INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Machine Learning-Based Reconnaissance Bee Colony with Custom AES & AE for Robust IoT Data Security and Transmission

R Caroline Kalaiselvi[1]*, **M Suriakala**[2]

1 Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), University of Madras, Chennai, Tamil Nadu, India
2 Assistant Professor and Research Guide, PG and Research Department of Computer Science, Government Arts College (Autonomous), University of Madras, Chennai, Tamil Nadu, India

OPEN ACCESS

Received: 08-11-2024

Accepted: 30-11-2024

Published: 17-12-2024

Citation: Kalaiselvi RC, Suriakala M (2024) Machine Learning-Based Reconnaissance Bee Colony with Custom AES & AE for Robust IoT Data Security and Transmission. Indian Journal of Science and Technology 17(46): 4828-4841. https://doi.org/10.17485/IJST/v17i46.3644

* **Corresponding author**.

carrie.jonna@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 a robust method to enhance data security and transmission in IoT to address the challenges in real-time data transmission and create a comprehensive security solution. The new method takes credit for the machine learning-based bioinspired method to minimize data loss and maximize end-to-end data transmission rate. **Methods:** Custom-AES with Avalanche Effect (AE) and Machine Learning-based Reconnaissance Bee Colony are employed to secure the data with enhanced encryption by creating a multi-layered IoT security solution. Key stretching is used to provide high resistance to cryptographic attacks. In order to optimize threat detection, Pareto-based selection and dynamic parameter tuning with ML-RBC are used. To improve attack resilience, rank, and tournament selection methods are employed to target DDoS and MMIT attacks with a minimized encryption time. The NSL-KDD IoT network dataset is used to test the proposed CAES-AE with the ML-RBC model using a network simulator. To assess the performance of the proposed work, the results are compared with prevailing IoT data transmission techniques such as ERSA, QoS-BFT, AES, Custom AES, and RBC. **Findings:** The suggested CAES-AE with ML-RBC data security and transmission method attains the promising results of 97% authentication success rate, 6 seconds response time to security actions, 96% vulnerability detection speed, 97% data encryption strength, 5 seconds incident response time, and 97.8% network performance (energy efficiency & lifetime), which is higher than earlier methods. **Novelty:** This research provides a secured data transmission method in an IoT environment to address the real-time data transmission challenges faced in sensor-based networks. This will function as a multi-layered IoT security model that optimizes real-time attack detection and resilience. The performance metrics are evaluated with multiple packet transfer rates to boost the network performance.

Keywords: Machine Learning; Advanced Networking; Data Security; Secured Data Transmission; BioInspired Algorithm

1 Introduction

Secured and reliable data transmission is essential in the rapidly growing IoT and 5G landscape, due to cyber and vulnerable attacks from intruders. Data security protocols such as ERSA, QoS-BFT, AES, Custom AES, and RBC play a significant role in addressing the security needs that enhance data encryption while passing from source to destination through lightweight cryptographic mechanisms. Yet the protocols face limitations in scaling with high sensor node counts, energy constraints, fault tolerance, incident response time to threats, dynamic adaptability, latency sensitivity in LS-IoT, etc. A few shortcomings of the prevailing methods are that the protocols do not meet IoT dynamic real-time demands lack of significant customization, suffer from computational overhead, have limitations in real-time IoT deployment, are lacking in resilience, sophisticated attack vectors like DDoS, MMIT, etc. In order to address these research gaps, there is a need for a dynamic, adaptable, secured transmission protocol to deploy in an IoT environment. This study introduces a hybrid CAES-AE with ML-RBC, integrating adaptive custom AES and machine learning-based bioinspired methods to improve security and performance in high-traffic LS-IoT environments. The new method effectively targets specific threats minimizes encryption time, maximizes strength, and mitigates vulnerable cyber-attacks, providing a promising solution to the IoT data transmission environment.

The main focus is to develop a robust IoT environment for secured end-to-end data transmission. Some of the state-of-the-art methods are discussed to study the security features incorporated in the IoT protocol, and its limitations are showcased. A distributed machine learning-based architecture [(1)] was proposed for smart recycling where an efficient M-Net protocol model was employed for data augmentation and hyperparameter tuning. In real time, it is connected to a cloud server and exchanges the data. The drawback is lacking of handling network traffic in an LS environment. Secured protocol [(2)] was introduced to handle massive data generated by smart cities using collaborative intelligence with advanced data encryption methods. The protocol transmits massive data with less energy and high performance. The model lacks in mitigating security assaults in distributed environments, which has to be improvised. Narrow-band IoT-based cloud computing architecture protocol [(3)] reduces the latency time with maximum data transmission. Healthcare datasets are used for testing during real-time cloud storage and exchange, which is adequate for remote health monitoring. Additional hardware and installation cost are the main drawback of the Narrow Band where third parties are required for deployment. A detailed background study has been done on efficient and secured protocols [(4)] for data links and bio-inspired dynamic approaches like RSVRP, RABCRP, and IWDARP to know the potentiality and limitations of secured data transmission mechanisms [(5)] to develop a robust model. IoT sensors and Big Data [(6)] were applied to enhance crop production to deal with 2D and 3D data and the communication process. The node strength was analyzed for energy efficiency and network performance to boost the data prediction based on environmental conditions. Massive data handling in real-time is the only drawback of the model that has to be considered. PUF authentication system [(7)] and blockchain-based network security management protocol [(8)] were proposed using machine learning supervised methods to detect threats and anomalies with real-time 6G networks. Sensor DS-1010 traffic dataset was employed for training and testing processes. A dynamic link failure detection model [(9)] was developed to deploy in the WSN environment to enhance the quality of data transmission with more security. IoT-enabled WSN protocol for RPL [(10)] is used for security enhancement by employing machine learning to record

