International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
ISSN: 3070-0515
Original Research Paper

Machine Learning Approaches for Intelligent Anomaly Detection

Mohammed Nasiruddin
Platform Engineer; AI/ML SaaS Architecture
London, United Kingdom
mnk.nasiruddin@gmail.com

Sultan Ahmad
Dept. of Computer Science, PSAU, Saudi Arabia
UCRD, Chandigarh University, India
s.alisher@psau.edu.sa

Mohammed Yousuf Uddin
Dept. of Information Systems
Prince Sattam Bin Abdulaziz University
m.yousuf@psau.edu.sa

Abstract*— Anomaly detection identifies objects or events that do not behave as expected or correlate with other data points. Anomaly detection has been used to identify and investigate abnormal data components. Anomaly detection in network traffic is a critical task for identifying malicious activities and ensuring the security of computer networks. Machine learning techniques, particularly deep learning has enabled tremendous advancements in the area of anomaly detection. This project aims to design and evaluate an intelligent intrusion detection system (IDS) capable of detecting both known and dynamic cyber-attacks with higher accuracy. The implementation uses a combined KDD and NSL-KDD dataset, which contains network traffic records described by 41 request signature features and labelled as either normal or attack traffic. The dataset includes nearly 30 different attack types, which are further categorized into five major classes: Normal, DoS, Probe, R2L, and U2R. During pre-processing, categorical features and attack labels are converted into numeric values to make the data suitable for machine learning algorithms. Existing models such as Support Vector Machine (SVM) and Random Forest are implemented to evaluate classical detection performance. However, these models show limited accuracy when handling dynamic or previously unseen attack patterns. To overcome this limitation, a Deep Neural Network (DNN) model with an optimized hidden layer structure is proposed. The DNN dynamically learns complex patterns from the data and achieves superior detection accuracy compared to traditional approaches. Additionally, Extreme Learning Machine (ELM) is also evaluated for performance comparison. Experimental results demonstrate that the proposed DNN-based model provides improved accuracy and robustness, making it more effective for modern network intrusion detection systems.

Keywords: Anomaly Detection, Network Traffic Analysis, Intrusion Detection System, Machine Learning, Deep Learning, KDD Dataset, NSL-KDD Dataset, Cyber Attack Detection, Support Vector Machine, Random Forest, Deep Neural Network, Extreme Learning Machine, Network Security, Dynamic Attack Detection.

I. INTRODUCTION

Anomaly detection is the process of finding data or events that do not follow normal or expected behaviour. As digital systems generate large amounts of data every day, automatically identifying unusual patterns has become very important in many fields such as finance, healthcare, cybersecurity, and manufacturing [3]. These unusual patterns often point to serious issues, including fraud, system failures, or security attacks. However, detecting anomalies is not easy because normal behaviour can change over time, and abnormal events are often rare and unpredictable [10]. Traditional anomaly detection methods usually rely on fixed rules or predefined limits, which makes them less effective when dealing with complex and changing data [6]. In cybersecurity, anomaly detection helps identify suspicious activities like unauthorized access, malware infections, or network intrusions. In the financial sector, it is used to detect unusual transactions that may indicate fraud [11]. In industrial systems, anomaly detection helps find early signs of equipment malfunction, allowing timely maintenance and reducing downtime. Overall, effective anomaly detection improves system security, reduces risks, saves costs, and supports better decision-making across various applications [9].

Anomaly detection techniques have evolved significantly over time, moving from simple statistical methods to more advanced machine learning-based approaches [15]. In the early stages, anomaly detection mainly depended on statistical techniques that defined what was considered normal behaviour and then identified values that deviated from it [10]. Methods such as Z-score and Interquartile Range (IQR) were commonly used to

Received: 26-10-2025 | Accepted: 05-12-2025 | Published: 13-12-2025 |

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

detect outliers, especially in simple, single-variable datasets [6]. While these approaches were easy to implement, they proved insufficient when applied to modern systems that generate large, complex, and high-dimensional data [3].

