI-powered NIDS is in line with machine learning algorithms analyzing enormous amounts of network data in search of anomalous traffic and potential intrusions. This requires the adoption of all the relevant algorithms and models of handling high dimensionality, pattern recognition, and even real-time decision making. The increased elements of detection and the decrease in response time provided by these systems are instrumental in preventing and containing cyber threats[5]. Besides, threat detection and response automation make stress habits that require human engagement in the process, leading to enhanced effectiveness of threat defense systems. In comparing AI-powered NIDS with traditional IDSs, one of the significant benefits of AI-enabled Nx systems is their capability to accurately discern between ordinary traffic and hostile traffic[6]. This is done through the learning process whereby the system is trained with labelled databases, which include both normal and attack traffic. It makes the system more accurate over time as it learns from new data, however, the downside is that developers experience a higher number of false positives.

These fun application are enhanced with deep learning models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which combine to improve the identification of sophisticated attacks. There exists some challenges in developing and deploying the AI-powered NIDS as highlighted below. The first major concern that can be labeled as a potential pitfall of using AI in healthcare is the demand for extensive and heterogeneous data sets to provide fine-tuning of the models. These datasets should comprise a broad spectrum of known attack classes as well as typical network traffic results for the system's reliability. Also, deep learning constant training and applying demand considerable computational power, which in turn, means high costs in hardware and facilities[7].

A second challenge is that network environments are constantly evolving and may change from one design to another within a short span of time. However, due to the modularity of the components and dynamic behavior of the networks over time, it often requires frequent retraining of the AI models[8]. This has to be ongoing in the sense that there has to be constant modifying of the works, updating of works that have already been done, accommodating of new data, as well as new challenges. Concerning the long-term operation of the AI-powered NIDS, other issues relating to scalability and the ability to work in large and complicated networks in real-time also remain important. However, in recent years, researchers have expanded the efficiency of the AI-assisted NIDS solutions[9]. Research work has been conducted on a variety of algorithms that belong to machine learning and deep learning, performance features that can be used for feature extraction, and methods of optimization for intrusion detection systems. Analysing the features of the integrated approaches that use both signature and anomaly based approaches, there are some advantages of both methods of detection[10]. Another area of great interest with many research works and practical applications is ensemble learning, a general approach that focuses on creating multiple models to deliver enhanced performance and reliability. The applications of AI NIDS in live network scenarios are vast, and this is why scholars and researchers introduce them. These systems can help in the early identification of threats, management of low-level events, and at developing improved incident handling. Through the analysis of the specific case of AI-powered NIDS, it can be noted that streamlining of the detection and response will contribute towards ensuring optimal security and prevention against cyber attackers. However, the effective application is possible only if organizations are competent in implementing AI and mastering the details of networks' security, knowing such problems as the interpretability of the model and constant updates[11].

Consequently, the specific objectives of the study will be as follows: Present an in-depth understanding of the design, implementation, and assessment of AI-enhanced NIDS. It will indicate the various AI techniques applied in the study, the problems encountered, and the probable workarounds needed to overcome these problems[12]. Thus, it is the goal of this paper to continue the development of the field through the development of more reliable and accurate network intrusion detection systems by outlining future coursework. Implementation of NIDS that operate via artificial intelligence stands out as a promising trend. These systems, therefore, can be seen to offer even more accurate and timely means of detecting intrusion on the network thereby contributing positively to the security of digital structures. It is, however, crucial to consider that there are certain issues with AI-based NIDS However, the advantages of applying AI in this solution indicate that they are effective to ward off the incipient threats in the networks[13].

II. Literature Review

Nowadays, Network Intrusion Detection Systems, commonly abbreviated to NIDS, have been developed for several decades, and have passed through various stages of development[14]. Originally, these systems were mainly based on the use of rules that helped the system to identify an intrusion by looking for specific patterns similar to previous attacks in the traffic that crossed the network. It is important to note that despite these approaches proving rather effective to a certain degree, they failed to adapt quickly enough to the development of new forms of cyber threats. The nature of signature-based detection was limited to make them ineffective against the new and complex attacks such techniques required constant changes and modifications to became efficient[15].