and transfer real-time data with robust security. A group model approach with ML-EOA, ANN, and CH[11] is developed for energy efficiency and WSN adaptability, where fuzzy logic is employed for data augmentation and aggregation. Revolutionary node optimization and attack mitigation in real time are the major shortcomings of the model, which has to be enhanced further. A virus swarm bio-inspired protocol[12] and SOS for a data security model[13] for UAV edge networks is deployed to detect dynamic link failure, potential threats, service attacks, and data attacks in an IoT-enabled WSN for efficient packet delivery with minimal latency. Data transmission protocol using ML-D2D and RBC[14,15] ensures attack mitigation and anomaly detection with less energy consumption and high performance. Link failure detection is also addressed by RBC, where population-based bioinspired techniques are employed. The drawback is computational complexity when handling data in huge traffic and loads. The stochastic classifier method[16] and multi-agent ML-based B5G model[17] are deployed for dynamic and adaptive routing processes when node energy fails. This model has a huge response in real-time sensor-based IoT, which has the full potential to take alternate routes to deliver the packets in a minimal time. Attack mitigation and flooding recovery are lacking, which is considered the only drawback of these models. Adaptive sleep scheduling mechanism[18] is developed with high security in data transmission for WSN-based IoT networks and VANETs using binary cross model, HARQ, and Q-learning[19] focused on S→D data transmission, adaptive sleep during network idle state, anomaly detection, attack resilience, big data analytics for cloud security[20] and high network performance. DL-based CNN[21] is employed with large-scale healthcare data for isolation, masking, and partition with the help of image data exchange between sensor devices in a healthcare-embedded environment. A blockchain-based FDL[22] and BIP-GANs model[23] for data security in IoT is developed using advanced AES and QLT models to detect multiple threats and mitigate DDoS attacks. The drawback of this model is deployment and lack of error recovery. 5G optimization network protocol[24] and cloud-based security protocol[25] are developed to enhance the security and robustness, which attains 87% accuracy and speed[26]. To overcome the limitations, the hybrid three-component model is aimed at the objective of threat detection and attack mitigation for smooth data transmission in an LS-IoT environment.

2 Methodology

The proposed hybrid multi-layered adaptable security protocol for LS-IoT environment integrates Custom AES with Avalanche Effect and ML-based Bee Colony bio-inspired method for dynamic threat detection, attack mitigation, and secured data transmission from source to destination. The security process begins with strengthening the crypto mechanism through Custom AES, which is enhanced by AE, where the minimal changes in plain text result in major variations in cipher text. In order to increase the encryption and offer high resilience against crypto attacks, a key stretching model is employed with CAES. In the RBC layer, the protocol dynamically adapts to any network conditions using PBS and DKD to optimize threat detection, which permits real-time adjustments based on traffic patterns and threat scores to enable responsive threat identification. The rank and tournament selection methods are employed to enhance the attack resilience, mainly focusing on DDoS and MMIT, which leads to an efficient balance on encryption time and handling LS-IoT traffic environments. Enabling secure and reliable communication between two devices, protecting against targeting traffic management systems, detecting unusual traffic spikes, protecting data leaks, robust security, adaptability, safe data exchange, and reliable functionality in LS-IoT environments are the main goals of the proposed method. The method is validated using NSL-KDD and IoT-23 datasets[27] on the simulation tool with proven results in performance metrics, which are clearly shown in further sections. (Dataset Link: https://dx.doi.org/10.21227/yjtm-6x74)

2.1 Proposed Data Transmission Technique in IoT Environment

The hybrid multi-layered LS-IoT data transmission technique is mainly focused on the integration of multiple techniques, which include cryptographic mechanisms, machine learning, and bio-inspired methods to create a robust security data transmission environment. Custom AES and ML-RBC, along with PBS, DPT, RS, and TSM methods, are employed, and the results are validated with the NSL-KDD and IoT-23 datasets. DoS, malware, and MiTM security attacks are mitigated to provide a strong environment. The model also discriminated between real and fake threats using the standard ranking score method. Threats like code injection, malware, anomalies, flooding, impersonation, etc. are detected using the bio-inspired bee colony method. Some of the potential threats in the IoT environment like MECT (Multi Edge Computing Threats), Visualization threats, and Generic Threats are detected and responded to dynamically in a real-time scenario. Let's assume that the IOT device transmits the data with a size of 512 bits and plain text $P = 11010101$. The CAES with AE is employed and the key is stretched using $K_{stretched}$ method. The Plain text $P = 11010101$ is encrypted using AES and C, cipher text is identified. $C = E(P.\, K_{stretched})$. If a single bit in P changes, $P = 11010100$, the cipher text $C^{'} = E(P^{'},\, K_{stretched})$ results is major change in C. For threat detection assume that, Packet Size (f_1) = 1000 bytes (HV indicates +ve attacks), Packet frequency (f_2)

= 15 packets per second transmission rate, Source Identity (f_3) = Unknown IP (High Risk). In order to begin, the initial weights $w_1 = 0.5$, $w_2 = 0.3 and\, w_3 = 0.2$ the threat score is calculated as,

$$Threat_{Score} = (0.5x1000) + (0.3\ x\ 15) + (0.2\ x\ 1) = 500 + 4.5\ + 0.2\ =\ 504.7 \quad (1)$$

where the threshold level is set as 300, and if the result exceeds, an alert is triggered where ML-RBC takes the security action based on the level and nature of threats and attacks to secure the data transmission and improve future detection accuracy. To prevent tampering, each device ID is encrypted using CAES-AE and ML-RBC. Packet headers are monitored and flagged by the protocol during potential impersonation attempts. This multi-layered model works with data encryption, threat detection, and attack mitigation in an LS-IoT network environment with high resilience compared to existing methods called ERSA, QoS-BFT, AES, Custom AES, and RBC. Isolation of suspected devices is monitored during attack mitigation, and the devices are removed completely and the routing path is optimized for smooth data transmission. The energy efficiency and performance of the IoT network are calculated and monitored to reinforce data transmission security.

2.2 Data Encryption with Multi-Layered Security

By In this new approach, each layer provides an additional security mechanism for the safe transmission of data packets from source to destination in a robust manner.

