International Journal of Research and Development in Engineering Science
ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/
Regular Issue, Vol. 7, Issue.2 (March – April), 2025 , Pages: 33 - 39
Received: 29 July 2024 ; *Accepted:* 03 January 2025 ; *Published:* 20 March 2025
https://doi.org/10.63328/IJRDES-V7RI2P6
Original Paper : Field Research – Case Study Paper

A Hybrid Cnn and Decision Tree Based Intrusion Detection System For Secure Wireless Sensor Networks

Y. Adline Jancy [1], Ashik S [2] , Bharathwaj P [3] , Gokulprenith J P [4]

Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India.;
adlinjan@gmail.com , ashik.2002019@srec.ac.in , bharathwaj.2002024@srec.ac.in , gokulprenith.2002037@srec.ac.in

** Corresponding Author:* adlinjan@gmail.com

Abstract: The By employing a machine learning algorithm to analyse traffic and identify intrusions, intrusion detection systems assist in identifying damaging hostile attacks in wireless sensor networks. The RSA encryption method is used to boost the performance of the wireless sensor network while also improving the security of data transmission. The goal of this research is to develop a hybrid algorithm for network intrusion detection in wireless sensor networks. This approach combines the principles of decision tree, convolutional neural networks (CNNs), and RSA encryption. Through the integration of these cutting-edge techniques, a comprehensive security solution for crucial applications is offered. This integration improves not only the detection and prevention of intrusions but also guarantees the confidentiality and integrity of sensitive data transmitted across wireless sensor networks.
Keywords: Convolutional Neural Network, Decision Tree Algorithm, RSA Encryption.

1. Introduction

Wireless sensor networks are systems of tiny devices equipped with sensors that wirelessly communicate to collect data without physical connections. For the purpose of obtaining real-time information, they are often used in a variety of industries, including industrial automation, healthcare, and environmental monitoring. Since these networks transfer data using radio waves, they are flexible and appropriate for a range of settings [1]. In machine learning, preprocessing and data collecting entail obtaining unprocessed data and getting it ready for examination. To prepare the data for training machine learning models, this entails organising, converting, and cleaning it. Proper data preprocessing ensures that the data is accurate, relevant, and structured, leading to better model performance and insights.

Intrusion refers to unauthorized access or interference with a system or network, often with malicious intent, posing a security threat. It encompasses various activities such as hacking, malware insertion, or unauthorized data access. In wireless sensor networks (WSNs), security is paramount due to vital information sharing and open deployment, with attackers targeting various protocol layers [2]. Signature-Based IDS relies on predefined attack patterns for high-accuracy detection but struggles with novel attacks, while Anomaly-Based IDS identifies deviations from normal behaviour, detecting zero-day exploits but prone to false positives due to legitimate variations. This wireless sensor network (WSN) intrusion detection system uses the RSA method for data encryption, decision trees to categorise attack behaviour, and convolutional neural networks (CNN) to automatically extract characteristics from network traffic data. Safeguarding data confidentiality and integrity, this method allows for the identification of many types of assaults, such as probing attacks, R2L (Remote-to-Local) attacks, U2R (User-to-Root) attacks, and Denial of Service (DoS) attacks [3].

CNN model training, and real-time intrusion detection are conducted in Jupiter notebook, with performance evaluation and optimization techniques applied to enhance detection accuracy and efficiency. Users may create and share documents with live code, equations, visualisations, and narrative prose using the open-source online application Jupiter Notebook. It is frequently used for tasks involving data analysis, scientific computing, and machine learning and supports a variety of programming languages [4]. The CNN-based intrusion detection system (IDS) is successfully validated, implemented, and integrated into the WSN environment. This enhances the accuracy and efficiency of the IDS and provides complete network security, hence bolstering the resilience and dependability of the network infrastructure. The system computes performance measures including accuracy,

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P6

recall, precision, and F-measure for the several methods used in intrusion detection and data encryption in wireless sensor networks (WSNs), in addition to integrating Convolutional CNN, decision trees [5], and the RSA algorithm. The algorithm that performs best overall and with the highest accuracy is chosen for deployment after thorough testing and comparison.

