Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

AN INTELLIGENT INTRUSION DETECTION FRAMEWORK FOR WIRELESS SENSOR NETWORKS USING MACHINE LEARNING

Hifza Rani[1*], Syed Younus Ali [2], Muhammad Zubair[3], Muhammad Waqas Riaz[4], Rimsha Zubair[5], and Muhammad Yousif[6]

[1]Department of Computer Science, Minhaj University, Lahore- , Pakistan, hifza.sarwar1@gmail.com

[2]Department of Computer Science, Green International University lahore, Pakistan, Younas.ali@giu.edu.pk

3 Department of computer science, Air University Islamabad Multan Campus, Pakistan , muhammad.zubair@aumc.edu.pk

4 Department of Artificial Intelligence, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan , mwaqaskp@gmail.com

5 Department of Artificial Intelligence, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan , RimshaZubair1515@gmail.com

[6]Department of Computer Science, National University of Modern languages Sub-Campus, Lahore, Pakistan, myousif.cs@gmail.com

DOI:- https://doi.org/10.5281/zenodo.20330341

Article History

Received: 17 April 2026

Accepted: 20 May 2026

Published: 21 May2026

Corresponding Author: *

Hifza Rani[1]

hifza.sarwar1@gmail.com

Abstract

Intrusion Detection system protects modern cybersecurity networks through continuous traffic and system activity inspection for identifying potential security threats. Such systems provide organizations with the ability to find and respond instantly to unauthorized access and cyber threats and policy violations. The security of contemporary cybersecurity systems heavily depends on IDS for WSN and ad hoc Wireless Sensor Networks specifically require IDS because traditional security measures fail due to network decentralization. This research paper investigates current intrusion detection approaches designed for ad hoc WSNs while focusing on the distinct security threats DoS, Sybil, and black-hole attacks. The paper examines data gathering strategies and detection methods for IDS models alongside their performance evaluation in WSN environments with limited resources to establish ways for algorithm optimization between security needs and energy efficiency. The recent research should focus on enhancing IDS security while establishing Machine learning methods for behavioral analytics in wireless systems SVM shows best performance as compared to others.

Key words: Wireless sensor networks, Ad hoc, Intrusion detection, IDs Types, Security

1. Introduction

Intrusion Detection system protects modern cybersecurity networks through continuous traffic and

system activity inspection for identifying potential security threats. Such systems provide organizations with the ability to find and respond instantly to unauthorized access and cyber threats and policy violations[1]. The mounting difficulty in cyber assault requires IDS to become an imperative security element for network protection alongside other protection systems. An Intrusion Detection System exists in two fundamental categories which include Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). This process of NIDS involves tracking network traffic for potential strange patterns while HIDS examines device activities for irregular conduct. IDS operates with two detection methods namely signature-based focusing on known attack signatures and anomaly-based identifying abnormal system behavior. IDS solves security problems by executing different detection methods which produces early alerts together with lessened data breach dangers[2].

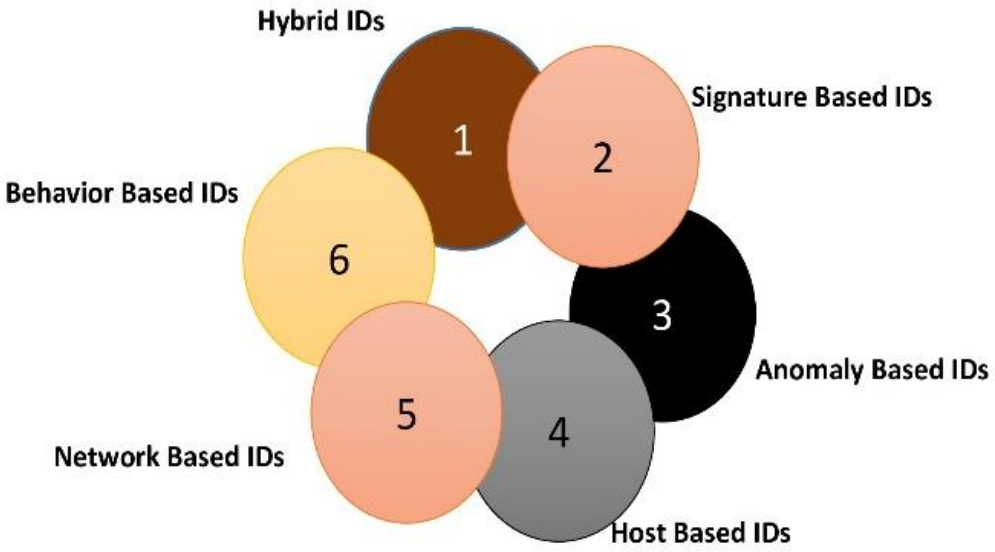

Figure 1.Types of IDs

Success of IDS solutions depends on correct threat identification mixed with minimal mistakes and fast detection capabilities. Organizations need to establish strong intrusion detection methods because cyber threats keep updating so they must protect both their proprietary information and their operational systems[3].

Important of the study

Research into intrusion detection within ad hoc wireless sensor networks (WSNs) becomes essential because these networks enter into critical usage for military surveillance tasks alongside disaster monitoring tasks and healthcare support systems and industrial automation. Traditional wired networks show substantial differences from ad hoc WSNs because they function in dynamic decentralized structures which creates significant security risks through denial-of-service (DoS) attacks and Sybil attacks and black-hole attacks [4]. Security defenders use real-time intrusion detection systems (IDS) as primary defenses because traditional security measures like encryption and authentication cannot protect systems well enough. Advanced detection techniques examined in this research work toward implementing anomaly-based systems with machine learning capabilities, which lead to better accuracy and decreased false alert rates when compared to traditional signature-based detection methods. The analysis of WSN intrusion detection frameworks through this research effort helps develop better

protective security solutions with enhanced protection capabilities for data and network reliability alongside improved resource-constrained system operation.

1. Literature Review

The survey work has been briefly investigated to produce this analysis. Acquiring research articles for this study proves to be an iterative and time-consuming manual process. Research was conducted using a systematic literature review framework to execute our study.

We adopted the selection and review process described in Snyder's research article to fetch articles[5].

