INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Enhancing Security Features in WSNs using Autoencoder-Based Intrusion Detection and ECC with Dynamic Key Rotation

Muhammad Puzhakkalaveettil[1]*, M Praveena[1]

1 Department of Computer Science, Dr. SNS Rajalakshmi College of Arts & Science (Autonomous), Coimbatore, Tamil Nadu, India

OPEN ACCESS

Received: 13/06/2025

Accepted: 26/06/2025

Published: 13/07/2025

Citation: Puzhakkalaveettil M, Praveena M (2025) Enhancing Security Features in WSNs using Autoencoder-Based Intrusion Detection and ECC with Dynamic Key Rotation. Indian Journal of Science and Technology 18(27): 2198-2213. https://doi.org/10.17485/IJST/v18i27.1102

* **Corresponding author**.

muhammadpvresearchcs@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To propose an intelligent, dual-layered security model to detect anomalies in wireless sensor networks for secured data transmission in large-scale WSN environments. The proposed model integrates deep learning and adaptive encryption methods to address security breaches in smart environments due to their lightweight and distributed nature. **Methods:** Auto-Encoder Neural Network (AEN) is employed to detect abnormal behavior in sensor nodes based on reconstruction error thresholds. Post validation, Elliptic Curve Cryptography (ECC) is integrated with Dynamic Key Rotation (DKR) to encrypt the data packets. It adjusts the cryptographic keys based on network conditions to enhance the node resistance to replay and key compromise attacks. Multi-hop swarm route optimization is used for the finest routing process to ensure the node reaches the destination in the optimal route. NS2 simulation is carried out with three sets of datasets, NSL-KDD, CICIDS, and simulated data with parameters to assess the performance of the proposed AEN-ECC model to ensure real-time attack resilience, end-to-end secure communication and scalability to larger WSNs under dynamic network conditions. AEN-ECC is compared against state-of-the-art machine learning-based security methods like SVM-AES, RF-KSS, and XGBoost-FR. **Findings:** The proposed intelligent, adaptive, and lightweight AEN-ECC model achieved promising results with a 90.2% Packet Delivery Ratio, 91.4% Confidentiality Rate, 90.6% Attack Detection Accuracy, 90.1% Robustness to Node Failures, 92.7% network life time and 28.5 ms reduced Latency and stands as a solution for WSNs that ensure both confidentiality and anomaly resilience. **Novelty:** This research moves beyond static security protocols and presents a unified security model that learns from network behavior and adapts dynamic encryption by using an unsupervised AEN enhanced with ECC and DKR to provide scalable and energy-aware model capable of addressing the real-world security challenges faced by WSNs.

Keywords: Wireless Sensor Networks; Network Security; Elliptic Curve Cryptography; Dynamic Key Rotation; Intrusion Detection

1 Introduction

WSNs have become the backbone of model smart environments, which enables real-time monitoring in sectors like healthcare, agriculture, defense, and urban environments. WSNs consist of energy-limited and lightweight sensor nodes that collaboratively operate to transmit sensitive data from source to destination. As WSNs are deployed in large-scale environments, secured data transmission in real-time is a high priority without degrading the network performance. The limited computational capabilities and open architecture allow intruders to attack and steal the data, making it easy for cyber threats like data interception, node compromise, and routing attacks. Traditional security mechanisms combining machine learning and encryption models like, SVM-AES offer reasonable classification accuracy but consume excessive energy due to computation load by AES; RF-KSS deals with synchronization challenges across distributed nodes, leading to high latency and increased attack surface. While XGBoost-FR performs well on pre-classified data, it struggles in dynamic WSN settings and fails to detect zero-day threats effectively. To overcome the limitations, this research proposes a hybrid deep learning approach that combines unsupervised AEN for anomaly detection with ECC enhanced by DKR to ensure lightweight, scalable encryption based on risk factors and energy levels. This dual-layered deep learning-based AEN-ECC security model addresses anomaly detection and confidential data transmission, making it highly suitable for LS-WSN environments, which demand intelligence and efficiency.

Various machine learning models[(1)] for intrusion detection in WSNs using benchmark datasets were proposed with techniques like Decision Trees, Naïve Bayes, SVM, etc., to evaluate the intrusion patterns. Feature-based learning was highly emphasized for pre-processing but suffers from high FPR due to static thresholding and lack of adaptive learning. Though an Accuracy of 82% was acceptable in simulated environments, the integration of a few significant components like dynamic routing, encryption handling, and hybrid learning strategy is lacking in the system, which limits the effectiveness in real-time deployments under adversarial conditions. TSO with Random Forest Classifier[(2)] was employed to enhance the feature selection to boost the IDS in LORA-WSNs. This hybrid technique refines the classifier boundaries under imbalanced data distributions. The model relies on static routing and cryptographic modules, which lack packet delivery rate and robustness to active attacks. The real-time adaptability is constrained by computational overhead that is unsuitable for energy-constrained nodes. The packet level security is not addressed in the TSO-RFC model, which is considered a significant drawback. A hybrid GSWO-Catboost[(3)] algorithm for IDS in WSN was proposed with the integration of global search optimization for feature weighting and catboost for classification. A notable improvement was noted during the implementation; the model handles nonlinear intrusion patterns dynamically and resists overfitting on noisy data. The major drawback of this framework is that it focuses only on data classification and omits encryption, trust modeling, key refresh mechanism, and routing intelligence, which limits data protection against session-based attacks. The dual classifier using SVM-AES[(4)] and RNN was employed in UWSNs to enhance the strong intrusion detection capabilities with sequence modeling mechanisms. The model works on static data and suffers from high latency and energy, particularly during sequential training. Additionally, the model focuses on a static key handling system and does not involve adaptive encryption or dynamic routing. It lacks its performance in secured data delivery, feature learning, and high retransmission rates. Though the model achieves an accuracy of 84%, it limits application in rapidly changing LS-WSN topologies. Dimensionality reduction and data balancing techniques prior to IDS are adopted using ensemble machine learning methods[(5)]. The ES-ML model enhances class separation and classification on imbalanced network-defined traffic datasets. 78% accuracy is achieved with a lack of robustness regarding attack replays. The model lacks encryption handling, routing behavior, energy-aware transmissions, dynamic session-key management, and adaptive learning. However, it limits the applications due to the static security layer and lack of integration of dynamic protocols. A bio-inspired ABC routing protocol[(6)] was proposed to detect dynamic link failure in WSNs, bypass failed paths, and identify alternate routes based on available high-energy nodes and quality metrics. The model focuses more on packet delivery and node transmission without addressing packet security or anomaly detection. The node-level link failures and other aspects like sleep schedules, dynamic response, etc., are not analyzed, which limits the RABC model's capacity to detect IDS from packet injection or replay attacks. The protocol lacks dynamic encryption schemes, making it vulnerable to surveillance in large-scale hostile WSN environments. A Generative Adversarial Network with bio-inspired protocol[(7)] was introduced to enhance security and data transmission in IoT-based WSN networks. In BIP-GANs, GAN generates synthetic data for testing and detecting anomalies with high accuracy while the routing layer optimizes the communication paths. The model innovatively combines route optimization and data generation, which shows a dynamic performance in robustness and data delivery. The only drawbacks of the model are the lack of dynamic key handling and the non-inclusion of encryption mechanisms. Also, GAN remains a computational burden for sensor nodes with limited processing capability during real-time synchronization. ML and DL classifiers[(8)] detect the physical layer spoofing by capturing the RF fingerprinting and transmission traits in multiple attempts. Though the approach is practical at the physical layer, it lacks the upper-layer anomaly detection and secure routing capacity. The model's strength lies in attribute diversity, but the scope is restricted to access-level validation. The major drawback is that there is no dynamic trust management, and key refreshing concepts are integrated to provide end-to-end security in multi-hop WSN topologies. Three

