Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

Sentinel AI: Revolutionizing Cybersecurity with Intelligent Intrusion Detection

Talib Nadeem Usmani
Honeywell, Duluth, Georgia, USA
talibosmani@gmail.com

Muhammad Zunnurain Hussain
Department of Computer Science, Bahria University Lahore Campus, Pakistan Zunnurain.bulc@bahria.edu.pk

Muhammad Zulkifl Hasan (Corresponding Author)
Department of Computer Science, Faculty of Information Technology, University of Central Punjab, Lahore, zulkifl.hasan@ucp.edu.pk

Abstract
The research paper evaluates the limitations of the Analysis of Host-Based and Network-Based Intrusion Detection System article regarding open-source host-based intrusion detection systems OSSEC and Snort while developing and presenting an AI-based intrusion detection system that improves detection accuracy, reduces false positives, and supports scalability. This paper introduces an AI-based IDS system that analyses existing host- and network-based IDS systems to find their missing elements. The training system requires a different network and hosts behavioural patterns through SVC and Decision trees, Logistic regression, and machine learning algorithms. The famous NLSKDDCUP99 Dataset is used. The AI-driven IDS produces errorless attack detection outcomes without generating any erroneous alerts. The study submits aid through recommendations, which conclude with a proposal that AI hardware should strengthen intrusion detection systems to protect cybersecurity operations.
Keywords: Artificial intelligence, Machine learning, Intrusion detection system

Introduction

IDS is a vital security defence that protects computer systems and networks from unauthorised user and hacking activities that fall under cybersecurity responsibilities. Security systems were produced to detect multiple danger types during information system protection operations. Two main IDS classifications exist: Agreed network-based IDS (NIDS) and Host-based IDS (HIDS). The article evaluates the problems found in two well-known IDS options, OSSEC and Snort, even though they offer unique advantages. Future security threats will pose difficulties for skilled IDS systems due to their inability to adapt or prevent many false positives from appearing at the system's surface. Machine learning functions as a modern approach to construct IDS systems of superior effectiveness that confront present security threats. The study investigates traditional IDS vulnerabilities through machine learning algorithm application on NSL-KDD dataset information. The NSL-KDD

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

dataset is an improved version of the KDDCup99 dataset for domain research because its extended information improves equal performance evaluation. Our research develops a next-generation AI intrusion detection system through SVC together with Naive Bayes and Decision Trees and Logistic Regression, which serves as our most recent machine learning application to determine higher accuracy with decreased false positives and improved adaptability. The study indicates a substantial lack of assessment research about intrusion detection systems, specifically evaluating the capabilities of OSSEC (HIDS) and Snort (NIDS). The current analytics of the effectiveness of intrusion detection tools HIDS (OSSEC) and NIDS (Snort) remains insufficient in academic works. However, these tools dominate the market for host-based and network-based intrusion detection. Insights about their scalability are missing from the report, preventing readers from understanding their performance when applied to extensive network networks. The analysis of cyber threat adaptation remains absent from the study, which creates serious doubts regarding their future performance capabilities. Any intrusion detection system requires a reliable assessment of its performance because the false positive rate remains an essential yet disregarded factor. The performance evaluation of OSSEC and Snort becomes unclear because their study lacks specific measurements such as detection rate, false positive rate and response time metrics[1].

The second research is proposing an artificial intelligence-based intrusion detection approach which works on NSL-KDD datase for performance enhancement. It is also possible to use the normal dataset which shows a greater reduction in false positive where the data distribution is more realistic, on the overall balance of intrusion detection methods KDD Cup 99, which is no longer relevant and have been improved in NSL-KDD which is part of the better detection of intrusion data set that re-balance data. The suggested system uses Support Vector Classification (SVC), Naive Bayes, Decision Trees and Logistic Regression from machine learning for line sequence analysis machine learning to obtain better precision in threat detection compared to traditional rule-based security systems. The platform utilized by the system for translation employs active learning on the dataset analyzed previously to minimize the frequency of false alert events and increase the precision of the output. The system will also increase the ability and adaptability of detection by means of refining models and continuing as emerging cyber threats materialize. This system shows multiscale elastic expansion capabilities, which results in protecting large-scale cybersecurity networks to secure different network systems. Many machine learning approaches established for enhancing the intrusion detection process in the project[2]. Conclusion• SVC forms the best decision boundary to separate network traffic into benign and malignant. Naive Bayes works as a probabilistic classifier, which uses Bayes' theorem to detect various types of intrusion quickly and accurately in classification. A decision tree is an iterative method that separates network traffic data into patterns of normal and attack behaviors. We present a modelling process of intrusion probability through network traffic features based on the application of supervision technique applied to the data using Logistic Regression, which allows us to reach a high classification precision. It utilizes the NSL-KDD data set embedded with modern technology in AI to formulate the intelligent intrusion detection technique capable of achieving higher accuracy and

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)
better scalability through a more lucrative adaptive way surpassing outdated models in the cybersecurity attack prevention system.

Literature Review

IDS is an essential cyber security tool for identifying unauthorised network attacks to protect systems and networks. The security system known as IDS operates through two principal detection methods: Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS). OSSEC and other HIDS tools operate at the host level to track system actions, alerting users about unapproved file edits and system registry tweaks. The analysis conducted by NIDS through network traffic allows the identification of unexpected activities, unauthorised access attempts, and potential security threats. The extensive use of these security systems produced detection rules as their primary method. However, it led to performance limitations that involved multiple types of errors and operational challenges and a reduced response to modern cyber threats [3].

Traditional IDS systems function well in set attack situations yet face challenges in dynamic threat response and solution growth. Traditional IDS detection methods that implement signature matching need frequent update cycles to recognize new attack patterns [4]. These systems consistently produce many false detection alerts that create an overwhelming situation for security teams because they do not always represent genuine security threats. Rules-based IDS prove ineffective for stopping APTs, zero-day exploits, and polymorphic malware since these threats transform their tactics to get past established security parameters [5]. Large enterprise networks face challenges regarding scalability because they need to analyse extensive real-time network traffic amounts. Existing intrusion detection systems face difficulties when handling large data streams that enter at high speeds, resulting in delayed responses to threats [6]. These security systems have no built-in self-learning ability that would grant them the power to improve their detection accuracy independently because they need regular human interaction to upgrade their systems and incorporate threat intelligence. The research community began studying how Artificial Intelligence (AI) and Machine Learning (ML) can be integrated into IDS systems because they overcome existing limitations. Through data-driven modelling, AI-powered intrusion detection tools enhance threat characterization and improve the accuracy of anomaly and attack pattern detection while performing threat classification. Support Vector Machines (SVM), Decision Trees, and Naïve Bayes show advancements in identifying standard traffic types instead of malicious traffic patterns [7]. The combination of clustering algorithms and anomaly detection techniques under unsupervised learning successfully detects unknown attack types known as zero-day threats[8].