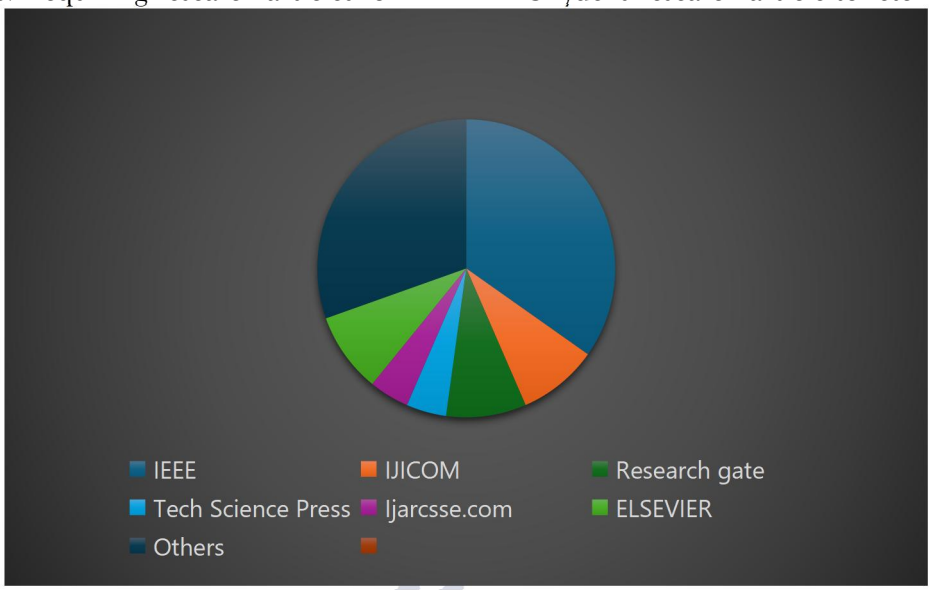

Figure 2. Paper count

Table 1. Publications and paper count

Publications	Paper count
IEEE	8
IJICOM	2
Research gate	2
Tech Science Press	1
Ijarcsse.com	1
ELSEVIER	2
Others	7

The research question is used to give direction and themes to this study. In an ad hoc network, security is of utmost importance, because it is distributed and decentralized and is susceptible to cyber-attacks. Support Vector Machines (SVMs) and K-Means clustering and Autoencoders work together in a vital capacity by detection of abnormal behavior in network traffic anomalies. The One Class SVM method performs well in the creation of "normal" traffic profiles as it can create boundaries around safe data points [6]. The system sets the boundary for the normal traffic and anything outside of it is classified as anomalous traffic. The K-Means clustering method creates clusters of similar traffic patterns but anomaly patterns are generally very small clusters of anomalies that are found in small numbers and far apart or as isolated points. Autoencoders serve as neural networks which can learn to reconstruct normal traffic flows, then use this reconstruction as a means to identify anomalies in traffic. Network security algorithms

begin by analyzing the crucial features of network data from raw server logs that contain IP addresses, protocols and statistics of network traffic. Normal traffic is used to establish a set point and then the system is then trained with this information. The system performs anomaly detection of the new traffic by analyzing variations from the pattern, during the monitoring process [7].

The models work best with the cooperation of data preprocessing process and feature selection implementation process adjustment elements. Implementation of preprocessing steps such as feature scaling and normalization has a significant role in making a system optimal for performance [8]. Analysis is very much reliant on the features selected that accurately mark anomalous traffic patterns from normal ones. Expert control over certain SVM kernel(s) and the number of K-Means clusters are crucial for efficient intrusion detection, as they allow to achieve maximum detection precision, and reduce measurement errors. Real-time detection remains a vital factor for intrusion detection systems because they must react promptly to active security threats. Cautious optimization and deployment of these algorithms remains essential for securing both the speed and accuracy of intrusion detection in challenging network situations[9].

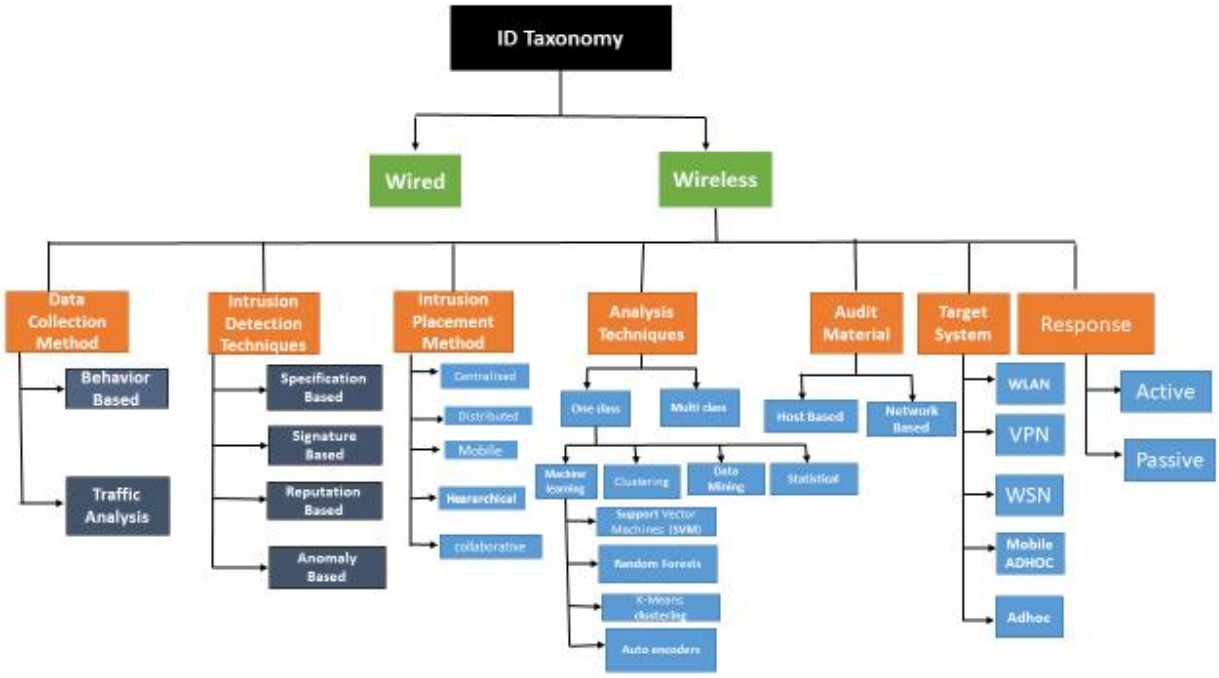

Figure 3. Intrusion Detection Taxonomy

An IDS operates as a network security tool which monitors both network traffic and devices for harmful activity as well as differing between suspicious actions and security policy violations. IDS automation and acceleration of network threat detection process become possible thanks to alerts which security administrators receive when identifying known potential threats or when security tools receive these alerts. A security information and event management (SIEM) system operates as a centralized security tool that merges information from multiple sources to assist security teams in detecting and managing cyber threats between other security instruments[10].

IDS systems offer assistance for meeting compliance standards. Organizations must use intrusion detection solutions according to the Payment Card Industry Data Security Standard (PCI-DSS) regulatory requirement[11].

Wireless Sensor Network (WSN) represents a wireless network infrastructure without bases which deploys

numerous wireless sensors autonomously to inspect system and physical conditions. A WSN relies on sensor nodes to implement onboard processors dedicated to monitoring specific environment zones. The Base Station exists as the processing unit that linked to sensor nodes within the WSN System. The base Station in a WSN System connects through Internet networks to share collected data. The data obtained from WSN enables processing along with analysis for storage and data mining operations[12].

Any Wireless Sensor Network requires at least two nodes to exchange wireless signals between RF transceivers, sensors, machine controllers, microcontrollers and user interface devices.

Table 2. wireless network pros and cons [13]

Network	Pros	Cons
Wireless network	The extensive network coverage together with unlimited access exposes the system to potential security threats. The scalability features of wireless networks operates independently from chosen platform arrangements.	Security measures must protect the wireless network.

