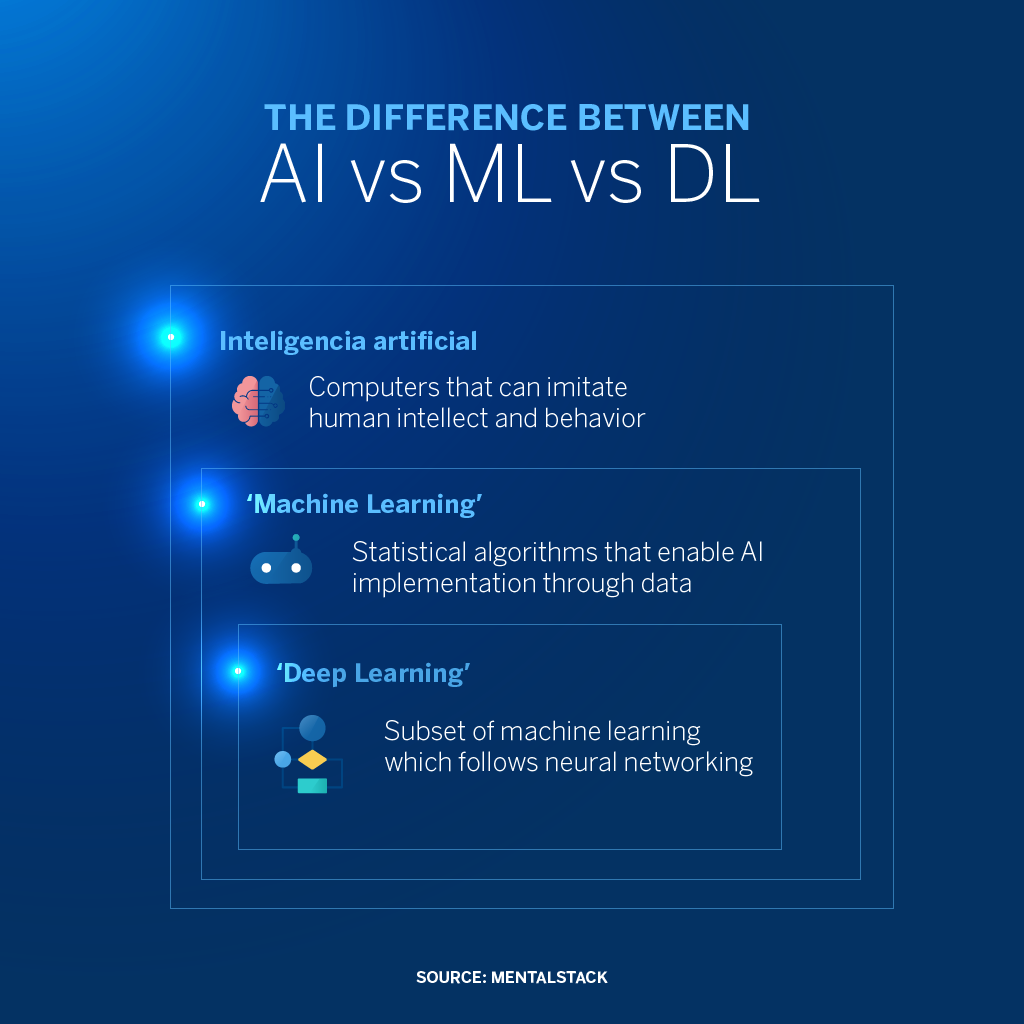
# A STUDY ON ANN MODEL Introduction:

Artificial intelligence (AI) was first introduced by John McCarthy in 1956 at the Dartmouth College Conference, which is considered the founding event of the field (Nedadur et al., 2021). The study of intelligent machine behaviour and its application to complex computation and analysis is known as artificial intelligence (AI). It has influenced both popular portrayals of current developments in the field and predictions about what may come next. Robots, computers that can communicate with us in our mother tongues, and astute computer "experts" are all part of the future that the media portrays for us. Divergent views exist, nevertheless, on whether these developments will turn our adversaries into dangerous and wicked forces or make them useful allies (Finlay et al.,). Artificial intelligence applications typically demand knowledge-based systems since knowledge is the essential source of intelligence. This chapter provides examples of several knowledge representation architectures and shows how they can be compared and hybridised. Beyond information representation and acquisition, a traditional knowledge-based system requires a great deal additional component (sajja et al.,).



**Figure 1:** Artificial Intelligence (Banafa, 2022)

# Machine Learning and Deep Learning:

Artificial Intelligence (AI) has become a transformative force across various fields, with machine learning and deep learning playing pivotal roles in this evolution. Machine learning encompasses a range of techniques that have significantly advanced AI capabilities (Udousoro etal., 2020). Recent developments in AI, particularly in radiology, have introduced non-deterministic deep learning algorithms that revolutionize traditional approaches by eliminating the need for explicit feature definitions (Hosny et al., 2018). This shift represents a fundamental change in machine learning paradigms.

Deep learning, a subset of machine learning, has gained prominence in various AI applications, including robotics and multimodal data fusion (Mouha, 2021; Gao et al., 2020). The importance of deep architectures in tackling complex tasks in vision, language processing, and other AI domains has been emphasized (Bengio, 2009). The introduction of AI in these areas has led to the exploration of new possibilities and challenges in utilizing advanced technologies effectively.

# Overview:

The main element of the plan to strengthen the cybersecurity systems is the ability of the datasets to be robust for training and testing the AI models. Another table that plays a very important role is the KDDCUP99 table. It consists of a comprehensive set of data which is specifically designed to resemble the intrusions seen in the real military networks environment and employs full scenarios. As the dataset consists of a real and comprehensive collection of all network traffic events the KDDCUP99 data set functions as a basic tool for the AI-driven creation of intrusion detection systems (Ngueajio et al., 2022).