2. Related Works

Convolutional neural networks (CNNs) and the RSA algorithm have been applied to Intrusion Detection Systems (IDS) for Wireless Sensor Networks (WSNs) in a number of studies. A wide range of assaults, such as Denial of Service (DoS), probing, grey hole, black hole, R2L (Remote-to-Local), and U2R (User-to-Root), are to be detected and mitigated by this integrated method. The IDS analyzes network traffic patterns using CNN for automatic feature extraction, while RSA encryption ensures data confidentiality and integrity during transmission. Real-time monitoring allows for the identification of suspicious activity, enabling proactive mitigation measures and dynamic network adjustments [6].

Dr. Vijay K Chaurasiya, Aman Goyal, and Sourav Mishra conducted research on enhancing the security of Wireless Sensor Networks (WSNs), which are increasingly utilized across various sectors like healthcare and manufacturing, characterized by limited power and bandwidth resources. Unlike traditional networks, securing WSNs demands novel approaches due to their unique constraints. This paper highlights the critical issue of intrusion prevention and suggests a Deep Learning (DL) method using Dense Artificial Neural Networks (Deep-ANN) for Intrusion Detection Systems (IDS) in WSNs. The created ANN model outperforms other machine learning models in terms of precision, recall, and F1 scores, with an accuracy of 96.45 percent. This means that it provides strong defence against possible attacks in WSN situations [7].

The security problems of Wireless Sensor Networks (WSNs), especially in military and civilian applications, are examined by Gebre Kiros Gebreyesus Gebremariam, J. Panda, and S. Indu. WSNs are characterised by their hierarchical and unmonitored nature at remote places. In light of WSNs' vulnerability to routing attacks such as wormholes, sinkholes, Black holes, and Sybils, they suggest an Advanced Intrusion Detection System (AIDS-HML) that uses hybrid machine learning to identify and categorise these types of assaults [8]. Using the NSL-KDD benchmark dataset using a hybrid random forest and extreme gradient boost (RF-XGB) model, the hybrid machine learning classifiers show promise in detecting WSN threats, attaining an impressive detection accuracy of 99.80%. Furthermore, for binary label attack classification, the hybrid cluster labelling K-Means (CLK-M) model obtains 100% accuracy in classification using UNSW_NB15 and CICIDS2017 datasets. After undergoing comprehensive assessments against reference datasets, the suggested system demonstrates exceptional performance metrics such as accuracy, precision, recall, and F1-score, indicating its effectiveness in identifying a range of WSN assaults. In addition, the system shows effectiveness in feature extraction, route finding, and assault detection simulations, with a 99.46% total accuracy [9].

A mix of signature-based and anomaly-based techniques is frequently used in the current intrusion detection system (IDS) landscape for wireless sensor networks (WSNs). Signature-based IDS involves comparing incoming data with predefined attack patterns for accurate detection but may struggle with new threats. Anomaly-based IDS establishes normal behaviour baselines using statistical or machine learning techniques, flagging deviations as potential attacks. While effective against novel threats, they may produce false positives due to normal behaviour variations [10]. Combining both methods enhances overall detection capabilities in WSNs.

3. Proposed System

By integrating the RSA algorithm, decision tree method, and convolutional neural networks (CNN), this research assesses the effectiveness of the suggested intrusion detection system (IDS) in wireless sensor networks (WSNs). It ensures the detection of various attacks while maintaining data confidentiality and integrity. Initial data collection, preprocessing, decision tree classifier and CNN model training enable real-time intrusion detection. Performance evaluation and optimization techniques enhance detection accuracy and efficiency [11].

In order to improve real-time threat identification and network security, the suggested intrusion detection system for wireless sensor networks integrates CNNs for feature extraction, RSA encryption for data security, and decision trees for behaviour classification .This method guarantees the secrecy and integrity of sensitive data while enabling the detection of a broad variety of assaults, such as probing attacks, R2L (Remote-to-Local), U2R (User-to-Root), Denial of Service (DoS), and black hole attacks. In order to extract pertinent characteristics and decrease dimensionality, data gathering and preprocessing are first carried out. The pre-processed data is then used to train a CNN model, which identifies hierarchical characteristics of both benign and malevolent activity. Normal behaviour refers to actions within a system that adhere to expected patterns and do not pose a threat to its integrity or security. Malicious behaviour, on the other hand, involves actions aimed at compromising the system's functionality, accessing

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P6

unauthorized information, or causing harm, often in violation of established protocols or norms [12]. The trained model is then deployed for real-time intrusion detection.