IDS capabilities receive more profound enhancement through Deep learning methods that use Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) for analysing sequential network traffic patterns. When IDS uses CNNs, it becomes more efficient at detecting complicated attack patterns that traditional systems would fail to detect. Detection of persistent cyber threats becomes possible through the use of RNNs, specifically Long Short-Term Memory (LSTM) networks . AI-driven IDS systems commonly use benchmark datasets

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

starting with NSL-KDD, which constitutes an enhanced version of KDD Cup 99. NSL-KDD fixes the data problems of redundancy together with a class imbalance that affected the original KDD dataset, thus creating better conditions for research on intrusion detection. The NSL-KDD dataset allows machine learning and deep learning models to surpass traditional IDS approaches because it produces more accurate results and compound detection capabilities while decreasing false alerts. Several research studies demonstrate that AI-driven solutions perform better detection than traditional IDS approaches. AI-based IDS controls false alarms effectively, adapts efficiently to emerging threats, and works proficiently in complex network environments. Through its continuous learning process, AI-driven IDS maintains up-to-date positions relative to emerging attack strategies, which traditional security systems cannot achieve. Several obstacles exist in AI-based IDS applications because top-quality data sets are required for training, while computation scales are significant and potential adversarial attacks. AI-based intrusion detection will use combined systems that fuse rule-based detection methods with AI-enhanced anomaly detection to achieve high accuracy and minimal false alarms. Federated learning emerges as a privacy-preservation solution by letting IDS models operate on dispersed data without disclosing sensitive information. Desired to explore reinforcement learning concepts for building real-time IDS systems with autonomous threat defense capabilities. Network security remains dependent on AI-driven intrusion detection, which will become essential because cybersecurity threats continue to evolve. Sentinel AI and similar next-generation IDS solutions will transform cybersecurity protection through their combination of deep learning algorithms, adaptive threat intelligence analysis, and real-time data monitoring technology[9].

Table 1: Comparative Analysis IDS

Feature	**Traditional IDS**	**AI-Driven IDS**	**Ref**
Detection Approach	Rule-based signature detection	Machine learning anomaly detection	[10]
Adaptability to New Threats	Low - requires frequent updates	High - learns from new attack patterns	[11]
False Positive Rate	High - frequent false alarms	Low - improved accuracy	[12]
Detection Speed	Moderate	Fast - real-time analysis	[13]
Scalability	Limited - struggles with large-scale networks	Highly scalable - suited for large networks	[14]
Data Processing Capability	Processes limited predefined patterns	Processes large-scale dynamic data	[15]
Ability to Detect Zero-Day Attacks	Poor - relies on known attack signatures	Excellent - detects emerging threats	[16]
Computational Resource Requirement	Low - minimal computational demand	High - requires GPUs or TPUs	[17]
Self-Learning	No - manual updates	Yes - continuously	[18]

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

Capability	needed	improves over time	
Real-Time Threat Mitigation	Limited - primarily alert-based	Advanced - can automate response actions	[19]

The field of network intrusion detection has also been greatly expanded by recent developments in big data analytics and IoT sensor networks, which facilitated the processing of real-time data at a greater speed [20]. Cloud data lakehouses have evolved to provide new methods to better store and process large volumes of data, which has improved the IT systems with AI-driven security systems to be more scalable and secure [21]. Deep learning models (e.g., text summarisation) are useful for improving automated decision-making systems in intrusion detection [22]. These findings showcase the promise of employing AI for recognizing and countering sophisticated, developing cyber strikes, exemplified through the specific use of AI-augmented cybersecurity solutions indicating where one can establish the most effective detection and prevention against digital bank explosions [23]. Reinforcement learning methods have been effective for robotics control, and its application to intrusion detection systems may also enhance adaptability against new attack patterns [24]. The healthcare sector is gradually being used with machine learning methods, and attack identification (AI) models can be implemented efficiently with great accuracy [25]. In addition, the use of cloud-native data and tools to optimize instance reliability and security has been shown to play a critical role in ensuring that the intrusion detection systems are running in a stable and secure environment [26].

Training data for such applications is often direct and well in place, offering insights into how machine learning models work for malicious activities detection [27]. Public service institutions have been early adopters of innovative clean energy solutions that may help provide lessons learned for implementing AI and machine learning into sustainable cybersecurity infrastructures [28]. We could also use smart city policy-formation with AI-based business intelligence to make urban cyber posture decisions and governing efforts [29]. Highlighting the role of AI for modeling and forecasting is an important component of predictive analytics towards the resilience of electricity consumption, which could prove a useful tool also for future threat prediction in the case of network security [30]. Just as cybersecurity threats may be detected only through analysis of various data points through which the threat may be hidden, remote sensing and AI models are increasingly mapping relationships in environmental data [31]. Behavioral-driven Quantum Cybersecurity potentially benefits from the business supply chain AI-quantum computing integration, which is a new fold in the chain that can be easily adjusted and adopted for cybersecurity systems for scalability and performance [32]. Innovations in load forecasting (in a short-term time frame), driven by intelligent approaches, could potentially be tailored to anticipate and deter breaches in mobile and evolving network settings [33]. The same transformative AI technologies for predictive analytics in healthcare may propose methodologies that can serve to improve proactive threat detection and mitigation in cybersecurity [34]. For instance, load forecasting in smart grids based on AI-driven solutions represents one application of

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

predictive models in cybersecurity, protecting essential infrastructures and decreasing susceptibility to attacks [35].