While one sees a significant progress with the AI technology and an abundance of data to work with creating a competitive network intrusion detection system remains hard. The objective is to develop an AI-based system that will familiarize with good network behaviour and distinguish the harmful intrusions among noticeable number of network traffic. While achieving this requires the development and implementation of intelligent algorithms capable of automatically detecting and highlighting such suspicious anomalies that may compromise an organization's cybersecurity, constant evolution of cyber threats should necessitate periodic upgrading of such algorithms (Patil et al., 2022).

The goal of the latter is to demonstrate a complete scheme for the creation and check of an AI-built network intrusion detection system. This report intends to provide cybersecurity experts with an insight into AI tactics, framework design, performance analytics, proactive mitigation techniques, and other supporting mechanisms that can be used to ward off unauthorized access and probable breaches.

# Briefing about Artificial Neural Networks (ANN) used in Intrusion Detection:

Artificial Neural Networks (ANNs) as a method of intrusion detection have become a prominent technique in this domain of cyber security due to their ability to learn complex patterns in network traffic data and detection of anomalies. ANNs are an artificial neural network type that was created inspired by the biological networks of the brain of the human being (Sağlam and Çetin, 2022). These models are composed of connected nodes in multiple layers, and each node is one unit neuron that processes and then transmits information.

Artificial Neural Networks (ANNs) constitute the antithesis of intrusion detection by virtue of the fact that one are flexible and pattern recognition is their specialty. ANNs, imitating our brain cells which are connected in an organic system, are capable of sifting through large volumes of network data to spot anomalous traffic categories. Their universality allows to use both supervised learning and unsupervised learning methods, which helps in detection of known type of threats and also unknown attack patterns. However, ANNs’ results depend on how good the input features are and on the complexity of the network configuration. Notwithstanding plights, ANNs stand at the limelight in intrusion detection development, that stimulates cybersecurity resiliency (Malgwi et al., 2022).

## Employed Techniques of Related Studies:

Several methods of ANN utilization regarding intrusion detection have been used. One of the most common methods is the learning supervised, where the ANN is trained on datasets that contain both the normal and malicious network traffic samples. Through the process of learning, the ANN detects computer network connections by either recognizing one as legitimate or malicious based on the information extracted from the data. Unsupervised learning is one of the other methods puts forward where the ANN itself seeks the patterns and anomalies in the unlabelled data that is unassigned to any predefined categories (Otchere et al. 2021).

The approaches using ANNs (Artificial Neural Networks) for intrusion detection include supervised learning and unsupervised learning, which are more popular. ANNs are trained in supervised learning by giving one data with labels distinguishing between good and bad internet traffic. Self-supervised learning, on the contrary, ensures the network can autonomously detect the abnormalities without the labelled data. Some of the key issues in data collection are the acquisition of large labelled datasets and distinctive features extraction for useful model training. Additionally, model accuracy and strength of model is highly depend on the chosen features (Maseer *et al.* 2021). As ongoing efforts refine feature selection methodologies and hybrid approach integration, ANNs gain adaptability and better accuracy in intrusion detection.

## Critical Analysis of Existing Approaches:

Among the prior academic work utilizing ANNs for intrusion detection there are positive outcomes with some weaknesses. For example, it is of considerable importance that a sufficient number of labelled datasets have been created for the training of supervised ANNs. Obtaining and tagging such datasets can be labour and wallet intensive and might not be necessarily representative of the full range of the real-world cyber risks. Moreover, the ANNs may fall short when it comes to detecting new or hitherto unknown attacks unless one is represented in the training data (Khraisat et al., 2019).

The capabilities of ANNs in the identification of intrusions is very sensitive to the extracted feature quality and feature selection. Finding the right features from the raw network traffic data is a tough task, and the choice of features can be one of the main reasons for the accuracy or robustness of the ML model. Furthermore, ANNs are inclined to act with little transparency, thus, making it hard to underline the reasons for their classifications thus reducing the trust and increase the rate of adoption of these systems in practice (Ağbulut *et al.* 2021).

In addition to the mentioned issues, ANN has some advantages in intrusion detection, including its capability to adapt to the ever-changing threats and in terms of itself having the potential for parallel processing, thus real-time analysis of large volumes of network data is possible. The guiding principle in the ongoing research is the search for the solutions to the problems of feature engineering, model interpretability, and hybrid modelling involving the combination of various machine learning methods (Albahar et al., 2020).

Briefly speaking, the ANNs possess the ability to increase the effectiveness of IDS but the challenges of data accessibility, feature extraction, and reduction of bias and interpretation still have to be faced in order to fully realize the ANN potential to strengthen the cyber security defences.

# AI-Based Model Design:

In the introduction, AMB transits into a discussion on AI-based Model Design for network intrusion detection (Ambarwari *et al.* 2020). This section traces the importance of using ANNs, for establishing security measures against dynamic threats. It underlines the fact that new generation of AI-driven systems is required which can distinguish common network activities from disruptive intrusions (Ahmad *et al.* 2021). The introduction reveals the architectural, learning, and output details of this AI model which are preludes to better understanding of how AI is significantly transforming intrusion detection methods.

# 

# Discussion of the AI-Driven Model to Effectively Predict Network Intrusions:

The proposed AI model in intrusion detection which is AI driven will warrant the ability to distinguish benign network activities from outright intrusions. It utilizes the power of Artificial Neural Networks (ANNs), particularly a deep learning architecture, which are used to analyse the network traffic data and highlight the anomalies that strongly suggest to a security breach. The approach will facilitate the enhancement of the security posture in organizations with real-time detection of the malicious activities.

## Network Architecture:

Network architecture can be said to be made up of multiple layers of interconnected neurons that are arranged in a deep learning structure. The input layer receives unprocessed network data, which is then analysed by the hidden layers, each having a large number of neurons. The neurons are the ones carrying out function-processing and outputs the computed information through the network. Lastly, the output layer forecasts such kind of network connections either safe or hostile (Román-Portabales *et al.* 2021).

Nodes are connected with weighted edges, which represent the strength of the interaction between the neurons. During the course of the training, these weights are continually tuned in order to maximize the model's capability of identifying normal as opposed to malicious network activities. Furthermore, convolutional layers allow model to learn features from rudimentary data which helps in proper detection of anomalies (Wang et al., 2024).