- Layer 1 - Encrypts data
- Layer 2 - Analyzes Network Traffic
- Layer 3 - Detect Threats and Mitigate Attacks
- Additional Layers - Finest Routing and Data Transmission Process

Each method is demonstrated in the further sections with proven results.

Table 1. Parameter Settings for Simulation and Testing

Parameters	Value / Settings	Description
$Network\ Monitoring$	Enabled	Real-Time Monitoring
$Node\ Count-Testing$	500 – 2250	No. of IoT nodes for network testing
$Network\ Range-IoT$	800 x 800 m^2	Area covered by IoT devices
$Size\ of\ the\ Packet/Data$	512 bytes	Fixed PS for data transmission
$Mobility$	Random Way Point	To simulate dynamic IoT nodes
$Traffic\ Model$	HTTP, FTP, MQTT	Various IoT Traffic to simulate load
$IoT\ Nature$	Heterogeneous	Sensors, Actuators, and WS Nodes
$Learning\ Rate\ of\ Model$	0.01 – 0.05 bits	Initial Learning Rate
$Initial\ Energy\ (IE)$	75 Joules	Starting Energy to calculate EC
$Range\ of\ Sensor$	20M – 50M	Coverage range of IoT sensor nodes
$Name\ of\ Simulator$	OMNET++ & NS3	For Testing and Validation
$Sample\ Nodes\ For\ Testing$	T = 200	For Each Simulation
$Num\ of\ Epocs$	M = 50	For Every Iteration
$Data\ Packet\ Width$	50 nJ/bit	EC per bit during data processing

2.3 Real-Time Threat Detection & Attack Mitigation using PBS, DPT, Rank and TSM

Efficient The response process during real-time threat detection is enhanced using Pareto-based selection, dynamic parameter tuning, rank, and tournament selection methods. Initially, PBS is employed, where multi-objective optimization is used in the threat detection layer to identify and prioritize the critical threats in the LS-IoT environment without affecting encryption time, speed, energy, performance, etc. To enhance security & efficiency, this adaptive CAES-AE with ML-RBC approach uses PBS for dynamic resource allocation by selecting the best parameters. The PBS is represented in the equation as,

$$Maximize\ f(x) = \left(w_1.S(x) + w_2.\frac{1}{E_x} \right) + w_3.\frac{1}{L(x)}) \tag{2}$$

where, $S(x)$ denotes detection accuracy (security level), E_x is energy consumption and L_x is latency time, w_1, w_2, w_3 is weights assigned to each parameter in the LS-IoT environment. If sensor data is processed in IoT with 1200 nodes with weights 0.5, 0.3, and 0.2, the PBD will evaluate potential configurations of ML-RBC parameters to choose the one that enhances security while conserving energy and reducing latency. Dynamic parameter tuning is employed to make the new protocol adapt ML-RBC's parameters in any network conditions, especially under attack and threat detection. DPT adjusts the parameters based on incident response time and feedback from the IoT network. Assume that, attack mitigation efficiency is M be an optimal function of DPT P_t. The DPT is represented as,

$$Mitigation\ M = \sum_{i=1}^{n} \alpha_i.Parameter_{i,t} \tag{3}$$

where, $P_{i,t}$ is Parameter i at time t. α_i is the weight assigned to each parameter based on attack impact. DPT dynamically enhances the sensitivity of anomaly and threat detection by adjusting the learning score of ML-RBC. DPT will automatically increase the threshold value at critical conditions to adapt and secure the data packets in a robust manner. In addition to PBS and DPT, rank and tournament selection methods are deployed to prioritize threat detection and attack resilience. RS technique prioritizes the threats based on severity to address. A rank score is assigned to mitigate critical vulnerabilities with high priority to ensure the maximum security of data, especially in huge traffic to deliver from source to destination. The threat score is calculated as,

$$Ranking\ Score\ R_i = \beta_1.A_i + \beta_2.D_i + \beta_3.I_i \tag{4}$$

where A is the anomaly score, D is detection confidence for threat (i) and I is the impact level of threat (i). β_1, β_2, β_3 are weights based on IoT network security policy. The system will calculate the ranking based on weights to ensure the threat priority in order to minimize attacks and data leaks. For attack resilience, TSM is employed to select the best-performing security mechanism along with bio-inspired ML-RBC to secure data from repeated attacks, where the most effective strategies are selected to mitigate attacks and increase the incident response time. The probability of selecting the attack defense strategy is based on TSM $J_{strategy}$ from the pool S_{score}. The probability is calculated using,

$$Probability_j \& Fitness\ Score = \frac{Fitness_j}{\sum_{k=1}^{|s|} Fitness_k} \tag{5}$$

where, $Fitness_j$ is effectiveness score of strategy $J_{strategy}$. The new approach adaptively selects the best defense model to respond to repeated attacks and ensures that data is delivered from source to destination effectively. Here the three components combined together and made a significant attack resilience mechanism in combination with machine learning, cryptography, and bio-inspired to detect threats and mitigate attacks in real-time traffic in LS-IoT environments. The following are the components that work in real-time with sensor and traffic data.

- Data Encryption with CAES-AE (521 Bits Packets)
- Threat Detection with ML-RBC (Anomaly score of 0.7 on a 0-1 scale)
- DPT parameter tuning and adjustments (Dynamic Adaptation)
- Threat Ranking and Selection (Auto Ranking Scores)
- Attack Mitigation and Resilience with TSM (DDoS and MMIT Attacks)

The integrated approach makes the IoT environment more secure for effective data packet transmission from source to destination.

