Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 10 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

A NOVEL SEMI-SUPERVISED FRAMEWORK FOR CYBERSECURITY THREAT DETECTION IN WIRELESS SENSOR NETWORKS

[1]Muhammad Hiyat, [2]Muhammad Usama Javed, [3]Maria Akhtar, [4]Salahuddin*, [5]Muhammad Tanveer Meeran

[1]Department of Computer Science, The University of Hertfordshire (UH), United Kingdom(UK).

[2]Department of Information Technology , Government College University Faisalabad.

[3]Department of Computer Science, COMSATS University Islamabad, Vehari Campus.

[4]Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan..

[5]Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, Malaysia.

****Corresponding Author:*** msalahuddin8612@gmail.com

Article Info

Abstract

In this work, we present a semi-supervised learning framework designed to detect four major categories of attacks in Wireless Sensor Networks (WSNs): Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R). The framework combines the strengths of both supervised and unsupervised learning, using Support Vector Machines (SVM) for classification and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) for clustering. We evaluated the proposed model on the NSL-KDD dataset, where it demonstrated strong performance in terms of accuracy and F1-score. Our analysis also explored how variations in DBSCAN parameters influence detection outcomes, emphasizing that careful parameter tuning is essential for achieving optimal performance. One of the key benefits of this semi-supervised approach is its ability to effectively handle large volumes of unlabeled data—a limitation often encountered when relying solely on supervised or unsupervised methods. By making efficient use of the available labeled data and incorporating clustering techniques, the model delivers improved accuracy and robustness in intrusion detection for WSNs.

In summary, this research contributes to the advancement of intrusion detection systems in WSNs by proposing a practical and efficient semi-supervised framework. The findings highlight not only enhanced detection across multiple attack types but also provide valuable guidance on parameter optimization and effective dataset utilization.

Keywords:

Intrusion Detection System; Supervised Learning; User to Root; Wireless Sensor Networks; Dataset.

INTRODUCTION

In this work, we study the deployment and operation of wireless sensor networks (WSNs), which consist of many sensor nodes distributed over an area to collect and monitor data from multiple locations. Each sensor node has a microprocessor and communicates through a central system connected to the Internet.

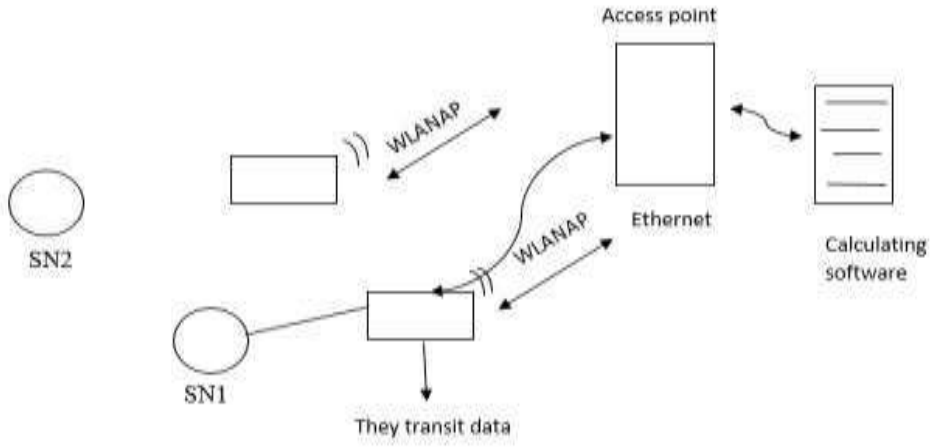

Figure 1.2 Components of WSN

Wireless Sensor Networks (WSNs) have gained significant attention for their applications across various domains, including environmental monitoring, military operations, and healthcare. However, despite their growing use, security remains a critical challenge because the limited computational and energy resources of WSN nodes restrict the implementation of conventional security techniques like encryption and authentication. As a result, WSNs are highly susceptible to numerous security threats such as node compromise, malicious intrusions, and denial-of-service (DoS) attacks. To address these vulnerabilities, Intrusion Detection Systems (IDS) are commonly employed. IDS can generally be classified into two categories: misuse-based IDS (MIDS) and anomaly-based IDS (AIDS). MIDS detect attacks by identifying known patterns of malicious behavior, whereas AIDS identify unusual activities that deviate from normal network behavior. While MIDS are ineffective against new or unknown attacks, AIDS typically produce a higher rate of false positives.