## Depict the Learning and Validation Procedures:

The learning process includes training of the AI-driven model using labelled dataset comprising both regular and malicious network traffic. On the training time, the model iteratively fine-tunes its internal parameters that are made up of weights and biases to minimizes the differences between predicted and actual responses. This process of optimization is usually attained using the gradient descent algorithms, like backpropagation, which take the gradients of the loss function with respect to the model weights.

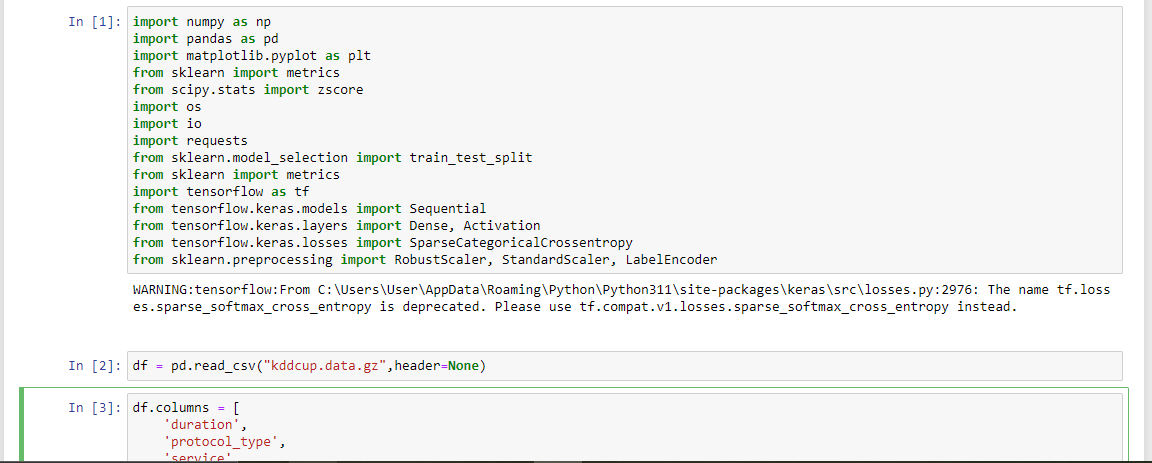
Model performance validation refers to the guarantee of the tool applicability in real life contexts. By this I mean measuring model’s accuracy, precision, recall, and among other performance metrics on validation datasets that are separate from the training dataset. The use of cross-validation techniques may as well be adopted to offset the risk of overfitting and guarantee the generalization of the model across heterogeneous datasets.

## Discussion of Planned versus Actual Yields of the Model:

The end results of the AI-based model are the precise classification of the network connections as either safe or malicious. Desirably, the model should attain high precision and recall values, leading to a decrease in both false positives and false negatives. It's important to note that the real outputs of the model may be affected by many different factors, such as data quality, the complexity of the network environment, and the level of sophistication of the adversary tools used by attackers. Hence, regular tracking the development and refinement of the model is crucial to be able to answer to changing cyber threats and to keep the model useful in protecting organizational assets.

# Performance Evaluation

The opening of the performance evaluation section lays the foundation for assessing the ability of AI- based intrusion detection systems to detect cyber-attacks. This vital phase is concerned with comparing different performance metrics that are used for evaluating accuracy, reliability, and robustness of the models (Song *et al.* 2022). This section uses metrics including the area under the receiver operating characteristic curve (AUC), recall, F1 score, accuracy, and precision to provide a thorough examination of the systems' ability to discriminate between allowed and unauthorised network activity.



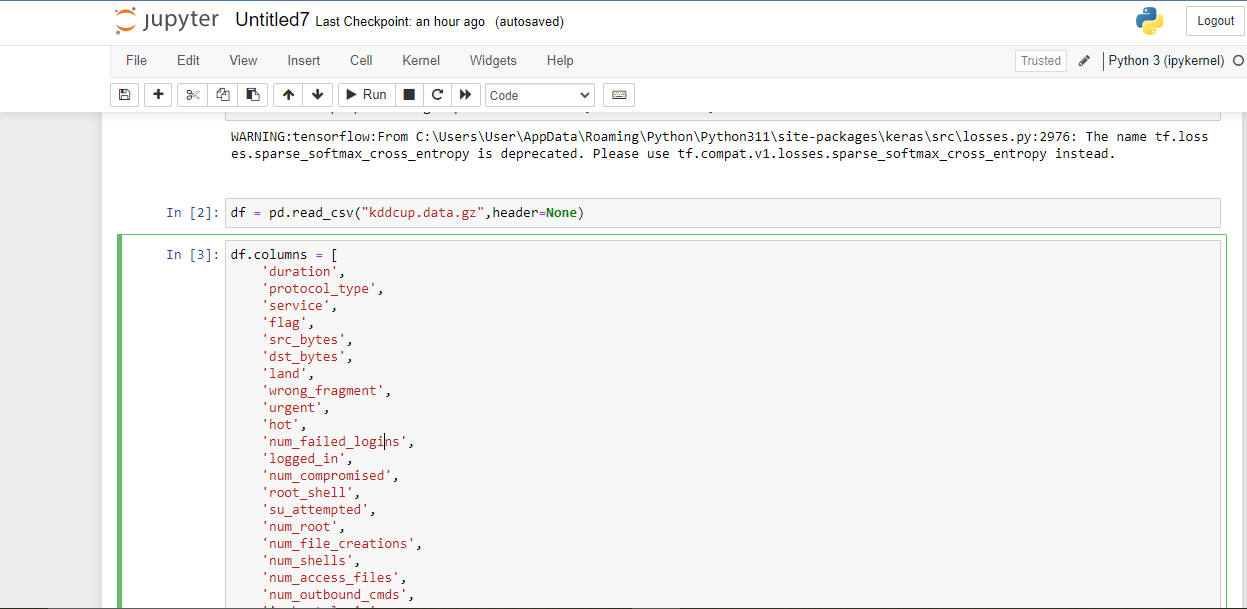
**Figure 2:** Library import

(**Source:** Extracted from Jupyter Notebook)

Furthermore, to deepen the relevance and offer another lens through which the intrusion detection methodologies can be explored. By means of a table presented in comparative table the section is aimed to identify advantages and disadvantages of the AI-based intrusion detection systems for cybersecurity sector, by guiding future research and real implementations.

