WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Artificial Intelligence based Security Solution for Data Encryption using AES Algorithm

Gadankush Yash[1], Mohammed Asaduddin[2], Mohammed Rizwan Khan Farooqui[3], Farheen Sultana[4]

Department of IT, Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad, India Email:yashgadankush45@gmail.com

Abstract:

This project proposes a hybrid artificial intelligence-based security framework for data encryption using the Advanced Encryption Standard (AES) algorithm. Designed with a layered architecture, the solution integrates AI-enhanced intrusion detection with encryption and steganographic methods to secure data communication across autonomous vehicles and IoT networks. Customized neural networks trained via particle swarm optimization offer real-time anomaly detection, while AES and RSA algorithms ensure dual encryption. Finally, steganography adds a concealment layer, safeguarding sensitive data in transit and storage. The proposed approach is implemented using Python, and validated through simulation to demonstrate enhanced data confidentiality and resilience against modern cyber threats.

Keywords AI Security, AES Encryption, Cybersecurity, Intrusion Detection, Autonomous Vehicles, Steganography

1. Introduction:

The rapid advancement of autonomous vehicles (AVs) and Internet of Things (IoT) technologies has revolutionized the modern transportation infrastructure. AVs, equipped with diverse sensors and real-time communication capabilities, are transforming logistics, public safety, and mobility. However, their reliance on interconnected systems exposes them to increasing cyber threats, making data privacy and system security a top priority. Modern AV networks—collectively referred to as the Internet of Transportation Systems—exchange sensitive information through cloud and network-based platforms. The security of these platforms is critical, as any breach could result in severe consequences, such as vehicle malfunction, traffic disruption, or loss of life. Cyber attackers can exploit vulnerabilities at multiple layers: from embedded sensors to cloud-stored data and OTA (Over-The-Air) updates. To mitigate these threats, this project proposes an AI-enhanced security solution that integrates machine learning models for intelligent intrusion detection with cryptographic measures. Specifically, it utilizes the Advanced Encryption Standard (AES) to protect data integrity, supported by a dual encryption model and steganographic techniques to prevent unauthorized data access and enhance confidentiality.

2. Literature Review:

The surge in IoT device usage has prompted extensive research into safeguarding these networks from emerging threats, especially botnet attacks. Researchers have focused on utilizing machine learning and deep learning techniques to develop intelligent intrusion detection systems capable of handling complex, high-dimensional network traffic. The following studies provide foundational insights and advancements relevant to the proposed hybrid model:

• **Siva Raja Sindiramutty (2015)** introduced the concept of *Autonomous Threat Hunting*, which integrates AI into cybersecurity frameworks. His work emphasized AI-driven threat intelligence for detecting and mitigating evolving cyber threats in real-time. By utilizing machine learning models like supervised, unsupervised, and reinforcement learning, the system adapts to new threats autonomously, reducing response time and enhancing cyber resilience.

• **J. Anitha Ruth, H. Sirmathi, A. Menakshi (2018)** proposed a *Secure Data Storage and Intrusion Detection System* using Modified Artificial Neural Networks (MANN) and a dual encryption mechanism (RSA + AES). Their model incorporated particle swarm optimization to enhance ANN performance and used steganography for additional security, offering a comprehensive multi-layer defense for cloud environments.

• **Murat Kuzla, Corfeinne Fair, Jacky Chan (2021)** studied the *Role of Artificial Intelligence in IoT and Cybersecurity*. They highlighted the benefits and threats posed by AI in modern security systems. Their review showed that AI can detect Distributed Denial-of-Service (DDoS) attacks, tampering,

and unauthorized access using models such as decision trees and neural networks. However, it also warned about adversaries exploiting AI for crafting advanced attacks, creating a complex security landscape.

