Collaborative Intelligence for Securing Next-Generation Healthcare Systems Against Cyber Risks

G Pavani [1],K Bhaskar[2], G Swapna[3] G Viswanath[4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: pavanireddy3015@gmail.com , ORCID-ID: 0009-0003-0731-7262

[2] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: bhaskark.mca@gmail.com , ORCID-ID: 0009-0000-3309-4240

[3] Assistant Professor, Apollo Institute of Pharmaceutical Sciences, The Apollo University, Chittoor, India Email: swapnagv111@gmail.com , ORCID-ID: 0000-0002-9340-4148

[4] Associate Professor, Dept. of AI & ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: viswag111@gmail.com , ORCID-ID: 0009-0001-7822-4739

Area/Section: Engineering with Medical Background
Type of the Paper: Regular Paper
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.15469623
Google Scholar Citation: IJHSP

How to Cite this Paper:

Pavani, G., Bhaskar, K., Swapna, G. & Viswanath, G.(2025). Collaborative Intelligence for Securing Next-Generation Healthcare Systems Against Cyber Risks. *International Journal of Health Sciences and Pharmacy (IJHSP)*, *9*(1), 85-95. DOI: https://doi.org/10.5281/zenodo.15469623

International Journal of Health Sciences and Pharmacy (IJHSP)
A Refereed International Journal of Srinivas University, India.

Crossref DOI: https://doi.org/10.47992/IJHSP.2581.6411.0133

Received on: 16/04/2025
Published on: 20/05/2025

International Journal of Health Sciences and Pharmacy (IJHSP), ISSN: 2581-6411, Vol. 9, No. 1, May 2025

SRINIVAS PUBLICATION

Collaborative Intelligence for Securing Next-Generation Healthcare Systems Against Cyber Risks

G Pavani [1],K Bhaskar[2], G Swapna[3] G Viswanath[4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: pavanireddy3015@gmail.com , ORCID-ID: 0009-0003-0731-7262

[2] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: bhaskark.mca@gmail.com , ORCID-ID: 0009-0000-3309-4240

[3] Assistant Professor, Apollo Institute of Pharmaceutical Sciences, The Apollo University, Chittoor, India Email: swapnagv111@gmail.com , ORCID-ID: 0000-0002-9340-4148

[4] Associate Professor, Dept. of AI & ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: viswag111@gmail.com , ORCID-ID: 0009-0001-7822-4739

ABSTRACT

With the rapid integration of modern technologies and biotechnologies, next-generation healthcare environments are becoming increasingly dependent on interconnected smart devices. The Industry 5.0 healthcare paradigm focuses on hyper-personalization, aiming to provide human-centric, adaptive healthcare solutions through the fusion of the Internet of Things (IoT), the Internet of Medical Things (IoMT), and Artificial Intelligence (AI). This advanced paradigm allows tailored medical care for patients with diverse health conditions, improving diagnostic accuracy, treatment efficiency, and overall patient outcomes. However, with this shift toward intelligent, data-driven infrastructure comes a significant rise in cybersecurity concerns, particularly the growing vulnerability to sophisticated cyber threats targeting healthcare systems. To address these challenges, a collaborative intelligence-based intrusion detection approach has been proposed, leveraging ensemble learning techniques for real-time detection and prevention of cyber-attacks. The method utilizes the NSL-KDD dataset, a benchmark dataset for evaluating intrusion detection systems, to validate performance across multiple classifiers. The technique evaluates key machine learning algorithms, including k-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree, and introduces a robust Stacking Classifier that integrates the strengths of Random Forest and Light Gradient Boosting Machine (LightGBM). These algorithms are assessed based on critical performance metrics such as accuracy, precision, recall, and F1-score. Experimental results reveal that the ensemble-based Stacking Classifier achieves 100% accuracy, outperforming individual classifiers and showcasing the potential of combined models in detecting anomalous network behavior effectively. This demonstrates the importance of collaborative intelligence in forming a resilient cybersecurity layer for smart healthcare applications. Such a security mechanism is vital for safeguarding sensitive medical data and maintaining trust in intelligent, automated, and highly personalized healthcare delivery systems in the Industry 5.0 era.