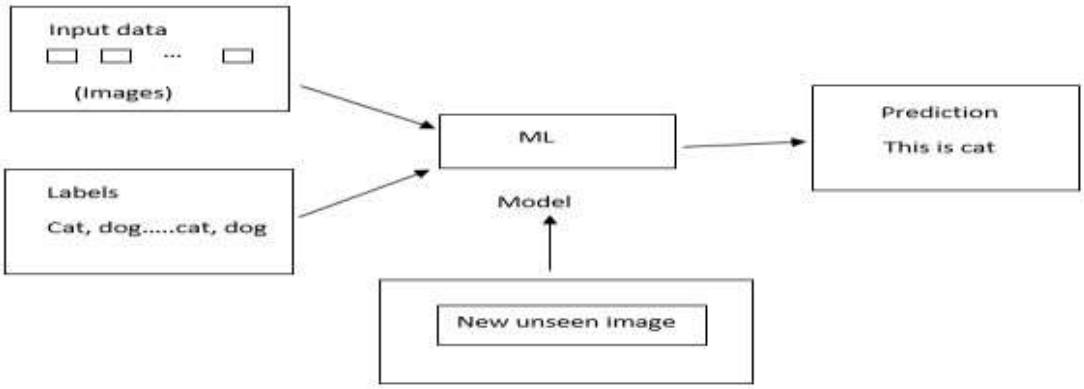

Figure 1.3 Supervised learning

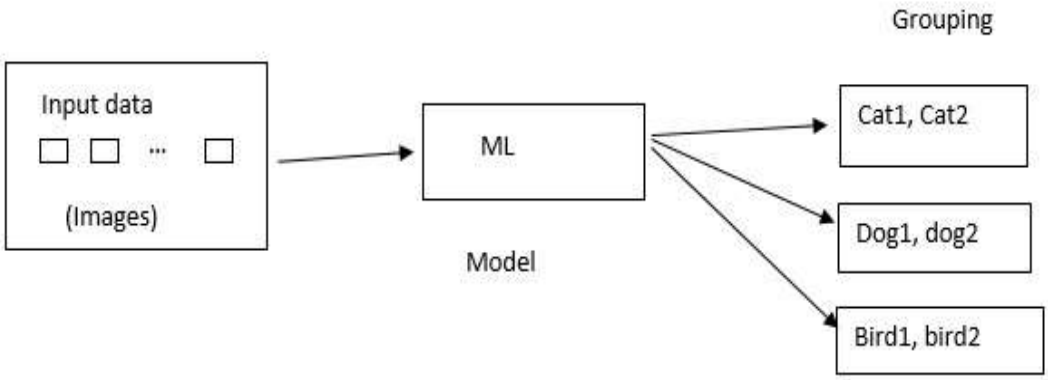

Figure 1.4 Unsupervised learning

To overcome these security challenges, numerous machine learning approaches—particularly supervised, unsupervised, and semi-supervised learning—are being explored to enhance Intrusion Detection Systems (IDS) in Wireless Sensor Networks (WSNs). In supervised learning, models are trained using labeled data to make accurate predictions on new or unseen data. Conversely, unsupervised learning works with unlabeled data to uncover hidden structures or patterns without prior knowledge. Semi-supervised learning, which combines both labeled and unlabeled data, is especially valuable when labeled data are scarce, as it helps build more generalized and unbiased models capable of handling complex problems. Various algorithms, including Support Vector Machines (SVM), Decision Trees, Density-Based Spatial Clustering of Applications with Noise (DBSCAN), and K-Means clustering, play a crucial role in designing effective IDS for WSNs. These techniques contribute significantly to enhancing the security, stability, and reliability of wireless sensor networks, thereby supporting their sustained growth and widespread adoption.

2. Materials and Methods

This research is designed to develop a semi-supervised learning-based intrusion detection system precisely intended for WSN. Core goal is to improve the detection accuracy while reducing body wear and saving energy. The main objectives include:

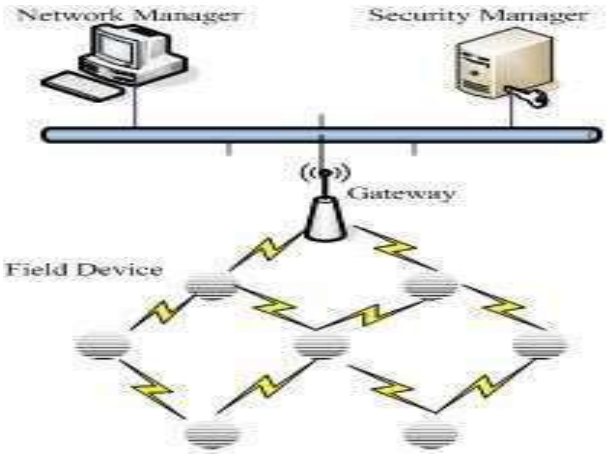

Figure 2.1 Architecture of WSN

- Data collection and prioritization:

The NSL-KDD dataset is utilized for training and validating the Intrusion Detection System (IDS) to ensure its effectiveness and reliability in real-world scenarios. Various feature extraction and selection methods are tested to enhance the system's capability to identify malicious activities more accurately. In this framework, unsupervised learning is employed to handle unlabeled data and identify patterns, while supervised learning is used for model training. This hybrid approach seeks to achieve an optimal balance between detection accuracy and system scalability.