With the increase in data complexity, machine learning and artificial intelligence techniques became more popular for anomaly detection [8]. These methods are better suited to handle large volumes of data and complex patterns [1]. Supervised learning approaches use labelled datasets containing both normal and abnormal instances to train models, making them effective when accurate labels are available [4]. On the other hand, unsupervised methods do not require labelled data and are especially useful in real-world scenarios where anomalies are rare or not clearly defined [2]. Several studies have compared different anomaly detection algorithms to understand their performance in various conditions [23]. These comparisons help highlight the strengths and weaknesses of each approach. For example, isolation-based algorithms like Isolation Forest are effective in high-dimensional datasets, while density-based methods such as Local Outlier Factor perform well when anomalies appear in clusters [6]. Some research has also focused on hybrid models that combine multiple techniques to improve overall detection accuracy and reliability [7]. Anomaly detection in network traffic has become a crucial research topic due to the rapid expansion of the internet, cloud computing, and IoT-based systems. Modern networks support a wide range of applications and services, which significantly increases the volume and diversity of network traffic [20]. This growth also attracts attackers who continuously develop sophisticated techniques to exploit system vulnerabilities [21]. As a result, traditional security mechanisms such as firewalls and rule-based systems are no longer sufficient on their own. Intrusion Detection Systems (IDS) play a key role in continuously monitoring network traffic, analysing patterns, and identifying abnormal behaviours that may indicate potential security threats or attacks [22].

Classical machine learning techniques such as Support Vector Machine (SVM), Random Forest, and Naive Bayes have been widely adopted for intrusion detection due to their simplicity and effectiveness in handling structured data [21]. These algorithms classify network traffic based on learned patterns from historical data [22]. However, their performance is highly dependent on the quality and completeness of training data. When attackers modify attack parameters or introduce new attack strategies, these models often fail to detect them accurately [23]. Moreover, classical models usually struggle with high-dimensional data and complex feature interactions, leading to reduced detection accuracy and higher false positive rates in dynamic network environments.

In recent years, deep learning techniques have emerged as powerful alternatives for network anomaly detection [13]. Deep Neural Networks (DNNs) can automatically learn hierarchical feature representations from raw input data, enabling them to capture complex patterns in network traffic [19]. This capability allows DNNs to identify subtle variations between normal and malicious behaviour that may be overlooked by traditional algorithms [22]. Additionally, DNNs can adapt better to evolving attack patterns, making them suitable for detecting both known and unknown threats [1]. Their success in fields such as image processing, speech recognition, and data classification further supports their application in intrusion detection systems [18]. The implementation of this project utilizes a combined KDD and NSL-KDD dataset, which is widely used for evaluating intrusion detection models [22]. The dataset consists of network connection records described by 41 request signature attributes, including traffic statistics, protocol information, and error rates [21]. Each record is labelled as either normal traffic or a specific attack type. Since some attributes and attack labels are represented as categorical strings, a pre-processing stage is necessary to convert them into numerical values [8]. This step ensures compatibility with machine learning algorithms and improves model training efficiency and accuracy [5]. To evaluate system performance, multiple classification models are implemented and compared. SVM and Random Forest are used as baseline models to represent classical machine learning approaches [21]. A DNN model with a defined hidden layer structure is then trained to improve detection performance [22]. The DNN repeatedly refines its internal parameters during training to build a robust predictive model. In addition, an Extreme Learning Machine (ELM) is included to assess its ability to deliver fast training and competitive accuracy. Performance metrics such as accuracy are analysed and visualized using graphs to provide a clear comparison between different algorithms [14].

Overall, this project highlights the importance of advanced learning techniques in modern network security systems. By combining effective data pre-processing with deep learning-based models, the proposed approach enhances the ability to detect anomalies and cyber-attacks in real time [13]. The comparative analysis demonstrates that DNN-based intrusion detection systems offer improved accuracy, adaptability, and reliability over traditional methods [22]. This makes the proposed model a promising solution for securing modern

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

networks against evolving cyber threats and supporting proactive network defence strategies.