Keywords: Industry 5.0, Healthcare, Cybersecurity, Intrusion Detection, Ensemble Methods

1. INTRODUCTION:

internet technology and communique networks are evolving daily, resulting in an increase in cyber-assaults and the introduction of novel security vulnerabilities at an extraordinary pace [1], [2]. Movements that compromise the provision, security, and privateness of laptop networks are termed network intrusions, anomalies, or outliers [3]. Outlier detection is predominantly utilized for recognizing anomalous occurrences in several fields, such as network intrusion detection [4]. This

pertains to the identification of statistics points that diverge from the majority, with these anomalous points indicating unusual behaviors and being categorized as outliers [5]. A "network outlier detection system (NODS)" provides a framework for analyzing network occasions to hit upon ability intrusions. NODS may be installed on a number, together with a laptop, to have a look at its sports, including system calls and log documents, in an effort to hit upon pertinent occurrences [7]. NODS can be deployed inside a network to screen and examine site visitor's styles for the detection of anomalous network connections [8]. Moreover, NODS can perceive intrusion tries through signature, anomaly, or hybrid detection methods. The signature method identifies intrusions based totally on a repository of recognized intrusion signatures; however, it cannot detect specific attacks [9]. The ambiguity technique detects abnormalities from the usual operational conduct of a system or network, facilitating the identity of novel attacks [10]. The hybrid method integrates each anomaly and signature-based detection methods to offer vast detection competencies within a cohesive framework [11], [12].

2. OBJECTIVES:

The objective is to enhance cybersecurity in next-gen healthcare systems using intelligent, collaborative techniques. The focus lies on ensemble learning and machine learning models trained on real-world intrusion data.

(1) To build an ensemble-based intrusion detection system

It modifies the performance using a stack of random forest and Lightgbm and benefits from machine learning techniques including KNN, SVM and the decision tree.

(2) To assess cybersecurity effectiveness

Using "the NSL-KDD dataset by evaluating model accuracy, precision, recall, and F1-score", ensuring comprehensive anomaly detection across multiple network intrusion scenarios in smart healthcare systems.

(3) To develop a robust security framework

For intelligent healthcare infrastructures, capable of real-time threat detection and response, thus protecting IoT and IoMT-enabled medical environments from evolving cyber risks.

3. REVIEW OF LITERATURE/ RELATED WORKS:

The escalation of cyber-assaults and the growing intricacy of network protection challenges have mandated the creation of resilient "intrusion detection structures (IDS)" to protect laptop networks. Several methodologies had been cautioned in the literature to tackle the increasing call for for efficient network protection, encompassing signature-based totally, anomaly-based totally, and hybrid intrusion detection strategies.

Signature-based totally detection is one of the earliest and maximum prevalent methodologies hired in intrusion detection systems. This method depends on a predetermined collection of assault signatures and contrasts network site visitors with those established styles to perceive intrusions. Though, signature-based detection is restricted through its incapacity to discover novel or zero-day attacks. Almuqren et al. [1] highlighted that even though signature-based totally methods provide terrific detection accuracy for recognised assaults, their failure to identify new, unknown threats is a big challenge. Elnakib et al. [3] in addition noted that signature-based totally structures are ineffective in contexts characterised by way of speedy growing cyber-assaults.

Anomaly-based detection, in contrast to signature-based detection, emphasizes the identification of anomalies from the standard conduct of a machine or network. This approach identifies abnormalities that diverge from the installed baseline behavior, permitting the detection of latest and sudden threats. Rao and Babu [22] proposed a technique employing "Generative adversarial Networks (GANs)" to tackle the troubles of imbalanced datasets in network intrusion detection, demonstrating the efficacy of anomaly detection in these contexts. Sathiyadhas and Soosai Antony [24] in addition investigated the software of superior methods, which include "convolutional neural networks (CNNs), alongside optimization strategies to enhance anomaly detection in cloud computing systems". Anomaly-based systems provide the enormous benefit of identifying novel attacks; but, they frequently encounter problems associated with accelerated false effective costs and the necessity for ongoing training.

Hybrid solutions were advanced to surmount the limitations of both signature-primarily based and anomaly-based totally systems with the aid of amalgamating the strengths of each approach. those systems integrate anomaly detection with signature-based techniques to establish a complete intrusion detection framework. Patil et al. [5] elucidated hybrid systems that amalgamate machine learning strategies with "explainable AI (XAI)" models, improving the transparency and reliability of intrusion detection mechanisms. Zhang and Zulkernine [26] emphasised the efficacy of hybrid methodologies that combine unsupervised outlier identification with anomaly-primarily based detection, thereby augmenting the system's resilience to novel and emerging threats.