QoS-enabled bio-inspired methods[9] are adapted to enhance the path-finding for robust data delivery in WSNs. The model works well on dynamic topologies, detects node link failures, and is self-attentive in finding alternate routes to deliver the packets to the destination. However, it lacks packet security and real-time anomaly detection and does not accommodate adaptive trust malicious node exclusion. Due to a lack of attack classification, the model's ability to secure packets or authenticate data transmissions remains limited. The model is compared with three state-of-the-art models and outperforms in dynamic routing and link failure detection. A transformer-based autoencoder fused with IF and XGBoost[10] for IDS and malfunction node detection in WSNs was explicitly introduced for forest fire prediction systems. Due to AEN integration, the hybrid architecture works with string temporal pattern recognition and unsupervised outlier detection. Though it is purely detection-oriented, it does not include routing schemes and encryption mechanisms to update the confidentiality controls. Its effectiveness is bound to centralized inference, where the energy constraints of nodes in real-time WSN deployments are not addressed. A multi-modal ML framework[11] was proposed to enhance IoT system security using classification algorithms for malicious nodes and anomaly detection. To identify attack patterns, the work is tested using multi-classifiers such as DT, RF, and GB on real-time IoT datasets. The model achieved good precision and recall but suffered from low adaptability in dynamically challenging WSN network conditions. The real-time routing inconsistencies were not addressed, which limits its deployment in high-security applications. RVSRP-DP[12] was proposed to detect dynamic link failure in WSNs using the intelligent swarm-based bio-inspired model. Though RVSRP-DP achieves dynamic path exploration, the model lacks real-time attack resilience due to the non-integration of the encryption mechanism. XGBoost[13] machine learning model was utilized to improve IoT security through anomaly prediction and classification. The model used feature selection and a boosting-based classifier to identify intrusions in search space across the connected nodes. Due to the absence of a key distribution and encryption rotation mechanism, the model is less effective for secure and scalable LS-WSN environments.

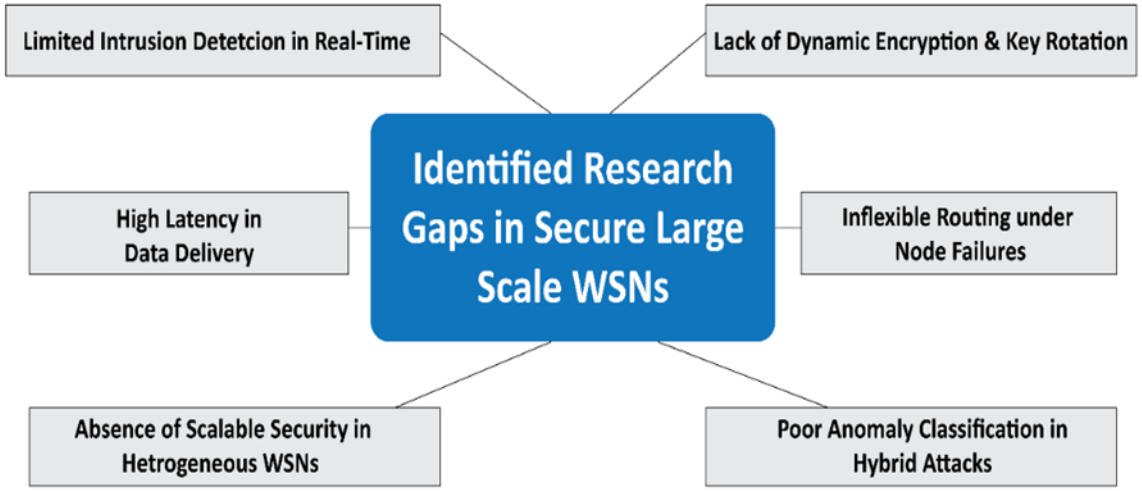

Fig 1. Research Gap

2 Methodology

This section presents a robust, multi-layered security framework for dynamic LS-WSNs operating in adversarial and resource-constrained environments. The proposed AEN-ECC with DKR is designed to detect anomalies using its adaptive learning and encryption strategy to secure data transmission with optimal routing. The bi-fold model enhances intrusion detection accuracy, data confidentiality, and delivery reliability using a deep learning algorithm and lightweight cryptographic protection. The target objective is to address security breaches in bright environments and to mitigate the security lapses caused by static cryptographic systems. This hybrid AEN-ECC framework operates in a distributed sensing environment deployed in sensitive and security-based monitoring applications with adequate settings like real-time response, resistance to node compromise, and secure communication over unpredictable network topologies. A need analysis revealed that the existing models struggle to address the multi-challenge of anomaly detection, encryption agility, and routing optimization, which is not recommended for volatile and high-risk WSN ecosystems. To address the gap, the proposed AEN-ECC with DKR is designed with multi-layer adaptive learning, securing, and routing to operate with seamless performance even under topology changes. For experimental

Table 1. Merits and Drawbacks of Related State of Art Models

Model	Methods Adopted	Merits	Limitations
Boosting Algorithms for WSN-LEACH DoS Detection [14]	ML-based boosting algorithms (AdaBoost, Gradient Boosting)	Improves detection in WSN-LEACH DoS datasets and handles attack-specific features	The model is not optimized for Node Mobility or Energy-Aware Deployment
ML-based Detection for Krack and Kr00k [15]	Anomaly classification using ensemble learning	Focused on Protocol-Specific Vulnerabilities (IEEE 802.11)	Fails to scale across low-energy nodes in WSNs
Intelligent Water Drop Algorithm [16]	Bio-inspired Water Drop Routing Algorithm	Improves QoS and bypasses Dynamic Link Failures in LoRA-WSNs	Does not encrypt Network Traffic and no Anomaly Resilience
Hybrid ML-NN for Industrial IDS [17]	ML Feature Extractor + NN Classifier	Accurate Detection in Industrial Control Environments	Limited Adaptability in Distributed Sensor Topologies
ML-based IoT Security Survey [18]	Review of supervised/unsupervised models for IoT	Comprehensive model taxonomy and future directions	Complete node-level Deployment Insights and Limitations on Security
EAP-IFBA Protocol [19]	Improvised Bio-Inspired Firefly Algorithm + Sleep Scheduling Method	Energy-aware Routing and Dynamic Load Balancing	No Detection of Packet Tampering or Spoofing
Reconnaissance Bee Colony with AES & AE [20]	ML-assisted Routing + Custom AES-AE Encryption	Combines Secure Routing and Lightweight Cryptography	High key setup delay; lacks anomaly feedback loop
3D CNN Model for Feature Detection [21]	Deep 3D CNN on DICOM data	Strong Spatial Feature learning for deep analysis	Not focused on Dynamic Network Layer Security
Deep Learning for Pattern Recognition [22]	CNN-RNN architecture for Gesture Recognition	Efficient real-time recognition from video frames	No Routing, Encryption, or Energy Awareness
Multivariable DL with AEN & Mask R-CNN [23]	Autoencoder-Based Region-based CNN Feature Analysis	Efficient Multi-Anomaly Feature Extraction	No support for Distributed Sensor Systems
YOLOv8 with CNN for Object Detection [24]	YOLOv8 and CNN Inference Engine	High-speed detection in soft computing applications	Does not offer any security or routing support in multi-layer WSN system
ROB-ENS Adversarial Ensemble Model [25]	Adversarial Ensemble + Anomaly Injection	Boosts Model Robustness against Spoofed Traffic	Scalability and Key Rotations are not addressed

analysis NSL-KDD, CICIDS, and simulated datasets are used. The model is compared with prevailing models such as SVM-AES [4], RF-KSS [5], and XGBoost-FR [5]. The flow diagram of the proposed AEN-ECC model is shown in Figure 2.