Proposed Framework for ML-Driven Sustainable Agriculture

The NSL-KDD dataset marks a significant research advancement for intrusion detection system (IDS) investigations through its upgraded version of the KDD Cup 99 dataset features. The researchers designed NSL-KDD to fix various issues in KDD Cup 99 since its predecessor had problems with redundant data and unbalanced classes alongside irrelevant elements. Therefore, it provides an essential form of cybersecurity by protecting networks from DoS and probing attempts, as well as unauthorised access. Table 3shows the NSL-KDD dataset's refined dataset with the attack type distribution normalised via removal of duplicate entries, providing improved research base for IDS research such as in this paper. Hinton DL, S. M., Dean, J., Jiang, D. (1998), This dataset has records of normal and malicious network traffic, while having distinct network features derived from TCP/IP data packets analysis. The data features important characteristics of the network itself, such as the duration of the connection, the number of bytes sent between two nodes, and protocol-specific characteristics that indicate certain patterns in the network. The functionality of these capabilities provides very granular inspections of traffic patterns to improve or detections of cyber threats. The primary advantage of the NSL-KDD dataset is that it achieves a balanced distribution of attack-types. This avoids detection biases in the evaluation process and allows the researchers to construct IDS models performing better than even in real settings [3]. The dataset contains also forty-one features computed from TCP/IP packet analyzing. Network traffic characteristics are basic information needed to build intrusion detection systems. The significant features include connection duration which records session duration; Protocol type TCP UDP or ICMP and service type HTTP FTP or SMTP. The source and destination bytes comprising the data transfer between different hosts, and the flag counts are the two primary parts of the system used to identify basic protocols and states on the network by monitoring SYN-ACK and RST activity.
The structure of the database is divided into two branches: attack database and normal traffic patterns. Regular users circulate their approved communication, resulting in traditional devices linking together to make up the regular class of emergency networks. The messages include standard data transmission patterns and authorized access to resources that abide by existing security patterns. This attack class covers all connections associated with malicious network-borne incidents. DoS attacks, reconnaissance-based probing operations, unauthorized access attempts, and other intrusion forms in the attacking category are the threats to network security. The structured organization of data between standard and attack classes offers instructions for building machines that can detect and prevent cyber-attacks.

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

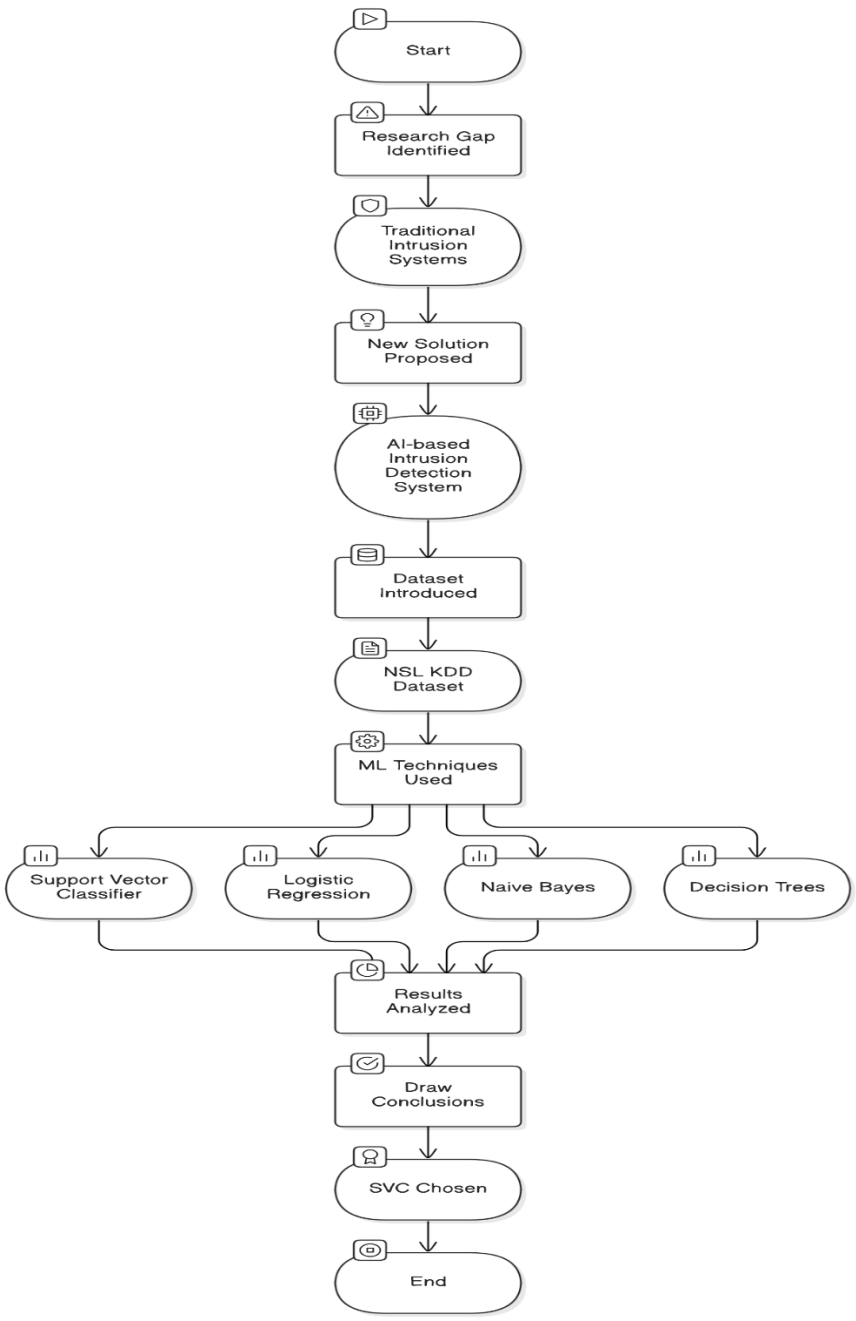

Figure 1: Flowchart for our research

Data Preprocessing and Feature Extraction

The initial stage of creating an AI-based Intrusion Detection System (IDS) demands preprocessing the dataset until data becomes clean and structured. The quality of input data is enhanced through preprocessing since this process produces better data inputs that boost machine learning model accuracy. The NSL-KDD dataset underwent duplicate removal to prevent the presence of wasted information that

Dialogue Social Science Review (DSSR)
www.thedssr.com
DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)
would introduce misleading outcomes. The dataset underwent duplication detection to eliminate patterns that could influence training since the data needed to show attacks and expected conditions in their whole variety. All duplicate entries received elimination. A strategy to handle null values was established to avoid training errors as part of the additional redundancy management process. The training process broke down when meaningful data was absent from necessary features because this deficiency generated prediction bias. Validation methods were therefore used to determine that missing data would not affect model training. The dataset moved past textual categories through a Label Encoder, turning class signs into machine-learning practical numeric form. The successful application of most ML models depends on numerical input rather than text-based categories.