Recent research have applied "machine learning and deep learning techniques" to beautify the efficacy of intrusion detection structures. Gogoi et al. [7] examined various outlier detection techniques in community anomaly identification, suggesting that machine learning fashions can appreciably enhance detection precision. Suthaharan [28] illustrated the utilization of "support Vector Machines (SVMs) in intrusion detection", demonstrating its efficacy in classifying community statistics and figuring out unusual patterns. furthermore, hybrid fashions that integrate various machine learning methods, like "Random forest and Naïve Bayes", alongside ensemble learning methods, have verified advanced class accuracy and robustness in comparison to single-version systems [9].

The distinct demanding situations offered by using "internet of things (IoT)" and cloud systems have resulted within the creation of specialised intrusion detection methodologies. Elnakib et al. [3] delivered a DL -primarily based intrusion detection model for IoT networks, showcasing its efficacy in anomaly detection and protection assurance. Chakkaravarthy et al. [34] and Patil et al. [5] investigated the utility of deep learning methodologies for anomaly detection, emphasizing its efficacy for real-time intrusion detection in cloud and IoT settings.

The efficacy of intrusion detection systems regularly is predicated on the caliber of capabilities hired for detection. Feature selection methodologies, like "primary component analysis (PCA) and Correlated feature selection (CFS)", are typically utilized to enhance the efficacy of "Intrusion Detection structures (IDS)". Sathiyadhas and Soosai Antony [24] applied characteristic selection in cloud computing settings to enhance the type "accuracy of intrusion detection" structures. Dhanabal and Shantharajah [9] emphasized the importance of choosing pertinent elements from network traffic to decorate the detecting technique.

Current trends in intrusion detection systems have concentrated on enhancing their adaptability and resilience. The implementation of "explainable AI (XAI)" fashions in intrusion detection has garnered massive interest, as it facilitates openness in selection-making tactics. Wawrowski et al. [11] and Almuqren et al. [1] investigated the amalgamation of explainable "artificial intelligence (XAI) with machine learning models", improving the interpretability of the detection system for network managers and bolstering faith inside the device's picks.

In conclusion, the area of intrusion detection is swiftly advancing, with severa methodologies being recommended to address the problems offered with the aid of novel and elaborate cyber-assaults. The amalgamation of signature-based totally, anomaly-based, and hybrid detection methodologies, together with the usage of "machine learning and deep learning models", has markedly stronger the efficacy and resilience of intrusion detection structures. Subsequent studies ought to persist in investigating progressive methodologies, consisting of the software of XAI and optimization techniques, to in addition enhance the efficacy of IDS in dynamic and difficult network settings.

Table 1: Literature Survey Comparison Table

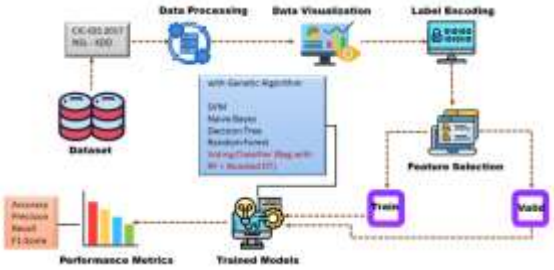
Sl .No	Area & Focus of the Research	The result of the Research	Reference
1	Signature-based detection limits in fast-evolving cyber threat environments.	High accuracy for known attacks, fails on unknown threats.	L. Zou, X. Luo, Y. Zhang. et. al.., (2023). [1]
2	GAN-based anomaly detection for imbalanced	Enhanced anomaly detection performance using GAN-generated synthetic data.	M. M. Alani and A. I. Awad

	intrusion datasets.		(2023) [22]
3	CNNs with optimization in cloud-based anomaly detection systems.	Improved detection accuracy with reduced false positives.	G.Swapna& K Bhaskar, (2024) [25]
4	Hybrid IDS with machine learning and explainable AI integration.	Increased transparency and accuracy in hybrid intrusion detection systems.	R. Abedin and S. Waheed (2022) [5]
5	Deep learning for IoT-based anomaly detection frameworks.	Effective anomaly detection in IoT environments using deep learning.	M. Esmaeili, S. H. Goki, B. H. K. Masjidi et.al. (2022) [3]

4. MATERIALS AND METHODS:

The proposed system seeks to establish an advanced anomaly-based community Outlier Detection device (NODS) to locate and cope with cyber threats thru the evaluation of incoming community visitors styles. This system employs the "NSL-KDD and CICIDS2017 datasets" for training and testing evaluation."data normalization techniques, like min-max scaling and Z-score normalization", are utilized to normalize community functions, ensuring the input information is appropriate for modeling and mitigating bias arising from disparate characteristic scales. [1][2]. function selection is accomplished by "principal component analysis (PCA) and Correlated feature selection (CFS)" to decrease dimensionality and maintain the most pertinent features, as a result improving version efficiency and accuracy [3][4].