2.4 Enhancing Crypto Strength Using Key Stretching

In order to strengthen the encryption key mechanism, the key stretching method is employed with C-AES and ML-RBC to make it computationally harder to break by intruders. In the key stretching process the initial key K_0 is processed multiple times to generate an extended key called $K_{stretched}$. It is represented as,

$$K_{stretched} = f(f(f(K_0) \oplus salt) \oplus salt \ldots\ldots n\ times \tag{6}$$

where, f is a crypto hash function, $\oplus$ denotes XOR operation and $salt$ is the random value added in the original key to increase entropy. Key stretching improvises the avalanche effect, where all the minute changes in the input result in major changes in output data. It gives a high score for unpredictable ciphertext and makes the encryption mode stronger. ML-RBC integration detects threats and anomalies and identifies the intruder's attempts to decipher the encryption. For example, if the sensor data with a size of 2014 bits is encrypted using $K_{stretched}$, the protocol monitors the unauthorized attempts through ML-RBC and analyzes the abnormal patterns during the real-time data transmission process. This is dynamically trained and tested using NSL-KDD and IoT-23 sensors and network traffic data in the testbed. Key stretching helps to increase cryptographic strength and makes the LS-IoT environment more secure in data transmission.

- Deliver the data to the destination
- Wait for the next data transmission
- Reconstruction of data for transmission
- Deliver the data to the destination

2.5 CAES-AE with ML-RBC Architecture

The CAES-AE with ML-RBC architecture shown in Figure 1 comprises a four-layer mechanism that includes an IoT network layer to represent communication points, an encryption layer to secure data packets, a threat detection layer for identifying anomalies in real-time by analyzing traffic patterns, and a selection and resilience layer. Once the data is captured, it is passed to all layers and reaches the destination fully, which ensures high security and data transmission with a minimized end-to-end delay.

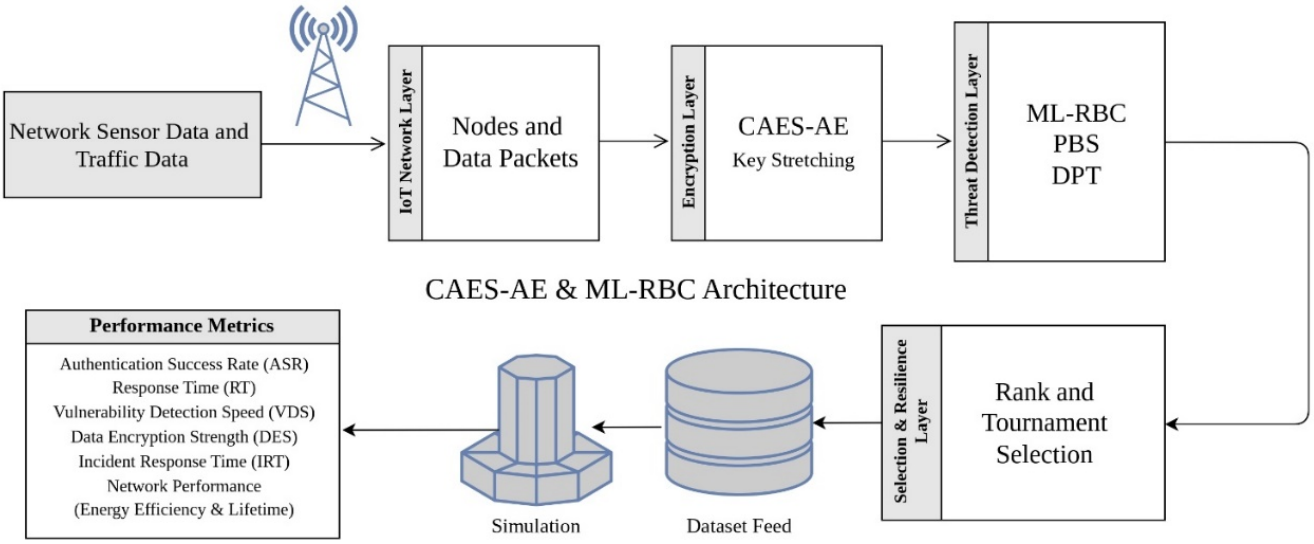

Fig 1. Network Packet Flow Diagram

CAES-AE with ML-RBC Step by Step Algorithm

1. **Input:** Initialize IoT network and Security Parameters
2. **Begin:** Start Data Transmission

Data Traffic and Security Metrics

3. Define Network Range $Range : R = 800x800\ m^2$
4. $Initialize\ Node\ Count : NC = 2250$
5. $Define\ Performance\ Metrics\ for\ Evaluation$

Set up Data Security Protocol

6. Data Encryption using Key Stretching (AES - 128)
$$E_{AES} = AES\ (P, K_{Stretched})$$
7. $Avalanche\ Effect = Measures\ C_{Text}\ and\ P_{Text}$
8. $Key\ Stretching\ (DEDK) = K_{Stretched} = f\ (K_{Original})$

Data Encryption and Authentication

9. For each Packet P_i from the Source node S and Destination node D
10. $Encrypt\ Data\ with\ AES\ \&\ Key\ Stretching\ C_i = E_{AES}\ (P_i, Key\ Stretched)$
where C_i is cipher text of packet P_i
11. $AE = \left[\frac{Bits\ Changed\ in\ C}{Total\ Bits\ in\ C}\right] \text{x } 100$
12. $Apply\ DEDK, K_{Stretched} = Hash\ (K_{Original}, Salt)$

Threat Detection and Dynamic Response using ML-RBC

13. Apply Pareto Based Model to prioritize threat detection for grave packets
$$Priority\ (P_i) = f\ (Threat\ Level, Network\ Load)$$
14. Apply Rank Tournament Selection for Attack Resilience, for each node N_j
15. $Rank\ Selection\ Rank\ (N_j) = Threat\ Level, Response\ Speed)$
16. $Tournament\ Selection\ (Selected\ N_j) = argmax_k (Rank\ (N_k))$
17. $Threat\ Logging\ \&\ Detection\ VDS = \frac{Threat\ Detetcion}{Detetcion\ Time}$

Data Transmission & Response Execution

18. Data Transmission $Transmit\ (C_i) \rightarrow D$
19. Response Time $RT = T_{initiation} - T_{detection}$
20. Incident Response Time $IRT = T_{completion} - T_{detection}$