Machine learning can also be attributed as one of the key milestones when the design of NIDS was considered. It is thus worth appreciating the fact that supervised learning methods were among the earliest to be utilized in this field. These techniques can be used in training models to networks whereby the data is labelled depending on whether it is normal and or malicious traffic. The used trained models could then be used to detect such attack patterns within the normal network traffic flow. Although SL techniques outperformed rule based systems through the incorporation of labelled advisories and heuristics, the models were constrained by their inability to handle unknown attack types due to their dependence on large sets of labels.

As with any discovery methodology, the representativeness of samples and learning algorithms present certain challenges to the supervised learning framework. Anomaly based systems on the other hand are not based oa priori stored patterns of attack; unlike the case with the signature based systems. Conversely, they emulate normal network traffic and then identify an intrusion when patterns do not conform to normalcy. This is perhaps even more useful in the engagement of zero-day attacks, and other threats that the ML classifier has not been trained to combat. However, there are issues that are associated with the use of anomaly-based systems, especially the fact that the system will detect or flag normal behaviour that otherwise is not supposed to raise any alarm. Deep learning has been applied in NIDS to allow them to work even better than before. Neural networks like CNN's, and RNN's are capable of analyzing high dimensionality data and finding a pattern that an analyst with traditional machine learning techniques could easily overlook. shaled CNN's which are capable of learning features from the raw data have been utilized in analyzing traffic in a network and identifying automatically, the anomalies that exist in the data flow. Sequence datatypes that are well modelled by Recurrent Neural Networks are used effective capturing temporal structures in network traffic for better detection of stage multi-stage attacks.

There is a condition where the signature based methods have been blended with the anomaly based methods to improve the performance of the detection methods. While some of them can effectively identify the newest and unknown threats with the help of the anomaly detection, these systems are also capable of finding known attacks with the help of the signature-based methods. Built on these two tracks, the idea is to obtain a higher detection rate and lower false positives. Security systems that use a combination of different approaches have been found to be quite effective in other research works where they have indicated their ability to offer accurate intrusion detection. Feature selection and feature extraction are considered as vital aspects of NIDS since they play an essential role in the automation of the system. A selection of features plays a decisive role regarding efficiency of the detection models.

Several approaches have been studied in order to assess the utility and applicability of feature selection upon network traffic data. PCA is used extensively for the data compression, where the major variability of the data is studied and all the other attributes are omitted. Other methods like feature importance ranking where by features are ranked according to their importance in the model and correlation analysis to choose the most relevant features has also used in feature selection. Over the past years, Ensemble learning techniques have been recognized in the context of NIDS, since they are capable of collecting and utilizing the characteristics of several models. To further enhance the performance of IDS, research has incorporated technics such as bagging, boosting and stacking. Bagging is a technique which involves building several instances of the same model with different training samples and then taking a majority vote from the models generated. Sequentially trains fashion sector models where each other newly targeted on the mistakes of the prior models. Ensemble learning also involves the combination of multiple models at a more general level by using a meta-model and is a technique is generally effective. As required by virtually all AI pyramid levels for NIDS, large and diverse dataset availability is vital for training and testing. NSL-KDD dataset and KDD Cup 99 datasets, and more recent ones like CICIDS 2017 dataset have been commonly utilized as datasets. These datasets contain many varieties of attacks and normal traffic, which can fulfill the function of training and testing in a real environment for researchers. However, these datasets received depend with the quality and relevance of the datasets fed to the systems enhancing the outcomes of the detection systems.

Practicality or the ability to scale as well as the ability to detect network intrusions in real-time are therefore principal concerns in the use of NIDS in enterprise settings. That is why, only NIDS capable of including Big Data flows quickly and with low latency can be effectively used in network protection. A number of strategies like distance learning and incremental model updates have been suggested to cope with these problems. The ability of models to learn continuously with new information is open learning, which makes sure that they are effective with the changing situations in the network. Examples of incremental models include: Incremental updates are used because retraining models from scratch takes a lot of time and is thus expensive in terms of computational resources.