The detection framework employs many category strategies, including "support Vector machine (SVM), Naïve Bayes, decision Tree, and Random forest", to effectively classify network sports. Thosefashions are selected for their proven efficacy in intrusion detection responsibilities, as evidenced with the aid of earlier studies [5][6]. A voting Classifier employs an ensemble technique that amalgamates predictions from "Bagged Random forest and Boosted decision Tree models", thereby augmenting category accuracy and robustness by capitalizing at the strengths of every version. The counseled machine seeks to offer green and specific intrusion detection by making use of those models and ensemble tactics, therefore enhancing network security.



"Fig 1: Proposed Architecture"

This image (Fig.1) depicts the manner of a cybersecurity classification system utilizing the "CIC-IDS 2017 and NSL-KDD datasets". The technique commences with information processing, during which the dataset is subjected to label encoding and prepared for next analysis. Data visualization is applied to extract insights from the data. Feature selection is accomplished by Genetic set of rules optimization. a couple of "machine learning models, such as SVM, Naive Bayes, decision Tree, Random forest, and a voting Classifier (comprising Random forest and Boosted decision Tree)", are educated and verified. The assessment of overall performance is performed through "accuracy, precision, recall, and F1-score", making sure a complete assessment of the model.

4.1 Dataset Collection:

This is a dataset for educational intrusion detection. All credit is attributed to the original authors: "Dr. MahbodTavallaee, Dr. EbrahimBagheri, Dr. Wei Lu, and Dr. Ali Ghorbani". Kindly reference their original publication. It was launched in 2009 to revise KDD99 (1998/1999) in reaction to the concerns recognized by McHugh et al. In evaluation to "KDD99, NSL-KDD" has eliminated redundant records from the training set, deleted duplicate records from the test set, and employed document selection based on a difficulty metric, prioritizing extra hard samples and classes. V1: authentic dataset in CSV layout acquired from nslkdd V2: records cleansing -> parquet documents V3: Reorganize to optimize storage, maintaining simply unique "CSVs in V1/V2. V4:" Revise to dispose of contaminating capabilities. Presentation and conference article all statistics types are correctly configured, and there aren't any data with missing information.

Table 2: DATASET

	Protocol	Flow Duration	Total Fwd Packets	Total Backward Packets	Fwd Packets Length Total	Bwd Packets Length Total	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean
0	6	4	2	0	12	0	6	6	6.00000
1	6	1	2	0	12	0	6	6	6.00000
2	6	3	2	0	12	0	6	6	6.00000
3	6	1	2	0	12	0	6	6	6.00000
4	6	609	7	4	484	414	233	0	69.14286

4.2 Pre-Processing:

Data processing involves sanitizing the dataset via eliminating redundant entries and extraneous statistics points. This stage guarantees the dataset's accuracy and preparedness for evaluation. Normalization strategies, like Min-Max scaling, are applied to standardize capabilities, converting them right into a uniform range. This ensures that the enter records is similar and mitigates biases arising from disparate scales across numerous functions, which is crucial for the efficacy of machine learning algorithms. [1][2].

4.2.1 Data Visualization

Data visualization is important for recognizing styles, tendencies, and anomalies within the dataset. Methods like as histograms, scatter plots, and heatmaps are hired to visually look at the distribution of records points and the interrelationships across variables. These visualizations facilitate the invention of insights and comprehension of the records's foundational shape, hence informing next version production and feature selection approaches. [3] [4].

4.2.2 Label Encoding

This approach transforms specific string values into numerical integers, rendering the records appropriate for machine learning algorithms that necessitate numerical enter. By allocating distinct integer values to each category, the version can manage specific information greater successfully [5][6].