2.1 Autoencoder Based Anomaly Detection

In the proposed multi-layer model, AEN is deployed as a first line of defense for anomaly detection in WSNs. AEN is trained by default exclusively on benign network traffic due to its unsupervised learning nature. This allows the system to learn the standard behavioural patterns of nodes and flag the deviations as potential anomalies. During the process, the encoder compresses the high-dimensional input to low-dimensional latent space, and the decoder reconstructs input from the compressed representation. During inference, the reconstruction error serves as the primary indicator for anomaly detection. Let the input vector of features at time t is represented as $X_t = [x_1, x_2 \ldots\ldots, x_n]$, where X_t is input vector, x_1, x_2 represents multi features like packet drop rate, signal strength, hop count etc. and n is the number of monitored features in each node for anomaly detection. Here, the encoder compression is mathematically represented in the below equation.

$$Z_t = f\left(W_e . X_t + b_e\right) \tag{1}$$

where, Z_t is the latent representation, W_e, b_e are the encoder weights and bias, $f(.)$ is a non-linear activation function. After encoding, the decoding reconstructs the input vector as

$$XR_t = g(W_d . Z_t + b_d) \tag{2}$$

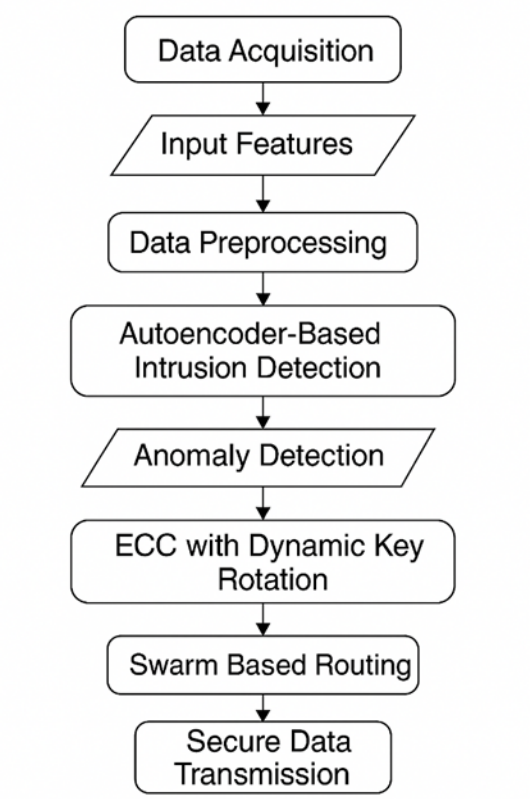

Fig 2. Flow Diagram of the Proposed Model

where, XR_t is the reconstructed input, W_d, b_d are decoder weights and bias and $g(.)$ is the sigmoid-linear activation function. The RC -Error is computed to detect anomalies such as,

$$RE_t = ||X_t - XR_t||_2^2 \tag{3}$$

If, RE exceeds a threshold limit, the node behavior is flagged as anomalies. The AEN process sets the threshold limit based on the statistical distribution of training reconstruction errors. (Example: 90th Percentile of Training). This dynamic approach enables the model to detect malicious packet injections from intruders during data transmissions, node behavior drifts with specific attacks, etc. Regarding the NSL-KDD and CICIDS datasets, the AEN is trained solely on benign traffic records to learn the baseline behavior on the datasets, including multiple network features like SD bytes, protocol type, and flag indicators in a pre-processed and normalized manner. During the testing, both normal and malicious records are passed through AEN for classification. This method dynamically detects novel attacks, such as port scanning, DoS, etc., without requiring labeled attack signatures.

2.2 Secure Communication with ECC and DKR

The The model's next phase is integrating ECC with DKR, a lightweight, robust encryption technique. ECC offers a low-overhead public key encryption scheme ideal for resource-constrained environments. ECC is augmented with key rotation to ensure temporal security by constantly updating keys during transmission cycles. This dual security framework prevents key compromise, MITM attacks, and replay attacks while maintaining data integrity and confidentiality in many applications.

2.2.1. Key Generation and Encryption

ECC operates with the principle of elliptic curve over finite fields. Let's assume that $E_p(a,b)$ as elliptic curve and each corresponding node is assigned a private key $d \in [1,\ n-1]$ and a corresponding public key $P = d.G$, where G is base point on elliptic curve with scalar multiplication. The key generation and encryption are mathematically expressed as,

$$E_p(a,b)\ : y^2 = x^3 + ax + b\ \ mod\ p \tag{4}$$

where, p is the field prime value, a and b are curve parameters and x, y are the set points from ECC domain. In order to transmit the data securely, the sender encrypts the message M using the receiver public key P_r which is expressed in the below equation.

$$C = (k.G, M + k.P_r) \tag{5}$$

where, k is the session key per transaction and C is the cipher text tuple sent over the network.

2.2.2. Dynamic Key Rotation

In DKR, the session key k is dynamically updated based on the node timestamp, residual energy, channel state and packet integrity. The key index k_i is updated and the equation is given below.

$$K_i = H_{hash}\,(k\ ||T||\,E_r||\,) \tag{6}$$

where, H_{hash} is the hash function, T is the time node stamp, E_r is the residual energy of node and SNR is signal to noise ratio. After rotating the new key is updated as $K_{new} = K_i\ mod\ n$. This updated key is used in further encryption rounds to ensure security and confidentiality in transmission process. The network packet features are fully extracted from NSL-KDD and CICIDS during real-time implementation.

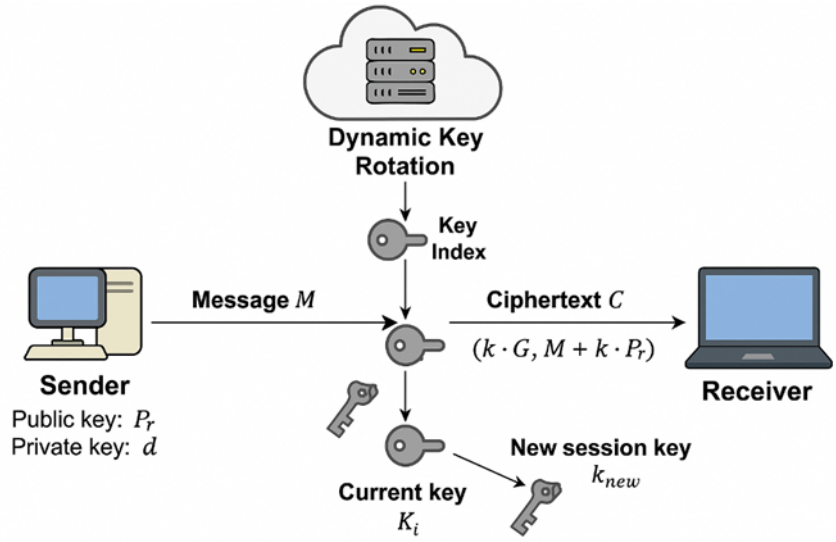

Fig 3. Secure Communication with ECC and DKR

Each packet is encrypted with ECC using the current key, and DKR refreshes the key simultaneously based on anomaly scores to transmit the data more securely which is shown in Figure 3. During attack scenarios in CICIDS, the model identifies abnormal node behavior and triggers the key rotation process to minimize data leakage and ensure stable confidentiality under various attack processes.