II. RELATED WORK

F. Salo et al., (2018) [1] highlight that network-based attacks have grown rapidly in recent years, posing serious threats to both organizations and individual users, as sensitive information is increasingly exposed to risks that can compromise confidentiality, integrity, and availability through unauthorized access, data breaches, and service disruptions. In response to these growing challenges, securing network infrastructures has become a critical priority, and researchers have increasingly turned to machine learning-based intrusion detection systems, which are capable of automatically analyzing network traffic and detecting suspicious behavior more effectively than traditional security measures. In this work, an efficient anomaly detection framework is proposed that focuses on enhancing the performance of widely used machine learning classifiers by employing Bayesian Optimization to automatically fine-tune the hyper parameters of Support Vector Machines with a Gaussian (RBF) kernel, Random Forest, and k-Nearest Neighbor algorithms, thereby enabling the models to achieve better generalization and improved detection capability. The framework is validated using the ISCX 2012 dataset, which contains realistic network traffic and a variety of attack scenarios, and experimental results demonstrate significant improvements in detection accuracy, precision, and recall, along with a notable reduction in false alarm rates, highlighting the robustness and effectiveness of the proposed framework for reliable network intrusion detection.
Rashid et al., (2022) [7] says that detecting anomalies in large-scale cybersecurity datasets is a critical yet challenging task due to the high dimensionality of security data, where many features may be irrelevant or redundant, increasing computational complexity and potentially lowering detection accuracy. To address this, Feature Selection (FS) techniques are employed to identify and retain only the most informative features, thereby improving the efficiency and performance of machine learning models and serving as an essential preprocessing step in anomaly detection systems. In this study, a novel approach called Anomaly Detection Using Feature Selection (ADUFS) is proposed to enhance both the accuracy and scalability of supervised and unsupervised anomaly detection techniques. The method was evaluated using five benchmark cybersecurity datasets, comparing the performance of models trained on full feature sets with those trained on reduced feature sets. Experimental results demonstrate that models trained on selected features consistently outperform those trained on the complete datasets, achieving higher true positive rates and lower false positive rates. Furthermore, models operating on selected features required substantially less computational time, and the overall results were validated through comparisons with multiple state-of-the-art techniques, confirming the effectiveness of the proposed approach in enhancing anomaly detection performance.
S. Agarwal et al., (2015) [8] highlight that in today's digital era, vast amounts of data are constantly generated, stored, and transmitted, making them vulnerable to unauthorized access, intrusions, and cyberattacks. While many security solutions exist, system loopholes still allow attackers to exploit data. Data mining techniques, particularly anomaly detection, have become essential for identifying unusual patterns that may indicate malicious activity. By detecting these abnormalities early, anomaly detection systems enhance security. Additionally, hybrid approaches combining multiple data mining and machine learning techniques have been developed to improve detection accuracy for both known and unknown attacks. This study reviews these techniques, aiming to guide researchers in creating more effective and robust anomaly detection models for future cybersecurity applications.

M.H. Bhuyan et al., (2013) [11] emphasize that network anomaly detection has become an essential and fast-growing research area due to the increasing complexity and frequency of cyber threats. Numerous network intrusion detection systems (NIDS) have been developed to monitor traffic and identify malicious activities. This paper provides a comprehensive survey of network anomaly detection, presenting key concepts, common attack types, and their impact on network security. Existing techniques are systematically classified based on computational and analytical methods, with comparisons highlighting their strengths, limitations, and practical applications. The paper also reviews tools for detecting anomalies and publicly available datasets for research and evaluation, while identifying open challenges and future directions to advance the field.