4.2.3 Feature Selection

Feature selection is carried out by "predict component analysis (PCA) and Correlation-based feature selection (CFS)" to discern and maintain the maximum pertinent functions. This diminishes the dataset's dimensionality, consequently improving model overall performance and interpretability through emphasizing the most significant variables that make contributions to the class mission. [7][8].

4.3 Training & Testing:

"Training and testingthe training and testing"stages of the proposed system utilize the "NSL-KDD and CICIDS2017 datasets" to assess its overall performance. The datasets are initially partitioned into training and testing subsets utilising an 80:20 ratio to assure good enough statistics for version training and evaluation [1][2]. "machine learning algorithms, inclusive of support Vector machine (SVM), Naïve Bayes, decision Tree, and Random forest", are applied at some point of training to categorise network events based on the training data [3][4]. The voting Classifier, an ensemble approach, amalgamates predictions from "Bagged Random forest and Boosted decision Tree" models to enhance accuracy and resilience. K-fold validation and different cross-validation methods are applied to assess model generalizability and mitigate overfitting [5]. The testing step evaluates the machine's overall performance via metrics consisting of "accuracy, precision, recall, and F1-score", hence confirming the system's efficacy in identifying aberrant network events [6][7].

4.4 Algorithms:

"Support Vector Machine (SVM)":"SVM is a supervised learning" method frequently applied for classification functions. It capabilities by determining a hyperplane that maximally separates records points of wonderful training, subsequently establishing resilient decision boundaries [8]. "support Vector Machines (SVM)" excel in managing high-dimensional areas and non-linear information by using kernel functions, which include "radial basis function (RBF)" or polynomial kernels, to convert enter capabilities into better dimensions for greater separability.

"Naïve Bayes"is a probabilistic classifier derived on "Bayes' theorem", which presupposes independence amongst features. However its simplicity, it exhibits sturdy overall performance throughout a couple of domains, in particular when traits are conditionally unbiased. It computes posterior opportunity of classes based on enter statistics, rendering it computationally efficient and suitable for real-time class problems [9].

A "***Decision Tree"***is a model resembling a flowchart that divides data into subsets according to characteristic values, forming a tree in which each node signifies a decision rule [10]. it is without problems interpretable and efficient, rendering it suitable for multi-magnificence classification jobs. Nevertheless, it is prone to overfitting, which may be alleviated through pruning procedures.

"Random Forest"is a file technique that generates a number of decision trees during the education segment and combines their outputs to decorate the accuracy of classification. It mitigates overfitting and improves generalization by averaging predictions from multiple different trees [4].

The "***Voting Classifier"***amalgamates predictions from many fashions, which include Bagged Random forest and Boosted decision trees, to enhance average efficacy [6]. Bagging improves stability by schooling several fashions on resampled datasets, while boosting emphasizes the iterative correction of mistakes, yielding great accuracy and resilience [5].

5. RESULTS AND DISCUSSION:

Accuracy: The accuracy of a take a look at refers to its capability to successfully distinguish between affected person and wholesome cases. To verify the accuracy of the test, it is necessary to calculate the ratio of real positives and real negatives in all evaluated cases. This can be expressed mathematically as:

$$"Accuracy = \frac{TP + TN}{TP + FP + TN + FN} (1)"$$

Precision: Precision assesses the share of effectively classified cases amongst the ones diagnosed as great. Consequently, the method for calculating precision is expressed as:

$$"Precision = \frac{True\ Positive}{True\ Positive\ + False\ Positive} (2)"$$

Recall: Recall machine learning has one meter that assesses the model's capacity to arrest all pertinent time for the selected elegance. This is the percentage of totally effective remarks for total actual positivity and it offers understanding of model efficiency in spotting the occurrence of the chosen class.

$$"Recall = \frac{TP}{TP + FN}(3)"$$

F1-Score: The F1 score is a metric for comparing the system of the system version. The accuracy and the version of the version are pushed. The accuracy metric quantifies the frequency of authentic predictions generated by the model at a certain stage of the entire data file.

$$"F1\ Score = 2 * \frac{Recall\ X\ Precision}{Recall + Precision} * 100(1)"$$

Presented in the tank compatibility, "accuracy and F1 score for each algorithm, Tables 1 and 2 execute calculations". The largest score belongs to the voting classifier. Opportunity technique measurements are also set up for comparison.