2.3 Swarm Based Intelligent Routing

This model integrates the swarm intelligence routing method as the third phase to ensure optimal, secure, and congestion-free paths are selected for the secured data transmission process in LS-WSNs. Swarm intelligence simulates the behavior of biological swarms (birds, ants, etc.), where the decentralized agents (sensor nodes) collaboratively identify the finest solutions through local integrations. Each node maintains its routing model, and its neighbours adapt dynamically as network conditions change, such as link failures, energy depletion, attacks, etc. Assume that the position of node i in routing is denoted as $X_i(t) = [x_1, x_2, \ldots . x_n]$, where $X_i(t)$ is the position vector of i^{th} node at time t. Each x_j represents the routing path parameter such as hop-count, residual energy and signal strength. Here, n is the number of routing features. Each node (agents) adjusts the routing path based on its personal best and global best P_i and G using the below equation.

$$V_i(t+1) = \omega V_i(t) + c_1 r_1 (P_i - X_i(t) + c_2 r_2 (G - X_i(t)) \tag{7}$$

where, $V_i(t)$ velocity, ω is inertia weight, $c_1 c_2$ refers the learning factors and $r_1 r_2$ are the random numbers for stochastic movement. Once the node adjustments are done, the updated routing path will be defined which is expressed mathematically in the below equation.

$$X(t+1) = X_i(t) + V_i(t+1) \tag{8}$$

According to network dynamics, the continual adjustment ensures routing decisions which remains more responsive and dynamic. A fitness function F_i is used to evaluate each path based on residual energy (E_r), noise ratio (SNR), hop-count (H), estimated delay (D) and weights $(\alpha, \beta, \gamma, \delta)$. The evaluated fitness function is expressed in the below equation.

$$F_i = \frac{\alpha E_r + \beta SNR}{\gamma H + \delta D} \tag{9}$$

In Swarm based model, the paths with the maximum F_{value} are used for transmission process. If a node's F_{value} degrades (e.g., due to low energy or high delay), the packets are re-routed through a stronger neighbour node using swarm intelligence. During real-time testing, the datasets are injected into NS2, each packet are associated with traffic descriptors like byte counts, flags and type of service which influences swarm-based decisions. If any anomaly is detected by AEN, the routing layer avoids the flagged node and triggers re-evaluation of fitness across neighbour node for alternate routing process through healthy and error free paths which guarantees the data delivery process. Figure 4 shows the re-routing process from source to destination with alternate node due to link failure.

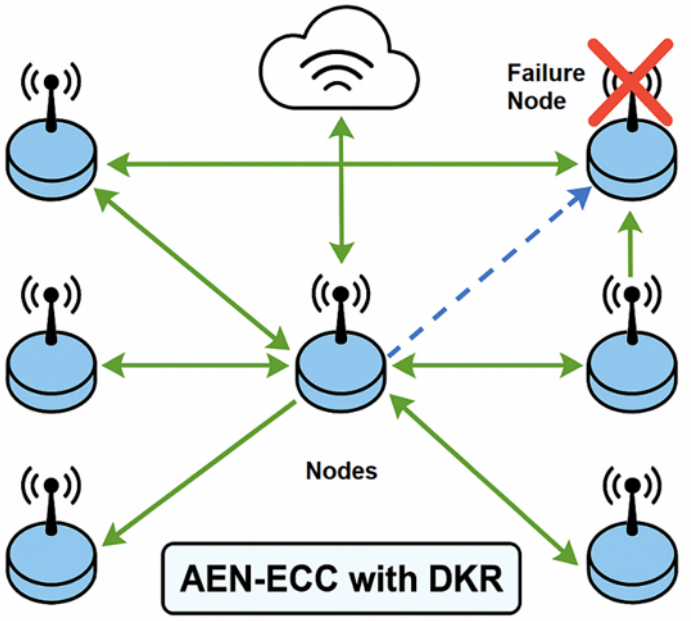

Fig 4. Intelligent Routing Process

2.4 Dataset Description and Simulation Setup

The proposed AEN-ECC with DKR is evaluated using two intrusion detection datasets, NSL-KDD and CICIDS, which comprise realistic traffic traces that simulate normal and abnormal behaviors. NSL-KDD has 41 features, and CICIDS provides detailed network flow attributes such as connection time, data size, service type, and flow flags. For this research, 22+ features are carefully selected to fit the constraints of WSN nodes. The simulation time was set to 1000 seconds, using CBR (Constant Bit Rate) traffic over UDP, with each packet sized at 512 bytes. Nodes used the RWM model for operations in search space. AEN anomaly detector analyzes the deviations in each deployed node using reconstruction error. Table 1 shows the experimental settings for simulation, and Table 2 shows the essential features of the testing process in LS-WSN environments.

Table 2. Experimental Settings for Simulation and Testing

Parameters	Value / Settings	Description
Number of Sensor Nodes	2500	Total number of sensor nodes deployed in simulation
Simulation Time	1000 seconds	Total simulation duration
Routing Protocol	Swarm-Based Intelligent Routing	Dynamic routing based on swarm intelligence
Security Layer	ECC with DKR	Lightweight encryption and key management layer
Anomaly Detection Model	Autoencoder Neural Network	Deep learning model for real-time anomaly detection
Encryption Technique	Elliptic Curve Cryptography (ECC)	Public-key cryptography suitable for low-power nodes
Key Rotation Strategy	Dynamic Key Rotation (DKR)	Keys are rotated dynamically per session or anomaly
Dataset Used	NSL-KDD, CICIDS 2017	Intrusion detection datasets used for traffic generation
Total Features Used	22	Selected features after preprocessing from datasets
Packet Size	512 bytes	Size of each data packet in bytes
Transmission Range	250 meters	Maximum range for node communication
Energy per Node	2 Joules	Initial energy allocated to each sensor node
Mobility Model	Random Waypoint	Movement pattern of sensor nodes
Traffic Type	CBR (UDP)	Type of traffic generated between nodes
Attack Injection	Yes (Real attack traffic from datasets)	Attack scenarios created using real dataset samples
Threshold for Anomaly	95th percentile RE	Dynamic threshold based on reconstruction error
Key Update Interval	30 seconds or on anomaly	Time interval or condition for key rotation

Table 3. Selected Dataset Features (Three Categories)

Category	Feature Name	Description	Data Type
Network Conditions	Packet Delivery Ratio	Ratio of successfully delivered packets	Percentage (%)
	Signal Strength (RSSI)	Received signal strength indication	Numerical (float)
	Hop Count	Number of intermediate nodes in path	Integer
	Network Load	Volume of traffic handled per unit time	Numerical (float)
Security Behaviour	Intrusion Flag	Binary flag indicating attack occurrence (0: No Attack, 1: Attack)	Binary
	Anomaly Score (RE)	Reconstruction Error score from Autoencoder	Numerical (float)
	Trust Level	Trust score of nodes based on past behavior (0 to 1)	Float
Environmental Data	Temperature	Local temperature reading from node sensor	Numerical (°C)
	Humidity	Local humidity level	Numerical (%)
	Motion Status	Indicates motion detection (0: No Motion, 1: Motion Detected)	Binary

Data Collected Source: NSL-KDD: https://www.kaggle.com/code/eneskosar19/intrusion-detection-system-nsl-kdd CICIDS: https://www.unb.ca/cic/datasets/ids-2017.html

2.5 AEN-ECC with DKR Architecture Diagram

AEN-ECC with DKR presents a robust architecture for security and an optimized data transmission process for large-scale wireless sensor networks. The model has three modules operating with AEN, ECC with DKR, and Swarm-based routing. Each node is deployed dynamically over a pre-defined network and monitored under various parameters like energy, signal strength, traffic, etc. Feature vectors are constructed using live and augmented data to compute AEN reconstruction errors. The packets are encrypted using ECC to prevent MITM attacks and intruders. DKR refreshes the keys periodically or when anomalies are detected to ensure smooth data transmission to the destination. Swam intelligence evaluates optimal next-hop paths to send data in the finest routing to boost the data delivery and link quality with the help of the fitness score of each node. Figure 6 shows the integrated architecture with high throughput, secure data transmission with low latency, and resilience to attacks and link failures in real-time LS-WSN environments.