Real Time Performance Monitoring

21. Calculate Energy Efficiency and Transmission Time
$Measure\ Total\ Energy\ Consumed\ and\ Transmission\ Time$
22. Update $C_{Textchanges}$ and P_{Text}
23. Update $Total\ Bits\ in\ C_{Text}$
24. Update $Constant\ Bit_{Rate}$
25. C_1 is transmitted from source to destination with calculated RT & IRT
26. Transmit data and update path
27. Calculate energy $Node_{Energy} = Transmission_{Time}$
28. Optimize Future Operations
29. Run & Validate Scores in Network Testbed
30. Record Metric Values and Compare
31. **End**

2.6 Performance Evaluation Using Simulator

Machine learning-based bio-inspired crypto transmission CAES-AE with ML-RBC mechanism is evaluated using NS3 and OMNET++ simulators. Six performance metrics are used to assess the performance of the proposed protocol to test the efficiency, network lifetime, response time, speed, encryption strength, success rate, packet delivery performance, etc. In addition to this, energy efficiency and network lifetime are also assessed to make sure that the protocol works well in the IoT environment during data transmission from source to destination. As the IoT model consists of sensors, multiple devices, and different topologies, different threshold limits are set as per the standards to test the robustness of the proposed protocol. Different iterations are carried out with the available IoT-23 and NSL-KDD sensors and traffic data to make sure that the new method transmits the data from source to destination in a robust manner. A detailed comparative analysis is made with existing methods to showcase the performance of CAES-AE with ML-RBC in real-time.

2.7 Evaluation Metrics of CAES-AE with ML-RBC

The performance evaluation metrics of the suggested machine learning bio-inspired IoT security and data transmission protocol CAES-AE with ML-RBC are compared against ERSA, QoS-BFT, AES, Custom AES, and RBC. The following are the six metrics used to evaluate the performance.

$$Authentication\ Success\ Rate\ = \left[\frac{No\ of\ Successful\ Authentications}{Total\ Authentication\ Limits}\right] x\ 100 \tag{7}$$

$$RT\ to\ Security\ Actions\ = \frac{Time\ of\ Action\ Initiation_i - Time\ of\ Threat\ Detection_i}{n\ (No.\ of\ Detected\ Security\ Threats)} \tag{8}$$

$$Detection\ Speed\ = \frac{Total\ No\ of\ Vulnerabilities\ Detected}{Total\ Detection\ Time} \tag{9}$$

$$Data\ Encryption\ Strength\ = \left[\frac{No\ of\ Bits\ Changed\ in\ Ciphertext}{Total\ Bits\ in\ Ciphertext}\right] x\ 100 \tag{10}$$

$$Incident\ Response\ Time\ = \frac{Time\ of\ Response\ Completion_i - Time\ of\ Incident\ Detection_i}{n\ (No.\ of\ Incident\ Responded)} \tag{11}$$

$$Network\ Performance\ = \frac{Total\ No\ of\ Data\ Transmitted\ (Bits)}{Total\ Transmission\ Time\ (Seconds)} \tag{12}$$

- **ASR:** Measuring the success rate of authentication attempts by CAES-AE with ML-RBC. ASR helps to measure unauthorized attempts and detect them same.
- **RTSA & IRS:** Response time to mitigate potential threats by the proposed protocol and measures the time taken to respond to resolve security incidents in IoT environments.
- **VDS:** Measures the detection rate of vulnerabilities, which helps to identify weak points and prioritize security measures to mitigate potential threats.
- **DES:** Ensures that the data is adequately protected, where access is denied by unauthorized users and intruders.
- **NP:** Measures the energy efficiency and lifetime of the network by calculating node strength, latency time, and packet delivery ratio, which helps to assess whether the network is secured, and reliable, and provides adequate connectivity and communication between the devices.

3 Findings and Discussions

This section shows the findings, comparative analysis, and discussions of the proposed CAES-AE with the ML-RBC method to secure data and fast transmission in the IoT network environment. Pareto-based selection, dynamic parameter tuning, rank, and tournament selection methods are employed additionally with custom AES and RBC to prevent the network from threats and to mitigate network attacks, especially DDoS and MMIT. The new IoT network protocol automatically detects network anomalies, ensuring robust data transmission without any failures, thereby enhancing the packet delivery ratio and performance of the network. The encryption strength of the data is increased to prevent data from intruders with the help of the custom AES key generation method. The key is accessed only by the sender and receiver, which gives more security and integrity to the data. In order to create a multi-layered security solution, the bioinspired RMC method is used to generate the key randomly and select the optimal routing path to send the data from source to destination. The results are compared with prevailing security protocols. Figures 2, 3, 4, 5, 6 and 7 shows the simulation graph with the X-axis as node count and the Y-axis as performance (%) ratio of the protocols.

3.1 Authentication Success Rate

The authentication success rate is measured and compared with existing protocols in order to demonstrate the reliability and efficiency under moderate network loads and tested with a sample of 500 node counts to 2250 node counts as shown in Figure 2. The authentication server gets overloaded when network congestion increases and high authentication requests lead to failure in verification. The new CAES-AE with ML-RBC technique has the ability to balance network load where it evenly distributes the load to each and every node in an optimized manner to streamline the process. The new protocol reduces bottlenecks in large IoT environments to stabilize the authentication success rate, leading to high reliability and security. 97% ASR is achieved, which is higher than the existing IoT security and data transfer protocols.

Table 2. Authentication Success Rate (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
ERSA [11]	81	77	74	70	68	65	63	60
QoS-BFT [13]	84	82	80	78	76	74	72	70
AES [20]	91	90	88	87	85	84	82	80
CAES-AE [25]	93	91	90	88	87	86	84	82
ML-RBC [17]	95	93	92	91	89	88	86	84
CAESAE+MLRBC	**97**	**96**	**95**	**94**	**93**	**92**	**91**	**88**

3.2 Response Time to Security Actions

The increase in data processing and routing demand across the IoT network environment leads to poor response time and unstable communication to the base station in order to mitigate security threats. The RTSA is measured and tested with 500 and up to 2250 node counts, and the results are achieved with 4 seconds and 6 seconds of response time which is portrayed in Figure 3. As more nodes participate in IoT communication, the response time will slow down due to network congestion and packet collisions. CAES-AE and ML-RBC address this by efficient packet handling under high network load, which helps to minimize latency and adaptability in order to maintain response efficiency even as the size of the network and node deployment grow.