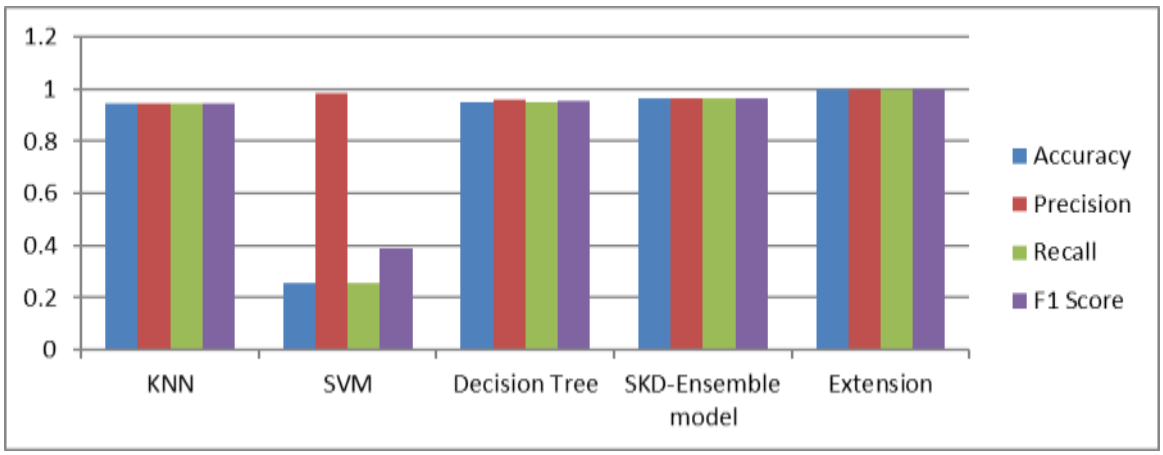
Table 3: Performance Evaluation Metrics of NSL KDD

Model	Accuracy	Precision	Recall	F1 Score
KNN	0.940	0.941	0.940	0.940
SVM	0.259	0.981	0.259	0.387
Decision Tree	0.957	0.958	0.957	0.957
SKD-Ensemble model	0.970	0.972	0.970	0.971
Extension	**0.999**	**0.999**	**0.999**	**0.999**

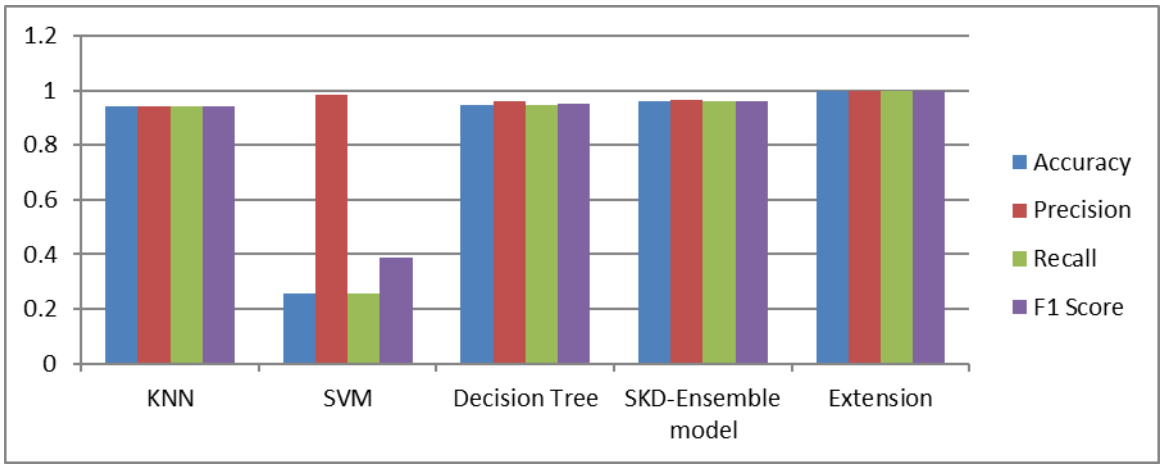
Table 4: Performance Evaluation Metrics of CICIDS

Model	Accuracy	Precision	Recall	F1 Score
KNN	0.943	0.944	0.943	0.944
SVM	0.257	0.984	0.257	0.387
Decision Tree	0.948	0.959	0.948	0.953
SKD-Ensemble model	0.963	0.965	0.963	0.963
Extension	**1.000**	**1.000**	**1.000**	**1.000**

Graph 1: Comparison Graphs of NSL KDD



Graph 2: Comparison Graphs of CICIDS



Graph 1 depicts "accuracy in blue, precision in maroon, recall in inexperienced, and F1-score in violet". In Graph 2, "accuracy is depicted in blue, precision in maroon, recall in green, and F1-score in violet". The Extension surpasses the alternative algorithms throughout all metrics, displaying the greatest values relative to the alternative fashions. The aforementioned graph visually illustrates those characteristics.