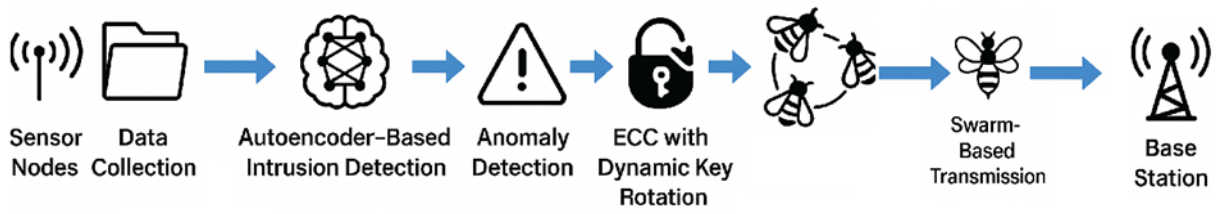

Fig 5. AEN-ECC with DKR Process Diagram

1. **Input:** Network Datasets
2. **Begin:** Start Data Sensing and Transmission Cycles

   Network Initialization Process

3. Define Network Range $Network\ Area : R = 1000x1000\ m^2$
4. $Deploy\ WSN\ Nodes\ Dynamically : N_c = 2500$

   Node Behavior

5. Input Data Vector from Node $X_t = [x_1 \dots \dots . . x_n]$

   Apply Auto Encoder

6. Trigger Anomaly Alert, If

   $Anomaly\ Behavior = True$, Else Transmit Data

   ECC Based Communication with DKR

7. $Encrypt\ Packet\ using\ ECC$

   $C_i = ECC_{Encrypt}$

   Rotate Keys / Refresh Keys Dynamically

8. $Generate\ Session\ Based\ Dynamic\ Key\ K_i$

   $K_i = H(K\ |T\ |\ E_r|\ SNR)$ and Update Keys

   Swarm Based Routing

9. $Evaluate\ Fitness\ for\ Next\ Hop\ Selection$

   $Find\ F_{Route}(i,j)$ and Forward Data Packets

   Sink Node Operations

10. $Decrypt\ and\ Validate\ using\ PrivateKey$

2.6 Performance Evaluation

The performance evaluation of the proposed AEN-ECC is to assess the model's reliability, adaptability, and security strength in real-world dynamic LS-WSN scenarios. The key performance metrics used in this research are Packet Delivery Ratio, Latency, Confidentiality Rate, Attack Detection Accuracy Network Performance, and Robustness to Node Failures, which reflect the effectiveness of the system and how well it maintains secured data transmission under attack and failure conditions. The model was tested under realistic constraints such as energy limits, node density, and dynamic topology. Anomaly detection was tested using 2500 node counts from simulated intrusion traces; NSL-KDD and CICIDS were injected. The AEN classifies normal, and

anomaly patterns based on reconstruction error with the threshold set at the 95th percentile of normal behavior to minimize FPR and adapt to pattern drift. NS2/NS3 simulation tool is chosen to simulate the encryption overhead and accurately capture the routing anomalies in LS-WSNs. During real-time deployment, the success rate of AEN-ECC is 91.3%, which indicates strong reliability in secured packet delivery and anomaly detection. The 8.7 failure rate was due to node disconnections and threshold margin overlaps in ambiguous data cases, which is acceptable in highly dynamic LS-WSN environments. Figure 6 clearly shows the success and failure rate of the proposed model

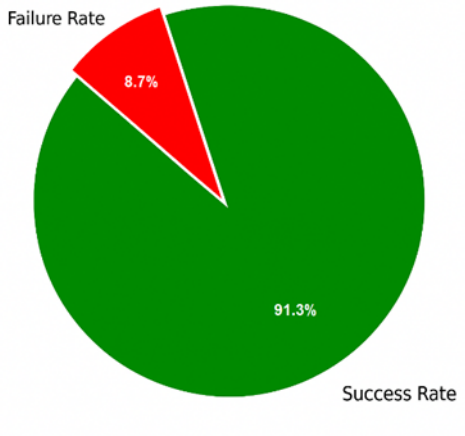

Fig 6. Success and Failure Rate of AEN-ECC with DKR

2.7 Performance Evaluation Metrics Equations

$$Packet\ Delivery\ Ratio\ =\ \frac{P_{Received}}{P_{Sent}}\ x\ 100 \tag{10}$$

where, P_{sent}, $P_{Received}$ is number of packets sent and received.

$$Latency\ =\frac{\sum\ [\ Packet\ Received\ Time-Packet\ Sen\ Time\ ]}{Total\ Packets\ Received\ (PR)} \tag{11}$$

where, PR is total packets in the networks

$$Confidentiality\ Rate\ =\ \left[\frac{Encrypted\ Packets\ Delivered\ Securely}{Total\ Packets\ Delivered}\ \right]x\ 100 \tag{12}$$

$$Attack\ Detetcion\ Accuracy=\left(\frac{TP+TN}{TP+TN+FP+FN}\right)\ x\ 100 \tag{13}$$

$$Robustness=\left(\frac{Successful\ Deliveries\ After\ Node\ Failures}{Total\ Expected\ Deliveries}\right)\ x\ 100 \tag{14}$$

$$Network\ Performance=\left(\frac{PDR+CR+ADR+RNF}{4}\right) \tag{15}$$

2.8 Ablation Study and Impact Analysis

To evaluate the individual contribution of each component, the ablation study has been conducted in this research work with 2500 node counts. The core components of this model are AEN, ECC, DKR, and Swarm Routing. Initially, anomaly detection was tested with AEN, achieving 84.3%, which lacks robust encryption, leading to moderate packet loss and a low confidentiality rate. When ECC was integrated with AEN without key rotation, the confidentiality was improved to 88.5% with some suspect key issues, which led to a slowdown in replay attacks. After the integration of DKR, the robustness is dynamically increased to 90.1% and the confidentiality rate to 91.4%. The integration of swarm routing significantly boosted the PDR to 90.2% and detection accuracy to 90.6%. The impact analysis shows that AEN was crucial in reducing FP. ECC with DKR contributes to secured data transmission under dynamic network topology, and swarm routing enables adaptive communication and packet delivery. This combination of deep learning and cryptographic modules demonstrated an intelligent multi-layered system rather than reliance on a single algorithmic implementation. All the core components are tested individually to get the real-time impact to assess the performance of proposed model.

2.9 Need for Real Time Implementation

The real-time implementation of AEN-ECC with the DKR model is crucial to assessing field-deployed WSN systems' practical viability. Some mission-critical applications use WSNs, such as battlefield surveillance, healthcare monitoring, wearable devices, smart agriculture, etc., where immediate response to the intrusion/attacks is more vital. These environments are unpredictable, and simulations cannot capture issues like sensor calibration drift, unstable communication, or fluctuating energy constraints. Real-time deployment helps validate whether the AEN adapts live data anomalies while maintaining low latency and false rates. ECC is assessed for its cryptographic handshake consistency, especially in node failure scenarios. Evaluating these elements in live LS-WSNs helps spot synchronization problems, overhead delays, and energy depletion spikes due to multi-encryption routines.