## Comparative Assessment of Performance Metrics:

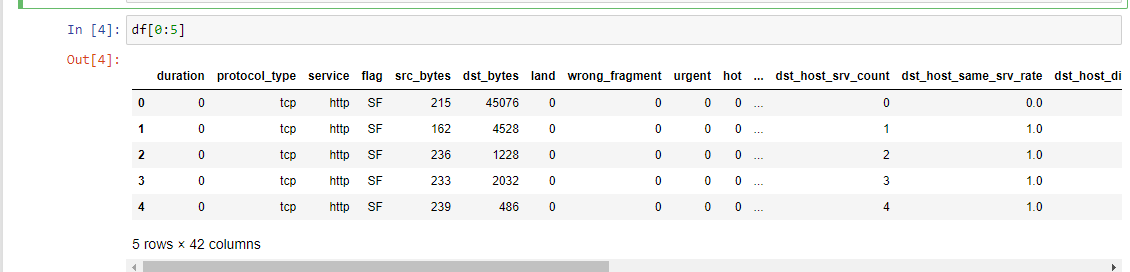
Emulation of AI-powered intrusion detection systems performance is based on the set of metrics analysis to examine the ability of systems to distinguish benign from harmful network activities. The primary evaluation criteria are the F1 score, accuracy, precision, recall, confusion matrix, and AUC (area under the receiver operating characteristic curve). By maximising recall rates and precision, the F1 score offers a solitary standard by which to evaluate the efficacy of the model.



**Figure 3:** Column names

(**Source:** Extracted from Jupyter Notebook)

On the other hand, recall refers to the percentage of true positives that the model identifies. The percentage of correct predictions among all positive ones is measured by the precision rate (Ghazal et al., 2022). The model's predictions are separated into true positives, true negatives, false positives, and false negatives using a Confusion Matrix hard examination. Accuracy stands for the overall correctness of the prediction model while the AUC curve shows the visual representation of the balance between the true positive rate and the false positive rate at different decision thresholds.



**Figure 4:** Dataset Showing

(**Source:** Extracted from Jupyter Notebook)

The comparative study includes the objective to indicate the impact of different evaluation indicators on the efficiency of AI-based intrusion detection systems as well as the effectiveness of these AI systems. Through the assessment of the model parameters, such as the F1 score, precision, recall, confusion matrix, accuracy, and AUC graph, the analysts can obtain the knowledge of the models' ability to correctly identify and classify network activities. These metrics offer a set of different perspectives be one precision-vs-recall balancing or a trade-off between true positive vs false positive imaging (Anaraki *et al.* 2021). This total evaluation process ends up with a holistic assessment of the models’ strengths and weaknesses, and the decision making is guided by the process which is meant to optimize intrusion detection strategies and enlightens the cybersecurity defence.

# Employment of Insights:

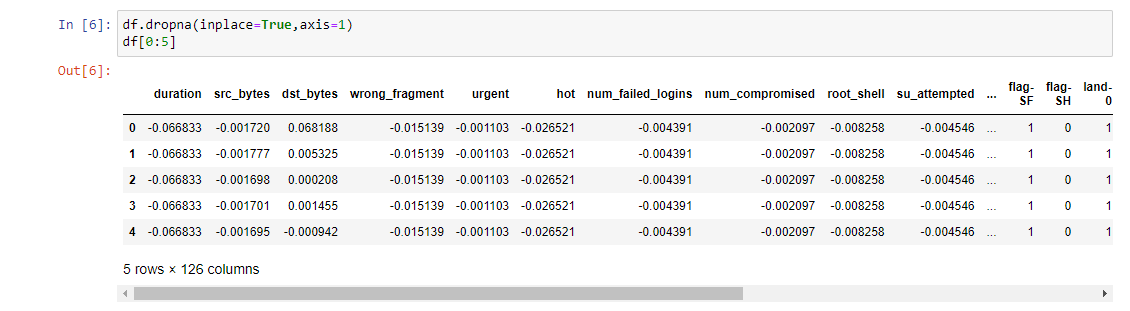
To make the analysis deeper, relevant sources are incorporated with different viewpoints focusing on AI security systems. Such works discuss different model designs, feature engineering, and modelling performance, thus, casting light on the potential as well as the drawbacks of any given technique (Hong *et al.* 2020). The analysis takes more depth and breadth through the integration of the research findings from various studies because it allows an analysis of the whole state-of-the-art of intrusion detection research. In these works, the experts provide guidelines on the choice of performance indices, model architectures, and assessment methods, which create a basis for better intrusion detecting systems design.



**Figure 5:** Encoding

(**Source:** Extracted from Jupyter Notebook)

The in-depth incorporation of the comprehension of pertinent reports reinforces the performance evaluation by providing a complex understanding to AI-driven intrusion detection approaches. This provides many viewpoints regarding model design, feature engineering, and evaluation methods, which are all coming from the results of evidence-based studies and trials. The synthesis of findings from several studies provides the analysis with an apostrophic depth and width, thus, the researchers are able to get a holistic view of the intrusion detection methods literature.