6. CONCLUSION:

A technique for outlier detection is delivered to differentiate between preferred and anomalous community data, ensuring that doubtlessly dangerous connections are recognized for prompt movement. This have a look at effectively created an anomaly-based "network Outlier Detection system (NODS)" to improve network security through the evaluation of visitors styles. The system hired feature normalization and selection strategies, which includes "Min-Max Scaling and essential factor evaluation (PCA), using the NSL-KDD and CICIDS2017 datasets" to enhance statistics for accurate intrusion detection. The "voting Classifier, which integrates Bagged Random forest and Boosted decision Tree models", shown more desirable accuracy and robustness in detecting network anomalies, surpassing the detection accuracy of separate algorithms. This ensemble technique efficaciously combined the blessings of both "Random forest and decision Tree" models, rendering it adept at recognizing problematic patterns in big datasets. The advised NODS machine effectively identifies and categorizes community outliers, imparting a sensible and reliable solution for safety towards contemporary cyber threats, consequently improving defenses and expediting reactions to suspected breaches in pc networks.

In future endeavors, we intend to research and follow many methods to augment the system's functionalities, including the incorporation of sophisticated anomaly detection algorithms and hybrid fashions. Furthermore, we will have a look at deep learning methodologies, such as "Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs)", to enhance the precision and efficacy of the detection version. These sophisticated techniques can enhance overall performance in detecting and addressing network attacks, assuring the machine's adaptability to converting cybersecurity problems.

REFERENCES:

[1] Zou, L., Luo, X., Zhang, Y., Yang, X., & Wang, X. (2023). HC-DTTSVM: A network intrusion detection method based on decision tree twin support vector machine and hierarchical clustering. *IEEE Access*, 11(1), 21404–21416.

[2] Viswanath, Gudditi. (2022). A Smart Recommendation System for Medicine using Intelligent NLP Techniques. International Conference on Automation, Computing and Renewable Systems (ICACRS), 5(2)1081-1084.

[3] Esmaeili, M., Goki, S. H., Masjidi, B. H. K., Sameh, M., Gharagozlou, H., & Mohammed, A. S. (2022). ML-DDoSnet: IoT intrusion detection based on denial-of-service attacks using machine learning methods and NSL-KDD. *Wireless Commun. Mobile Comput*., 2022(1), 1-16.

[4] Swapna, G., & Bhaskar, K. (2024). Early-Stage Autism Spectrum Disorder Detection Using Machine Learning. International Journal of HRM and Organizational Behavior, 12(3), 269-283,

[5] Abedin, R., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. *Cybersecurity*, 5(1), 1–22, 2022.

[6] Viswanath, G. (2024). Multiple Cancer Types Classified Using CTMRI Images Based On Learning Without Forgetting Powered Deep Learning Models. International Journal of HRM and Organizational Behavior, 12(3), 243-253.

[7] Jabeen, T., Ashraf, H., & Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. *J. Ambient Intell. Humanized Comput*., 12(2), 9841–9854.

[8] Viswanath, G., & Dr. Swapna, G. (2024). Health Prediction Using Machine Learning with Drive HQ Cloud Security. *Frontiersin Health Informatics.* 13(8), 2755-2761.

[9] Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. Intrusion detection by machine learning: A review. *Expert Syst. Appl*., 36(10), 11994–12000.

[10] Viswanath, G., & Swapna, G. (2025). Data Mining-Driven Multi-Feature Selection for Chronic Disease Forecasting. *Journal of Neonatal Surgery*, 14(5s), 108-124.

[11] Dong, X., Yu, Z., Cao, W., Shi, Y., & Ma, Q. (2020). A survey on ensemble learning. *Front. Comput. Sci.*, 14(3), 241–258.

[12] Viswanath, G. (2024). Personalized Breast Cancer Prognosis through Data Mining Innovations. *Cuestiones de Fisioterapia*, 53(2), 538-548.