2.10 Complexity Analysis

In this model, time complexity, computational complexity and space complexity analysis was conducted. The AEN primarily impacts time complexity during the training phase, with a theoretical cost of $O\ (n\ x\ m\ x\ e)$, where $n = input\ features$, $m = hidden\ neurons$ and $e = number\ of\ epochs$. The inference remains constant $(O(n))$, making it suitable for real-time anomaly detection. ECC introduces low computational overhead compared to AES and RSA models due to shorter key strengths (256-bit ECC = 3072-bit RSA), maintains encryption and decryption in $O\ (\log k)$ time, where k is key size. DKR executes all the communication session which enhances the resilience of the LS-WSNs under multiple key rotation scenarios. In terms of space complexity, the model maintains a lightweight foots where the compact and minimal storage is required. The overall AEN-ECC with DKR model operates within $O\ (n+k)$ space suitable for memory-constrained sensor nodes. Operationally, the AEN-ECC model design favours combined distributed intelligence with centralized training and decentralized inference. The proposed model ensures energy-aware routing, reduced delay, high success rate & detection accuracy and secured packet handling without overstress the deployed sensor nodes making it ideal for scalable, real-world LS-WSN environments.

3 Results and Discussions

A detailed evaluation of the proposed AEN-ECC with DKR model is presented in this section to assess the secure and intelligent data handling in LS-WSNs. The model is tested using the NS2/NS3 simulator, which can emulate real-time network behaviors such as packet drops, node failures, and encryption overhead. The simulations were conducted across 2500 sensor nodes with multiple iterations to ensure statistical consistency and reproducibility. A real-world intrusion multi-hop dataset such as NSL-KDD and CICIDS was injected into the simulation environment. These datasets were embedded into packet streams to test the realistic attack and benign conditions. The AEN-ECC model is trained offline and deployed within nodes to classify real-time anomalous traffic. EE with DKR is periodically tested with multiple key rotations to prevent replay and cryptanalytic attacks. Multi-hop swarm routing techniques are tested along with AEN to check the finest routing in the test bed. The results of the proposed hybrid AEN-ECC WSN security model is compared with the selected security enabled baseline models SVM-AES [4], RF-KSS [5], and XGBoost-FR [5].

3.1 Packet Delivery Ratio (PDR)

The efficiency of data transmission is measured using the packet delivery ratio metric. In this research, the baseline PDR observed in traditional models such as SVM-AES, RF-KSS, and XGBoost-FR ranged between 78.6% and 79.2% due to delayed anomaly detection, static routing process and encryption overheads, which causes packet loss and retransmissions. The proposed hybrid model integrated AEN-ECC with DKR for real-time anomaly detection, lightweight encryption, and a key-based session renewal process. This secure stack ensures malicious packets are filtered early, authentic packets are delivered securely, and PDR is boosted to 85.6%. A significant jump of 90.2% for 2,500 node counts was achieved after incorporating swarm-based routing, which dynamically selected the optical routing for data delivery based on energy levels. Path failures and retransmissions are entirely reduced with the synchronization of intelligent detection, secure transmission, and efficient path selection, making the system resilient in attack-prone environments. The comparative analysis is shown in Table 4.

Table 4. Comparative Analysis of Packet Delivery Rate (%)

Node Counts / Protocols	500	1000	1500	2000	2500
SVM-AES [4]	84.4	85.6	83.2	81.4	79.2
RF-KSS [5]	85.7	84.4	82.5	80.8	78.6
XGBoost-FR [5]	87.2	86.5	84.3	83.7	82.4
AEN-ECC with DKR [Proposed]	94.7	93.6	92.4	91.6	90.2

3.2 Confidentiality Rate (CR)

The comparative analysis confidentiality rate of the proposed AEN-ECC hybrid model against baseline machine learning models is shown in Table 5. CR quantifies that the transmitted data remains protected from unauthorized access during WSN communication. Baseline models achieved only 84.6% and 80.2% due to a lack of resistance against advanced eavesdropping and cryptanalysis, especially in prolonged sessions. AEN-ECC provides a strong key rotation mechanism by integrating DKR that ensures each communication is a unique, time-variant encryption key, thereby eliminating key reuse vulnerabilities. This continuous process makes it extremely difficult for intruders to decrypt the data, even with partial keys. The AEN anomaly detection layer pre-filters malicious requests and ensures encryption resources are not wasted on corrupted packets. This secure pre-selection process prevents fake nodes and payloads. As a result, the CR is boosted to 91.4%, a noticeable improvement in high-risk environments.

Table 5. Comparative Analysis of Confidentiality Rate

Node Counts / Protocols	500	1000	1500	2000	2500
SVM-AES [4]	85.2	84.6	82.5	79.4	77.8
RF-KSS [5]	86.5	84.3	83.6	81.8	80.2
XGBoost-FR [5]	89.3	87.8	86.7	85.8	84.6
AEN-ECC with DKR [Proposed]	95.8	94.2	93.6	92.7	91.4

3.3 Attack Detection Accuracy (ADA)

ADR measures the ability of the proposed AEN-ECC system to identify and isolate malicious activity from normal network behavior precisely. Due to a lack of adaptive learning capacity and high false rates, the existing models attained between 76.6% and 80.4% which is shown in Table 6. These models struggle to discriminate between legitimate anomalies and intrusions like spoofing or flooding. The proposed AEN-ECC learns a compact latent representation of normal behavior during training instead of relying on predefined static threshold labels. During the inference, the AEN flags the deviations based on reconstruction error and provides a dynamic context-aware anomaly assessment. This adaptive hybrid AEN-ECC model allows early and precise detection of malicious activities to ensure zero-day attacks. Additionally, DKR indirectly aids by minimizing repeated attack vectors, and the keys evolve constantly to reduce the effectiveness of replay and brute-force attacks. The proposed model achieved 90.6% ADR and outperforms baseline models by providing smarter, adaptive, and security-integrated sensor communication environments.

Table 6. Comparative Analysis of Attack Detection Accuracy (%)

Node Counts / Protocols	500	1000	1500	2000	2500
SVM-AES [4]	84.7	82.5	80.4	78.9	76.6
RF-KSS [5]	88.2	86.8	84.5	82.4	80.4
XGBoost-FR [5]	89.3	87.4	86.2	84.5	82.7
AEN-ECC with DKR [Proposed]	94.8	93.6	92.5	91.2	90.6

3.4 Robustness Against Node Failures (RNF)

Uninterrupted data flow is crucial to sustain secure communication even when sensor nodes drop out due to energy depletion, mobility, or physical damage. This is measured by a metric called robustness to node failures. Table 7 shows the comparative analysis of RNF metrics with different node counts. Existing models led to communication bottlenecks, increased transmission attempts, and particle data losses, limiting robustness to 81%. The proposed AEN-ECC integrated swarm-based routing significantly enhances robustness through successful data delivery via optimal routing and decentralized adaptive path selection. When a node fails to respond, the swarm recalculates alternative paths to transmit the data packets. This dynamic multi-hop swarm routing strategy ensures secure data delivery without compromising cryptographic integrity. Also, to mitigate the ripple effects of such failures, DKR ensures session security during the transmission process. Together, these components achieved a robustness score of 90.1% with superior adaptability and fault tolerance performance.

Table 7. Comparative Analysis of Robustness (%)

Node Counts / Protocols	500	1000	1500	2000	2500
SVM-AES [4]	85.7	82.6	80.5	78.7	77.5
RF-KSS [5]	88.6	86.4	84.7	83.5	81.6
XGBoost-FR [5]	89.4	87.5	86.8	85.7	83.8
AEN-ECC with DKR [Proposed]	94.4	93.6	92.7	91.4	90.1

3.5 End to End Latency (EEL)

The latency measures the total time taken for data packets from source to destination. High latency indicates the routing inefficiency and disrupts the time-sensitive applications. Table 8 shows the latency comparative analysis of existing and proposed models. The AEN-ECC model introduced a lightweight AEN to perform rapid anomaly detection based on reconstruction error and operates with minimal cycles to reduce detection delay. Integration of swarm-based routing proactively selects optimal paths based on hop count and link quality and bypasses the high-delay nodes, which ensures smoother dataflow with minimal retransmissions. ECC maintains the encryption efficiency without increasing the computational delay. Overall, 28.5 ms latency is reduced by the AEN-ECC model, making it suitable for real-time LS-WSN environments like healthcare, industrial automation, and disaster monitoring.