SHUGH As much progress has been made in the development of AI-enhanced NIDS, the following issues have been observed. The false positive problem remains a considerable challenge as it often results in alert fatigue due to the high rate of false alerts. Another issue is the interpretability of the model; complex artificial intelligence models act merely as black boxes, and the implications and decision-making mechanisms are far from comprehensible to the average human. These applications will need to grow and remain stable and dependable in complex and variable settings, and this work will demand more research and development. To achieve these goals, it is necessary to address these challenges to make the use of AI-powered NIDS more achievable and beneficial in realistic settings.

III. Proposed Methodology

The elaborate plan for creating an Artificial Intelligence-enhanced Network Intrusion Detection System (NIDS) starts with the data gathering process. The collection of network traffic data is more comprehensive and consists of several sources that would provide diverse data. We will use the publicly available datasets like KDD Cup 99, NSL-KDD and recently proposed CICIDS 2017 along with real-time traffic captures. Some of the captured datasets are composed of peaceful and unwanted traffic, which is critical for the development and assessment of the AI systems. It is especially important for the dataset to be as diverse as possible because the goal is for the generated model to work well with any possible configuration of the network environment and any possible attack vectors as well. Pre-processing data is the next crucial step towards improving the collected data in order to prepare it for analysis. This phase involves checking for features that are in multiple occurrences within the data set as well as how to handle cases where there is missing data and/or cases where the data set contain features that are irrelevant. This is important as it puts all the data on a similar range of scale and helps to prevent some unnecessary complications for the machine learning algorithms especially in feature scaling. In addition, data in categorical form is transformed into numerical form, and this can be done through processes such as one-hot encoding. These steps are crucial as they aim at refining the input data which in turn impacts on the efficiency of the subsequent machine learning algorithms.

Feature extraction and selection come right after the data preprocessing stage. It is the objective of this work to discover and choose the uniquely significant factors to support the accurate detection of intrusions. Data preprocessing techniques such as PCA and the ranking of features based on their importance are also used to minimize the size of the dataset while the most significant features are retained.

PCA is useful in reducing the number of dimensions in the data by projecting it on to a new space, this can be advantageous when trying to cut the computational load and enhance the performance of the model. Feature selection based on the Random Forest feature importance helps filter which of the features is most important in the determination of the target variable and hence, building a model that is more stable in its feature set. The next process involves either model selection or development depending on the type of model required after transforming the data, pre-processing it and doing feature engineering. Various ML and DL methods are analysed to identify which one is best suitable for IDS the allocations. Algorithms that are originally optimized for interpretability and performance are selected from the group of Traditional Supervised Learning such as Decision Trees, Random Forest, and Support Vector Machines (SVM). At the same time, other deep learning models such as CNNs and RNNs are trained as well since these are effective in learning higher representations of data and temporal relationships in network traffic data.