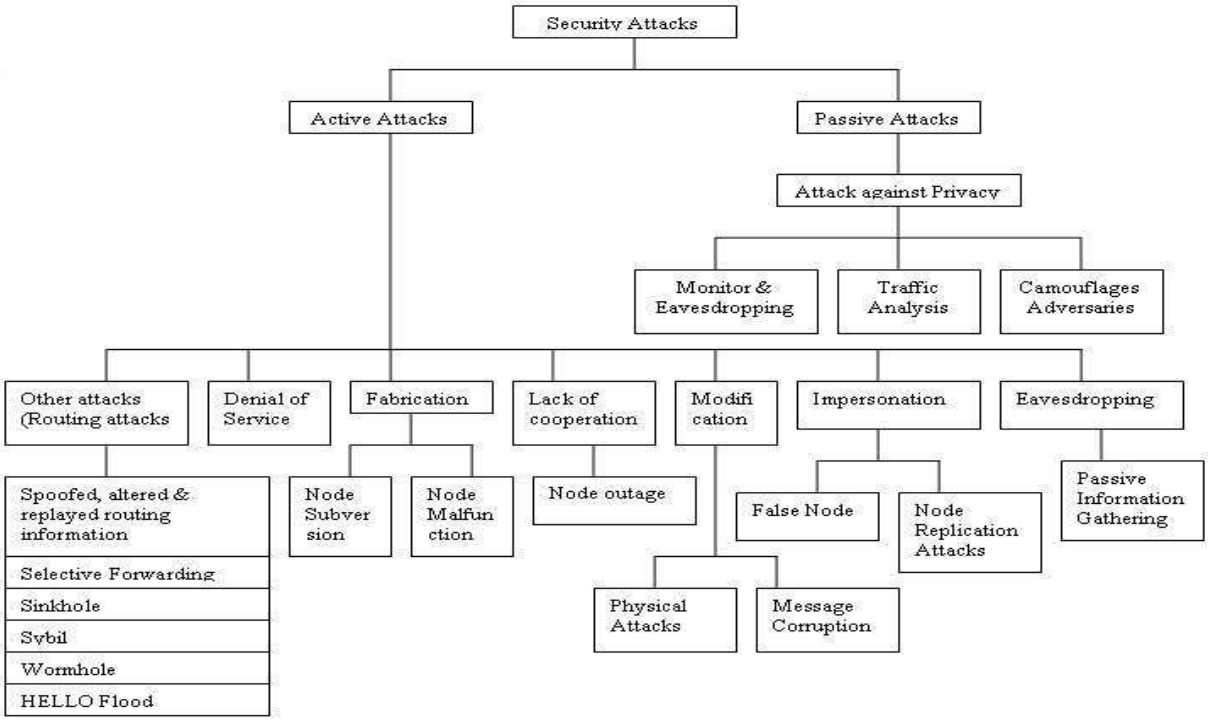

Figure 2.2 General Classification

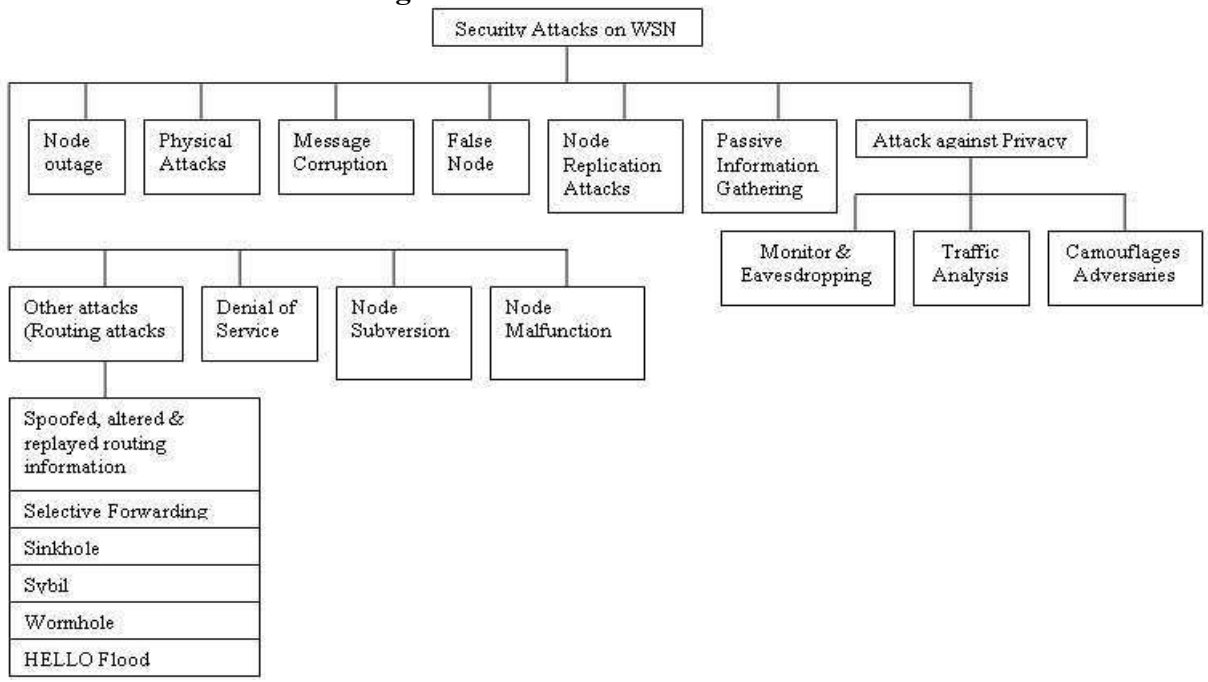

Figure 2.3 Security Attacks on WSN

- Performance Evaluation:

Evaluate the performance of the Intrusion Detection System (IDS) based on key metrics such as detection accuracy, precision, recall, and F1-score to assess its effectiveness in addressing security threats within WSN traffic.

Research Significance: The proposed IDS framework helps overcome the drawbacks of systems that rely solely on monitored or unmonitored data. By leveraging both recorded and unrecorded information, the model enhances the ability to detect intrusions even in resource-constrained environments. This approach contributes significantly to advancing technological capabilities across various domains.

- Unsupervised Learning:

Analyze anonymized data to identify hidden patterns, such as customer behavior, derived from aggregated information.

Semi-supervised approach: Integrate both labeled and unlabeled datasets to develop a more efficient and accurate model, particularly useful when data collection is limited or costly. The system comprises a network of interconnected sensor nodes specifically designed to gather data from remote environments.

- Sensor Node:

consists of various components like sensors, processors and Transceivers, usually powered by batteries or energy harvesting technology.