V. Hodge et al., (2003) [15] discuss outlier detection as a long-standing method for identifying and, when necessary, removing anomalous data points. Outliers can occur due to mechanical failures, system behavior changes, fraud, human or instrument errors, or natural variations within populations. Detecting these outliers is crucial because it helps prevent potential system failures or financial losses by addressing errors before they escalate. Outlier detection also serves to clean and purify datasets, ensuring more accurate analysis and processing. While early methods for detecting outliers were often arbitrary, modern approaches are

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

systematic and principled, drawing from advanced techniques in computer science and statistics. This paper presents a survey of contemporary outlier detection methods, examining their motivations, highlighting their strengths and weaknesses, and providing a comparative review to help researchers understand and select suitable techniques for different applications.

R. Zou et al., (2017) [18] highlight that research in geochemical data analysis and the detection of geochemical anomalies has progressed significantly in recent decades. Techniques such as fractal and multifractal modelling, compositional data analysis, and machine learning (ML) have been widely applied in this field. Among these, ML has gained prominence due to its ability to manage complex, high-dimensional, and nonlinear geochemical datasets. Machine learning methods are especially effective in modelling unknown multivariate distributions and uncovering meaningful elemental associations relevant to mineral exploration and environmental monitoring. With the rapid advancement of big data technologies and artificial intelligence, ML is expected to play an increasingly important role in geochemical mapping and anomaly detection in the near future. This study reviews contemporary applications of machine learning for identifying geochemical anomalies, analysing their advantages and limitations in geochemical prospecting. While existing research demonstrates the promise of ML in solving complex geoscience problems, further real-world implementations are needed to validate its effectiveness and demonstrate clear advantages over traditional analytical methods.

F. Tsai et al., (2009) [22] note that while the widespread use of the Internet offers many benefits, it also introduces significant risks from network attacks. Intrusion detection has emerged as a key research area in network security, aiming to identify unusual access patterns or malicious activities to protect internal networks. Various machine learning techniques have been applied to develop intrusion detection systems (IDS), yet until this work, no comprehensive review existed that examined the current status of these approaches. This chapter reviews 55 studies conducted between 2000 and 2007, focusing on the development of single, hybrid, and ensemble classifiers for intrusion detection. The reviewed studies are compared in terms of classifier design, datasets used, and experimental setups. The paper also discusses the achievements and limitations of applying machine learning to IDS development and identifies several directions for future research to enhance the effectiveness and reliability of intrusion detection systems.

III. DATASET DETAILS

The dataset used in this work is a combination of the well-known KDD and NSL-KDD intrusion detection datasets, which are widely adopted benchmarks in network security research. These datasets are designed to simulate real-world network environments by capturing a wide range of normal and malicious network activities. Each record in the dataset represents a single network connection and is described using 41 request signature features along with a class label. The labels indicate whether the network traffic corresponds to normal behaviour or a specific type of attack, making the dataset suitable for supervised machine learning and deep learning-based intrusion detection systems. The 41 features in the dataset capture diverse aspects of network behaviour, including basic connection attributes, content-based features, and traffic statistics. Examples include connection duration, protocol type, source and destination bytes, login attempts, error rates, and service-related information. Some attributes are numeric, while others are categorical in nature, such as protocol type, service, and flag. These features collectively provide a detailed representation of network traffic patterns, allowing learning algorithms to distinguish between normal connections and malicious activities based on behaviour and statistical properties.

The dataset contains nearly 30 different attack types, each representing a specific form of malicious behaviour. Examples include DoS attacks such as Neptune and Smurf, probing attacks like Nmap and Ipsweep, remote-to-local (R2L) attacks such as Guess_Passwd, and user-to-root (U2R) attacks like Buffer_Overflow. Although the dataset includes many individual attack names, they are commonly grouped into five major attack categories: Normal, Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). This categorization helps in understanding attack severity and supports higher-level analysis during model evaluation. Since machine learning algorithms cannot directly process string-based values, a comprehensive pre-processing stage is applied to the dataset. Categorical features and attack labels are converted into numerical representations by assigning unique numeric identifiers to each attack type. For example, normal traffic is assigned an ID of 0, while Neptune attack is assigned an ID of 1, and so on. Non-essential or redundant string attributes are removed to reduce noise and computational overhead. The resulting cleaned dataset is stored in a separate file, which is then used for training and testing the models.