Table 3. Response Time to Security (in seconds)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
ERSA [11]	12	12	13	14	15	16	17	18
QoS-BFT [13]	11	12	12	13	13	14	15	16
AES [20]	10	10	10	10	11	11	11	12
CAES-AE [25]	7	7	7	7	8	9	9	10
ML-RBC [17]	6	6	7	7	7	7	7	8
CAESAE+MLRBC	**4**	**4**	**4**	**5**	**5**	**5**	**5**	**6**

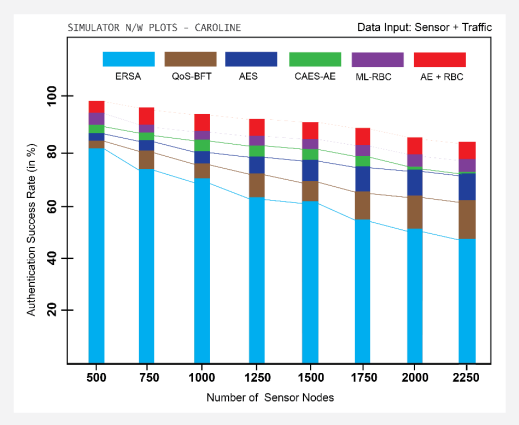

Fig 2. Comparative Analysis of ARS

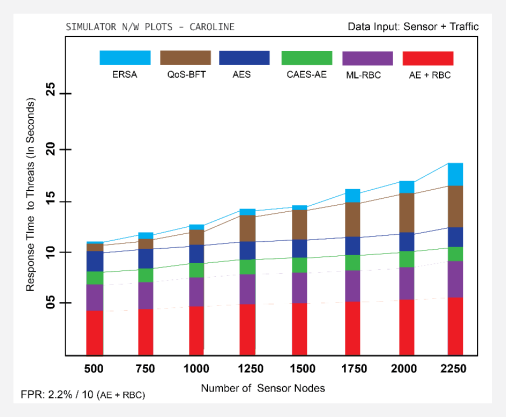

Fig 3. Comparative Analysis of RTSA

3.3 Incident Response Time

Figure 4 portrays the comparative analysis of incident response time to network security threats. Due to the complexity of dealing with security measures across IoT networks, there is an increase in IRT when the node counts are high. The proposed model has full potential for decentralized security checks, and threat prioritization helps to distribute workload across the IoT network environment with a minimized bottleneck effect. CAES-AE with ML-RBC allows more agile response times even as the size of the network increases, which illustrates scalable and distributed methods to prompt incident response in a large IoT environment. 3 seconds of IRT are marked with 500 NC, and 5 seconds are marked with 2250 NC, which is a promising result compared to existing protocols.

Table 4. Threat Incident Response Time (in seconds)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
ERSA [11]	8.2	9.1	10.3	12.4	12.8	13.6	14.2	15
QoS-BFT [13]	7.3	7.6	7.9	8.3	8.7	9.6	10.3	11
AES [20]	7	7.3	7.6	7.7	7.9	8.3	8.5	9
CAES-AE [25]	6	6.3	6.7	7.2	7.5	7.6	7.9	8.2
ML-RBC [17]	5.5	5.7	5.9	6.3	6.6	6.8	7.1	7.3
CAESAE+MLRBC	**3**	**3.2**	**3.5**	**4.1**	**4.3**	**4.5**	**4.6**	**5**

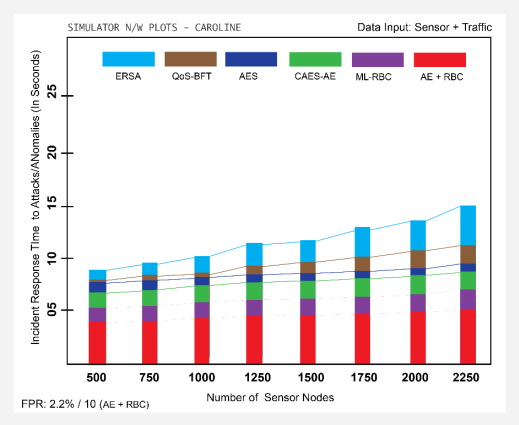

Fig 4. Comparative Analysis of IRS

3.4 Vulnerability Detection Speed

The detection speed of the protocol is analyzed in the network testbed simulator and compared with the prevailing data security and transmission protocols. The results are shown in Figure 5. Threat detection and mitigation will slow down due to the increase in data flow in the larger network. To address the issue, CAES-AE with ML-RBC model with key stretching method is deployed to resist crypto attacks and ensure robust security of data transmission from S→D. RTS were incorporated to counter DDoS and MMIT attacks, which reduces encryption delays. The new method dynamically adapts to maintain strong data encryption across node scales and maximizes the detection speed. The results of the new model with 96% speed are achieved with an NC of 500 and 84% with an NC of 2250, which is relatively high compared to the existing methods.

Table 5. Vulnerability Detection Speed (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
ERSA [11]	78	70	66	63	62	60	58	57
QoS-BFT [13]	84	82	80	78	76	75	74	72
AES [20]	90	88	87	86	85	84	82	81
CAES-AE [25]	91.5	88	86	85	84	83	82	82
ML-RBC [17]	93	90	87	85	85	84	84	83
CAESAE+MLRBC	**96**	**94**	**92**	**90**	**88**	**85**	**84**	**84**