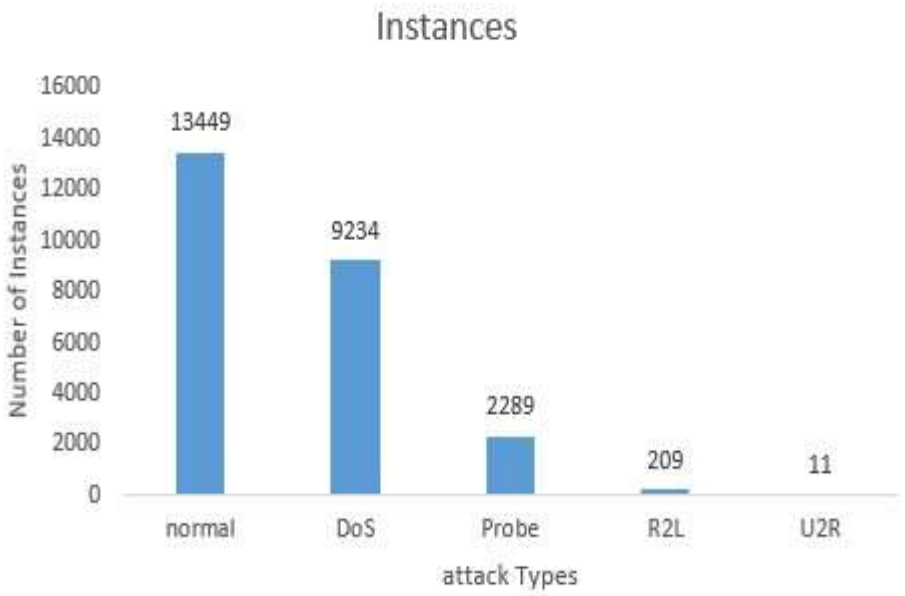

Figure 4.2 Dataset Instances

Attribute No.	Attribute Name	Narrative	Sample
1	Duration	Period span for the link	0
2	Protocol_type	Protocol that was employed in the connection construction	Tcp
3	Service	Use of final location networking service	ftp_data
4	Flag	Connection's quality good or faulty	SF
5	Src_bytes	Number of data reassigned from origin to recipient in just one linking	491
6	Dst_bytes	Number of data transferred from origin to recipient in just one connection	0
7	Land	If origin and recipient Internet Protocol(IP) addresses and number of ports are same, then this parameter has value of 1 else it possess are value of 0	0
8	Wrong fragment	Overall extents of improper segments in this link	0
9	Urgent	Quantity of crucial packets in this link imperative packets are those that have vital bit set	0
10	Hot	There are several "hot" indications in data such as reaching system directory , producing programs and executing programs	0
11	Num_failed_logins	The number of unsuccessful attempts to login	0
12	Logged_in	Login situation: 1 if logged in successfully;0 else	0
13	Num_compromised	Numerous "compromised" scenarios	0
14	Root_shell	If root shell is achieved 1 is returned otherwise 0 is returned	0
15	Su_attempted	If "su root " function attempts to be executed or employed 1 is returned otherwise 0 is returned	0

16	Num_root	Count of "root" visits or activities conducted in the link as root	0
17	Num_file_creations	Entire number of file generation processes carried out through the linking	0
18	Num_shells	Count of shell prompts	0
19	Num_access_files	Numeral of activities performed on admittance resistor files	0
20	Num_outbound_cmds	The total number of outbound commands in single ftp Session	0
21	Is_hot_login	1 if login is on 'hot' list of items i.e. root or admin ; otherwise 0	0
22	Is_guest_login	If login is "guest" login 1 is returned otherwise 0 is returned	0
23	Count	In last two seconds total number of connections to exactly same destination host as present connection	2
24	Srv_count	In preceding two seconds, total number of connections to accurately alike amenity port as current connection	2
25	Serror_rate	Fraction of associates in count(23) that have triggered the flag (4) ,s0 ,s1, s2 or s3 out of all connections	0
26	Srv_serror_rate	Fraction of associates in srv_count(24) that have triggered the flag (4) ,s0 ,s1, s2 or s3 out of wholly influences	0
27	Rerror_rate	Fraction of associates with flag(4)REJ that have been activated among the connections aggregated in count(23)	0
28	Srv_rerror_rate	Fraction of associates with flag(4)REJ that have been activated among the connections aggregated in srv_count(24)	0

29	Same_srv_rate	Fraction of associates to identical same service among all connections collected in count (23)	1
30	Diff_srv_rate	Proportions of associates to unlike service amongst connections together in count (23)	0
31	Srv_diff_host_rate	The proportion of connection collected in srv_count(24) that were to various destination machines	0
32	Dst_host_count	Number of connections that have equivalent terminus host IP address	150
33	Dst_host_srv_count	Number of connections consuming the alike port number	25
34	Dst_host_same_srv_rate	Number of connections to alike service that were serene in dst_host_count(32)	25
35	Dst_host_diff_srv_rate	Number of connections to different service that were collected in dst_host_count(32)	0.03
36	Dst_host_same_src_port_rate	Proportion of connections to unchanged origin port that were assembled in dst_host_srv_count(33)	0.17
37	Dst_host_srv_diff_host_rate	The proportion of connections to different origin port that were gathered in dst_host_srv_count(33	0
38	Dst_host_serror_rate	The fraction of connections in dst_host_count(32) that have the flag (4) s0, s1, s2, s3 enabled	0
39	Dst_host_srv_serror_rate	Fraction of associates amongst associates aggregated in dst_host_srv_count(33) that have triggered flag(4) s0, s1, s2 or s3	0
40	Dst_host_rerror_rate	Fraction of associates with flag(4)REJ that have been initiated among the associates aggregated in dst_host_count(32)	0.05
41	Dst_host_srv_rerror_rate	Fraction of associates with flag(4)REJ that have been triggered among the connections aggregated in dst_host_count(33)	0

Figure 4.2 Table of Attributes of Dataset

This study highlights the potential of semi-supervised learning to enhance the performance of Intrusion Detection Systems (IDS) in Wireless Sensor Networks (WSNs), thereby improving network security and dependability in critical applications such as perimeter surveillance, transportation, and military operations. The proposed approach aligns with current advancements in both machine learning and WSN technologies, focusing on improving detection accuracy and operational efficiency.