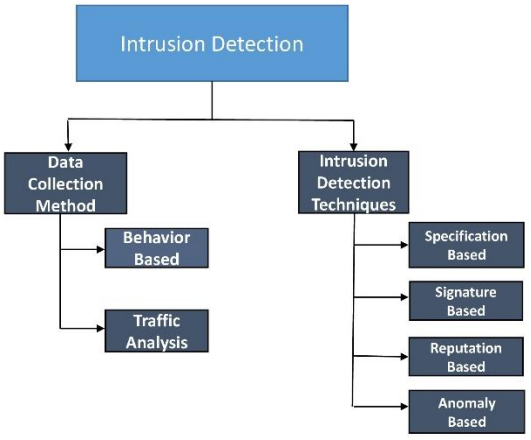

Figure 4. Focus research Area

Intrusion Data Collection Methods

Behavior-based and traffic analysis provide the two possible means by which data is gathered in both wired and wireless networks for intrusion detection purposes. Most behavior based data collection monitors system performance and includes metrics like Windows error reporting and web server performance together with CPU usage and console log files[14]. Suitability of behavior data collection exists when research areas differ significantly from network analysis. Operating system level malware detection requires behavior analysis as its preferred method of choice. Behavior-based data collection proves ineffective for network attack detection since these attacks primarily manifest at the network or transport or data link levels. Traffic analysis proves most effective for these circumstances. Attack and non-attack data logs for different Open System Interconnection (OSI) layers can be created through traffic analysis. Every network layer serves as a symbol

for matching various data types. At the network layer network attacks can be monitored through analyzing source and destination IP address data as well as time to live measurement and packet length specifications[15]. At the transport layer port numbers along with sequence numbers and flags reveal data abnormalities by distinguishing normal patterns from abnormal patterns. Most attacks on network systems (such as Denial of Service [DOS] and flooding and botnet) demonstrate that traffic data remains the most crucial information available to investigators acting against these crimes. Wireless system and specifically ad hoc networking benefits more from traffic based collection over behavior based techniques[16].

Intrusion Detection Techniques

This part explains the principal intrusion detection methods that are currently employed.

Signature Based

Immune System detection systems demonstrate structured matching patterns which serve to detect intrusions as outlined in the survey. Diverse mechanisms operate for detection with distinct representation and matching algorithms serving to differentiate them. Expert systems together with pattern recognition and state transition analysis follow colored petri nets as approaches in the framework. Signature based detection provides simple and dependable attack discovery capabilities yet struggles to recognize unknown threats. The maintenance of current signatures remains difficult because signature updates require substantial time and effort[17]. Signature based IDS features minimized false positive detection due to its ability to monitor disruptive network behavior with precision. The system needs to monitor particular signatures which the dictionary maintains comprehensive attack vectors matching those signatures. This IDS system monitors either univariate sequences such as byte transfer statistics and system logs or multivariate data with specific timing patterns in its analysis. The principal difficulty in applying this strategy arises from creating extensive signature databases to improve attack predictions. A database with a large number of signatures leads to processing delays which extends the overall detection period[18]. The essential element for an optimal signature-based IDS are both an adequate signature size and system performance. Similar to antivirus functionality Signature Base Intrusion Detection detects already known signatures or attack patterns yet proves ineffective against unidentified threats. SNORT operates as a signature-based IDS through using header parameters including source and destination addresses and ports as signature references to validate network traffic versus signatures through option field analysis regarding payload. Kumar et al built a signature detection IDS utilizing virtual machine infrastructure to monitor cloud intrusions.[19]

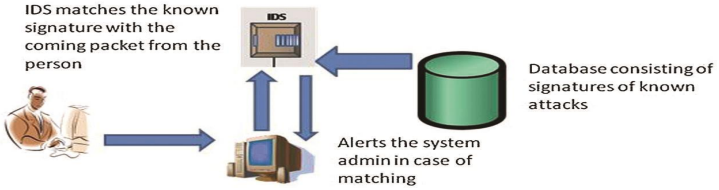

Figure 5. IDS with signature-based detection functions as a receptor for incoming attacks [19]

Anomaly Based

The anomaly detection solution functions through maintaining a system record of typical network traffic patterns as shown in Figure 5. An anomaly indicator occurs when system detection identifies unusual traffic patterns outside normal statistical patterns. Data mining alongside neural networks along with statistics makes up the typical techniques employed in these systems[20]. A collection of training data that stems from supervised, semi-supervised and unsupervised

methods allows operators to build a normal profile database. The anomaly-based intrusion detection approach consists of three main domains that include statistical-based and knowledge-based and machine learning-based systems.

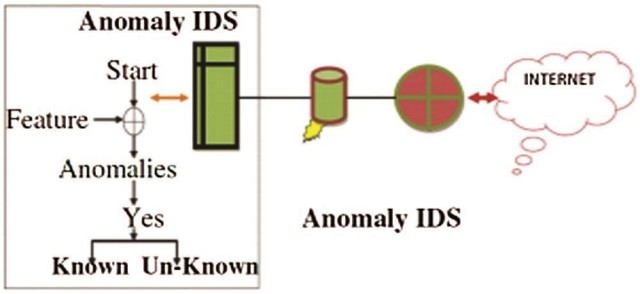

Figure 6. Anomaly based IDs [19]

A statistical based anomaly IDS uses network traffic behavior profiles to create them. Network traffic in normal situations uses the profile as a benchmark reference. Continued reference profiling occurs as the IDS operates through its data comparison process. The system flags activities as abnormal whenever the profile measurement deviates substantially from its reference values. The detection of intrusion through knowledge-based anomaly IDS utilizes existing network traffic data to identify normal or abnormal conditions. Expert systems and Unified Modelling Language (UML) and Finite State Machine (FSM) along with clustering algorithms serve as tools for knowledge based intrusion detection[21].

Machine learning systems automatically learn network profiles to identify unorthodox behaviors within network spaces. The following section examines machine learning based IDs in detail because this technique has become popular. In 1959 Arthur Samuel established Machine learning (ML) as "field of study that gives computers the ability to learn without being explicitly programmed"[22]. During its training phase Machine Learning systems acquire data properties through which they predict and classify new input information. Also, ML requires an objective. London School of Economics The work of Bhatti et al demonstrates support vector machines as one widespread approach within these methods. The artificial neural network (ANN) functions according to the structure of the human brain. ANN achieves greater capabilities than conventional machine learning models because of its design. A neural network consists of artificial units known as units which connect from layer to layer. A layer contains units that establish network connections to every unit within the subsequent layer. A standard ANN requires at least three layers consisting of input then hidden then output layers. ANN uses the input layer to intake data before output processing through units completes learning. Artificial Neural Networks consist of one or more structured hidden layers which form the main components of their artificial brain architecture. The ANN has an essential feature named weight which operates between its connections. The weight of each link within ANN maintains either positive or negative values. The essential function of ANN exists in the ability to both learn from and retrain data while following input and output specifications. The ANN implementation exists in multiple domains including both image processing and character recognition applications[23].