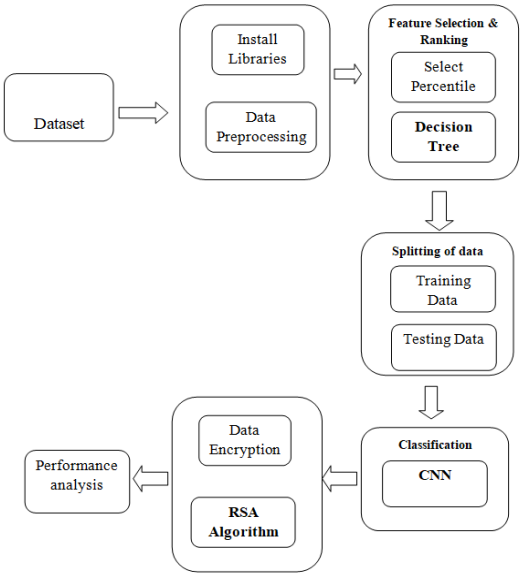

Fig.1 Flow Chart for IDS in WSNs

The intrusion detection flow chart for wireless sensor networks involves several key stages: data collection, preprocessing, and feature selection to construct a classification model. It encompasses the use of decision trees, optional CNNs for classification, and RSA encryption for data security [13]. Performance analysis ensures the system's effectiveness in detecting and mitigating intrusions, guiding further refinement, while an iterative process ensures continuous adaptation and optimization to evolving threats in wireless sensor networks.

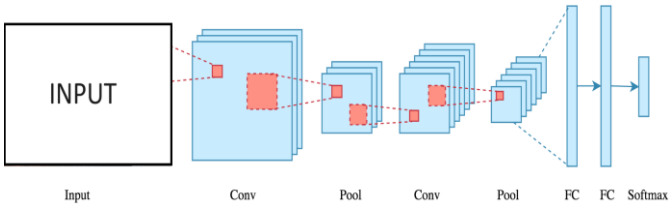

Fig.2 Functional Flow

In wireless sensor networks, the CNN architecture for intrusion detection first extracts spatial features from raw data, then pools layers to preserve pertinent information. By capturing complicated patterns, stacked convolutional layers improve the network's comprehension of nuanced interactions [14]. Refined learnt representations are produced by fully connected layers, while probability distributions over classes are produced by a softmax layer to assist with classification. This CNN is trained on labelled data and is capable of accurately detecting intrusions in wireless sensor networks by differentiating between regular network traffic and malicious activity.

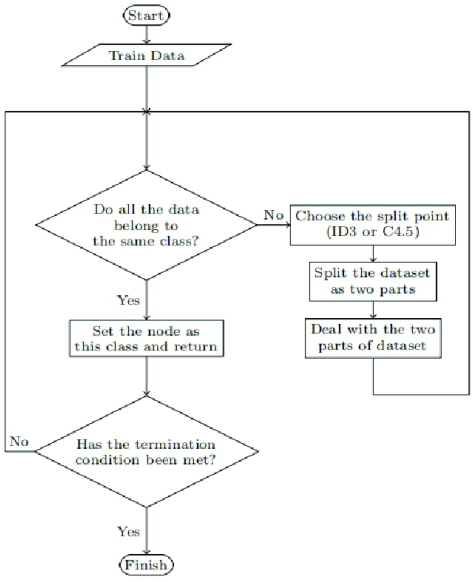

Fig.3 Flow Chart for Decision Tree

(a). **Preprocessing:** Preprocessing data involves converting raw data into an understandable format, addressing missing values and standardizing input data for network training. Techniques such as normalization and numerical processing aim to provide uniform input data. Label Encoder assigns unique integer labels to categorical features, while OneHotEncoder creates binary columns representing category presence.

(b). **Feature Extraction:** Feature extraction reduces dimensionality of high-dimensional data by selecting sensitive features crucial for constructing optimal feature vectors. This process prunes useless and low-influence features from the dataset, improving machine learning model performance and efficiency.