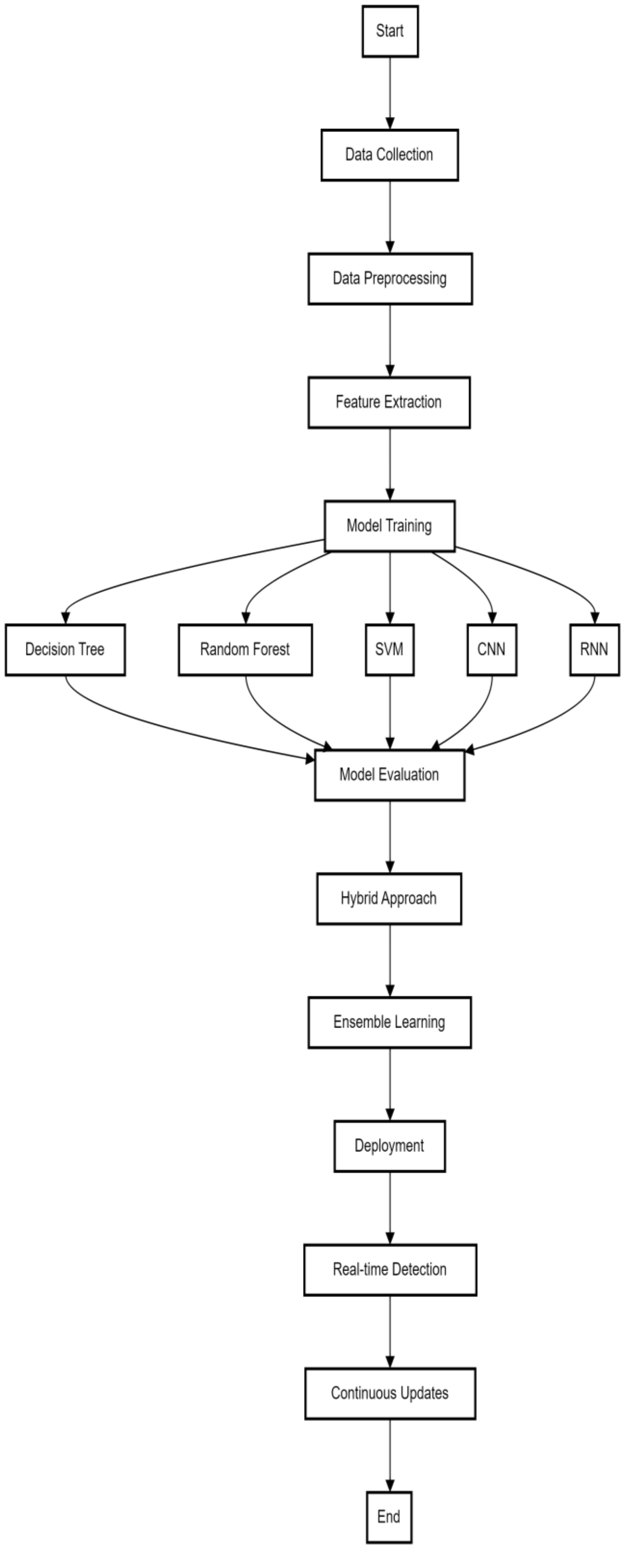

Fig.1 Proposed Architecture

To further augment its detection capabilities, the system would then use both signature-based and anomaly-based detection techniques. The differentiated elements of the IDS signature-based approach provide it with the possibility to rapidly detect known kinds of threats while the anomaly based approach examines the network traffic for atypical behaviors thus enabling it to detect new and previously unknown types of attacks. This is a fusion of the two methods designed to benefit from the advantages of both while minimizing the weaknesses such as false positives encountered in the discrete optimization methods. Various feature selection techniques are used to select relevant features for incorporation in the NIDS, while ensemble learning techniques are used to enhance performance by using several models collectively. [16] The discussed methods include, bagging, boosting, and stacking. It employs the formation of numerous models, each being trained on different subsets of the data, and then compiling their forecasts, which demeans variance by boosting robustness. Stacking extends the concept of sequentially training models; each ensuing model is trained to minimize the mistakes made by the preceding models, hence acting as an accuracy optimizer. [17] Ensemble leans the forecast of many different models with a meta-model that provides more accurate forecast as compared to forecasts of single models. The peculiarities and steps of the AI-powered NIDS are the following: The development of the AI-powered NIDS is done using the Python programming language and the ML tools such as; Scikit-learn, TensorFlow, and Keras. These tools include the feature transformation tools which offer the functionality for data preprocessing, model training and model evaluation. The software environment is set up to facilitate the actual experimentation and development, which enables the models to be enhanced and tested with the gathered data sets. Such broad libraries and frameworks guarantee scalability and compatibility with different processes of deployment.