After pre-processing, the dataset is structured to support effective model training and evaluation. The

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

cleaned data is divided into training and testing sets to ensure unbiased performance assessment. The training set is used to learn network behaviour patterns, while the testing set evaluates the model's ability to detect anomalies in unseen data. By combining KDD and NSL-KDD datasets and applying systematic pre-processing, the dataset offers a balanced and comprehensive foundation for comparing classical machine learning models with deep learning approaches in network anomaly detection.

IV. PROPOSED METHODOLOGY

The proposed methodology for anomaly detection in network traffic begins with the collection and integration of standard intrusion detection system (IDS) datasets, specifically KDD and NSL-KDD. These datasets contain a wide range of network traffic records, including normal requests and various attack types, with each record represented by multiple attributes such as duration, protocol type, service, src_bytes, dst_bytes, among others. These features collectively define the behaviour of network traffic and serve as the input for machine learning algorithms. Since some features in the dataset are non-numeric or irrelevant, pre-processing is a crucial first step to prepare the data for model training. During pre-processing, string values like tcp or ftp_data are converted into numerical representations, while redundant or unnecessary features are removed. Additionally, each attack type is assigned a unique numeric ID to ensure that the algorithms can correctly interpret and classify attack categories.

Once the dataset is pre-processed, it is divided into training and testing sets to allow the algorithms to learn patterns from historical data and evaluate their predictive performance on unseen records. Three algorithms are implemented for performance comparison: Support Vector Machine (SVM), Random Forest (RF), and Deep Neural Network (DNN). SVM and Random Forest represent classical machine learning methods, while DNN represents a more advanced deep learning approach capable of adapting to dynamic attack signatures. The DNN model is configured with a hidden layer containing eight neurons, allowing the network to filter and extract meaningful patterns from the input features. During training, the DNN iteratively adjusts its weights to minimize classification errors, producing a highly accurate model for detecting both known and evolving attacks.

The training process involves running each algorithm on the training dataset to build models capable of recognizing normal and anomalous traffic. After training, the models are evaluated using the test dataset to measure their accuracy, precision, recall, and false alarm rates. Experimental results indicate that classical algorithms such as SVM and Random Forest achieve moderate accuracy due to their limited ability to generalize to dynamic attacks, while the DNN consistently outperforms them. The DNN's superior performance is attributed to its deep architecture, which allows it to capture complex nonlinear relationships between network traffic features, making it more robust in identifying new and evolving attack patterns.

To visualize and compare the performance of each algorithm, accuracy graphs are generated where the x-axis represents the algorithm names and the y-axis represents the corresponding prediction accuracy. These visualizations provide an intuitive understanding of which model performs best under the given experimental setup. Additionally, the Extreme Learning Machine (ELM) is also tested as part of the methodology to further validate the robustness of neural network-based approaches for anomaly detection. This step allows researchers to explore alternative models for network security applications and evaluate trade-offs between accuracy and computational efficiency.

Finally, once the models are trained and evaluated, they are deployed to predict new network traffic records. The system takes test data as input and produces classifications indicating whether each record corresponds to normal traffic or an attack. This end-to-end methodology—from dataset pre-processing, model training, and evaluation, to prediction—demonstrates a practical approach for implementing anomaly detection in network environments. The proposed DNN-based framework, in particular, provides a reliable and scalable solution for identifying both known and previously unseen network attacks, ensuring enhanced security and resilience for modern network infrastructures.