(c). **Training the Data:** Neural networks train data to obtain optimal features. Comprising input, hidden, and output layers, neural networks utilize forward and backward propagation phases. Forward propagation processes positive signals, while backward propagation adjusts model parameters based on deviation between calculated and actual output values.

(d). **Classification of Data:** Convolutional Neural Networks (CNNs) are instrumental in classifying intrusion detection data, particularly through iterative CNNs (ICNNs). In ICNNs, the process involves backpropagation, where weights and biases are adjusted iteratively to minimize loss using stochastic gradient descent. By leveraging convolution kernels across multiple network layers, ICNNs expand the extracted feature information. Furthermore, through the application of the chain rule, ICNNs refine the classification process based on the

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P6

intricacies of intruder detection data, thus enhancing the network's ability to detect and classify potential threats in wireless sensor networks.

(e). **RSA Algorithm:** The RSA algorithm is a form of asymmetric cryptography, which operates using two distinct keys: the public key and the private key. This means that while the public key is shared openly, the private key remains confidential. This helps the intrusion detection system to be secure while transferring data [15].

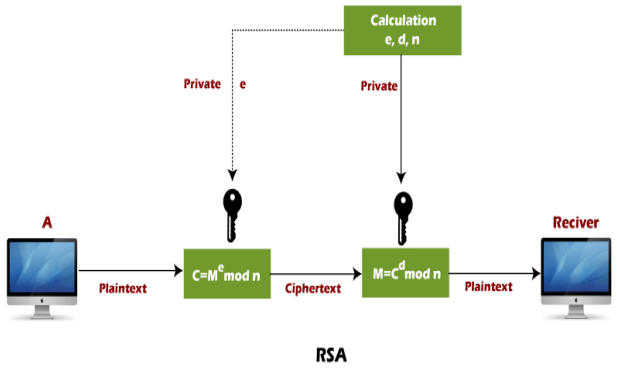

Fig.4 RSA Algorithm

(f). **Attacks in Network Layer:** These various types of attacks pose significant threats to the security and integrity of wireless sensor networks (WSNs), ranging from disrupting network operations to compromising sensitive data and system integrity.

(g). **Denial of Service (DoS) Attacks:** These attacks try to stop the network from operating normally by flooding it with a lot of unauthorised requests or traffic. Attacks that deplete network resources, including computing power or bandwidth, prevent users from accessing proper network services.

(h). **Probe Attacks:** Probe attacks involve unauthorized entities gathering network information for potential malicious activities, either by passively observing traffic or actively sending probing packets to identify vulnerabilities and potential targets.

(i). **R2L Attacks:** R2L attacks occur when external entities exploit network vulnerabilities to gain unauthorized access to local systems. By bypassing authentication mechanisms, attackers can execute commands, escalate privileges, or extract sensitive data from compromised systems.

(j). **U2R Attacks:** U2R attacks involve unauthorized users attempting to elevate their privileges within the network to gain administrative or root-level access. By exploiting software vulnerabilities, attackers aim to escalate their access rights and carry out further malicious activities undetected.

(k). **Gray Hole Attacks:** Malicious nodes can deliberately discard or alter data packets travelling over the network in Grey Hole attacks, all while keeping connection open. By causing data transmission to be disrupted or tainted, this selective packet dropping puts the network's dependability and integrity at risk.

(l). **Black Hole Attacks:** Black Hole attacks involve a malicious node falsely advertising itself as having the shortest path to the destination. As a result, legitimate data traffic is routed through the black hole node, where it is either dropped or intercepted by the attacker.

4. Module Description

(a). **Preprocessing from sklearn:** preprocessing import Label Encoder, OneHotEncoder These modules are used for encoding categorical variables into numerical representations, which is a common preprocessing step in machine learning tasks.

- LabelEncoder assigns a unique integer label to each category in a categorical feature.
- OneHotEncoder generates binary columns for every category, using 1s and 0s to indicate if a category is present or absent, accordingly.

	protocol_type	service	flag
0	1	20	9
1	2	44	9
2	1	49	5
3	1	24	9
4	1	24	9

Fig 6. Label Encoder

	Protocol_type_icmp	Protocol_type_tcp	Protocol_type_udp	service_IRC	service_X11	service_Z39_50	service_aol	service_auth	service_bgp	service_courier	...
0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	...
1	0.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	...
2	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	...
3	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	...
4	0.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	...