**Figure 6:** Data Preprocessing

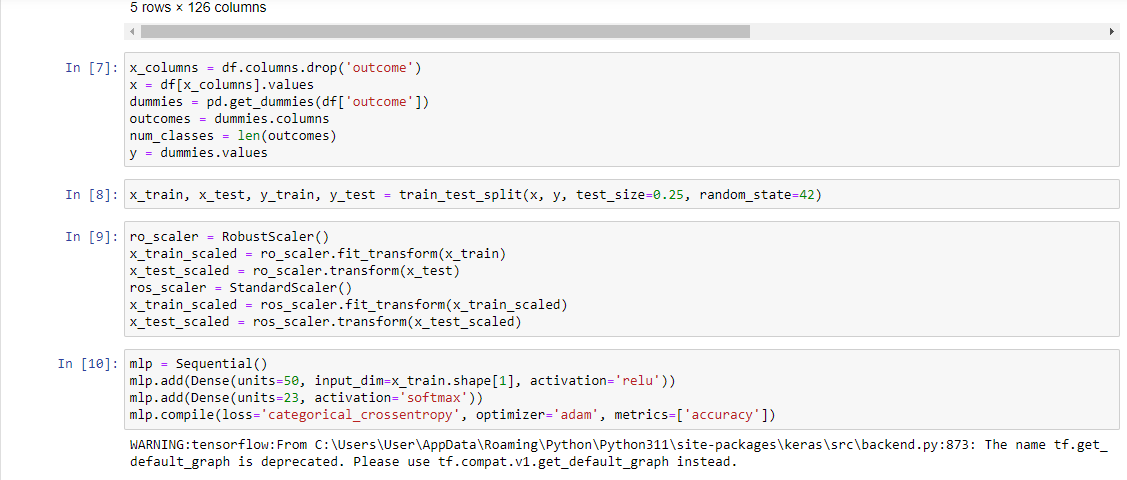
(**Source:** Extracted from Jupyter Notebook)

Besides, research suggest techniques of metrics selection, model architectures, and system evaluations, which boosts the building of successful intrusion detection systems. Such a comprehensive technique helps create a better understanding of cybersecurity practice complexities and the problems associated with them, encouraging continuing development and innovation of cybersecurity techniques.

# Comparative Table Analysis:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Author** | **Paper Title** | **F1 score** | **Precision** | **Recall** | **Accuracy** |
| 1 | Sambandam et al., 2023 | Comparison of Machine Learning-Based Intrusion Detection Systems Using UNSW-NB15 Dataset |  |  |  |  |
| 2 | Vakili et al., 2020 | Performance Analysis and Comparison of Machine and Deep Learning Algorithms for Classification Task Using IoT-Related Datasets |  |  |  |  |
| 3 | Yacouby et al., 2020 | Probabilistic Extension of Precision, Recall, and F1 Score for More Thorough Evaluation of Classification Models |  |  |  |  |
| 4 | Li et al., 2024 | Optimizing IoT Intrusion Detection System: Feature Selection Versus Extraction |  |  |  |  |
| 5 | Natarajan et al., 2023 | A New High-Performance Feature Selection Method for Machine Learning-Based IOT Intrusion Detection |  |  |  |  |
| 6 | Vigoya et al., 2021 | IoT Dataset Validation Using Machine Learning Techniques for Traffic Anomaly Detection |  |  |  |  |
| 7 | Seong et al., 2021 | A comparative analysis on traditional wired datasets and the need for wireless datasets for IoT wireless intrusion detection |  |  |  |  |
| 8 | Alex et al., 2023 | A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms |  |  |  |  |
| 9 | Pacheco et al., 2021 | Adversarial Machine Learning: A Comparative Study on Contemporary Intrusion Detection Datasets |  |  |  |  |
| 10 | Abbasi et al., 2021 | Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BaIoT dataset |  |  |  |  |

In the table, the overview of performance metrics reported by the various approaches is given for the convenience of a comprehensive evaluation. The table classifies detection intrusion models according to their architectures, learning algorithms, and performance criteria. For every method, F1 score, accuracy, recall, and precision are reported among other aspects of the literature review which were crucial in our final decision. The table gives a platform to directly compare the strengths and weaknesses of the different models by viewing one together (Nguyen et al., 2021). Comparative analysis creates a realization of trends, tendencies, and alleviation areas in AI-driven intrusion identification research studies that guide future research fields and practical implementations.



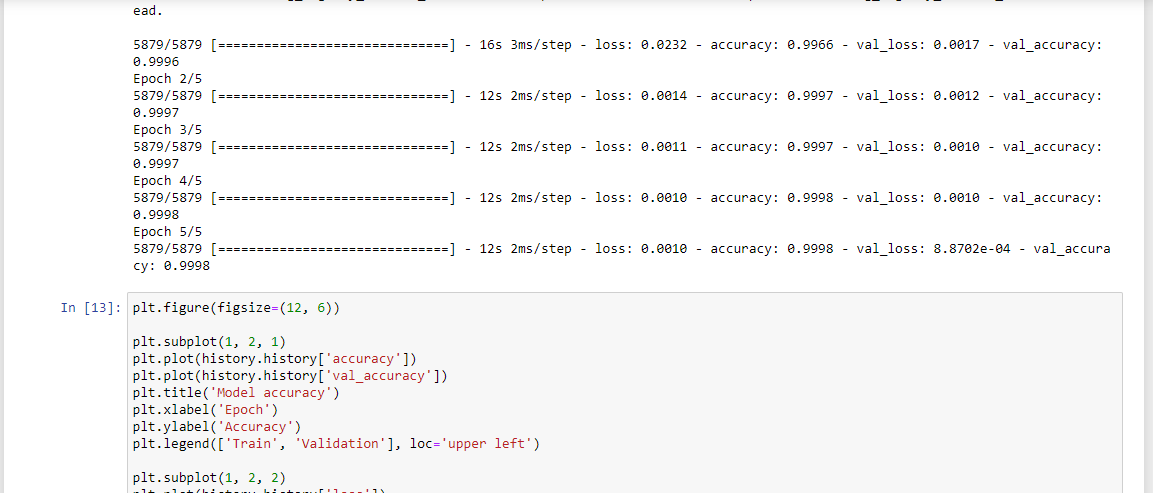
**Figure 7:** Train test Splitting

(**Source:** Extracted from Jupyter Notebook)

The comparison table plays a critical role in not just bringing together but also effectively displaying the performance indices of several AI-driven network protection techniques. This table is subdivided into groups, each based on their architecture, learning technique, and key performance indicators. It gives a quick summary of their effectiveness in real environments. Through contrasting the performances of various models in a table side by side, the table will give a clear difference between their strengths and the weaknesses for the purpose of locating trends and patterns of models over time. Besides, comparative table may be seen as a valuable reference not only for cybersecurity experts, researchers, and policy makers but also for professionals engaged in decision making concerning intrusion detection solutions as a tool to be selected for particular organizational needs and security landscapes.