The data formatting process completed before the model evaluation required dividing the information between training and testing data. Splitting data ensures proper generalisation for new observations instead of pattern memorisation during training. Standard Scaler normalisation allowed numerical features to operate on a standardised dimension scale. Standardisation optimises algorithm performance because it prevents features with large numerical ranges from distorting the model's predictions and helps Support Vector Machines (SVC) algorithms maintain optimal conditions. Machine learning-based intrusion detection requires thorough preprocessing work to establish sound and efficient operation.

Performance Comparison

The evaluations measured how well the AI-based IDS operated through assessments that included classical IDS tools OSSEC and Snort alongside the AI-incorporated IDS that processed NSL-KDD dataset information. Despite their extensive market use, both OSSEC and Snort use predefined rule sets that depend on signature detection methods. These systems offer strong protection against initial threats but face multiple challenges, including highly incorrect positive detections, poor response to modern threats, and scalability issues when targeting big network environments. The detection capabilities of these systems are limited because they cannot recognise unknown zero-day attacks along with anomalous behaviour outside their signature database. This results in more cyber threats managing to avoid detection.

The AI-based IDS uses machine learning algorithms to dynamically recognise attack patterns that standardise various network attacks. Through NSL-KDD dataset training, the model acquires historical attack pattern knowledge, enabling it to find unknown threats along with existing ones effectively. The AI-based detection system outperforms standard IDS because its methodology learns from time-based adjustments that enhance operational capacity. The performance evaluation examined three aspects of multiple Machine Learning models: Support Vector Classification (SVC), Naive Bayes, Decision Trees, and Logistic Regression based on accuracy metrics, response time, and false positive rate results.

Performance Metrics

Multiple performance metrics helped determine the effectiveness of the implemented models. Performance accuracy in IDS operations was measured by dividing correct classifications between regular traffic and security attacks. A model with a high

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

accuracy score demonstrates a strong capability to differentiate between safe and dangerous network traffic. The False Positive Rate (FPR) measurement played a vital role by indicating the attacked traffic identified incorrectly as threatening activities. Excessive false alarms from IDS systems minimise operational efficiency in security analysis since they provide too many alerts to security analysts. The time taken by the IDS to detect threats and classify and respond to potential threats was examined through response time analysis. Real-time intrusion detection is a vital security measure because it stops data breaches and safeguards networks in advance from significant cyber-attacks. The system's ability to handle new unpredictable cyber threats was analysed due to its position as a superior feature to traditional IDS approaches. Machine learning technologies serve as main components within intrusion detection because they reveal concealed patterns in network traffic to determine whether they represent benign or harmful actions. In this research, the authors implemented Support Vector Classification (SVC), Naive Bayes, and Decision Trees Logistic Regression to detect attacks and judge their accuracy rates.

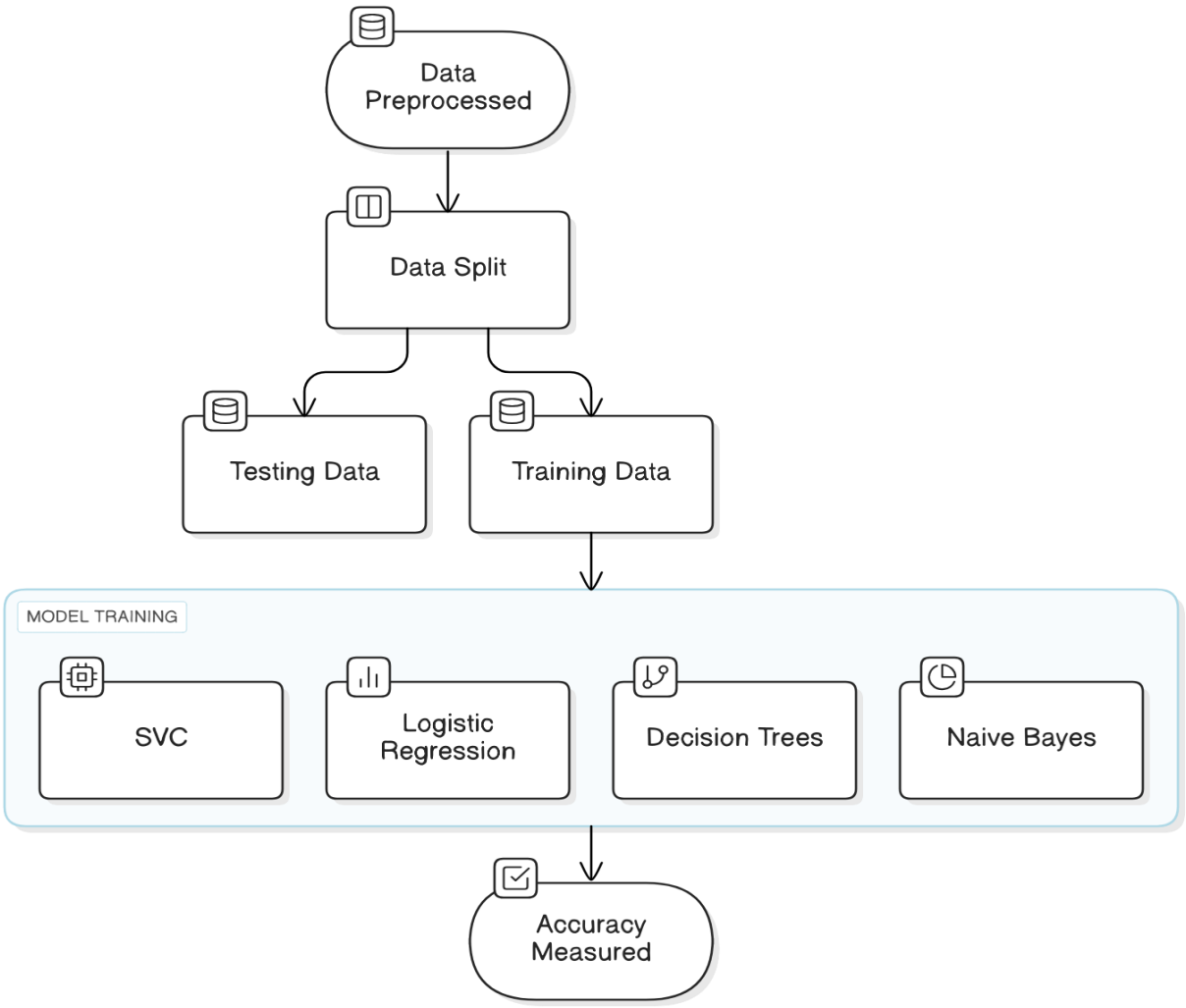

Figure 2 Flow chart for Accuracy measurement

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

Support Vector Machine Classification (SVC)