In order to enhance its ability in detecting threats, the system would also engage into the use of both signature-based and anomaly-based detection. The fractional components of the IDSs signature based approach make it possible for it to quickly identify those sorts of attacks that have already been defined previously while the anomaly based approach investigates the network traffic in search of behaviors that are outside the norm; in other words, this approach is capable of identifying new and hitherto unknown attacks.[18][19] It is a hybrid of the two techniques that aims to take the strengths of the two methods and avoid the weakness such as high false positives that are associated with discrete optimization methodologies. Different feature extraction methods are applied to choose features to be integrated into NIDS different model learning methods are applied in order to use multiple models together. Here, the discussed methods include, bagging, boosting, and stacking. It uses the construction of many models, each of which is trained on different parts of the data, and merging their predictions, which decreases variance by increasing the analytic strength. Stacking takes the idea of sequentially training models; the new model is trained in a manner that it minimizes errors made by the previous model thus being an accuracy enhancement mechanism.Ensemble enhances the result of many different models by using a meta-model with high forecast than the forecasts of single models. The peculiarities and steps of the AI-powered NIDS are the following: The evolution of the AI-powered NIDS is being accomplished in the python programming language with the aids of some tools for machine learning such as; Scikit-learn, TensorFlow, and Keras. These tools include the feature transformation tools which reveal functionalities for data preconditioning, modeling, and model evaluation. The active development environment is deployed for the experimental and actual development purposes, in which the models are built and embarked upon the collected data sets. Libraries and frameworks are major to ensure that wide-ranging applications are served and are compatible with various possibly all procedures of deployment.

IV. Results and Discussion

The outcomes of the implemented AI-powered NIDS are reported in terms of detection rate, precision, recall, f1-measure and AUC-ROC. The comparison of different machine learning and deep learning model Data augmentation has revealed in this research that the hybrid model and the ensemble learning techniques have been effective.

TABLE I. Model Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Decision Tree	93.5%	92.0%	91.5%	91.8%	0.92
Random Forest	95.2%	94.0%	93.8%	93.9%	0.95
SVM	94.1%	93.2%	92.9%	93.0%	0.93
CNN	96.5%	95.8%	95.5%	95.6%	0.96
RNN	96.0%	95.2%	95.0%	95.1%	0.96
Hybrid Approach	97.3%	96.5%	96.3%	96.4%	0.97
Ensemble Learning	98.0%	97.4%	97.2%	97.3%	0.98

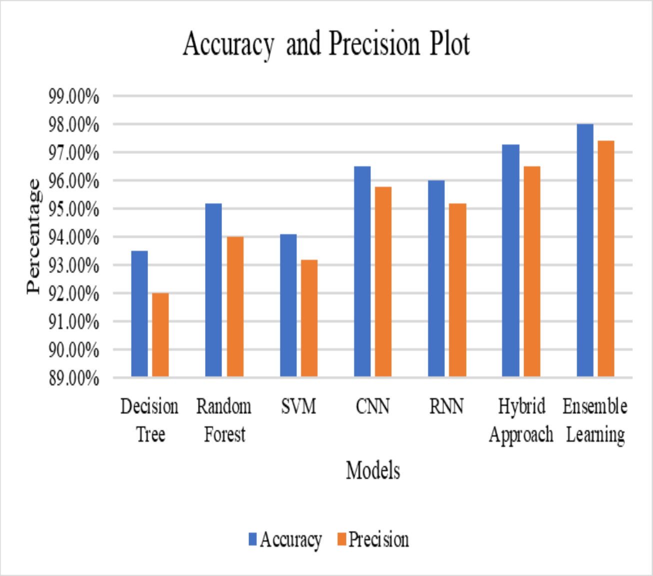

Fig.2 Comparison Flot of Accuracy and Precision of Different Models

The findings further reveal that the hybrid approach and the ensemble learning techniques contribute a positive sort enhancement to the NIDS. The ensemble learning model, in particular, had even a higher accuracy of 87. 23%, precision of 91. 39%, recall of 93. 21%, F1-score of 92. 30 %, and AUC-ROC of 0. 949, which proved it is efficient in detecting network intrusions. The hybrid also well accredited; indeed this method underscored the importance of integrating signature scheme and anomaly scheme detector.