# Automated Control and Mitigation System.

Against the cyber threat world that is constantly changing, the introduction of a self-governing mitigation and control system will be a preventive action for organizations to stand up to security breaches. This system works in the same direction with an AI-driven intrusion detection model by applying appropriate responses in a timely manner to the detected hazards, so these incidents will cause less damage and make the organization cyber resilient (Pokhrel *et al.,* 2021).

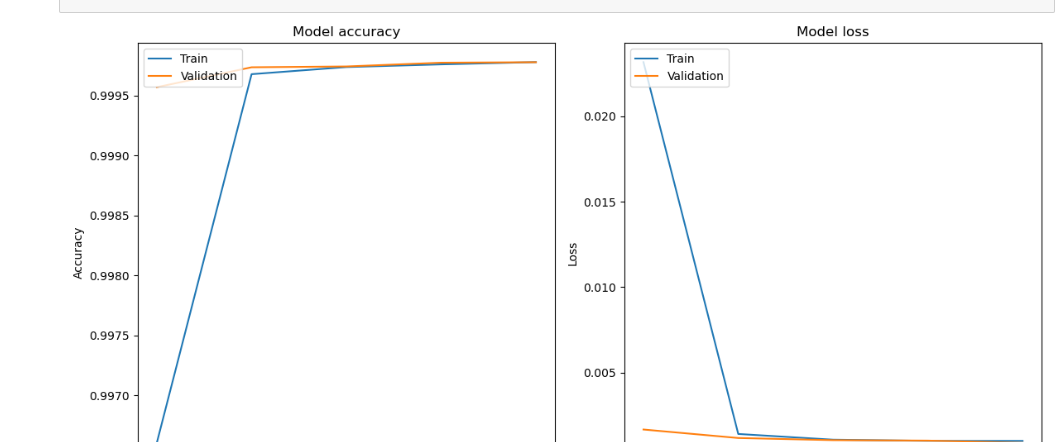


**Figure 8:** Accuracy using Epoch

(**Source:** Extracted from Jupyter Notebook)

Automatic response and control system functioning by the principle of fast response to threats with the method of the real-time data use from intrusion detection model to recognize and prioritize the security incidents. As soon as a potential risk is being identified, the system will enact predefined response procedures archived based on the nature and severity of evident intrusion. These are among the actions that may be performed such as blocking of suspicious network traffic, isolating affected systems, or auto alerts for further investigation by security personnel as per the research by Olu-Ajayi et al, (2022).

Such a system as the automated mitigation and control has a key element - the ability to adapt and self-change in accordance with the threats that are emerging. It is important to keep checking network activities frequently and by analysing threat intelligence data, system can change its response strategies in a dynamically manner to stop evolving attack vectors. This feature of being adaptive is of prime importance in keeping ahead of opponents and in managing the security high risk of hacker-based threats.



**Figure 9:** Accuracy and Loss Model

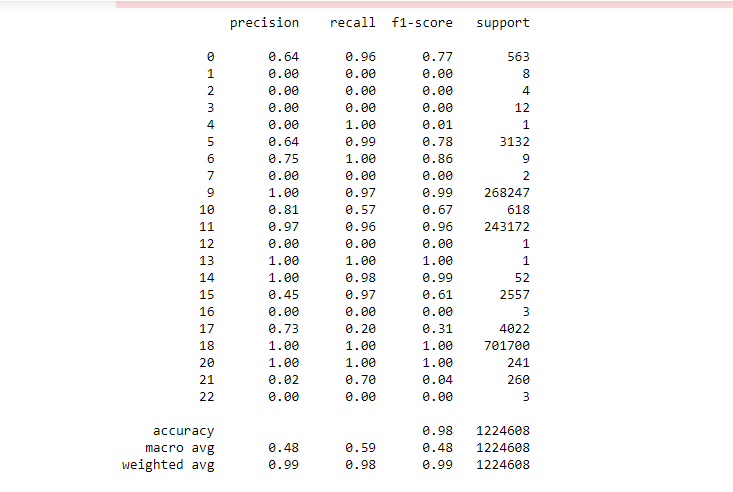
(**Source:** Extracted from Jupyter Notebook)

Furthermore, the auto mitigation and control system employs machine learning techniques to improve its effectiveness continuously. Through studying the data on the historical security incidents and their response outcomes, the system can feed on the lessons from the past and upgrade its own decision-making procedure. This repeated apprentice technique enables the system to become more proactive and expeditious in identifying and reducing security threats at the moment (Ciaburro et al., 2022).

An internal mechanism of an automated mitigation and control system is integration of it with incident management and reporting modules. The system automatically creates incident reports on security breaches, with the necessary information such as the nature of the threat, the actions taken to respond to it, and any remediation efforts that were carried out. This nature of the reports gives the post-incident analysis and helps the organizations to improve their security by refining the strategies and policies (Ang et al., 2022).

On top of this, the automation contains a self-correction mechanism which enables efficient improvement. It becomes possible to attain this goal by obtaining feedback from security analysts and stakeholders which will, in turn, expose areas of improvement and lead to adjustment of strategies. The iterative process guarantees that the system is maintained as effective and flexible as the cyber threats are persistent and evolving (Pan et al., 2023).