Researchers have conducted various ANN based IDS experiments and conducted a survey to evaluate different ANN models as described in Shah et al. Among available ANNs a popular implementation choice is the concept of Back Propagation Neural Networks (BPNN). Numerous investigators choose the BPNN because it grants various beneficial characteristics.

Shah et al. [24]has used this model because of the precise prediction and finer perseverance. The deep learning network utilizes various frameworks including [25] who integrated H2O framework for Python and Scala applications. While implementation covers

multiple interfaces it displays limited model support together with challenges in flexibility. Refined vulnerabilities detection is a noteworthy strength of anomaly-based methods which operate independently from the operating system. Anomaly-based IDs deliver poor detection results during constant operational changes and these detection systems often lack access to necessary profile data at profile development time. The key advantage of anomaly-based IDs depends on their ability to avoid strict pattern matching between specific activities and on their ability to update attack vectors independently of dictionary updates. This approach may lead to additional wrong positive alerts. Systems present multiple threats during the testing or profiling phase. The frequent variance in network behavior requires regular updates for the normal behavior models in anomaly detection systems [26].

Specifications Based

A specification-based intrusion detection system examines system-level anomalies beyond the scope of user profile and data flow anomalies that anomaly-based IDS monitors. This detection method tracks standard operating behaviors to identify anomalies that emerge when systems step outside defined parameters. This IDS provides better false positive performance than anomaly-based IDS because it learns which expert-defined legitimate behaviors constitute normal while everything else is considered abnormal. The protection achieved by this system depends on uncommon activities which violate the system's defined parameters. This system works right away without requiring any training phase therefore making it effective. The definition of formal specifications requires significant effort which represents the sole limitation of the method[27]. The system proves efficient at searching insider attack activity by detecting unusual system activity patterns that result from disruptions. This method proves ineffective for detecting outside threats because its focus remains on monitoring insider-led actions while staying tightly bound to application details[28]. The system detects anomalies without requiring pre-defined profiles from users or groups or information types. Human-defined legitimate behaviors form the baseline norms which match all activities that move beyond these parameters qualify as malicious behavior nodes. The security solution operates effectively on resource-constrained nodes where storage of user and group This IDS model diverges from previous IDS tactics because it hunts for selfish nodes instead of detecting malicious nodes. When the reputation manager detects a misbehavior node they must investigate network protection strategies to protect the network reputation[29]. Challenge scores in this system include event types such as packets sourced surpassing packets destined and packets forwarded surpassing packets sourced along with multiple other categories. Such applications serve extensive networks that cannot rely on preliminary trust information. The reputation management system demonstrates exceptional utility for spontaneous networks including both Vehicular Area Network (VANET) and Mobile Ad-hoc Network (MANET)[30].

Profiles and data profiles remains impossible. According to Sobh [31] anomaly based systems find unwanted results from abnormal conduct while misuse detection focuses on detecting flawed activities. The specification-based IDS detects legitimate system actions through manually set constraints which capture both behavioral requirements from anomaly detection and explicit signatures from signature-based methods.

Reputation Based

These models operate optimally based on the collaborative effectiveness between data preprocessing work and feature selection implementation and parameter adjustment elements. Performance optimality depends heavily on the implementation of preprocessing steps that include feature scaling and normalization[30]. The success of analysis depends heavily on selecting features which precisely identify anomalous traffic patterns from normal patterns. Efficient intrusion detection depends heavily on expert control over specific SVM kernel use and K-Means cluster quantity selections since this determines maximum detection precision and lowers measurement errors[32]. Real-time detection remains a vital factor for intrusion detection systems because they must react promptly to active security threats. Cautious optimization and deployment of these

algorithms remains essential for securing both the speed and accuracy of intrusion detection in challenging network situations[33].

Discussion:

The limitation of resources, dynamic topology and various possibilities of attack make the study of intrusion detection a priority in ad hoc wireless sensor networks (WSNs). The deployed traditional IDSs for wired networks are not feasible in WSNs due to its unique constraints. Research is now underway to create tailored solutions for the intrusion detection system (IDS) problem in wireless sensor networks. These network security solutions are based on signature-based detection, anomaly detection and data mining techniques detect cyber-attack [34].

Discovery research in WSN intrusion detection focuses primarily towards various detection approaches. Anomaly detection analysis attempts to identify abnormal activities on the network as these patterns may be signs of intrusions.

Operation works through machine learning algorithms which recognize typical network behavior patterns to detect anything beyond typical performance. The approach of signature-based detection uses existing patterns in predefined attack signatures to locate intrusions. A signature-based system depends on an extensive database of attack patterns yet needs continuous database maintenance as criminals keep developing new threats. WSNs leverage diverse data mining approaches for intrusion detection by analyzing network data to reveal attack signatures and detect suspicious network behavior patterns.

Research focusing on WSN intrusion detection centers on energy efficiency and security protocols while studying different deployment approaches alongside detection methods[35]. The limited battery existence of sensor nodes outlines energy efficiency as a central aspect because of its importance. Due to WSN nodes' limited energy capacity many IDS solutions for WSNs have been developed to have minimal overhead impact. Security protocols demonstrate essential importance by guarding networks against initial intrusions. Multiple security protocols for WSNs exist through researcher proposals which address their distinctive needs. Intrusion detection effectiveness depends on the deployment strategies researchers select. IDS detection capabilities undergo enhancement through studies of distributed and hierarchical deployment models. [36]

Security Vulnerabilities in Wireless Ad Hoc Networks

Wireless ad hoc networks (WANETs) encounter multiple security threats from their decentralized nature and dynamic topology and their lack of centralized control. Repeatable attacks which target ad hoc networks include eavesdropping alongside data tampering impersonation and message replay and denial of service (DoS) attacks because these systems lack permanent infrastructure[37]. Without centralized authority systems become unable to differentiate trusted nodes from non-trusted ones thus creating a higher probability of internal network attacks. Through manipulations of routing protocols malicious nodes manage to establish artificial network paths while transmitting false content to trigger Byzantine failures that lead to network congestion problems.[38]

Challenges in Deploying IDS in Wireless Ad Hoc Networks

IDS implementation within ad hoc networks must overcome important obstacles which stem from limited resources while also addressing dynamic structure and instantaneous intrusion detection abilities. Ion limitations of WANET connectivity combined with processing capacity constraints prevents the implementation of intensive IDS solutions on many network nodes. Adaptation of IDS mechanisms to frequent topology changes in ad hoc networks increases attack detection complexity as well as mitigation challenges. IDS agents need secure communication channels to stop adversaries from modifying their alert signals. The current research develops lightweight IDS frameworks powered by energy-efficient artificial intelligence technologies integrated with block chain features to improve security and defense against mutating cyber threats[39]. Network security depends heavily on Intrusion Detection Systems (IDS) as they defend networks from modern cyber threats. Results from recent research showcase how different approaches have been developed for IDS enhancement specifically for

Mobile Ad-Hoc Networks (MANETs) Wireless Sensor Networks (WSNs) and cloud-based contexts[40].