In this work, we carried out a detailed performance assessment of IDS models using key evaluation metrics, including accuracy, precision, recall, and F1-score. The study compared the semi-supervised DBSCAN (SSDBSCAN) combined with a Support Vector Machine (SVM) against the unsupervised DBSCAN method. By adjusting the *MinPts* and *epsilon* parameters of DBSCAN, we analyzed their influence on network intrusion detection performance. The experiments addressed four main attack categories—Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R)—using a dataset containing 22,638 instances and 29 features. After model training and clustering through SSDBSCAN, overlapping clusters representing DoS attack patterns were effectively identified and examined.

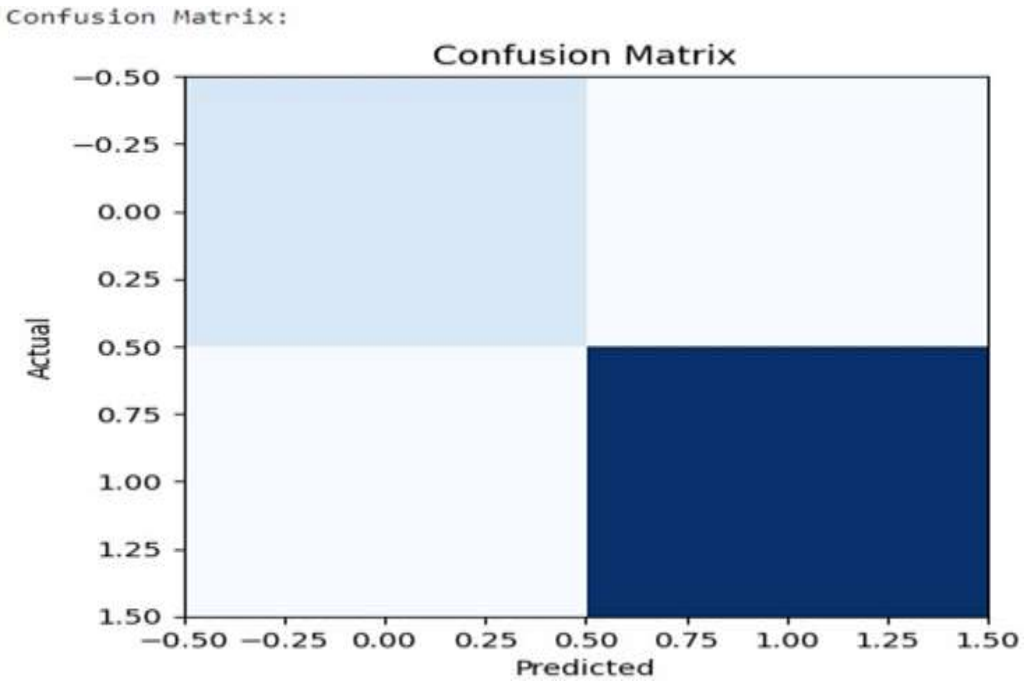

Figure5.1 Graph of Confusion Matrix

We experimented with varying MinPts (3, 5, 8, 10) and epsilon (0.2, 0.5, 0.8, 1) values in DBSCAN, resulting in the following performance metrics:

- Comparison of Accuracy with different Eps and MinPts for DoS Dataset:

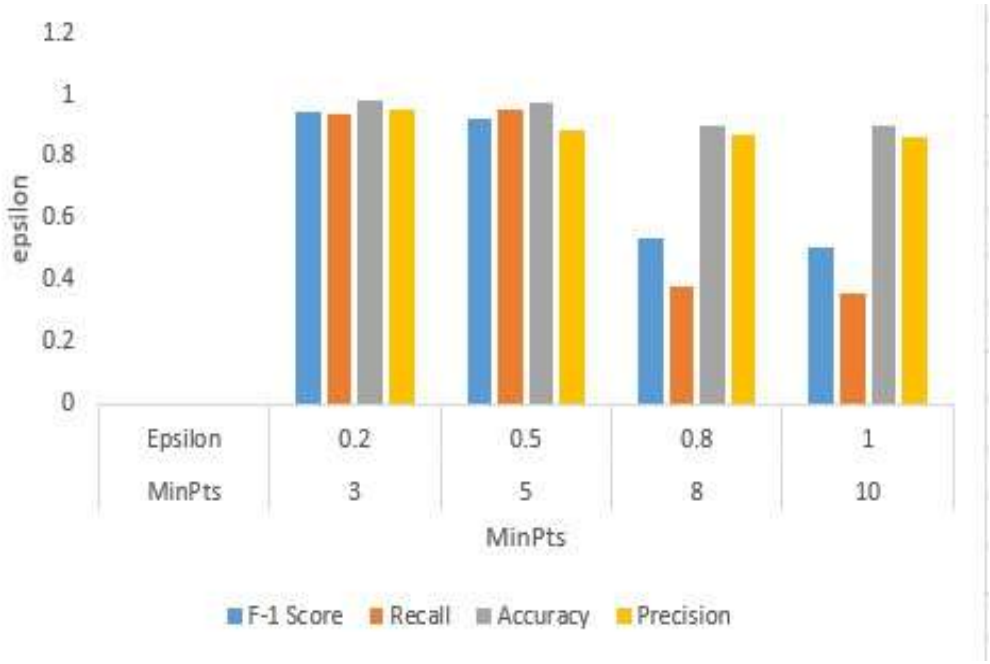

Figure 5.1 Comparison Graph

Similarly, we analyzed the Probe dataset from NSL-KDD, which contains 15,738 instances with the same 29 attributes.