Fig 7. One Hot Encoder

(b). **Feature Selection:** Feature selection employs univariate selection with ANOVA F-test and Recursive Feature Elimination (RFE) to enhance model efficiency and interpretability by retaining informative features while reducing dimensionality. ANOVA F-test selects features based on relevance to the target variable, while RFE iteratively identifies the

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P6

most informative subset of features based on model performance.

(c). **Confusion Matrix:** Classes such as 'Probe,' 'DOS,' 'R2L,' and 'U2R,' which indicate the model's classification performance, are included in a confusion matrix for IDS in WSNs. To help with intrusion type categorization, rows show real classes, columns show expected classes, and cell counts show instance combinations.

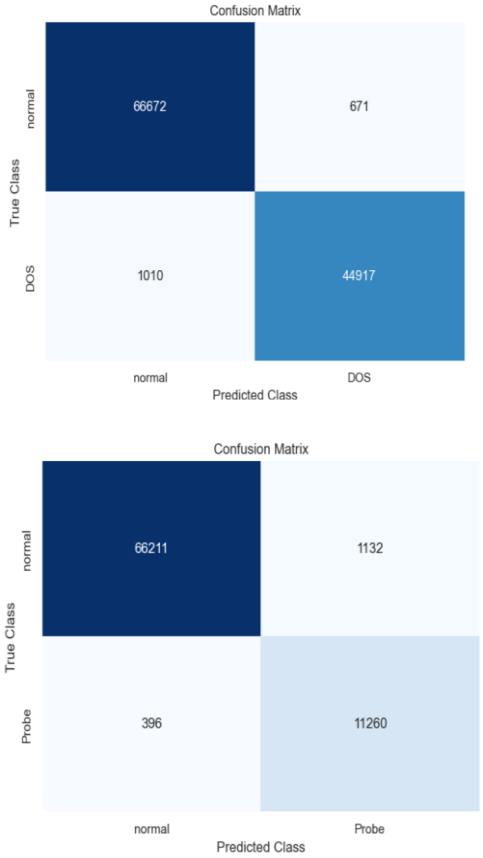

Fig.8 Confusion Matrices

(d). Performance Analysis

True Negatives (TN): Accurately detects negative values in which the assumed 'no' class and the real 'not' class coincide.

True Positives (TP): Precisely detects positive values in which the expected and actual results coincide.

False Negatives (FN): When a positive class is really forecasted as negative, positive occurrences are missed.

False Positives (FP): When a real negative class is forecasted as positive, positive results are mistakenly identified.

Accuracy: Evaluates overall accuracy by comparing the number of accurate predictions to the total number of forecasts produced.

(TN+TP)/(TN+FP+TP+FN) = Accuracy.

Precision measures how accurate a positive prediction is in comparison to all other positive forecasts.

TP/(TP + FP) = Precision.

Recall: Evaluates the capacity to recognise good examples while taking into account all real positive incidents.

T P/(TP + FN) = Recall.

F-measure: Provides a weighted average for an extensive assessment by balancing recall and accuracy.

Table.1 Performance evaluation of Decision tree, Naïve Bayes and Random Forest

Decision Tree	Accuracy	Precision
DOS	0.99639	0.99505
PROBE	0.99571	0.99391
R2L	0.97920	0.97150
U2R	0.99663	0.86481

Naive Bayes	Accuracy	Precision
DOS	0.99819	0.99879
PROBE	0.99670	0.99577
R2L	0.98134	0.97491
U2R	0.99734	0.95725

Random Forest	Accuracy	Precision
DOS	0.86733	0.98822
PROBE	0.97898	0.97323
R2L	0.93562	0.89097
U2R	0.97259	0.60157

5. Simulation And Result

The experimental results in IDS for WSN showcase the system's effectiveness in detecting intrusions, guiding future security measures.