Machine learning techniques serve as the core focus of Zainab et al. (2021) MANET-based IDS research investigation[41]. Self-managing and dynamic nature of MANET nodes demands robust protocol routing systems to enable both effective performance and protection capabilities. The authors show how anomaly-based threat detection systems detect zero-day attacks because signature-based methods fail to recognize emerging threats. The investigation applies artificial neural networks (ANN) to intrusion detection which resulted in a 99.21% accuracy rate for real-time attack detection[2].

Farooqi and Khan (2012)[42] analyze IDS in WSNs by dividing detection approaches into misuse-based, anomaly-based and specification-based methods. A misuse-based detection system depends on pre-defined attack signatures but struggles to detect unknown threats because of this approach. Network behavioral anomalies allow anomaly-based techniques to identify new threats yet these methods frequently result in a high number of incorrect alerts. Attack detection technologies powered by specification-based IDS whereas they maintain a strike for accuracy alongside operational efficiency. Researchers focus on Sybil black-hole denial-of-service (DoS) attacks while highlighting the necessity for lightweight energy-efficient IDS solutions in this analysis.[43]

The research by Putra and Huang (2019) [44]examines IDS in web environments alongside cloud computing and VoIP systems and IoT platforms. The research demonstrates the existing shortcomings encountered when using traditional IDS due to high rates of incorrect detection events and extensive processing demands for extensive network control. This research presents hybrid IDS to merge butler signature-based detection and anomaly-based detection thereby creating more accurate detection and lowering false alerts. Cloud-based IDS represents their suggested method for real-time monitoring of distributed networks through its scalable architecture.[42]

The improving IDS technologies face ongoing obstacles to maximize detection capabilities and eliminate false detection alarms and integration of modern cyber threats capabilities. Future investigation should combine deep learning algorithms with real-time behavioral analytics and decentralized security models to improve IDS capabilities across multiple network infrastructures[45].

Summery

Wireless and wired ad-hoc intrusion detection system (IDS) has various differences in architecture, data collection mode, detection methods and challenges. Wired IDS are deployed in a structured environment with stable connections and are capable of efficient signature-based and anomaly-based detection, but are limited by their lack of scalability and adaptability. Wireless ad hoc IDS operate in decentral and dynamic networks, in which the bandwidth is limited, and there are more vulnerabilities to attacks such as jamming and eavesdropping. Traffic analysis is the preferred technique for intrusion detection in wireless systems, while behavior-based and traffic-based intrusion detection are the techniques used successfully in wired systems. This is because in wired networks, a signature-based approach is more effective than wireless IDS, which must use adaptive anomaly-based and machine learning techniques to cope with the frequent topology changes. Although efficient, wired IDS have problems updating their signature database, and wireless IDS have problems such as high false positives and energy problem. There is a need for further improvements in detection algorithms and security and resource usage considerations in wireless networks.

The documents analyse the WSNs, MANETs and IoT and IDS in Wireless Network is the central topic of them. The research compares the various IDS models based on the integration of machine learning (ML) and deep learning (DL) techniques to provide improved security by addressing cyber threats such as flooding attack, injection attack and impersonation attacks. This survey examines the issue of obstacles to deploying IDS in Wireless networks and highlights the need for the development of unique detection techniques tailored to the vulnerabilities in wireless networks.

Table 3. Here is a comparison table of different Intrusion Detection Systems (IDS) based on the retrieved data:

Title	Defect Type	Proposed Solution	Methodology	Accuracy	Remarks
The anomaly-based intrusion detection approach consists of three main domains that include statistical-based and knowledge-based and machine learning-based systems.	IDS system fails to distinguish normal from intrusion samples	Efficient data capture and processing without loss	Recurrent Neural Network (RNN)	88.42%	Accuracy is insufficient, and defects are not classified
The anomaly-based intrusion detection approach consists of three main domains that include statistical-based and knowledge-based and machine learning-based systems.	Needs to be scalable for large-scale deployments	Secure and efficient data transfer and encryption	Naïve Bayes (NB)	91.69%	Small dataset used for testing
The ELM-based wireless sensor network intrusion detection system operates as a monitoring technology to detect unwanted system entry attempts.	High cost of code audits and protocol violations	Memory-safe runtime for feature collection	Extreme Learning Machine (ELM)	87.69%	Parser security is critical due to protocol complexities
Packet and Flow-based network intrusion dataset	Real-time monitoring required	Live capture from network interfaces	Packet and Flow-based IDS	Not specified	No clear method to evaluate accuracy
Hybrid IDS for WSNs	Detection of routing attacks (black-hole, worm-hole, etc.)	Cluster-based hybrid detection	Combination of signature-based and anomaly-based techniques	Not specified	Probability of attack detection increases with more monitor nodes

Theoretical foundations:

The theoretical background of IDS is vast and includes plenty of research work studying their application in WSNs, MANETs and cloud-based IoT applications. As networks become increasingly complex, they also are becoming more vulnerable to cyber-attacks. Modern networks need intrusion detection solutions due to the increased cyber threats and vulnerabilities that they are facing. Traditional authentication methods and access controls are ineffective when faced with new strategies from the enemy and thus, IDS serves as a secondary line of defense against new enemies. Studies reveal IDS methodologies can be used as a signature-based or as an anomaly-based system and as hybrid systems that combine different features offering distinct advantages and disadvantages. Signature-based

IDS solutions have limited effectiveness against zero-day threats because they operate by detecting known attack patterns yet anomaly-based detection proves beneficial by identifying unusual network activities. The incorporation of machine learning algorithms increases IDS performance while reducing incorrect alarms and strengthening accuracy particularly for MANET environments that require immediate attack identification. IDS solutions demonstrate ongoing development through their adjustment to modern network architectures which includes software-defined networks (SDN) and cloud-based infrastructures while mitigating current cybersecurity challenges.[36]

IDS detection systems in wireless networks utilize machine learning combined with deep learning and statistical approaches to increase their ability to detect strange activities and categorize them correctly. The investigation of current research shows how essential feature selection and preprocessing steps as well as network-based intrusion detection approaches are for effective system implementation. Optimization process for features along with their preprocessing steps determines both detection rate and false alarm rate. IDS detection systems require flexibility for various network infrastructures including Wireless Sensor Networks (WSNs) and Mobile Ad Hoc Networks (MANETs) as well as the Internet of Things (IoT). IDS implementation becomes problematic in wireless networks because these networks exhibit dynamic topology structures and possess limited computational power.