Table 8. Comparative Analysis of End to End Latency (in ms)

Node Counts / Protocols	500	1000	1500	2000	2500
SVM-AES [4]	38.4	39.6	41.8	43.7	45.8
RF-KSS [5]	36.7	38.5	40.3	42.6	43.7
XGBoost-FR [5]	33.8	34.5	35.8	36.7	38.9
AEN-ECC with DKR [Proposed]	20.6	22.4	24.3	26.2	28.5

3.6 Network Performance (NP)

Network performance is measured to evaluate the stability, throughput, secure delivery, fault recovery, and responsiveness under dynamic conditions. The new AEN-ECC model aligned three components: AEN, ECC with CKR, and swarm routing in real-time. The model achieves 92.7% overall network performance with a 2500 node count test under adversarial traffic conditions, which is comparatively higher than the existing models portrayed in Table 9. This reflects operational consistency where the network maintained high throughput and dynamic performance during node link failures and avoided bottlenecks due to a

self-optimized routing process with an efficient security stack. Additionally, the model is tested with SDN datasets to assess the performance level in key rotation and dynamic routing process. As a result, AEN-ECC achieves 94.6% of overall network performance.

Table 9. Comparative Analysis of Network Performance (%)

Node Counts / Protocols	500	1000	1500	2000	2500
SVM-AES [4]	80.5	78.4	76.6	74.4	72.2
RF-KSS [5]	85.7	82.6	80.5	78.7	77.5
XGBoost-FR [5]	85.7	84.4	82.5	80.8	78.6
AEN-ECC with DKR [Proposed]	96.4	95.2	94.4	93.6	92.7

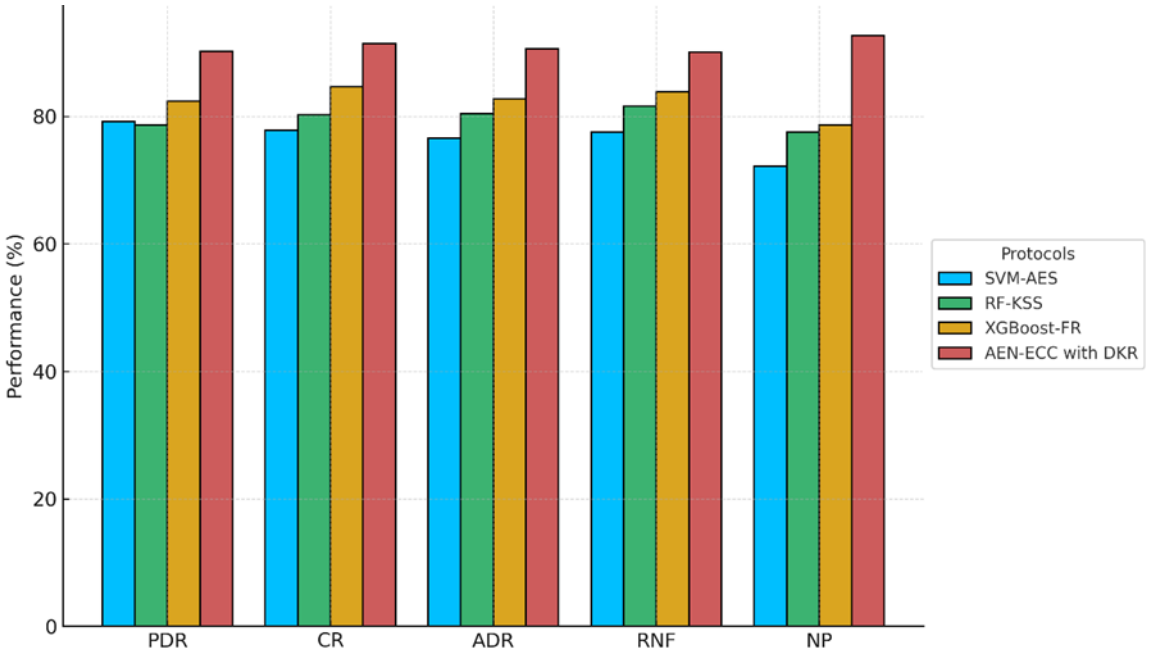

Fig 7. Comparative Analysis of Models (PDR, CR, ADR, RNF and NP)

4 Conclusion

This research introduced a novel unified and intelligent security model, AEN-ECC, to tackle one of the most pressing concerns in WSNs, ensuring secure and efficient data transmission in hostile and resource-constrained environments. By utilizing AEN for anomaly detection with ECC fortified through DKR, the proposed work bridges the critical gap between intrusion detection and adaptive encryption. The AEN-ECC security model has shown a full potential to learn the node behavior and detect deviations without labeled data, significantly enhancing the model's responsiveness to zero-day attacks and threats. A lightweight cryptographic layer is framed to refresh the keys dynamically based on energy and threat levels, which provides data confidentiality without affecting node performance. Multi-hop swarm route optimization is adapted for the finest routing process to ensure optimal routing. NS2 simulations were carried out by deploying 2500 nodes and tested with NSL-KDD and CICIDS data and compared against security methods like SVM-AES, RF-KSS, and XGBoost-FR to assess the performance of AEN-ECC. The model achieved promising results with a 90.2% Packet Delivery Ratio, 91.4% Confidentiality Rate, 90.6% Attack Detection Accuracy, 90.1% Robustness to Node Failures, 92.7% network lifetime and 28.5 ms reduced Latency which is shown in Figure 7 & 8. The model enhanced the WSN's performance, proved the adaptability of real-time learning and lightweight cryptography coexist in sensor networks, and provided a scalable blueprint for next generation secured IOT models. This AEN-ECC paradigm shift from a static rule-based to an intelligent, energy-conscious, and behavior-aware model highlights the potential of performance.

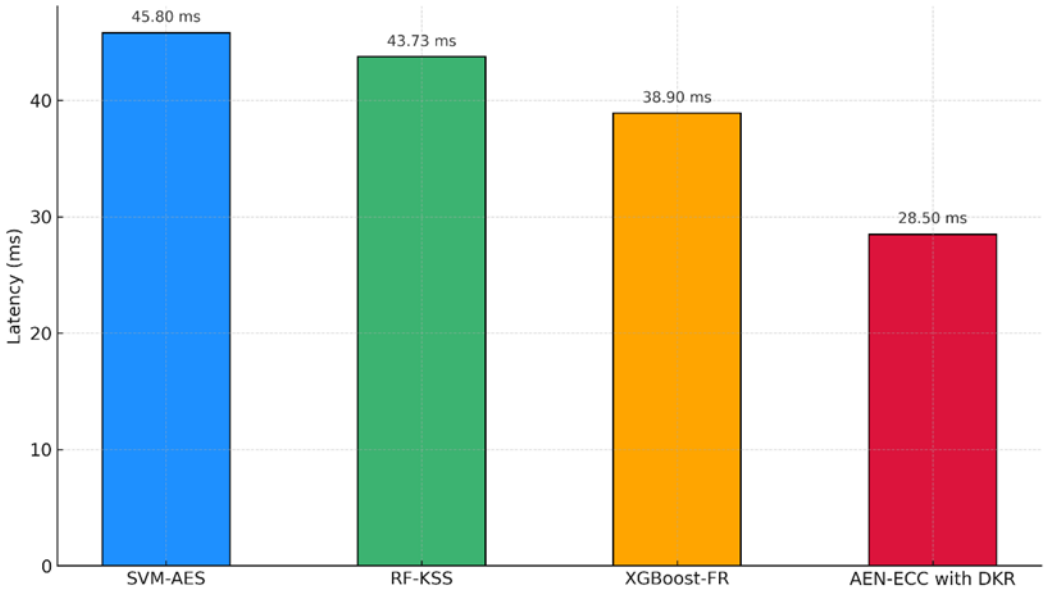

Fig 8. Comparative Analysis of Models (End to End Latency)

Though AEN-ECC with DKR demonstrates superior performance in LS-WSN environments, its real-world deployment faces challenges like i) communication overhead during key rotation, ii) computational delays in high-density node settings, iii) overfitting, etc. Additionally, usage of AEN and lightweight ECC require additional tuning in environments with fluctuating traffic. These aspects can be considered for future enhancements by integrating RF learning-based routing and AI-based sleep scheduling mechanisms.