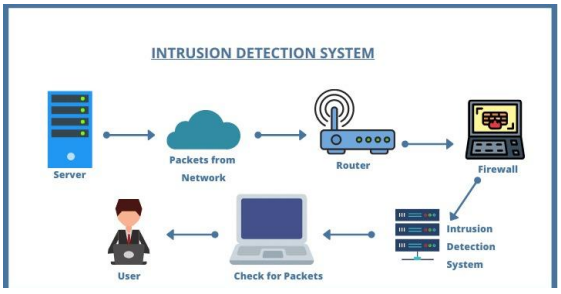

Figure 1: System Architecture of the Anomaly Detection model.

Received: 26-10-2025 | Accepted: 05-12-2025 | Published: 13-12-2025 |

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

V. RESULT AND DIS CUSSION

In the below figure [2] we can see the "Generate Training Model" button this button allows us to prepare the dataset for model training. Both the input features and numeric attack labels are aligned, allowing algorithms like SVM, Random Forest, DNN, and ELM to build and optimize their models effectively.

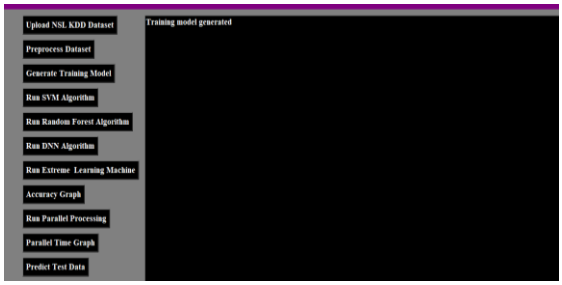

Figure 2: Uploading Dataset

Figure [3] displays the results after running the SVM algorithm on the pre-processed dataset. The SVM achieved a prediction accuracy of **52%,** demonstrating moderate performance but highlighting its limitations in detecting dynamic attacks that differ from the training set.

Figure 3: Results of SVM Predictions

Here, the results after executing the Random Forest algorithm are shown in Figure [4]. The accuracy is similar to SVM **approximately 52%**, confirming that classical algorithms may not adapt well to new or modified attack patterns.

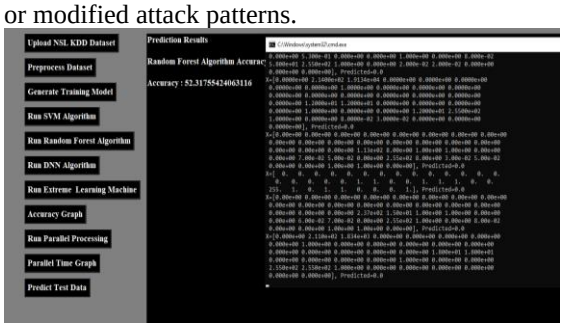

Figure 4: Results of Random Forest Predictions

Figure [5] shows the prediction results after running the DNN algorithm with a hidden layer of 8 nodes. The DNN achieved a higher accuracy compared to SVM and Random Forest due to its ability to model complex nonlinear relationships and adapt to dynamic attack signatures. The accuracy may slightly vary depending on the random initialization of the hidden layers.

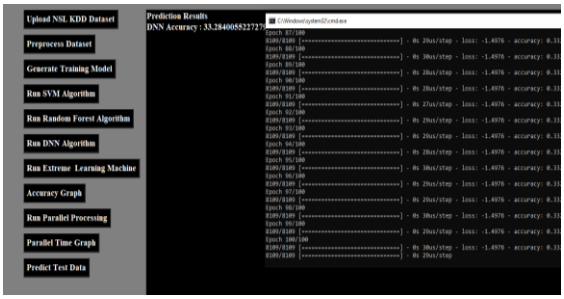

Figure 5: Results of DNN Predictions

Figure [6] shows the results after running the ELM algorithm on the pre-processed dataset. ELM provides faster training times with competitive accuracy, demonstrating its potential as an alternative to DNN for real-time anomaly detection scenarios.