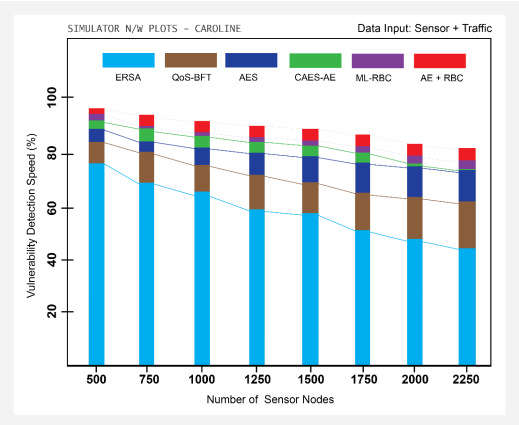

Fig 5. Comparative Analysis of VDS

3.5 Data Encryption Strength

Figure 6 shows the effectiveness of the proposed CAES-AE with ML-RBC model in terms of dynamic data encryption strength, and the results are compared with prevailing machine learning approaches such as ERSA, QoS-BFT, AES, Custom AES, and RBC. The new model maximizes the encryption strength by using alternative keys and making minor changes in plaintext to enhance resilience against crypto attacks. Also, it is further reinforced by key stretching to increase the strength of data encryption. As the new model follows a multi-layer approach, Pareto-based with dynamic tuning is adapted to add a robust layer against potential breaches. The TSM method is additionally employed to counter DDoS and MMIT attacks without affecting the speed of data exchange and delivery. Even as the node count increases, the encryption time remains stable at a certain rate, which ensures maximum data delivery with high security. 97% DES is achieved with a constant bit rate and transmission speed.

Table 6. Data Encryption Strength (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
ERSA [11]	85	80	76	73	68	64	61	58
QoS-BFT [13]	89	87	86	85	81	77	74	70
AES [20]	92	90	88	86	84	82	80	78
CAES-AE [25]	92.7	90	88	86	84	83	82	80
ML-RBC [17]	94	92	90	88	86	85	84	84
CAESAE+MLRBC	**97**	**95**	**93**	**91**	**87**	**85**	**83**	**82**

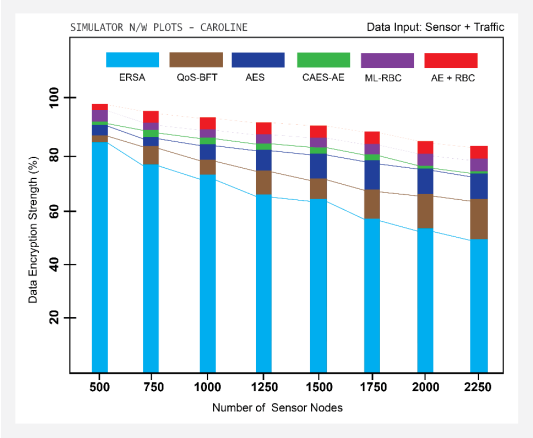

Fig 6. Comparative Analysis of DES

3.6 Network Performance

With the help of key stretching and minimization of repetitive encryption overhead under high loads, the energy consumption is reduced, which leads to an increase in network performance and lifetime. Figure 7 portrays the performance of CAES-AE with the ML-RBC network protocol, where the results are outperformed compared to existing baseline protocols. Sustainable performance is recorded across IoT network scales during testing and simulation with less energy and high performance. As the new approach is multilayered, the unnecessary energy drain is reduced, which helps an effective packet delivery ratio and minimizes latency and network failure. CAES-AE with ML-RBC boosts the network performance and lifetime up to 97.8%, which shows full potential for data delivery.

Table 7. Network Performance (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
ERSA [11]	84	81	76	75	69	65	60	58
QoS-BFT [13]	89	87	85	83	81	76	73	70
AES [20]	93	90	88	86	84	82	80	78
CAES-AE [25]	94	90	88	88	86	84	81	80
ML-RBC [17]	96	94	92	90	88	86	84	82

Continued on next page

Table 7 continued

CAESAE+MLRBC	**97.8**	**95**	**93**	**91**	**89**	**88**	**87**	**85**

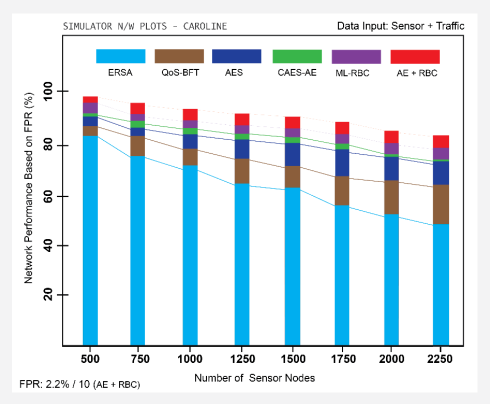

Fig 7. Comparative Analysis of Network Performance

4 Conclusion

The proposed CAES-AE with ML-RBC protocol secures the data in the IoT environment and transports it from source to destination efficiently. This new approach not only focuses on data authentication but also provides better security results in high transmission rates. Crypto package methods such as AES, DEDK, AE, RTS, and PBDP are utilized to create a secured IoT environment during the real-time data transmission process. In order to optimize threat detection and attack resilience and to provide high resistance to cryptographic attacks, key stretching, pareto-based selection, and dynamic parameter tuning with ML-RBC, rank, and tournament selection methods are employed. The NSL-KDD and IoT-23 traffic and sensor datasets are utilized to test in the network testbed using NS3 and OMNET++ simulators. During the testing process, the maximum node count sample is 2250 with a network range of 800x800 m2. The total number of iterations is denoted as N = 200. We assess the proposed method's performance using six performance metrics, achieving promising results such as a 97% authentication success rate, a 6 seconds response time to security actions, a 96% vulnerability detection speed, a 97% data encryption strength, a 5 seconds incident response time, and a 97.8% network performance (energy efficiency & lifetime). The new CAES-AE with ML-RBC protocol outperforms the existing IoT data transmission techniques such as ERSA, QoS-BFT, AES, Custom AES, and RBC. The results highlight that the proposed method has full potential to secure the data in an IoT environment compared to baseline models.

A few limitations of this model are scalability, less adaptability due to rapid environmental change, and high computational complexity during data testing. In the future, the model can be enhanced by the integration of auto backup and secured transmission technologies using artificial intelligence, which helps to minimize errors and maximize data security and integrity.