- Confusion Matrix for Probe Dataset:

We evaluated performance metrics for different MinPts and epsilon values:

Properties of Dataset	Measure
The total number of instances in dataset	13658
The number of features in Dataset	29
Features data types	Nominal, numeric

Figure 5.9 R2L Dataset Attributes

- Comparison of accuracy of different probe data Eps and MinPts:

These tests show the sensitivity of SSDBSCAN performance to measurement parameters. The agreement between minPts and epsilon values can affect the accuracy and precision of detection, which indicates that the access parameter for accessing wireless sensor networks should be carefully selected.

MinPts	Epsilon	F1-score	Recall	Accuracy	Precision
3	0.2	0.09132	0.04784	0.98542	1.0
5	0.5	0.09132	0.04784	0.98542	1.0
8	0.8	0.09009	0.04784	0.98521	0.7692
10	1	0.0896	0.04784	0.98513	0.71428

Figure 5.12 Determining Eps and MinPts in DBSCAN

4. Discussion

That's right! This is a better way to write and view content together. Here are examples of tools used:

Support Vector Machines (SVM)

SVM is an advanced machine learning technique used to classify tasks and can work on both linear and non-linear features. Famous. It works by creating a hyperplane that separates different clusters in a given space. SVM works well with numerical and categorical data. w \cdot x_i + b \geq +1 \) has the form: \(y_i = +1 \)

- \(w \cdot x_i + b \leq -1 \) = \(y_i = -1 \ ) >

Combining these constraints we obtain the following condition:

\[y_i (w \cdot x_i + b) - 1 \geq 0, \forall i \]

Map* * < br > An object map provides a list of categories. In clustering algorithms, clustering datasets are used to create clusters based on other features. The SVM learning model then determines the appropriate text for this group. Cluster analysis algorithm based on object density. It has two values:

- Eps:

Defines the maximum radius of the surrounding area. The key points are close to major sites but do not meet the MinPts requirements. Noise is not suitable for certain groups. It then creates clusters by connecting key points in Eps and assigns cluster symbols to the closest points. The algorithm handles noise well and handles different groups and sizes well without any prior sharing. We monitor the performance of the model using the following metrics:

- Confusion Matrix:

Clues are Positive (TP), Negative (TN), Factor Negative (FP) and Computed Factor Negative (FN)). The formula is as follows:

\[\text{Recall} = \frac{TP}{TP + FN} \]

- Precision:

Shows the success of each prediction rig. Nice The important thing is that price and output are equal to these two parameters. The formula is as follows:

$$\text{F-Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall }}$$

- Accuracy:

Measurement of the accuracy of the model. The formula is as follows:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

5. Conclusion:

This parameter also plays a crucial role in the operation of the testing framework. Large-scale operational models—particularly semi-supervised approaches like SSDBSCAN—are essential for identifying potential intrusions in real-world systems and assessing their impact. The proposed model integrates both supervised learning (Support Vector Machine, SVM) and unsupervised learning (DBSCAN) techniques to detect four major attack categories: Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R). The NSL-KDD dataset was employed to validate the model, yielding promising results in terms of accuracy and F1-score.

Adjusting the DBSCAN parameters revealed variations in accuracy, demonstrating the model's sensitivity to parameter changes and its ability to balance between normal and malicious data. For future work, multi-class classification using SVMs could be implemented to simultaneously address all four attack categories rather than relying on binary classification. Furthermore, investigating alternative unsupervised algorithms beyond DBSCAN may lead to enhanced detection accuracy and improved overall system performance. This research lays the groundwork for future advancements aimed at increasing the efficiency, accuracy, and security of network intrusion detection in wireless sensor systems.

References

[1] Khan, S. U. R., & Khan, Z. (2025). Detection of Abnormal Cardiac Rhythms Using Feature Fusion Technique with Heart Sound Spectrograms. Journal of Bionic Engineering, 1-20.

[2] Khan, M.A., Khan, S.U.R. & Lin, D. Shortening surgical time in high myopia treatment: a randomized controlled trial comparing non-OVD and OVD techniques in ICL implantation. BMC Ophthalmol 25, 303 (2025). https://doi.org/10.1186/s12886-025-04135-3

[3] Mahmood, F., Abbas, K., Raza, A., Khan,M.A., & Khan, P.W. (2019). Three Dimensional Agricultural Land Modeling using Unmanned Aerial System (UAS). International Journal of Advanced Computer Science and Applications (IJACSA) [p-ISSN : 2158-107X, e-ISSN : 2156-5570], 10(1).

[4] Hekmat, A., et al., Brain tumor diagnosis redefined: Leveraging image fusion for MRI enhancement classification. Biomedical Signal Processing and Control, 2025. 109: p. 108040.

[5] Khan, Z., Hossain, M. Z., Mayumu, N., Yasmin, F., & Aziz, Y. (2024, November). Boosting the Prediction of Brain Tumor Using Two Stage BiGait Architecture. In 2024 International Conference on Digital Image Computing: Techniques and Applications (DICTA) (pp. 411-418). IEEE.