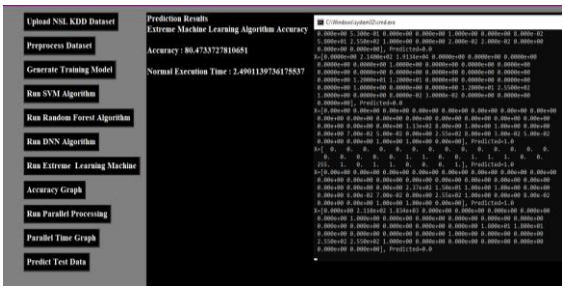

Figure 6: Results of Extreme Machine Learning Algorithm Predictions

his below Figure [7] displays the final outputs of the model on the test dataset. Each network record is classified as either "Attack" or "Normal", providing a clear indication of detected anomalies and demonstrating the effectiveness of the proposed DNN-based detection method over classical algorithms.

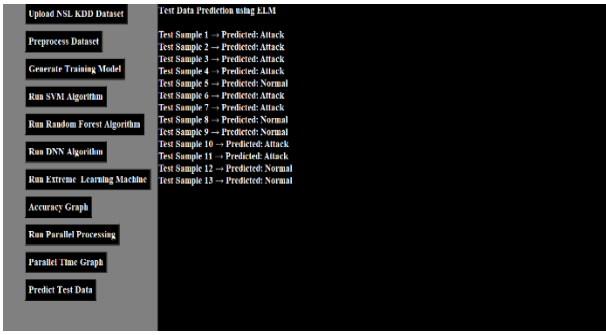

Figure 7: Test Data Prediction Results

In the below Figure [8] the graphs visually compare the prediction accuracies of different algorithms. The X-axis represents the algorithms (SVM, Random Forest, DNN, ELM), and the Y-axis represents their respective accuracies. It is clear from the graph that the proposed DNN technique

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

outperforms the classical algorithms, emphasizing its suitability for detecting both known and novel network attacks.

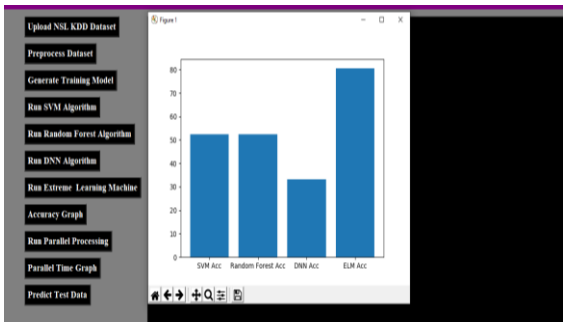

Figure 8: Comparison Graph

DISCUSSION

The results of this project highlight the effectiveness and limitations of different machine learning approaches in network anomaly detection. Classical algorithms like SVM and Random Forest provided moderate detection accuracy but struggled to adapt to dynamic attacks, emphasizing their reliance on pre-trained knowledge and their limited capacity to generalize to unseen attack patterns. In contrast, the Deep Neural Network (DNN) demonstrated superior performance due to its ability to model complex nonlinear relationships within the network traffic data and iteratively optimize its hidden layers for improved prediction. The pre-processing steps, including feature encoding and dataset cleaning, proved crucial in ensuring that the models could effectively interpret the input data and avoid misclassification due to irrelevant or categorical values. The inclusion of Extreme Learning Machine (ELM) further improved the robustness of neural network-based methods, giving faster computation times and competitive accuracy. Overall, the discussion confirms that while traditional models can serve as a baseline, deep learning approaches like DNN provide a more adaptive, scalable, and accurate solution for detecting both known and unknown cyberattacks, making them highly suitable for modern intrusion detection systems.