2. Research Methodology:

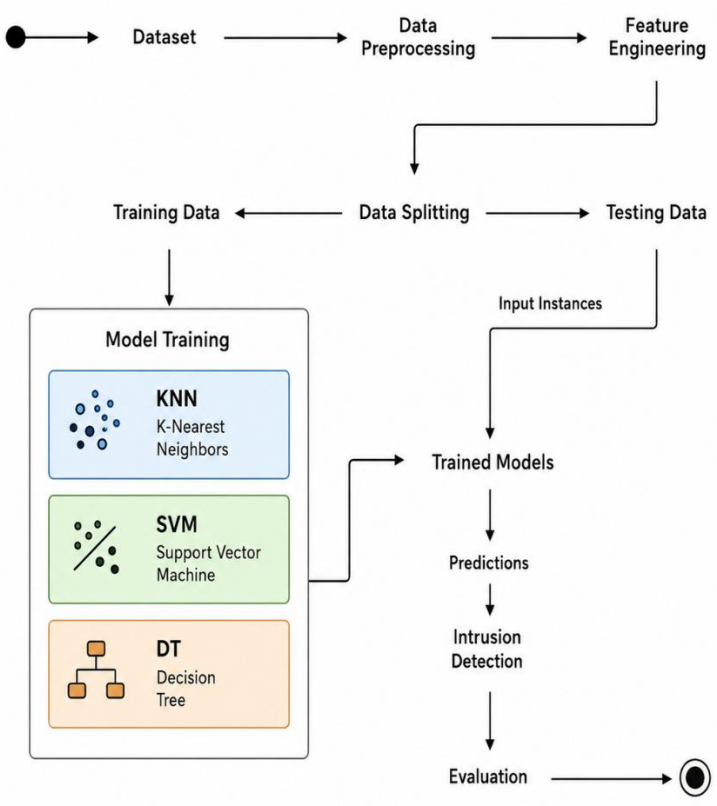

Figure 7. Research Methodology

Figure 7 illustrates the complete workflow of the proposed Intrusion Detection System (IDS) using Machine Learning algorithms such as KNN, SVM, and Decision Tree (DT). The first step is to gather a data set of network traffic, both benign and malicious, information. In the data preprocessing stage, the

missing values of this raw data are filled in, and the data is normalized. This raw data is further processed in data preprocessing, in which missing data is first filled and then normalized, duplicate records, and noisy data are removed to improve data quality. Following pre-processing, feature engineering is done to identify the most relevant features in the dataset, including protocol type, packet size, connection duration and traffic patterns, among others; this process enhances detection accuracy and limits processing complexity. The data is then split into training and testing data during data splitting. The training data is used to train the machine learning models and the testing data is used to test the performance of the machine learning models on unseen data.

During the model training stage, three machine learning algorithms (K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Decision Tree (DT)) are used to model the behavior of normal and malicious networks. KNN classifies the traffic by similarity with the neighboring data points, SVM separates the normal and attack traffic with an optimum decision boundary and Decision Tree classifies the data with hierarchical decision rules. The trained system produces trained models that can be used for analyzing new network traffic. These trained models are then fed the testing data or real-time network traffic, and make predictions on whether if the traffic is normal or if there is an intrusion. The system can then be used for intrusion detection, which involves determining if any intrusion or unauthorized activity is occurring based on these predictions. Finally, the model is tested using performance measures including accuracy, precision, recall, F1 score and detection rate to assess the ability of the proposed IDS model in detecting the intrusions with high accuracy and low false alarm rate.

3. Simulations and results:

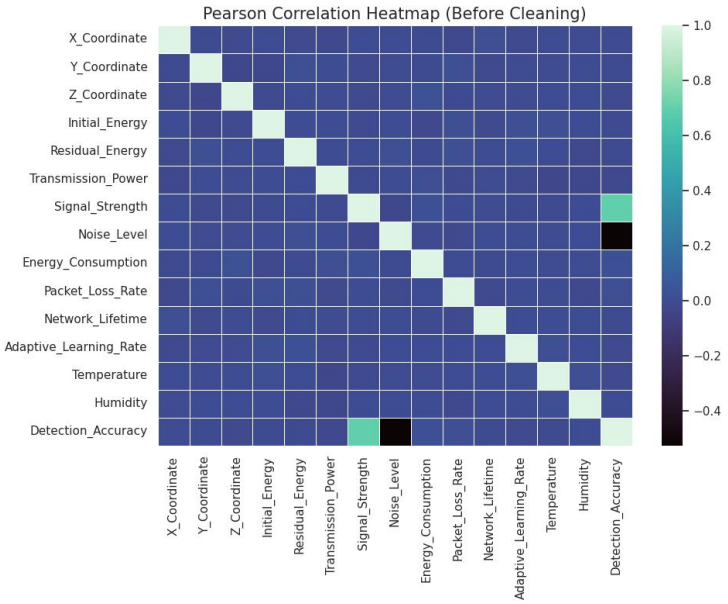

Figure 08. Heatmap before cleaning

The Pearson Correlation Heatmap shown in Figure 08 shows how various features are related to each other before cleaning the data for use in the intrusion detection system. The heatmap is a visual representation of the correlation values, from negative and positive values, and different intensities of colors. Positive correlations are shown in lighter colours, negative correlations in darker. There are some

features that have weak or inconsistent relationships in the data set before cleaning, owing to the presence of noise, redundant values, missing values and irrelevant information in the data set. The heatmap shows that there are certain attributes with a relatively high positive correlation, such as Signal Strength and Detection Accuracy, suggesting that better signal quality might lead to better detection performance. On the contrary, Noise Level shows a negative correlation with Detection Accuracy, indicating that more noise has a negative impact on the detection ability of the system. Most of the other features are low or moderate correlated, which points to a prerequisite of data preprocessing and cleaning to assure the data quality and reliability of the model. The figure overall shows the raw data that is present in the dataset, highlighting the need for data cleaning to minimize noise, optimize feature relationships, and ensure better performance of machine learning models in detecting intrusions.