List of Abbreviations

1. Custom Advanced Encryption Standard (CAES)
2. Avalanche Effect (AE)
3. Internet of Things (IoT)
4. Enhanced Robust Security Adapted Protocol (ERSA)
5. Quality of Service (QoS)
6. Reconnaissance Bee Colony (RBC)
7. Machine Learning (ML)
8. Distributed Denial of Service Attack (DDoS)
9. Man in Middle Attack (MiMT)
10. Convolutional Neural Network (CNN)

References

1) Ziouzios D, Tsiktsiris D, Baras N, Dasygenis M. A Distributed Architecture for Smart Recycling Using Machine Learning. *Future Internet*;2020(9). Available from: https://doi.org/10.3390/fi12090141.
2) Islam N, Haseeb K, Ali M, Jeon G. Secured Protocol with Collaborative IoT-Enabled Sustainable Communication Using Artificial Intelligence Technique. . *Sustainability*;2022. Available from: https://doi.org/10.3390/su14148919.
3) Daraghmi Y, Daraghmi E, Daraghma R, Fouchal H, Ayaida M. Edge-Fog-Cloud Computing Hierarchy for Improving Performance and Security of NB-IoT-Based Health Monitoring Systems. *Sensors*;2022(22). Available from: https://doi.org/10.3390/s22228646.
4) Hasan M, Hanapi ZM. Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review. *Electronics*. 2023;12(2). Available from: https://doi.org/10.3390/electronics12020458.
5) Nithyanandh S, Jaiganesh V. Interrogation of Dynamic Node Link Failure by Utilizing Bio Inspired Techniques to Enhance Quality of Service in Wireless Sensor Networks. *Shodhganga*. 2020;400513. Available from: http://hdl.handle.net/10603/400513.
6) Alahmad T, Neményi M, Nyeki A. Applying IoT Sensors and Big Data to Improve Precision Crop Production: A Review. *Agronomy*;2023(10):2603–2603. Available from: https://doi.org/10.3390/agronomy13102603.
7) Tun N, Mambo M. Secure PUF-Based Authentication Systems. *Sensors*;2024(16):24–24. Available from: https://doi.org/10.3390/s24165295.
8) Chinnasamy P, Babu G, Ayyasamy R, Amutha S, Sinha K, Balaram A. Blockchain 6G-Based Wireless Network Security Management with Optimization Using Machine Learning Techniques. *Sensors*;2024(18):6143–6143. Available from: https://doi.org/10.3390/s24186143.
9) Jaiganesh NS, 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. Available from: https://doi.org/10.17485/IJST/v13i16.19.
10) Wakili A, Bakkali S, Alaoui A. Machine learning for QoS and security enhancement of RPL in IoT-Enabled wireless sensors. *Sensors International*. 2024;5:100289–100289. Available from: https://doi.org/10.1016/j.sintl.2024.100289.
11) Surenther I, Sridhar KP, Roberts MK. Enhancing data transmission efficiency in wireless sensor networks through machine learning-enabled energy optimization: A grouping model approach. *Ain Shams Engineering Journal*;2024(4). Available from: https://doi.org/10.1016/j.asej.2024.102644.
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. Available from: https://doi.org/10.35940/ijrte.b2271.078219.
13) Zhang H, Xue J, Wang Q, Li Y. A security optimization scheme for data security transmission in UAV-assisted edge networks based on federal learning. *Ad Hoc Networks*;150. Available from: https://doi.org/10.1016/j.adhoc.2023.103277.
14) Shitharth S, Yonbawi S, Manoharan H, Shankar A, Maple C, Alahmari S. Secured data transmissions in corporeal unmanned device to device using machine learning algorithm. *Physical Communication*. 2023;59. Available from: https://doi.org/10.1016/j.phycom.2023.102116.
15) 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. Available from: https://doi.org/10.35940/ijstr.b2271.0986231.
16) Mara, Satori H. Machine learning attack detection based-on stochastic classifier methods for enhancing of routing security in wireless sensor networks. . *Ad Hoc Networks* ;163:103581. Available from: https://doi.org/10.1016/j.adhoc.2024.103581.
17) Duan Y, Wu Q, Zhao X, Li X. Mobile edge computing based cognitive network security analysis using multi agent machine learning techniques in B5G. *Computers & Electrical Engineering*. 2024;117:109181–109181. Available from: https://doi.org/10.1016/j.compeleceng.2024.109181.
18) 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(34):2753–2766. Available from: https://doi.org/10.17485/IJST/v16i34.1706.
19) Mohammad AS, Pradhan MR. Machine learning with big data analytics for cloud security. *Computers & Electrical Engineering*. 2021;96. Available from: https://doi.org/10.1016/j.compeleceng.2021.107527.
20) Zhang S, Lagutkina M, Akpinar KO, Akpinar M. Improving performance and data transmission security in VANETs. *Computer Communications*. 2021;180:126–159. Available from: https://doi.org/10.1016/j.comcom.2021.09.005.
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(10):899–910. Available from: https://doi.org/10.17485/IJST/v17i10.3085.
22) Wang C, Li X, Tian J, Yin Y. Data transmission optimization based on multi-objective deep reinforcement learning. *The Computer Journal*. 2024. Available from: https://doi.org/10.1093/comjnl/bxae105.
23) 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(35):3609–3622. Available from: https://doi.org/10.17485/IJST/v17i35.2342.
24) Rezaei S, Javadpour A. Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission. *Multimed Tools Appl*. 2024;83:82247–82280. Available from: https://doi.org/10.1007/s11042-024-18776-x.
25) Kalaiselvi R, Caroline. Custom-AES: A Novel Framework To Enhance Data Security In Cloud Environment. *International Journal of Future Generation Communication and Networking*;2021(1):314–323. Available from: https://www.researchgate.net/publication/350106371.
26) 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);vol. 2024. 2024;p. 1–6. Available from: https://doi.org/10.1109/ICDSNS62112.2024.10690989.
27) Dataset: Maria Balega. IoT Data from IoT-23, NSL-KDD, and TON_IoT, IEEE Dataport; 2023. 2023. Available from: https://dx.doi.org/10.21227/yjtm-6x74.