[6] Khan, S. U. R., Raza, A., Shahzad, I., & Ali, G. (2024). Enhancing concrete and pavement crack prediction through hierarchical feature integration with VGG16 and triple classifier ensemble. In 2024 Horizons of Information Technology and Engineering (HITE)(pp. 1-6). IEEE https://doi.org/10.1109/HITE63532

[7] O. Bilal, Asif Raza, S. ur R. Khan, and Ghazanfar Ali, "A Contemporary Secure Microservices Discovery Architecture with Service Tags for Smart City Infrastructures ", VFAST trans. softw. eng., vol. 12, no. 1, pp. 79–92, Mar. 2024

[8] S.ur R. Khan, Asif. Raza, Muhammad Tanveer Meeran, and U. Bilhaj, "Enhancing Breast Cancer Detection through Thermal Imaging and Customized 2D CNN Classifiers", VFAST trans. softw. eng., vol. 11, no. 4, pp. 80–92, Dec. 2023.

[9] Khan, S.U.R., Asif, S., Bilal, O. et al. Lead-cnn: lightweight enhanced dimension reduction convolutional neural network for brain tumor classification. Int. J. Mach. Learn. & Cyber. (2025). https://doi.org/10.1007/s13042-025-02637-6.

[10] Khan, U. S., Ishfaque, M., Khan, S. U. R., Xu, F., Chen, L., & Lei, Y. (2024). Comparative analysis of twelve transfer learning models for the prediction and crack detection in concrete dams, based on borehole images. Frontiers of Structural and Civil Engineering, 1-17.

[11] Khan, M. A., Khan, S. U. R., Rehman, H. U., Aladhadh, S., & Lin, D. (2025). Robust InceptionV3 with Novel EYENET Weights for Di-EYENET Ocular Surface Imaging Dataset: Integrating Chain Foraging and Cyclone Aging Techniques. International Journal of Computational Intelligence Systems, 18(1), 1-26.

[12] Latif, Sadia, Sami Ullah, Aafia Latif, Ghazanfar Ali, Muhammad Hassnain Azhar, and Salman Ali. "PREDICTIVE MODELING OF CARDIOVASCULAR DISEASE USING MACHINE LEARNING APPROACH." Kashf Journal of Multidisciplinary Research 2, no. 02 (2025): 207-232.

[13] Irtaza, G., Latif, S., Nadeem, R. M., Hussain, N., & Ijaz, H. M. (2025). Real-time Satellite Image Classification Using Convolutional Neural Networks for Earth Observation and Video Feed Analysis. Kashf Journal of Multidisciplinary Research, 2(03), 204-216.

[14] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li, Y., & Xiao, C. (2026). ShallowMRI: A novel lightweight CNN with novel attention mechanism for Multi brain tumor classification in MRI images. Biomedical Signal Processing and Control, 111, 108425.

[15] Khan, S.U.R., Zhao, M. & Li, Y. Detection of MRI brain tumor using residual skip block based modified MobileNet model. Cluster Comput 28, 248 (2025). https://doi.org/10.1007/s10586-024-04940-3

[16] Al-Khasawneh, M. A., Raza, A., Khan, S. U. R., & Khan, Z. (2024). Stock Market Trend Prediction Using Deep Learning Approach. Computational Economics, 1-32.

[17] Khan, U. S., & Khan, S. U. R. (2025). Ethics by Design: A Lifecycle Framework for Trustworthy AI in Medical Imaging From Transparent Data Governance to Clinically Validated Deployment. arXiv preprint arXiv:2507.04249.

[18] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li, Y., & Xiao, C. (2026). ShallowMRI: A novel lightweight CNN with novel attention mechanism for Multi brain tumor classification in MRI images. Biomedical Signal Processing and Control, 111, 108425.

[19] HUSSAIN, S., Raza, A., MEERAN, M. T., IJAZ, H. M., & JAMALI, S. (2020). Domain Ontology Based Similarity and Analysis in Higher Education. IEEEP New Horizons Journal, 102(1), 11-16.

[20] Raza, A., & Meeran, M. T. (2019). Routine of Encryption in Cognitive Radio Network. Mehran University Research Journal of Engineering and Technology [p-ISSN: 0254-7821, e-ISSN: 2413-7219], 38(3), 609-618.

[21] Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). FOLC-Net: A Federated-Optimized Lightweight Architecture for Enhanced MRI Disease Diagnosis across Axial, Coronal, and Sagittal Views. arXiv preprint arXiv:2507.06763.

[**22**] Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). Flora Syntropy-Net: Scalable Deep Learning with Novel Flora Syntropy Archive for Large-Scale Plant Disease Diagnosis. arXiv preprint arXiv:2508.17653.

[23] Khan, Z., Khan, S. U. R., Bilal, O., Raza, A., & Ali, G. (2025, February). Optimizing Cervical Lesion Detection Using Deep Learning with Particle Swarm Optimization. In 2025 6th International Conference on Advancements in Computational Sciences (ICACS) (pp. 1-7). IEEE.

[24] Bilal, O., Hekmat, A., Shahzad, I. et al. Boosting Machine Learning Accuracy for Cardiac Disease Prediction: The Role of Advanced Feature Engineering and Model Optimization. Rev Socionetwork Strat (2025). https://doi.org/10.1007/s12626-025-00190-w

[25] Raza, Asif, Inzamam Shahzad, Muhammad Salahuddin, and Sadia Latif. "Satellite Imagery Employed to Analyze the Extent of Urban Land Transformation in The Punjab District of Pakistan." Journal of Palestine Ahliya University for Research and Studies 4, no. 2 (2025): 17-36.