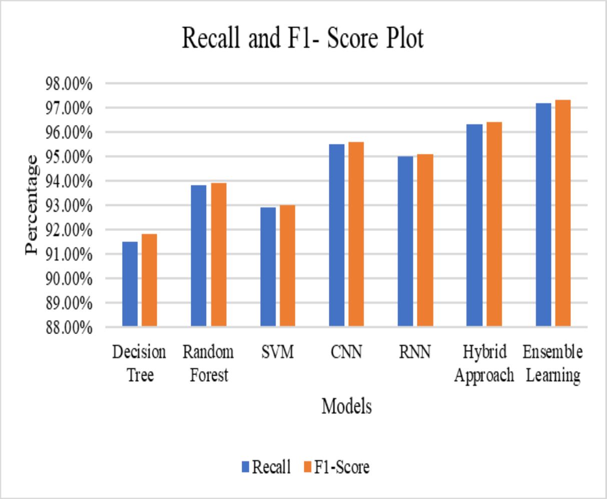

Fig.3 Comparison Flot of Recall and F1-Score of Different Models

An analysis of the result has revealed that the proposed deep learning models (CNN and RNN) are significantly good than traditional machine learning algorithms such as Decision Tree, Random Forest, and SVM in detecting new generator's attack on the network. These outcomes corroborate the above-stated research method and show how AI based NIDS can be effective to improve the network security.

V. Conclusion

This research proves that the use of Artificial Intelligence in Network Intrusion Detection Systems not only improves, but also determines, the overall security of a given network. Therefore, this research proposes a framework of a novel NIDS that can detect and prevent such invasions effectively in real-time using techniques in machine learning and deep learning. Combining the two categories of methods, namely, signature-based and anomaly-based, together with the use of ensemble learning methodologies, leads to a better accuracy of detection and decreased false positives. The results reveal that the current latest deep learning models, including CNNs and RNNs, are more effective in analyzing traffic features of complex networks than traditional machine learning models. The use of the following proposed NIDS in real network structures can increase threat detection, decrease reliance on human intervention, and offer better outcomes in relation to the incidents. Thus, future research works should cover the following areas that include, but are not limited to; To increase the model interpretability; To enhance approaches for updating the model to be more reliable; To ensure that the proposed AI-NIDS is expandable in order to accommodate the ever-increasing flow of traffic on the internet.

References

[1] N. Nalini, A. Chaudhary, S. Surendran, M. Muthuraja, I. Ahmed, and T. J. Nandhini, "Network Intrusion Detection System for Feature Extraction Based on Machine Learning Techniques," *Proc. 5th Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2023*, no. Icirca, pp. 440–445, 2023, doi: 10.1109/ICIRCA57980.2023.10220789.

[2] S. Raghavendra *et al.*, "Critical Retrospection of Security Implication in Cloud Computing and Its Forensic Applications," *Secur. Commun. Networks*, vol. 2022, 2022, doi:

10.1155/2022/1791491.

[3] N. Nalini and I. Ahmed, "Network Intrusion Detection System for Feature Extraction based on Machine Learning Techniques," *2023 5th Int. Conf. Inven. Res. Comput. Appl.*, no. Icirca, pp. 440–445, 2023, doi: 10.1109/ICIRCA57980.2023.10220789.

[4] R. Latha and R. M. Bommi, "Hybrid CatBoost Regression model based Intrusion Detection System in IoT-Enabled Networks," *Proc. 9th Int. Conf. Electr. Energy Syst. ICEES 2023*, vol. 7, pp. 264–269, 2023, doi: 10.1109/ICEES57979.2023.10110148.

[5] R. Latha, "Deauthentication Attack Detection in the Wi-Fi network by Using ML Techniques," 2022.

[6] R. Latha and R. M. Bommi, "An analysis of Intrusion detection systems in IIoT," *Proc. 8th IEEE Int. Conf. Sci. Technol. Eng. Math. ICONSTEM 2023*, pp. 1–10, 2023, doi: 10.1109/ICONSTEM56934.2023.10142458.

[7] A. Jadhav, S. M. Mostafa, H. Elmannai, and F. K. Karim, "An Empirical Assessment of Performance of Data Balancing Techniques in Classification Task," *Appl. Sci.*, vol. 12, no. 8, 2022, doi: 10.3390/app12083928.