VI. CONCLUSION

In conclusion the proposed approach to network anomaly detection gave optimistic results by using both classical machine learning algorithms, such as SVM and Random Forest, and a Deep Neural Network (DNN) model, this highlights the superior capability of DNN in identifying both known and dynamic cyberattacks. Through careful pre-processing of the combined KDD and NSL-KDD datasets, including conversion of categorical data into numeric IDs and removal of irrelevant features, the system ensures high-quality input for training robust models. While classical algorithms provide baseline performance, they struggle with evolving attack patterns, whereas the DNN, with an optimized hidden layer, effectively captures complex patterns and relationships in network traffic, achieving higher accuracy and reduced false alarm rates. The inclusion of Extreme Learning Machine (ELM) further demonstrates the flexibility and scalability of neural network-based detection. Overall, the methodology—from pre-processing to model training, evaluation, and real-time prediction—offers an efficient, and adaptive solution for network security, confirming that deep learning models can significantly enhance intrusion detection systems and provide a reliable defence against a wide range of sophisticated cyber threats.

REFERENCES

1. F. Salo, A. B. Nassif, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018
2. P. Seeböck, S. U. Schmidt-Erfurth, and G. Langs, *Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery*, vol. 10265, no. 2. Cham, Switzerland, Springer, 2017.
3. Thudumu Srikanth, B. Philip, Jin Jiong "A comprehensive survey of anomaly detection techniques for high dimensional big data" (2020).
4. F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018.
5. F. Salo, M. N. Injadat, A. Moubayed, A. B. Nassif, and A. Essex, "Clustering enabled classification using ensemble feature selection for intrusion detection," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2019.
6. P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. K. Kalita, "A survey of outlier detection methods in network anomaly identification," *Comput. J.*, vol. 54, no. 4, pp. 570–588, Apr. 2011.
7. Rashid ANM, Ahmed Mohiuddin, F. Haskell, Bazlur, Sikos Leslie Dowland Paul "Anomaly detection in cybersecurity datasets via cooperative co-evolution-based feature selection" (2022).
8. S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," *Procedia Comput. Sci.*, vol. 60, no. 1, pp. 708–713, 2015.

Received: 26-10-2025 | Accepted: 05-12-2025 | Published: 13-12-2025 |

International Journal of
AI Electronics and Nexus Energy
www.zesterapublications.com
Original Research Paper
ISSN: 3070-0515

9. R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, "Real-time big data processing for anomaly detection: A survey," *Int. J. Inf. Manage.*, vol. 45, pp. 289–307, Apr. 2019.
10. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 823–839, Nov. 2012.
11. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools,"
12. I. Bose and R. K. Mahapatra, "Business data mining—A machine learning perspective," *Inf. Manage.*, vol. 39, no. 3, pp. 211–225, 2001.
13. F. Palmieri, A. Castiglione, and A. De Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing*, vol. 122, pp. 13–23, Dec. 2013.
14. B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering version 2.3," *Engineering*, vol. 45, no. 4, p. 1051, 2007.
15. V. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artif. Intell. Rev.*, vol. 22, no. 2, pp. 85–126, Oct. 2004
16. M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Future Gener. Comput. Syst.*, vol. 55, pp. 278–288, Feb. 2016.
17. A. Sodemann and B. J. Borghetti, "A review of anomaly detection in automated surveillance," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1257–1272, Nov. 2012.
18. R. Zuo, "Machine learning of mineralization-related geochemical anomalies: A review of potential methods," *Natural Resour. Res.*, vol. 26, no. 4, pp. 457–464, Oct. 2017.
19. J. Zhu, P. He, and M. R. Lyu, "Experience report: System log analysis for anomaly detection," in *Proc. IEEE 27th Int. Symp. Softw. Rel. Eng. (ISSRE)*, Oct. 2016, pp. 207–218.
20. O. Ibidunmoye, F. Hernández-Rodriguez, and E. Elmroth "Performance anomaly detection and bottleneck identification," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1–35, Sep. 2015.
21. Y. Yu, "A survey of anomaly intrusion detection tchniques," *J. Comput. Sci. Coll.*, vol. 28, no. 1, pp. 9–17, 2012.
22. C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion dtection by machine learning: A review," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, Dec. 2009.
23. J.-M. Park, et al., "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Comput. Netw.*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007.