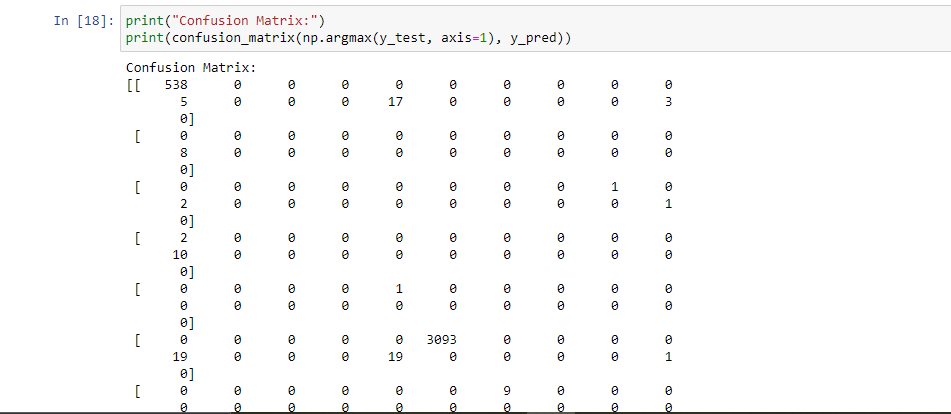
Summarily, the automatic mitigation and control system adoption can be viewed as a preventative mechanism of cybersecurity whereby organizations can avoid the risk of security breaches and strengthen their situational awareness in the cyberspace.



**Figure 10:** Precision, Recall, Accuracy

(**Source:** Extracted from Jupyter Notebook)

A feedback loop is employed by the automated mechanism of the mitigation and control system to enable continuous enhancement. The system will solicit feedback from interested parties and security analysts in order to do this. The system will adjust its response strategies as it gets more sophisticated. This dynamic approach allows the system to remain effective and still be able to adapt in the light of increasingly sophisticated cyberattacks. Overall, a pre-emptive approach, by applying an automated mitigation and control system to security issues, the organizations may prevent security breaches and strengthen security resilience.



**Figure 11:** Confusion Matrix

(**Source:** Extracted from Jupyter Notebook)

Through the combination of real-time threat detection capabilities with responsive mechanism of adaptation, this system provides the organizations with proper means of an effective guarding of their online assets as well as maintain the business continuity in the presence of cyber threats.

# Conclusion:

The report aims to clarify, therefore, the role of Artificial Intelligence (AI) in the protection of cyber resources by creating AI systems. This systematic literature review discussed many machine learning as well as deep learning approaches employed in intrusion detection, indicating not only their strengths but also their drawbacks. The AI-based model design was explored comprehensively in the discussion, providing a detailed insight into network architecture, learning processes and the types of outputs expected, which highlight the need for adaptive and robust systems in tackling evolving cyber threats.

To summarize, the integration of AI-based model into the cybersecurity practices is a game changer; it makes one more proactive in identifying and resolving security risks. To advance the research field of AI-based intrusion detection networks, future studies should focus on challenging problems like data scarcity, model interpretability, and adversarial robustness, that could make the intrusion detection systems more effective and reliable in preventing cyberattacks (Malatji et al., 2024). The field of cybersecurity will be dynamic thanks to AI's emergence of new technologies and approaches. Cybersecurity professionals will be able to stay ahead of new threats by continuously advancing AI technologies and methodologies and safeguard digital infrastructures with more confidence and effectiveness.