References

1) Fares H, Vibhute AD, Mouniane Y, Bouijij H. Intrusion Detection in Wireless Sensor Networks using Machine Learning. *Procedia Computer Science*. 2025;252:912–921. https://doi.org/10.1016/j.procs.2025.01.052.
2) Pandey VK, Prakash S, Gupta TK. Enhancing intrusion detection in wireless sensor networks using a Tabu search based optimized random forest. *Science Reports*. 2025;15:18634. https://doi.org/10.1038/s41598-025-03498-3.
3) Nguyen TM, Vo HHP, Yoo M. Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach. *Sensors*. 2024;24(11):3339. https://doi.org/10.3390/s24113339.
4) Altameemi AI, Mohammed SJ, Mohammed ZQ, Kadhim QK, Ahmed ST. Enhanced SVM and RNN classifier for cyberattacks detection in Underwater Wireless Sensor Networks. *International Journal of Safety and Security Engineering*. 2024;14(5):1409–1417. https://doi.org/10.18280/ijsse.140508.
5) Talukder MA, Khalid M, Sultana N. A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. *Science Reports*. 2025;15:4617. https://doi.org/10.1038/s41598-025-87028-1.
6) Nithyanandh S, Jaiganesh V. Reconnaissance Artificial Bee Colony Routing Protocol to Detect Dynamic Link Failure in Wireless Sensor Network. *International Journal of Scientific & Technology Research*. 2019;10(10):3244–3251. https://doi.org/10.35940/ijstr.b2271.0986231.
7) Devi PA, Megala D, Paviyasre N, Nithyanandh S. Robust AI Based Bio Inspired Protocol using GANs for Secure and Efficient Data Transmission in IoT to Minimize Data Loss. *Indian Journal of Science and Technology*. 2024;17(35):3609–3622. https://doi.org/10.17485/IJST/v17i35.2342.
8) Pourghasem A, Kirner R, Tsokanos A, Mporas I, Mylonas A. Machine Learning and Deep Learning-Based Multi-Attribute Physical-Layer Authentication for Spoofing Detection in LoRaWAN. *Future Internet*. 2025;17(2):68. https://doi.org/10.3390/fi17020068.
9) Nithyanandh S, Jaiganesh V. Interrogation of Dynamic Node Link Failure by Utilizing Bio Inspired Techniques to Enhance Quality of Service in Wireless Sensor Networks. 2020.
10) Haque A, Soliman H. A Transformer-Based Autoencoder with Isolation Forest and XGBoost for Malfunction and Intrusion Detection in Wireless Sensor Networks for Forest Fire Prediction. *Future Internet*. 2025;17(4):164. https://doi.org/10.3390/fi17040164.
11) El-Sofany H, El-Seoud SA, Karam OH. Using machine learning algorithms to enhance IoT system security. *Science Reports*. 2024;14:12077. https://doi.org/10.1038/s41598-024-62861-y.
12) Nithyanandh S, Jaiganesh V. Dynamic Link Failure Detection using Robust Virus Swarm Routing Protocol in Wireless Sensor Network. *International Journal of Recent Technology and Engineering*. 2019;8(2):1574–1578. https://doi.org/10.35940/ijrte.b2271.078219.
13) Doghramachi DF, Ameen SY. Internet of Things (IoT) Security Enhancement Using XGboost Machine Learning Techniques. *Computers, Materials and Continua*. 2023;77(1):717–732. https://doi.org/10.32604/cmc.2023.041186.
14) Dharini N, Katiravan J, M SPD, A SSV. Intrusion Detection in Novel WSN-Leach Dos Attack Dataset using Machine Learning based Boosting Algorithms. *Procedia Computer Science*. 2023;230:90–99. https://doi.org/10.1016/j.procs.2023.12.064.

15) Salah Z, Elsoud EA. Enhancing Network Security: A Machine Learning-Based Approach for Detecting and Mitigating Krack and Kr00k Attacks in IEEE 802.11. *Future Internet*. 2023;15(8):269. https://doi.org/10.3390/fi15080269.
16) Nithyanandh S, Jaiganesh V. Quality of service enabled intelligent water drop algorithm-based routing protocol for dynamic link failure detection in wireless sensor network. *Indian Journal of Science and Technology*. 2020;13(16):1641–1647. https://doi.org/10.17485/IJST/v13i16.19.
17) Sun D, Zhang L, Jin K, Ling J, Zheng X. An Intrusion Detection Method Based on Hybrid Machine Learning and Neural Network in the Industrial Control Field. *Applied Sciences*. 2023;13(18):10455. https://doi.org/10.3390/app131810455.
18) Alfahaid A, Alalwany E, Almars AM, Alharbi F, Atlam E, Mahgoub I. Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey. *Sensors*. 2025;25(11):3341. https://doi.org/10.3390/s25113341.
19) Nithyanandh S, Omprakash S, Megala D, Karthikeyan MP. Energy Aware Adaptive Sleep Scheduling and Secured Data Transmission Protocol to enhance QoS in IoT Networks using Improvised Firefly Bio-Inspired Algorithm (EAP-IFBA). *Indian Journal of Science and Technology*. 2023;16(34):2753–2766. https://doi.org/10.17485/IJST/v16i34.1706.
20) Kalaiselvi RC, Suriakala M. Machine Learning-Based Reconnaissance Bee Colony with Custom AES & AE for Robust IoT Data Security and Transmission. *Indian Journal of Science and Technology*. 2024;17(46):4828–4841. https://doi.org/10.17485/IJST/v17i46.3644.
21) Eldho KJ, Nithyanandh S. Lung Cancer Detection and Severity Analysis with a 3D Deep Learning CNN Model Using CT-DICOM Clinical Dataset. *Indian Journal of Science and Technology*. 2024;17(10):899–910. https://doi.org/10.17485/IJST/v17i10.3085.
22) Arularasan R, Balaji D, Garugu S, Jallepalli VR, Nithyanandh S, Singaram G. Enhancing Sign Language Recognition for Hearing-Impaired Individuals Using Deep Learning. In: 2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India. 2024;p. 1–6. https://doi.org/10.1109/ICDSNS62112.2024.10690989.
23) Selvam N, Joy JK. Plant Leaf Disease Detection with Multivariable Feature Selection Using Deep Learning AEN and Mask R-CNN. *Biotech Res Asia*. 2024;21(4). http://dx.doi.org/10.13005/bbra/3333.
24) Nithyanandh S. Object Detection & Analysis with Deep CNN and Yolov8 in Soft Computing Frameworks. *International Journal of Soft Computing and Engineering (IJSCE)*. 2025;14(6):19–27. https://doi.org/10.35940/ijsce.E3653.14060125.
25) Alkadi S, Al-Ahmadi S, Ismail MMB. RobEns: Robust Ensemble Adversarial Machine Learning Framework for Securing IoT Traffic. *Sensors*. 2024;24(8):2626. https://doi.org/10.3390/s24082626.