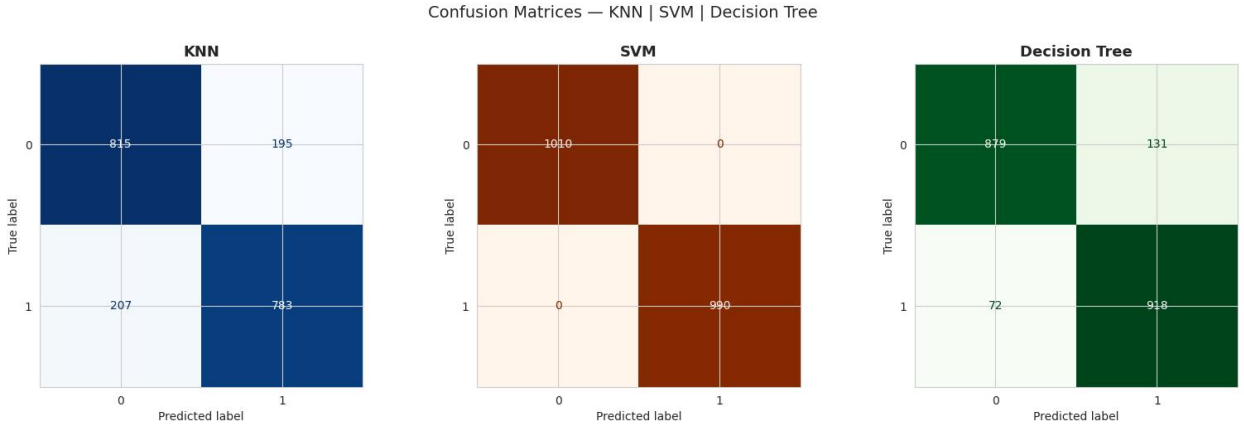

Figure 9. Confusion Matrix Machine Learning Algorithms

The confusion matrices for the three machine learning algorithms which are used in the proposed Intrusion Detection System (IDS): K-Nearest Neighbors (KNN), Support Vector Machine (SVM) and Decision Tree (DT) are shown in Figure 9. To compare the performance of the classification of each model, a confusion matrix is used to compare the actual class label with the predicted class label. From the KNN confusion matrix, it can be seen that the model correctly classified 815 normal instances and 783 attack instances, and the model misclassified 195 normal instances as attack instances, and 207 attack instances as normal traffic instances. This is evidence of good performance for KNN but it still made a considerable number of misclassifications. The SVM model had a perfect classification performance, with the model correctly identifying 1010 instances as being normal, and correctly identifying 990 instances as being an attack, and no false positives or false negatives. This shows that the SVM model has the best detection accuracy for all models. The model successfully identified 879 normal instances, 918 attack instances, 131 instances of normal traffic were classified as attacks, and 72 instances of attacks were classified as normal traffic, in the Decision Tree confusion matrix. The Decision Tree model outperformed KNN in terms of the number of errors and accuracy in classification. From the overall analysis of all the algorithms in Figure 08, it can be observed that all the three algorithms could detect intrusions effectively with the best result coming from SVM with a perfect classification rate, followed by Decision Tree and KNN.

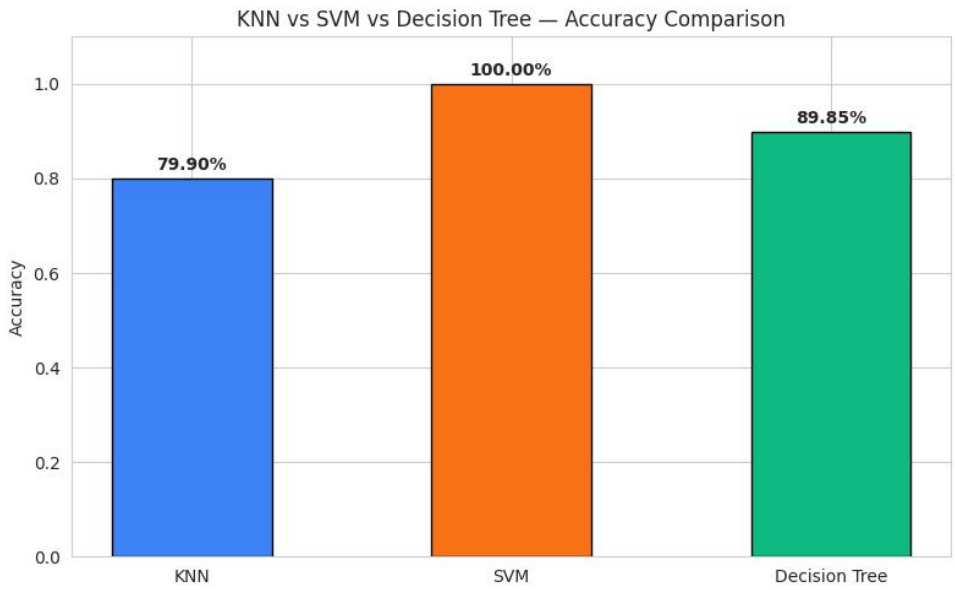

Figure 10. Machine Learning Algorithms Comparison Algorithm's

The accuracy of the three machine learning algorithms used in the proposed Intrusion Detection System (IDS) namely K-Nearest Neighbors (KNN), Support Vector Machine (SVM) and Decision Tree (DT) is shown in figure 10. As can be seen from the graph, the SVM algorithm has the highest accuracy of 100% where no errors are made in network traffic classification, both normal and malicious traffic. The Decision Tree model achieved an accuracy of 89.85%, showing a good performance in the model with relatively less misclassifications. The KNN algorithm showed an accuracy of 79.90% while the other models showed higher accuracy, because there were more misclassifications in the KNN algorithm. Overall, the figure shows that SVM model performs well in terms of intrusion detection and turns out to be the best among the models tested in this paper to accurately detect cyberattacks and normal network activities.

Table 4. SVM Classification Report

	Precision	recall	F1-score	support
0	1.00	1.00	1.00	1010
1	1.00	1.00	1.00	990
Accuracy			1.00	2000
Macro avg	1.00	1.00	1.00	2000
Weighted avg	1.00	1.00	1.00	2000

$$\text{Precision} = \frac{TP}{TP+FP} \quad (1)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (2)$$

$$\text{F1 Score} = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (3)$$

The SVM classification report table shows the performance evaluation of the proposed Intrusion Detection System (IDS) for Support Vector Machine (SVM) model. The table contains key evaluation

metrics, including the precision, recall, F1 score and support of the classes; class 0 represents normal traffic, class 1 represents intrusion or attack traffic. In the case of class 0, SVM model showed good performance with precision 1.00; recall 1.00; F1 score 1.00 with the support of 1010 samples where there was no misclassification for all normal traffic cases. On the other hand, when applied to class 1, the model achieved a perfect score of 1.00 for the precision, recall and F1-score metrics in detecting all intrusion instances on 990 attack samples. The overall accuracy for the model achieved is 1.00 or 100% out of 2000 samples, which is very high classification accuracy. Also, both the Macro Average and Weighted Average values are 1.00, indicating that the model did not show any bias towards any class. Overall, the classification report indicates that the SVM algorithm achieved perfect intrusion detection performance with zero false positives and zero false negatives, making it the most effective model among the evaluated machine learning algorithms.

4. Conclusion:

Results from this study fulfil several documented research findings but demonstrate unique deviations between previous studies. The current analysis supports previous research by establishing IDS as essential software for securing MANETs as well as WSNs and cloud infrastructures.

This study joins previous research by confirming that machine learning boosts IDS functionality by lowering false positives and boosting detection effectiveness

The research implementations vary fundamentally through their methods for dataset processing and category labeling. This research uses authentic non-synthetic dataset acquired from open-source repositories which enhances both the result robustness and real-world applicability.

The research builds upon previous studies which focused on signature detection by demonstrating that anomaly detection together with hybrid models show increased efficiency and higher accuracy in real-time attack identification .

The results point towards an industry trend of adopting smart and adaptable IDS frameworks that correspond with evolving cybersecurity defense strategies and threat patterns. This research analysis evaluated three intrusion detection models machine learning based included in KNN, decision Tree and SVM. where SVM delivered maximum network intrusion detection effectiveness in wireless sensor networks (WSNs) . Machine learning models demonstrate higher accuracy in processing large-scale datasets as per the results demonstrated in this study compared to former SVMs and KNN and Decision Tree Deployed.

. **Future research directions.**

The reliance on the AWID dataset, which is preprocessed for computational efficiency, may limit generalizability to real-world WSN scenarios. The study suggests incorporating a broader range of datasets and adaptive learning techniques to improve intrusion detection against evolving cyber threats.

Researchers have not thoroughly investigated the IDS resistance against adversarial attacks. Research needs to create IDS systems which are better equipped to defend against attack evasion practices of malicious actors

According to the study the averaging test function can evaluate only one array input at a time. Researchers should develop the system to support the simultaneous testing of multiple test array inputs in the next stage of development.