The SVC algorithm in the SVM family of classification algorithms, executes a procedure to find the optimal hyperplane separating different classes in data. To classify packets, intrusions detection system (IDS) analyses the core properties of normal and bad network traffic by using semi-variable clustering (SVC). SVC is able to divide traffic patterns of network connections to traffic on the NSL-KDD data into normal behaviour or an attack This method delivers the input traits into multi-dimensions, in the process applying hyperplane edges to categorise diverse classes. SVC's capability to handle nonlinear data relationships has established it as a powerful tool for detecting complex cyber-related threats. It refines its discrimination for normal suspicious traffic and improves its detection of suspicious traffic patterns. SVC adaptable with Cybersecurity task, and it performs a good job in handling multiple stream data from the network with high speed while not sacrificing its accuracy level.

Naive Bayes

Naive Bayes is a type of a probabilistic classification algorithm that makes use of the Bayes theorem to make decisions using the independent features contained in every dataset. Naive Bayes structure results in high-speed performance and simple operational speed across the board in this application, even if these environmental setups are not available in actual systems [4,34]. Databases of oustealing NSL-KDD enable Naive Bayes to sufficiently calculate individual probability distributions for attack and normal traffic and classify objects according to their behaviour type. It employs a features-based approach to predict probabilities such as protocols used, connection length, or byte transfer rate. It processes the probability distribution for all classes and predicts the one with the highest probability. The operation speed of Naive Bayes is efficient, which provides fast threat classification, hence, it is suitable for IDS security applications that require fast responses.

Decision Trees

This entire system is a terrific layered structure where users' features are arranged into nodes and classifications diverge through branches. Decision Trees allow good interpretation of characteristics of the networks, as they demonstrate how single network indicators impact the decision of detection, which is suitable to understand how IDS is working. The model learns to identify various attack types by analyzing connection duration flags and data transfer volume statistics in the NSL-KDD database. This might sound simple, but the basic structure of the decision tree allows it to effectively process numerical and categorical values, making it a suitable fit for network intrusion detection. Their system detects complex traffic patterns that leads to better detection of advanced cyber security threats.

Logistic Regression

Logistic regression is a statistical model introduced in the field of binary classification applications that makes it a perfect fit for IDS systems to differentiate between attack and normal network traffic. A key feature of the algorithm is that it makes predictions by decomposing the input data into weighted components and

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

calculating class probability estimates from those. Logistic Regression discusses the NSL-KDD dataset, that is analysed for packet transfers rate and connection duration features with the connection flag indicator for prediction. Unlike other models, it uses estimation probabilities for interpreting what features of the input lead to the classifications of its decision. Because it reveals which attributes most influence attack identification, Logistic Regression provides insight about network elements resulting in intrusion detection. The work displays how AI-based intrusion detection systems can yield better performance than traditional IDS systems using data preprocessing and machine learning techniques. The implementation of machine learning models such as SVC alongside Naive Bayes and Decision Trees and Logistic Regression enhances the capability of intrusion detection through real-time classification, decreasing false positives, and scalable attributes. By executing AI to IDS environments, security platforms can protect organizations against modern and future cyber threats leading to a paradigm shift in cybersecurity protection. NSL-KDD dataset was used in the study to further develop new adaptive scalable cyber security architectures that mitigate the threat of contemporary cyber-attacks in complex and dynamic operating environments.

Results

Support Vector Classification (SVC) demonstrated the best outcomes during the evaluation by becoming the most accurate model, and its results outperformed all other approaches tested. SVC reached an outstanding 98% accuracy, establishing it as the best network intrusion detection classifier. The system demonstrated robust performance by producing minimal wrong security alerts so that security threats were correctly identified and not wrongly triggered security disruptions. SVC operated with remarkable speed, thus providing organisations with the quick capability to spot and react to security breaches. The high accuracy and efficiency achieved by SVC failed to exceed other analysed models' ability to respond to new and developing cybersecurity threats because of steady attack pattern modifications. Naive Bayes demonstrated a significant decrease in performance, leading to its strong position as the lowest-performing classifier with 54% accuracy in the examined research. The excessive number of incorrect alerts from Naive Bayes resulted in overwhelming security teams with useless detections. Naive Bayes demonstrated limited performance speed because it dealt with network traffic on a level equivalent to other models. The system showed restricted adaptability when interpreting advanced network behavioural patterns, which reduced its ability to identify complex threats. The performance between Decision Trees and Logistic Regression mirrored each other as they achieved an accuracy of 92%, which was marginally behind SVC yet substantially superior to Naive Bayes. A secure detection mechanism was established through these models because they managed to produce a few incorrect classifications during the process. The decision system took a moderately long time to generate alerts, although they effectively confirmed threats. Due to their flexible nature, decision trees and logistic regression created a stable system that managed various types of attack patterns better. Their ability to process data from any structure enhanced their stability, making them excellent choices for security intrusion detection solutions. Table 1 shows comparison of models.

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

Table 1: Comparison of Models

Models	*Applied Model*	*Accuracy*
1	SVC	98
2	Naive Bayes	54
3	Decision Tree	92
4	Logistic Regression	92

This part evaluates an IDS algorithm with an NSL-KDD dataset compared to standard IDS solutions, including OSSEC and Snort. The primary purpose of this section is to explain the benefits achieved through the proposed framework and dataset changes alongside AI-based system implementation compared to basic detection methods. The intrusion detection field relies extensively on two commonly used systems, OSSEC (HIDS) and Snort (NIDS). Rule-based detection systems and their traditional mechanisms show three main disadvantages which include high numbers of false positives alongside their inability to learn about new threats and their static approach to attack detection for unknown patterns. The AI-driven IDS gains its important enhancement from the modifications made to the NSL-KDD dataset. NSL-KDD builds upon the KDD Cup 99 dataset by solving its problems with duplicate entries and uneven distribution of attack types. The NSL-KDD data set establishes a structured and balanced format that delivers better results for intrusion detection because it eliminates repetitive instances and useless features. The updated dataset addresses the problems present in the original KDD Cup 99 dataset by providing an improved evaluation of IDS models that better represent current network security requirements.