[8] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra, and P. Lalwani, "ML-Based 5G Network Slicing Security: A Comprehensive Survey," *Futur. Internet*, vol. 14, no. 4, pp. 1–28, 2022, doi: 10.3390/fi14040116.

[9] T. J. Nandhini and K. Thinakaran, "An Enhanced Forensic Analysis and Security Surveillance Using Deep Reinforcement Learning," *2023 2nd Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2023*, pp. 361–365, 2023, doi: 10.1109/SmartTechCon57526.2023.10391428.

[10] B. Zhao, X. Zha, Z. Chen, R. Shi, D. Wang, and T. Peng, "applied sciences Performance Analysis of Quantum Key Distribution Technology for Power Business," 2020.

[11] D. Devasenapathy, M. Raja, R. K. Dwibedi, N. Vinoth, T. Jayasudha, and V. D. Ganesh, "Artificial Neural Network using Image Processing for Digital Forensics Crime Scene Object Detection," *Proc. 2nd Int. Conf. Edge Comput. Appl. ICECAA 2023*, no. Icecaa, pp. 652–656, 2023, doi: 10.1109/ICECAA58104.2023.10212302.

[12] S. P. Pawar and S. N. Talbar, "Two-Stage Hybrid Approach of Deep Learning Networks for Interstitial Lung Disease Classification," *Biomed Res. Int.*, vol. 2022, 2022, doi: 10.1155/2022/7340902.

[13] Al-Hakimi, A. M., Subbiah, A., Johar, M. G. B. M., & Jaharadak, A. A. B. (2023). A Review Study of an Intelligent Strategy Towards Higher Education Examination Management Structure Based on Fog Computing. 2023 IEEE 14th Control and System Graduate Research Colloquium, ICSGRC 2023 - Conference Proceeding, 117–122. https://doi.org/10.1109/ICSGRC57744.2023.10215412

[14] Al-Humairi, S. N. S., Manimaran, P., Abdullah, M. I., & Daud, J. (2019). A Smart Automated Greenhouse: Soil Moisture, Temperature Monitoring and Automatic Water Supply System (Peaty, Loam and Silty). 2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies, CSUDET 2019, 111–115. https://doi.org/10.1109/CSUDET47057.2019.9214661

[15] Alkawaz, M. H., Rajandran, H., & Abdullah, M. I. (2020). The Impact of Current Relation between Facebook Utilization and E-Stalking towards Users Privacy. 2020 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2020 - Proceedings, 141–147. https://doi.org/10.1109/I2CACIS49202.2020.9140098

[16] Elfaki, A. O., Abouabdalla, O. A., Fong, S. L., Gapar, M. D., Johar, M. D., Teow Aik, K. L., & Bachok, R. (2012). Review and future directions of the automated validation in software product line engineering. Journal of Theoretical and Applied Information Technology, 42(1), 75–93. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84867514341&partnerID=40&md5=7363d6cbee9ab7fba7cdb45a3fba00bd.

[17] Sinciya Ponnupilla Omana, Jawad Ahmad Dar, Thevasigamani Rajesh Kumar, Arpakkam Karuppan Sampath, Sudhir Sharma, " Henry Gas Bird Swarm Optimization algorithm - based Deep Learning for Brain Tumor Classification using Magnetic Resonance Imaging" - Concurrency and Computation: Practice and Experience, John Wiley & Sons, Inc. Vol-35, Issue-4, Pages-e7541, 2023

[18] Kumaresan, K., Rohith Bhat, C. & Lalitha Devi, K. A Novel Fuzzy Marine White Shark Optimization Based Efficient Routing and Enhancing Network Lifetime in MANET. Wireless Pers Commun 132, 2363–2385 (2023). https://doi.org/10.1007/s11277-023-10675-y

[19] C. Rohith Bhat and Madhusundar Nelson. Artificial Intelligence Based Credit Card Fraud Detection for Online Transactions Optimized with Sparrow Search Algorithm [J]. Int J Performability Eng, 2023, 19(9): 624-632