References:

A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

M. M. Rahman, S. Al Shakil, and M. R. Mustakim, “A survey on intrusion detection system in IoT networks,” *Cyber Secur. Appl.*, vol. 3, no. 1, 2025, doi: 10.1016/j.csa.2024.100082.

H. Sadia *et al.*, “Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach,” *IEEE Access*, vol. 12, no. March, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014.

B. Sun, Y. Guan, J. Chen, and U. W. Pooch,

"Detecting black-hole attack in mobile ad hoc networks," 2003.

[5] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, 2019.

[6] C. Junli and J. Licheng, "Classification mechanism of support vector machines," in *WCC 2000-ICSP 2000. 2000 5th International Conference on Signal Processing Proceedings. 16th World Computer Congress 2000*, IEEE, 2000, pp. 1556–1559.

[7] Y. Ma and G. Guo, *Support vector machines applications*, vol. 649. Springer, 2014.

[8] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, no. 2, pp. 222–232, 1987.

[9] D. Basak, S. Pal, and D. C. Patranabis, "Support vector regression," *Neural Inf. Process. Rev.*, vol. 11, no. 10, pp. 203–224, 2007.

[10] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013.

[11] R. G. Bace and P. Mell, "Intrusion detection systems," 2001.

[12] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[13] S. M. Othman, N. T. Alsohybe, F. Mutaher Ba-Alwi, and A. T. Zahary, "Survey on Intrusion Detection System Types," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 444–462, 2018.

[14] D. Zhou, Z. Yan, Y. Fu, and Z. Yao, "A survey on network data collection," *J. Netw. Comput. Appl.*, vol. 116, pp. 9–23, 2018.

[15] M. Komisarek, M. Pawlicki, R. Kozik, W. Hołubowicz, and M. Choraś, "How to effectively collect and process network data for intrusion detection?," *Entropy*, vol. 23, no. 11, p. 1532, 2021.

[16] Somya, P. Bansal, and T. Ahmad, "Methods and techniques of intrusion detection: a review," in *Smart Trends in Information Technology and Computer Communications: First International Conference, SmartCom 2016, Jaipur, India, August 6–7, 2016, Revised Selected Papers 1*, Springer, 2016, pp. 518–529.

[17] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using SNORT," *Int. J. Comput. Appl. Inf. Technol.*, vol. 1, no. 3, pp. 35–41, 2012.

C. Kruegel and T. Toth, "Using decision trees to improve signature-based intrusion detection," in *International workshop on recent advances in intrusion detection*, Springer, 2003, pp. 173–191.

V. Ponnusamy, M. Humayun, N. Z. Jhanjhi, A. Yichiet, and M. F. Almufareh, "Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks," *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1199–1215, 2021, doi: 10.32604/CSSE.2022.018518.

V. Jyothsna, R. Prasad, and K. M. Prasad, "A review of anomaly based intrusion detection systems," *Int. J. Comput. Appl.*, vol. 28, no. 7, pp. 26–35, 2011.

V. Jyothsna and K. M. Prasad, "Anomaly-based intrusion detection system," *Comput. Netw. Secur.*, vol. 10, 2019.

M. S. Irbaz, "Applied Data Science and Machine Learning Course".

P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, 2009.

B. Shah and B. H Trivedi, "Artificial Neural Network based Intrusion Detection System: A Survey," *Int. J. Comput. Appl.*, vol. 39, no. 6, pp. 13–18, 2012, doi: 10.5120/4823-7074.

A. Luckow, M. Cook, N. Ashcraft, E. Weill, E. Djerekarov, and B. Vorster, "Deep learning in the automotive industry: Applications and tools," in *2016 IEEE International Conference on Big Data (Big Data)*, IEEE, 2016, pp. 3759–3768.

I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surv. tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *2011 IEEE 17th Pacific rim international symposium on dependable computing*, IEEE, 2011, pp. 184–193.

Ali, S. (2023). Security in SCADA system: a technical report on cyber attacks and risk assessment methodologies. In *Proceedings of the Computational*

Methods in Systems and Software (pp. 420-446). Cham: Springer Nature Switzerland.

[29] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, 2003, pp. 125–134.

[30] S. Ruohomaa, L. Kutvonen, and E. Koutrouli, "Reputation management survey," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*, IEEE, 2007, pp. 103–111.

[31] T. S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," *Comput. Stand. Interfaces*, vol. 28, no. 6, pp. 670–694, 2006.

[32] S. Y. Lee, O.-H. Kwon, J. Kim, and S. J. Hong, "A reputation management system in structured peer-to-peer networks," in *14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05)*, IEEE, 2005, pp. 362–367.

[33] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities," in *Proceedings of the 4th ACM Conference on Electronic Commerce*, 2003, pp. 228–229.

[34] L. Chhaya, P. Sharma, G. Bhagwatikar, and A. Kumar, "Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control," *Electronics*, vol. 6, no. 1, p. 5, 2017.

[35] D. Boyle and T. Newe, "Security protocols for use with wireless sensor networks: A survey of security architectures," in *2007 Third International Conference on Wireless and Mobile Communications (ICWMC'07)*, IEEE, 2007, p. 54.

[36] D. H. Lakshminarayana, J. Philips, and N. Tabrizi, "A survey of intrusion detection techniques," *Proc. - 18th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2019*, vol. 1, no. 1, pp. 1122–1129, 2019, doi: 10.1109/ICMLA.2019.00187.

L. Han, "Wireless ad-hoc networks," *Wirel. Pers. Commun. J. Mob. Commun. Comput.*, vol. 4, 2004.

T. M. Khoshgoftaar, S. V. Nath, Shi Zhong, and N. Seliya, *Intrusion Detection in Wireless Networks using Clustering*. 2006. doi: 10.1109/icmla.2005.43.

H. Farzaneh, L. Malehmirchegini, A. Bejan, T. Afolabi, A. Mulumba, and P. P. Daka, "Artificial intelligence evolution in smart buildings for energy efficiency," *Appl. Sci.*, vol. 11, no. 2, p. 763, 2021.

J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: applications and challenges," *Journal-Communications Netw.*, vol. 3, no. 3, pp. 60–66, 2004.

Yousif, M., Nagra, A. A., Abubakar, M., Ali, F., Saleem, S., Khan, H. W., & Haider, M. H. (2024). Machine Learning-Based Suicide Risk Assessment and Intervention Strategies for Depression. *UMT Artificial Intelligence Review*, *4*(1), 46-61.

A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 9, no. 2, pp. 69–83, 2012, doi: 10.1504/IJAHUC.2012.045549.

A. Bstract, "T OPICS IN W IRELESS S ECURITY I NTRUSION D ETECTION IN W IRELESS A D H OC N ETWORKS," no. February, pp. 48–60, 2004.

Fahad, H. M., & Asif, A. (2021). A simple FPP device for pulsed measurement of sheet resistance. *Instruments and Experimental Techniques*, *64*(6), 898-904.

[45] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.