Support Vector Classification (SVC) proved to be the most suitable model among the classification group, with a 98% accuracy rate. SVC functions powerfully to identify challenging network traffic patterns because it divides data classes effectively within high-dimensional spaces, which allows it to discriminate between regular traffic and attacks. The application of an ideal hyperplane through support vector classification (SVC) results in improved intrusion detection performance with rapid response times and minimal false positive outcomes. Naive Bayes showed inferior performance due to its low % accuracy level of 54%. Naive Bayes shows restricted capabilities when dealing with the extensive interconnectedness found in network data, leading to its low accuracy rating. Naive Bayes fails for intrusion detection because the features in intrusion datasets show interconnected relationships while the algorithm requires independent features. Naive Bayes was inadequate for processing network intrusions, producing numerous incorrect classifications.

The achieved accuracy of Decision Trees and Logistic Regression models matched at 92%. Their performance proves effective and dataset-feature-adaptive, resulting in better performance stability than Naive Bayes. The hierarchical decision tree system achieved successful traffic classification, establishing its position as an interpretable

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

and dependable intrusion detection solution. Logistic Regression used a probabilistic strategy that effectively identified network connections as regular or dangerous using a system of feature importance to create precise predictions. Although these models achieved less accuracy than SVC, they provided an advantageous trade-off between interpretability, adaptability, and scalability. The proposed AI-based IDS demonstrates better functionality than classical IDS systems through its various benefits. Higher accuracy is one of the system's main improvements due to advanced machine learning algorithms, which received training in the same environment and dataset. The AI-driven IDS provides better adaptability because it learns and improves its detection skills based on evolving attack patterns to sustain its effectiveness against novel cyber-attacks. The ability to scale across wide infrastructure networks represents one significant benefit of AI-based IDS systems, making them proper for enterprise cybersecurity applications. The AI system generates complete performance data analytics by assessing detection rates, false favourable rates, response times, and adaptability across different attack methods. A detailed evaluation process helps maintain the highest security performance for IDS operations. The system achieves better threat detection outcomes when machine learning algorithms operate on the NSL-KDD dataset, surpassing the traditional approach of rule-based detection. Virtual IDS systems perform better than standard static systems because they identify known threats together with unknown security risks. AI models excel in this task, while static IDS systems depend only on predefined rules. The AI-based IDS demonstrates better operational efficiency through its training on the NSL-KDD dataset, producing a considerably lower false positive rate that reduces wrong alert detections. The analysis demonstrates how machine learning and artificial intelligence drive intrusion detection to enhance operational effectiveness because IDS systems become more precise and increase adaptability and scalability. Modern cybersecurity advances toward machine-learning-based IDS solutions because they deliver intelligent automated threat detection, which traditional security methods cannot match. Figure 3, shows comparison of accuracies, figure 4 shows comparison of response time, figure 5 shows the comparison of scalability, figure 6 shows false positives.