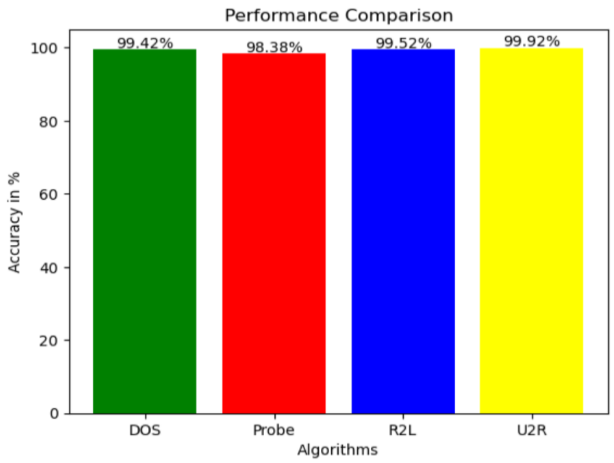

Fig.9 Accuracy Performance Graph

Fig.9 Performance Graph illustrates the accuracy comparison of different attack types, including DOS,

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P6

Probe, R2L, and U2R, providing valuable insights into the effectiveness of the intrusion detection system. Notably, the graph highlights that the U2R attack exhibits the highest accuracy among the analyzed attack types.

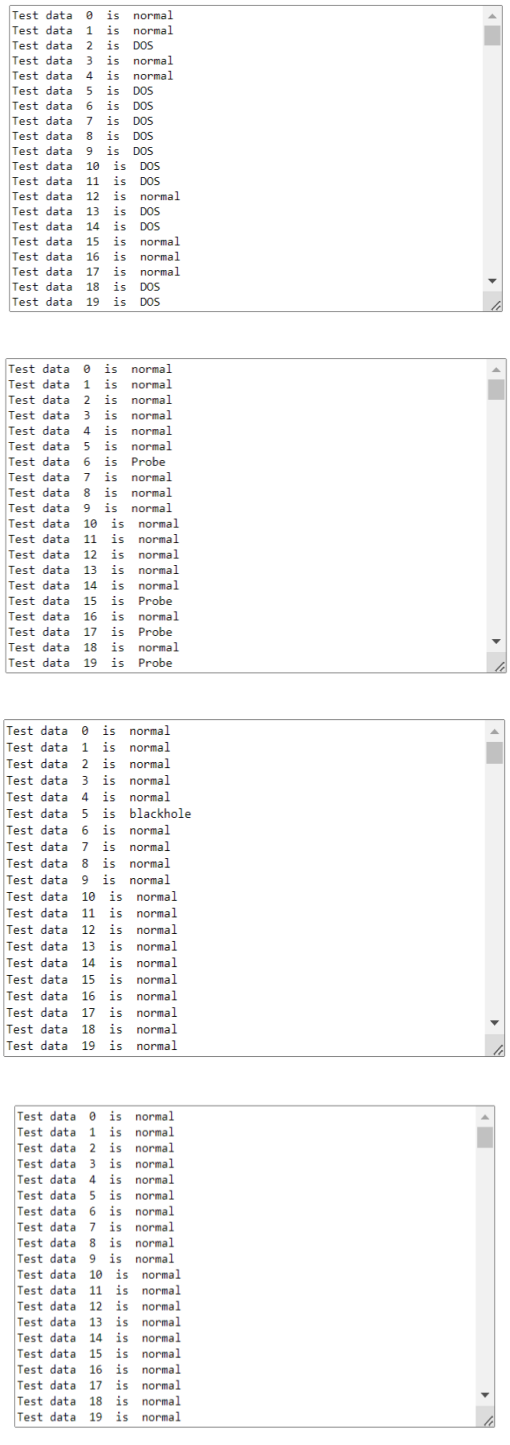

Fig.10 Result

The `rsa()` function initializes prime numbers `p` and `q`, along with a test message. It then calls `rsa_algo()` to perform encryption and decryption. Within `rsa_algo()`, the modulus `n` and Euler's totient function `z` are computed. Public and private exponents `e` and `d` are found using helper functions `find_e()` and `find_d()`, respectively. The message is encrypted by raising each character to the power of `e` modulo `n`, while decryption follows a similar process using `d`. The `gcd()` function computes the greatest common divisor. This code demonstrates the core RSA encryption and decryption process, showcasing its fundamental principles for securing data transmission.