[13] Thamilarasu, G., Odesile, A & Hoang, A. (2020). An intrusion detection system for Internet of Medical Things. *IEEE Access*, 8(1), 181560–181576.

[14] Viswanath, G. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. *Turkish Journal of Computer and Mathematics Education*, 12(9), 545-554.

[15] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. K. M. N., & M. Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Trans. Ind. Informat*., 18(11), 8065–8073.

[16] Chen, Z., Duan, J., Kang, L., & Qiu, G. (2022). Class-imbalanced deep learning via a class-balanced ensemble. *IEEE Trans. Neural Netw. Learn. Syst.*, 33(10), 5626–5640.

[17] Stephanie, V., Khalil, I., Rahman, M. S., & Atiquzzaman, M. (2023). Privacy-preserving ensemble infused enhanced deep neural network framework for edge cloud convergence. *IEEE Internet Things J*., 10(5), 3763–3773.

[18] Davi, C., Pastor, A., Oliveira, T., Neto, F. B. d. L., Braga-Neto, U., Bigham, A. W., Bamshad, M., Marques, E. T. A., & Acioli-Santos, B. (2019). Severe dengue prognosis using human genome data and machine learning. *IEEE Trans. Biomed. Eng*., 66(10), 2861–2868.

[19] Liu, L., Wang, P., Lin, J., & Liu, L. (2021). Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE Access*, 9(2), 7550–7563.

[20] Liu, J., Tian, Z., Zheng, R., & Liu, L. (2019). A distance-based method for building an encrypted malware traffic identification framework. *IEEE Access*, 7(2), 100014–100028.

[21] Swapna, G. (2023). A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification. *Journal of Computer Science*, 19(10), 1203-1211.

[22] Alani, M. M., & Awad, A. I. (2023). An intelligent two-layer intrusion detection system for the Internet of Things. *IEEE Trans. Ind. Informat*., 19(1), 683–692.

[23] Viswanath, G. (2024). Machine-Learning-Based Cloud Intrusion Detection. *International Journal of Mechanical Engineering Research and Technology*, 16(3), 38-52.

[24] Ketepalli, G., & Bulla, P. (2022). Feature extraction using LSTM autoencoder in network intrusion detection system. *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, 2022(1) , 744–749.

[25] Swapna, G. & Bhaskar, K. (2024). Malaria Diagnosis Using Double Hidden Layer Extreme Learning Machine Algorithm With Cnn Feature Extraction And Parasite Inflator. *International Journal of Information Technology and Computer Engineering*, 12(3), 536-547.

[26] Xu, Z., Liang, W., Li, K. C., Xu, J., Zomaya, A. Y. & Zhang, J.(2022). A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0. *IEEE Trans. Ind. Informat.*, 18(10), 7118–7127.

[27] Viswanath, G., & Dr.Swapna, G. (2025). Diabetes Diagnosis Using Machine Learning with Cloud Security. *Cuestiones de Fisioterapia*, 54(2), 417-431.

[28] Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, 8(2), 106576–106584.

[29] Viswanath, G. (2024). Improved Light GBM Model Performance Analysis and Comparison for Coronary Heart Disease Prediction. *International Journal of Information Technology and Computer Engineering*, 12(3), 658-672.

[30] Khan, M. B., Yang, Z. S., Lin, C. Y., Hsu, M. C., Urbina, A. N., Assavalapsakul, W., Wang, W.,H., Chen, Y. H., & Wang, S. F. (2023). Dengue overview: An updated systemic review. *J. Infection Public Health*, 16(10), 1625–1642.

[31] Viswanath, G., (2024). Enhancing Cloud Security: A Blockchain-Based Verification Framework for Multi-Cloud Virtual Machine Images. *Frontiers in Health Informatics*, 13(3), 9535-9549.

[32] Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. *IEEE Access*, 7(3), 82512–82521.

[33] Viswanath, G. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary intelligence*, 14(2), 691-698.

[34] Gupta, R., Bhattacharya, P., Tanwar, S., Kumar, N., & Zeadally, S. (2021). GaRuDa: A blockchain-based delivery scheme using drones for healthcare 5.0 applications. *IEEE Internet Things Mag.*, 4(4), 60–66.

[35] Viswanath, G. (2023). A Real-Time Case Scenario Based On URL Phishing Detection Through Login URLS. *Material science and technology*, 22(9), 103-108.

****