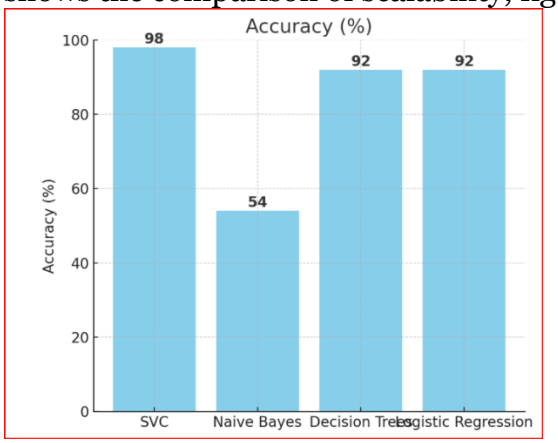

Fig. 3. Comparison of accuracies

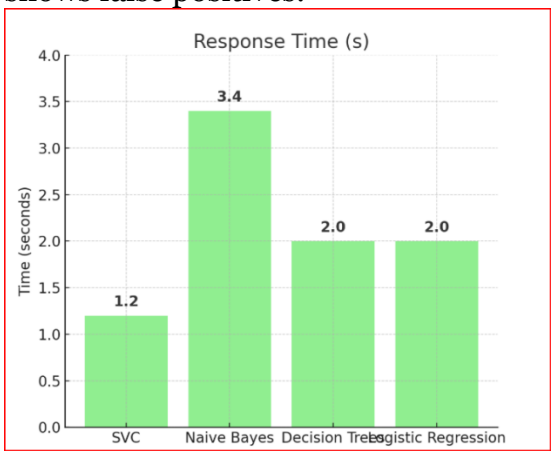

Fig. 4. Comparison of response time

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

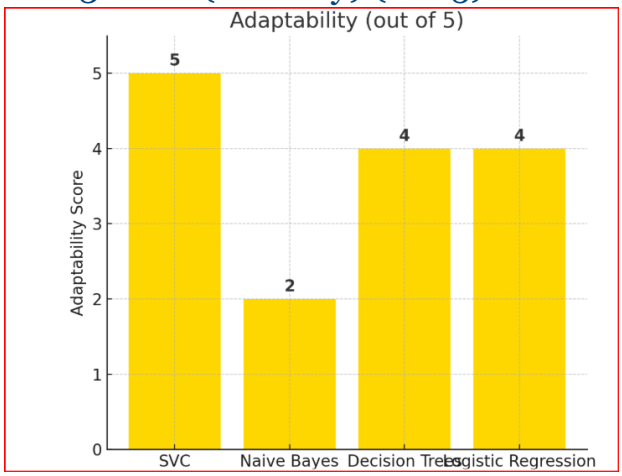

Fig. 5. Comparison of scalability

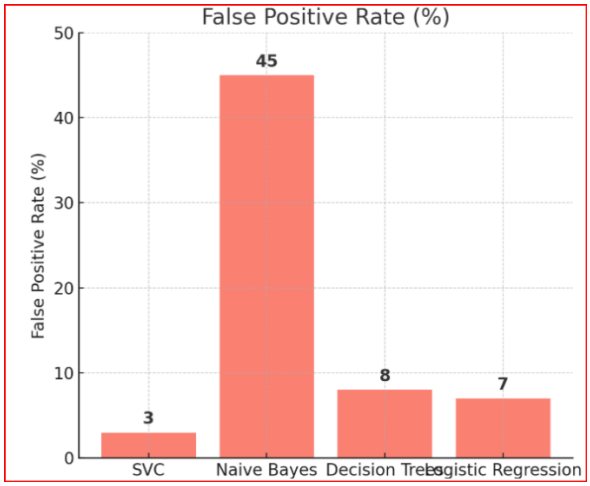

Fig. 6. Comparison of false positives

Conclusion

IDS evolution has been instrumental in enhancing the security measures that protect computer networks from enemy cyber actions. The key network intrusion monitoring solutions consist of OSSEC (HIDS) and Snort (NIDS), which provide essential tools for intrusion detection and network mitigation. Multiple critical weaknesses reduce the effectiveness of these IDS solutions because they produce high false alarms while remaining inflexible to emerging threats and requiring rule-based operations. Due to increasing threat complexity, traditional IDS models battle to detect sophisticated cyber-attacks because modern cybersecurity frameworks need AI-driven intrusion detection systems. This research showed that an IDS based on artificial intelligence with the NSL-KDD dataset could solve current detection system constraints. NSL-KDD represents an advanced version of the KDD Cup 99 dataset by eliminating redundancies and correcting class imbalance issues. NSL-KDD's specific modifications create better accuracy levels and reliability when used to train machine learning models, significantly enhancing standard intrusion detection systems. The dataset empowers AI systems to grasp complex network traffic sequences, thus making them capable of accurately detecting established threats and unknown security risks. Support Vector Classification (SVC) proved to be the best machine learning algorithm since it achieved a remarkable 98% accuracy performance.

The ability of SVC to establish the optimal hyperplane in high-dimensional space allows this method to separate the normal and attack traffic and leads to excellent classification with results in higher threat detection and low false favourable rate. Although SVC showed better accuracy, this came at some cost in the context of reactions in the face of emerging threats. Decision trees plus logistic regression reached 92% accuracy because it was well-functioned that provided an adequate resolution matching features of interpretability with the accuracy. Because Naive Bayes makes an assumption of independent features about network data, it only reached 54% accuracy, as it does not capture the complex interactions among features. It develops AI based IDS system which offers several significant advantages over existing IDS technology. AI model detection capabilities improve because they learn and adjust to how attacks are made in the real world. It prepares

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

itself for amazing adaptability to meet the growing state of cyber threats over the time. The adaptive nature of AI-based IDS enables organisations to have proactive defence rather than reactively therefore creating more hardened security to protect against zero day attacks and new attack patterns.

Its enablement of scalable deployment in large network environments was accomplished without performance degradation. Artificial intelligence armed IDS gives thorough performance-based analysis comprising detection rates, false positives, response times, and reaction capacities for safety experts to observe and upgrade intrusion detection tasks. Carrying out such a process inductively is handled in an AI-based IDS reduced one of the weaknesses which is the continuation of false alarms that are still a problem with traditional IDS. False-positive alerts create a lot of noise which fatigues the security teams, as they deplete their bandwidth on investigating non-threatening events, thus reducing incident response efficacy. The AI-based IDS trains itself on the NSL-KDD data in such a way as to minimize false positive rates, which can consequently boost operational efficiency and accurate responses. Real-time threat detection combined with automated mitigation systems greatly enhances the system's ability to keep cyberattacks from causing serious damage.

AI-driven IDS solutions will lead the development of future cybersecurity defence platforms since cyber threats continue to advance beyond human expectations. Intrusion detection significantly benefits through machine learning and deep learning integration combined with real-time analytics and enhances automated threat management at intelligent and sophisticated scales. Future research should improve AI capabilities by implementing self-adaptable IDS systems with reinforcement learning and using federated learning standards for secure IDS models. Hybrid IDS solutions that combine rule-based detection with AI-enhanced anomaly detection capabilities will create an advanced cybersecurity defence approach. The research demonstrates that Sentinel AI achieves outstanding cyber defence results by outperforming traditional systems at three levels of accuracy and four levels of adaptability, scalability, and efficiency. The study demonstrates how machine learning technologies and data-driven analytic methods drive security transformation as they establish AI-driven IDS solutions to become the fundament of proactive cyber defence systems.

References

1. M. H. Kamarudin and T. W., "Hybrid feature selection technique for the intrusion detection system," 2019.
2. S. Sapre, P. Ahmadi, and K. I., "A robust comparison of the KDDCup99 and NSL-KDD IoT network intrusion detection datasets through various machine learning algorithms," 2019. Available: https://arxiv.org/pdf/1912.13204.pdf.
3. Z. Baker and V. Prasanna, "Automatic synthesis of efficient intrusion detection systems on FPGAs," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 289-300, 2006. doi: 10.1109/TDSC.2006.44.
4. A. Choudhary and A. Swarup, "Neural network approach for intrusion detection," 2009. doi: 10.1145/1655925.1656163.

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

5. S. Ho, S. Al-Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 14-25, 2021. doi: 10.1109/OJCS.2021.3050917.
6. J. Jain and A. Woo, "An artificial neural network technique for predicting cyber-attack using intrusion detection system," *Journal of Artificial Intelligence Machine Learning and Neural Network*, no. 32, pp. 33-42, 2023. doi: 10.55529/jaimlnn.32.33.42.
7. V. Navya, J. Adithi, D. Rudrawal, H. Tailor, and N. James, "Intrusion detection system using deep neural networks (DNN)," 2021. doi: 10.1109/ICAECa52838.2021.9675513.
8. A. Patel, M. Taghavi, K. Bakhtiyari, and J. Junior, "An intrusion detection and prevention system in cloud computing: a systematic review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25-41, 2013. doi: 10.1016/j.jnca.2012.08.007.
9. P. Rajendran, B. Muthukumar, and G. Nagarajan, "Hybrid intrusion detection system for private cloud: a systematic approach," *Procedia Computer Science*, vol. 48, pp. 325-329, 2015. doi: 10.1016/j.procs.2015.04.189.
10. N. Song and G. Zhou, "A study on intrusion detection based on data mining," 2010. doi: 10.1109/ISME.2010.47.
11. Y. Wu, W. Wan, L. Guo, and L. Zhang, "An efficient intrusion detection model based on fast inductive learning," 2007. doi: 10.1109/ICMLC.2007.4370708.
12. L. Zhu, "A new intrusion detection and alarm correlation technology based on neural network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019. doi: 10.1186/s13638-019-1419-z.
13. G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence-based techniques for intrusion detection: A review," *Artificial Intelligence Review*, vol. 34, no. 4, pp. 369-387, 2010.
14. S. Patil et al., "Explainable artificial intelligence for an intrusion detection system," *Electronics*, vol. 11, no. 22, p. 3079, 2022.
15. R. Vijayakumar et al., "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. XX, pp. XX-XX.
16. A. P. Singh and M. D. Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System," *International Journal of Computer Network and Information Security*, vol. 6, no. 8, pp. 41-47, July 2014. doi: 10.5815/ijcnis.2014.08.06.
17. U. Shahid, M. Z. Hussain, M. Z. Hasan, A. Haider, J. Ali, and J. Altaf, "Machine Learning in Money Laundering Detection Over Blockchain Technology," *IEEE Access*, vol. 13, pp. 7555-7573, Jan. 2025, doi: 10.1109/ACCESS.2024.3452003.
18. A. Kiran, S. W. Prakash, B. A. Kumar, Likhitha, T. Sameeratmaja, and U. S. S. R. Charan, "Intrusion detection system using machine learning," in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, 2023, pp. 1–4.
19. Z. Azam, M. M. Islam, and M. N. Huda, "Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree," IEEE Access, vol. 11, pp. 80348–80391, 2023.