6. Conclusion

In conclusion, the integration of a Hybrid algorithm with Convolutional Neural Network, decision tree and RSA algorithm in Wireless Sensor Networks (WSNs) offers significant advancements in intrusion detection systems. By learning to detect unusual patterns and suspicious activities, the system effectively identifies intrusions and alerts users via cloud data, thereby enhancing network security. Decision trees in intrusion detection for wireless sensor networks classify normal and anomalous behaviours efficiently, using features like packet size and frequency for real-time threat identification. Their transparent and interpretable framework, achieved through recursive partitioning of the feature space, enhances network security robustness by detecting diverse intrusion patterns. This approach not only improves threat detection but also reduces false alarms, making networks more resilient against attacks. Moreover, the proposed wireless network intrusion detection system based on an improved CNN addresses the limitations of traditional deep learning methods, resulting in higher accuracy and true positive rates while lowering the false positive rate.

References

[1]. Abhale, A. B., and Manivannan, S. S. "Deep Learning Algorithmic Approach for Operational Anomaly Based Intrusion Detection System in Wireless Sensor Networks." 2021.

[2]. Asha, R. N. "Data mining based intrusion detection system for securing wireless sensor network." Harbin Gongye Daxue Xuebao/Journal of Harbin Institute of Technology, vol. 53, no. 10, pp. 22–32, 2021.

[3]. Baraneetharan, E. "Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey." Journal of Information Technology, vol. 2, no. 03, pp. 161-173, 2020.

[4]. Chandre, P. R., Mahalle, P. N., and Shinde, G. R. "Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification." Proc. - 2018 IEEE Glob. Conf. Wirel. Comput. Networking, GCWCN 2018, pp. 135-140, 2019, doi: 10.1109/GCWCN.2018.8668618.

[5]. Divyashree, G., Durgabhavani, A., Kavya, M., Gudoor, A., and Shetty, M. B. "Intrusion detection system in wireless sensor network." Int. J. Recent Technol. Eng., vol. 8, no. 1, pp. 2047–2051, 2019.

[6]. Halbouni, T. S. Gunawan, M. H. Habaebi, M.Halbouni,

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 7, Issue 2, 2025 , https://doi.org/10.63328/IJRDES-V7RI2P6

M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp.99837-99849, 2022, doi:10.1109/ACCESS.2022.3206425

[7]. Ifzarne, S., Tabbaa, H., Hafidi, I., and Lamghari, N. "Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks." J. Phys. Conf. Ser., vol. 1743, no. 1, 2021, doi: 10.1088/1742-6596/1743/1/012021.

[8]. Kalnoor, G., and Gowrishankar, S. "Minimizing energy consumption for intrusion detection model in wireless sensor network." In Applications of Artificial Intelligence and Machine Learning, pp. 527–537, Springer, Singapore, 2021.

[9]. S. T, M. N. S, H. V. G, N. P, and A. C, "Chatbot for Mental Health Support utilizing Neural Network Technologies," *International Journal of Computational Science and Engineering Research*, vol. 1, no. 4, p. 61, Nov. 2025, doi: 10.63328/ijcser-v1ri4p12.

[10]. Lohiya, R., and Thakkar, A. "Intrusion detection using deep neural network with anti rectifier layer." In Applied Soft Computing and Communication Networks, pp. 89–105, Springer, Singapore, 2021.

[11]. Maheswari, O. U., and Jayasankari, S. "Secure communication in wireless sensor network using intrusion detection system for agriculture." International Journal of Modern Agriculture, vol. 10, no. 2, pp. 1829–1845, 2021.

[12]. Singh, N., Virmani, D., and Gao, X. Z. "A fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset." International Journal of Computational Intelligence and Applications, vol. 19, no. 3, article 2050018, 2020.

[13]. D Ramachandra Reddy , M Mohammed Fazil Khan , Farooq , T Mahesh , M Nagendra Babu, "Prediction of Machine Failure Status using Machine Learning Techniques" ,International Journal of Computational Science and Engineering Research, vol. 1, no. 3, p. 9, July. 2024, doi: https://doi.org/10.63328/IJCSER-V1RI3P3

[14]. Vadapalli, P. "Label Encoder vs One Hot Encoder in Machine Learning." upGrad, 2021. [Online]. Available: https://www.upgrad.com/blog/label-encoder-vs-one-hot-encoder/.

[15]. W. Yang, S. Wang, and M. Johnstone,"A comparative study of ML-ELM and DNN for intrusion detection," in 2021 Australasian Computer Science Week Multiconference, Dunedin New Zealand, 2021.