[26] Asif Raza, Inzamam Shahzad, Ghazanfar Ali, and Muhammad Hanif Soomro. "Use Transfer Learning VGG16, Inception, and Reset50 to Classify IoT Challenge in Security Domain via Dataset Bench Mark." Journal of Innovative Computing and Emerging Technologies 5, no. 1 (2025).

[27] Waqas, M., Bandyopadhyay, R., Showkat Ian, E., Muneer, A., Zafar, A., Alvarez, F. R., ... & Wu, J. (2025). The Next Layer: Augmenting Foundation Models with Structure-Preserving and Attention-Guided Learning for Local Patches to Global Context Awareness in Computational Pathology. ArXiv, arXiv-2508.

[28] Khan, M. A., Khan, S. U. R., Rehman, H. U., Aladhadh, S., & Lin, D. (2025). Robust InceptionV3 with Novel EYENET Weights for Di-EYENET Ocular Surface Imaging Dataset: Integrating Chain Foraging and Cyclone Aging Techniques. International Journal of Computational Intelligence Systems, 18(1), 204.

[29] Latif, Sadia, Sami Ullah, Aafia Latif, Ghazanfar Ali, Muhammad Hassnain Azhar, and Salman Ali. "PREDICTIVE MODELING OF CARDIOVASCULAR DISEASE USING MACHINE LEARNING APPROACH." Kashf Journal of Multidisciplinary Research 2, no. 02 (2025): 207-232.

[30] Latif, Aafia, Sadia Latif, and Furqan Jamil. "UTILIZING BIG DATA ANALYTICS TO OPTIMIZE INFORMATION COMMUNICATION TECHNOLOGY STRATEGIES." Kashf Journal of Multidisciplinary Research 1, no. 12 (2024): 122-140.

[31] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li, Y., & Li, X. (2025). Optimized deep learning model for comprehensive medical image analysis across multiple modalities. Neurocomputing, 619, 129182.

[32] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., & Li, Y. (2025). Optimize brain tumor multiclass classification with manta ray foraging and improved residual block techniques. Multimedia Systems, 31(1), 1-27.

[33] Muneer, Amjad, Muhammad Waqas, Maliazurina B. Saad, Eman Showkatian, Rukhmini Bandyopadhyay, Hui Xu, Wentao Li et al. "From Classical Machine Learning to Emerging Foundation Models: Review on Multimodal Data Integration for Cancer Research." arXiv preprint arXiv:2507.09028 (2025).

[34] Khan, S.U.R., Raza, A., Shahzad, I., Khan, S. (2025). Subcellular Structures Classification in Fluorescence Microscopic Images. In: Arif, M., Jaffar, A., Geman, O. (eds) Computing and

Emerging Technologies. ICCET 2023. Communications in Computer and Information Science, vol 2056. Springer, Cham. https://doi.org/10.1007/978-3-031-77620-5_20

[35] Khan, S. U. R., Asif, S., & Bilal, O. (2025). Ensemble Architecture of Vision Transformer and CNNs for Breast Cancer Tumor Detection from Mammograms. International Journal of Imaging Systems and Technology, 35(3), e70090.

[36] Maqsood, H., & Khan, S. U. R. (2025). MeD-3D: A Multimodal Deep Learning Framework for Precise Recurrence Prediction in Clear Cell Renal Cell Carcinoma (ccRCC). arXiv preprint arXiv:2507.07839.

[37] Khan, S. R., Asif Raza, Inzamam Shahzad, & Hafiz Muhammad Ijaz. (2024). Deep transfer CNNs models performance evaluation using unbalanced histopathological breast cancer dataset. Lahore Garrison University Research Journal of Computer Science and Information Technology, 8(1).

[38] Raza, A., Salahuddin, & Inzamam Shahzad. (2024). Residual Learning Model-Based Classification of COVID-19 Using Chest Radiographs. Spectrum of Engineering Sciences, 2(3), 367–396.

[39] Raza, A., Soomro, M. H., Shahzad, I., & Batool, S. (2024). Abstractive Text Summarization for Urdu Language. Journal of Computing & Biomedical Informatics, 7(02).

[40] Hekmat, A., Zuping, Z., Bilal, O., & Khan, S. U. R. (2025). Differential evolution-driven optimized ensemble network for brain tumor detection. International Journal of Machine Learning and Cybernetics, 1-26.

[41] Khan, S. U. R. (2025). Multi-level feature fusion network for kidney disease detection. Computers in Biology and Medicine, 191, 110214.

[42] Bilal, O., Hekmat, A., & Khan, S. U. R. (2025). Automated cervical cancer cell diagnosis via grid search-optimized multi-CNN ensemble networks. Network Modeling Analysis in Health Informatics and Bioinformatics, 14(1), 67.

[43] Latif, Sadia, Azhar Mehboob, Muhammad Ramzan, and Muhammad Ans Khalid. "DETECTION OF HCV LIVER FIBROSIS APPLYING MACHINE LEARNING TECHNIQUE." Kashf Journal of Multidisciplinary Research 1, no. 12 (2024): 11-44.

[44] Irtaza, Ghulam, Sadia Latif, Rana Muhammad Nadeem, Nasir Hussain, and Hafiz Muhammad Ijaz. "Real-time Satellite Image Classification Using Convolutional Neural Networks for Earth Observation and Video Feed Analysis." Kashf Journal of Multidisciplinary Research 2, no. 03 (2025): 204-216.