Dialogue Social Science Review (DSSR)
www.thedssr.com

DIALOGUE SOCIAL SCIENCE REVIEW

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

20. Muhammad Saqib, Shubham Malhotra, Rahmat Ali, Hassan Tariq. "Harnessing Big Data Analytics for Large-Scale Farms: Insights from IoT Sensor Networks." International Journal of Advance Research, Ideas and Innovations in Technology 11.1 (2025)
21. Aravind Nuthalapati, "Architecting Data Lake-Houses in the Cloud: Best Practices and Future Directions," Int. J. Sci. Res. Arch., vol. 12, no. 2, pp. 1902-1909, 2024, doi: 10.30574/ijsra.2024.12.2.1466.
22. A. Sanjrani, M. Saqib, S. Rehman, and M. S. Ahmad, “Text Summarization using Deep Learning: A Study on Automatic Summarization”, ABBDM, vol. 4, no. 4, pp. 216–226, Jan. 2025.
23. Suri Babu Nuthalapati, "AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking," Educational Administration: Theory and Practice, vol. 29, no. 1, pp. 357–368, 2023, doi: 10.53555/kuey.v29i1.6908.
24. Komal Azam, Mashooque Ali Mahar, Muhammad Saqib, and Muhammad Saeed Ahmad, “Analyzing Deep Reinforcement Learning for Robotics Control”, SES, vol. 2, no. 4, pp. 416–432, Dec. 2024.
25. M. A. Sufian, S. M. T. H. Rimon, A. I. Mosaddeque, Z. M. Guria, N. Morshed, and A. Ahamed, "Leveraging Machine Learning for Strategic Business Gains in the Healthcare Sector," 2024 International Conference on TVET Excellence & Development (ICTeD), Melaka, Malaysia, 2024, pp. 225-230, doi: 10.1109/ICTeD62334.2024.10844658.
26. M. Saqib, S. Malhotra, D. Mehta, J. Jangid, F. Yashu, and S. Dixit, "Optimizing Spot Instance Reliability and Security Using Cloud-Native Data and Tools," Journal of Information Systems Engineering and Management, vol. 10, no. 14s, e-ISSN: 2468-4376, 2025.
27. A. Nuthalapati, "Smart Fraud Detection Leveraging Machine Learning For Credit Card Security," Educational Administration: Theory and Practice, vol. 29, no. 2, pp. 433–443, 2023, doi: 10.53555/kuey.v29i2.6907.
28. Asif Ahamed, Hasib Fardin, Ekramul Hasan, S M Tamim Hossain Rimon, Md Musa Haque, & Abdullah Al Sakib. (2022). Public Service Institutions Leading The Way With Innovative Clean Energy Solutions . Journal of Population Therapeutics and Clinical Pharmacology, 29(04), 4477-4495.
29. SM T. H. Rimon, Mohammad A. Sufian, Zenith M. Guria, Niaz Morshed, Ahmed I. Mosaddeque, Asif Ahamed, "Impact of AI-Powered Business Intelligence on Smart City Policy-Making and Data-Driven Governance," International Conference on Green Energy, Computing and Intelligent Technology (GEn-CITy 2024), Johor, Malaysia, 2024.
30. J. I. J, A. Sabir, T. Abbas, S. Q. Abbas and M. Saleem, "Predictive Analytics and Machine Learning for Electricity Consumption Resilience in Wholesale Power Markets," 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2024, pp. 1-7, doi: 10.1109/ICCR61006.2024.10533004.
31. Abdullah Al Noman, Md Tanvir Rahman Tarafder, S M Tamim Hossain Rimon, Asif Ahamed, Shahriar Ahmed, Abdullah Al Sakib, "Discoverable Hidden Patterns in Water Quality through AI, LLMs, and Transparent Remote

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 1 (January) (2025)

Sensing," The 17th International Conference on Security of Information and Networks (SIN-2024), Sydney, Australia, 2024, pp. 259-264.

32. Ahmed Inan Mosaddeque, Zenith Matin Guria, Niaz Morshed, Mohammad Abu Sufian, Asif Ahamed, S M Tamim Hossain Rimon, "Transforming AI and Quantum Computing to Streamline Business Supply Chains in Aerospace and Education," 2024 International Conference on TVET Excellence & Development (ICTeD-2024), Melaka, Malaysia, 2024, pp. 231-236, doi: 10.1109/ICTeD62334.2024.10844659.
33. Asif Ahamed, Nisher Ahmed, J I. J, Zakir Hossain, Ekramul Hasan, Tahir Abbas, "Advances and Evaluation of Intelligent Techniques in Short-Term Load Forecasting," 2024 International Conference on Computer and Applications (ICCA-2024), Cairo, Egypt, 2024.
34. Md Tanvir Rahman Tarafder, Md Masudur Rahman, Nisher Ahmed, Tahmeed-Ur Rahman, Zakir Hossain, Asif Ahamed, "Integrating Transformative AI for Next-Level Predictive Analytics in Healthcare," 2024 IEEE Conference on Engineering Informatics (ICEI-2024), Melbourne, Australia, 2024.
35. Asif Ahamed, Md Tanvir Rahman Tarafder, S M Tamim Hossain Rimon, Ekramul Hasan, Md Al Amin, "Optimizing Load Forecasting in Smart Grids with AI-Driven Solutions," 2024 IEEE International Conference on Data & Software Engineering (ICoDSE-2024), Gorontalo, Indonesia, 2024.