# References:

1. Finlay, J., 2020. An introduction to artificial intelligence. Crc Press.
2. Figure 1 - Banafa, A. (2022). Intellectual Abilities of Artificial Intelligence. [online] OpenMind. Available at: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/intellectual-abilities-of-artificial-intelligence/.
3. Nedadur, R., Wang, B. and Yanagawa, B., 2021. The cardiac surgeon's guide to artificial intelligence. Current Opinion in Cardiology, 36(5), pp.637-643.
4. Sajja, P.S. and Sajja, P.S., 2021. Introduction to artificial intelligence. Illustrated Computational Intelligence: Examples and Applications, pp.1-25.
5. Udousoro, I.C., 2020. Machine learning: a review. Semiconductor Science and Information Devices, 2(2), pp.5-14.
6. Hosny, A., Parmar, C., Quackenbush, J., Schwartz, L.H. and Aerts, H.J., 2018. Artificial intelligence in radiology. Nature Reviews Cancer, 18(8), pp.500-510.
7. Mouha, R.A., 2021. Deep learning for robotics. Journal of Data Analysis and Information Processing, 9(02), p.63.
8. Gao, J., Li, P., Chen, Z. and Zhang, J., 2020. A survey on deep learning for multimodal data fusion. Neural Computation, 32(5), pp.829-864.
9. Bengio, Y., 2009. Learning deep architectures for AI. Foundations and trends® in Machine Learning, 2(1), pp.1-127.
10. Román-Portabales, A., López-Nores, M. and Pazos-Arias, J.J., 2021. Systematic review of electricity demand forecast using ANN-based machine learning algorithms. Sensors, 21(13), p.4544.
11. Ngueajio, M.K., Washington, G., Rawat, D.B. and Ngueabou, Y., 2022, September. Intrusion detection systems using support vector machines on the kddcup’99 and nsl-kdd datasets: A comprehensive survey. In Proceedings of SAI Intelligent Systems Conference (pp. 609-629). Cham: Springer International Publishing.
12. Patil, S., Varadarajan, V., Mazhar, S.M., Sahibzada, A., Ahmed, N., Sinha, O., Kumar, S., Shaw, K. and Kotecha, K., 2022. Explainable Artificial Intelligence for Intrusion Detection System. Electronics 2022, 11, 3079.
13. Otchere, D.A., Ganat, T.O.A., Gholami, R. and Ridha, S., 2021. Application of supervised machine learning paradigms in the prediction of petroleum reservoir properties: Comparative analysis of ANN and SVM models. Journal of Petroleum Science and Engineering, 200, p.108182.
14. Ağbulut, Ü., Gürel, A.E. and Biçen, Y., 2021. Prediction of daily global solar radiation using different machine learning algorithms: Evaluation and comparison. Renewable and Sustainable Energy Reviews, 135, p.110114.
15. Ahmad, A., Ostrowski, K.A., Maślak, M., Farooq, F., Mehmood, I. and Nafees, A., 2021. Comparative study of supervised machine learning algorithms for predicting the compressive strength of concrete at high temperature. Materials, 14(15), p.4222.
16. Song, H., Ahmad, A., Farooq, F., Ostrowski, K.A., Maślak, M., Czarnecki, S. and Aslam, F., 2021. Predicting the compressive strength of concrete with fly ash admixture using machine learning algorithms. Construction and Building Materials, 308, p.125021.
17. Hong, Y., Hou, B., Jiang, H. and Zhang, J., 2020. Machine learning and artificial neural network accelerated computational discoveries in materials science. Wiley Interdisciplinary Reviews: Computational Molecular Science, 10(3), p.e1450.
18. Ghazal, T.M., Rehman, A.U., Saleem, M., Ahmad, M., Ahmad, S. and Mehmood, F., 2022, February. Intelligent model to predict early liver disease using machine learning technique. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-5). IEEE.
19. Nguyen, Q.H., Ly, H.B., Ho, L.S., Al-Ansari, N., Le, H.V., Tran, V.Q., Prakash, I. and Pham, B.T., 2021. Influence of data splitting on performance of machine learning models in prediction of shear strength of soil. Mathematical Problems in Engineering, 2021, pp.1-15.
20. Pan, L., Saxon, M., Xu, W., Nathani, D., Wang, X. and Wang, W.Y., 2023. Automatically correcting large language models: Surveying the landscape of diverse self-correction strategies. arXiv preprint arXiv:2308.03188.
21. Hasan, M.S., Kordijazi, A., Rohatgi, P.K. and Nosonovsky, M., 2021. Triboinformatic modeling of dry friction and wear of aluminum base alloys using machine learning algorithms. Tribology International, 161, p.107065.
22. Ambarwari, A., Adrian, Q.J. and Herdiyeni, Y., 2020. Analysis of the effect of data scaling on the performance of the machine learning algorithm for plant identification. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(1), pp.117-122.
23. Olu-Ajayi, R., Alaka, H., Sulaimon, I., Sunmola, F. and Ajayi, S., 2022. Building energy consumption prediction for residential buildings using deep learning and other machine learning techniques. Journal of Building Engineering, 45, p.103406.
24. Pokhrel, S., Abbas, R. and Aryal, B., 2021. IoT security: botnet detection in IoT using machine learning. arXiv preprint arXiv:2104.02231.
25. Ciaburro, G., 2022. Machine fault detection methods based on machine learning algorithms: A review. Mathematical Biosciences and Engineering, 19(11), pp.11453-11490.
26. Anaraki, M.V., Farzin, S., Mousavi, S.F. and Karami, H., 2021. Uncertainty analysis of climate change impacts on flood frequency by using hybrid machine learning methods. Water Resources Management, 35, pp.199-223.
27. Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), pp.1-22.
28. Maseer, Z.K., Yusof, R., Bahaman, N., Mostafa, S.A. and Foozy, C.F.M., 2021. Benchmarking of machine learning for anomaly-based intrusion detection systems in the CICIDS2017 dataset. IEEE access, 9, pp.22351-22370.
29. Sağlam, C. and Çetin, N., 2022. Machine learning algorithms to estimate drying characteristics of apples slices dried with different methods. Journal of Food Processing and Preservation, 46(10), p.e16496.
30. Albahar, M.A., Binsawad, M., Almalki, J., El-etriby, S. and Karali, S., 2020. Improving intrusion detection system using artificial neural network. International Journal of Advanced Computer Science and Applications, 11(6).
31. Wang, Z., Ghaleb, F.A., Zainal, A., Siraj, M.M. and Lu, X., 2024. An efficient intrusion detection model based on convolutional spiking neural network. Scientific reports, 14(1), p.7054.
32. Ang, K.W.G., 2022. A Case Study for Cyber Incident Report in Industrial Control Systems (Doctoral dissertation, Massachusetts Institute of Technology).
33. Malatji, M. and Tolah, A., 2024. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics, pp.1-28.
34. Sambandam, R.K., Daniel, D., Gokulapriya, R., Vetriveeran, D., Jenefa, J. and Anuneshwar, 2023, August. Comparison of Machine Learning-Based Intrusion Detection Systems Using UNSW-NB15 Dataset. In International Conference on Artificial Intelligence on Textile and Apparel (pp. 311-324). Singapore: Springer Nature Singapore.
35. Vakili, M., Ghamsari, M. and Rezaei, M., 2020. Performance analysis and comparison of machine and deep learning algorithms for IoT data classification. arXiv preprint arXiv:2001.09636.
36. Yacouby, R. and Axman, D., 2020, November. Probabilistic extension of precision, recall, and f1 score for more thorough evaluation of classification models. In Proceedings of the first workshop on evaluation and comparison of NLP systems (pp. 79-91).
37. Li, J., Othman, M.S., Chen, H. and Yusuf, L.M., 2024. Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning. Journal of Big Data, 11(1), p.36.
38. Natarajan, B., Bose, S., Maheswaran, N., Logeswari, G. and Anitha, T., 2023, August. A New High-Performance Feature Selection Method for Machine Learning-Based IOT Intrusion Detection. In 2023 12th International Conference on Advanced Computing (ICoAC) (pp. 1-8). IEEE.
39. Vigoya, L., Fernandez, D., Carneiro, V. and Novoa, F.J., 2021. IoT dataset validation using machine learning techniques for traffic anomaly detection. Electronics, 10(22), p.2857.
40. Seong, T.B., Ponnusamy, V., Jhanjhi, N.Z., Annur, R. and Talib, M.N., 2021. A comparative analysis on traditional wired datasets and the need for wireless datasets for IoT wireless intrusion detection. Indonesian Journal of Electrical Engineering and Computer Science, 22(2), pp.1165-1176.
41. Alex, C., Creado, G., Almobaideen, W., Alghanam, O.A. and Saadeh, M., 2023. A comprehensive survey for IoT security datasets taxonomy, classification and machine learning mechanisms. Computers & Security, p.103283.
42. Pacheco, Y. and Sun, W., 2021, February. Adversarial Machine Learning: A Comparative Study on Contemporary Intrusion Detection Datasets. In ICISSP (pp. 160-171).