• **Yusuf Alkali, Indira Routray, Pawan Whig (2021)** investigated *Secure IoT Networking Using AI*. They proposed a hybrid framework combining supervised, unsupervised, and reinforcement learning for anomaly detection in cloud-based IoT environments. Their study showcased how intelligent models can dynamically adapt to traffic anomalies and policy violations in real-time.

3. Methodology:

This project proposes a layered security framework that integrates Artificial Intelligence (AI)-based anomaly detection with a hybrid encryption pipeline for secure data processing and transmission. The methodology is structured into modular components to ensure data confidentiality, integrity, and availability in autonomous and IoT-enabled environments.

3.1 System Overview

The core objective is to enhance the security posture of Autonomous Vehicles (AVs) and cloud-integrated IoT systems by implementing an intelligent encryption strategy. The system comprises the following key stages:

- Preprocessing and Intrusion Detection
- Dual Encryption (AES + RSA)
- Steganographic Data Embedding
- Cloud Storage and Access Management

The entire architecture is implemented using Python and deployed in a simulated environment to assess its efficiency and robustness under various security scenarios.

3.2 Preprocessing and Anomaly Detection

Raw text or data is initially cleaned and preprocessed to eliminate redundant or irrelevant features. This includes:

- Removing stop words
- Extracting top keywords
- Eliminating repetitions

Once cleaned, the data is passed through a Modified Artificial Neural Network (MANN) for real-time anomaly detection. This MANN model is trained using a Modified Particle Swarm Optimization (MPSO**)** algorithm to dynamically update network weights, thereby enhancing detection accuracy and reducing false positives.

3.3 Dual Encryption System

Data that passes anomaly detection is subjected to a two-layer encryption process RSA provides secure key transmission using asymmetric cryptography and similarly AES Encryption Implements fast and secure symmetric encryption for data blocks. This dual approach ensures both key confidentiality and efficient data protection during transmission and storage.

3.4 Steganographic Layer

To further reinforce confidentiality, encrypted data is embedded within benign carrier files (such as images or plain text) using steganographic techniques. This ensures that the data is not easily detectable even if intercepted, adding an additional layer of obfuscation.

3.5 Cloud Storage Integration

The final output secure, encrypted, and steganographically protected data is uploaded to the cloud. Access to this storage is governed by a combination of Secure login authentication and Role-based access control.

3.6 Secure Cloud Storage

The final encrypted and embedded data is stored in a secure cloud infrastructure. The storage layer is protected through Access control mechanisms, Role-based user authentication and Optional blockchain-based record tracing (in future enhancement)

4. Illustrations:

```python
@app.route("/features_selection" )
def features_selection():
    return render_template("features_selection.html")

@app.route("/selected_features",methods =["GET", "POST"] )
def selected_features():
    fname = request.form.get("file")
    df = pd.read_csv(fname)
    print("date=",df.head())
    features_list,targetcol=getFeatures(df)
    X=df[features_list]
    print("date2=",df.head())
    y=targetcol
    dict['X'] = X
    dict['y'] = y
    df2=df[features_list]
    df2["class"]=y
    df2.to_csv("features.csv",index=False)

    return render_template("features_selection.html",features_list=features_list)
```

Fig. 1 – Data Preprocessing

Fig. 2 – Feature Selection

```python
@app.route("/evaluations")
def evaluations():
    rf_list=[]
    etc_list = []
    ann_list = []
    cnn_list = []
    metrics=[]
    X=dict['X']
    y=dict['y']

    # Split train test: 70 % - 30 %
    X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=15)


    accuracy_rf, precision_rf, recall_rf, fscore_rf = rfc_evaluation(X_train, X_test, y_train, y_test)
    rf_list.append("RFC")
    rf_list.append(accuracy_rf)
    rf_list.append(precision_rf)
    rf_list.append(recall_rf)
    rf_list.append(fscore_rf)

    accuracy_etc, precision_etc, recall_etc, fscore_etc = etc_evaluation(X_train, X_test,y_train, y_test)
    etc_list.append("ETC")
    etc_list.append(accuracy_etc)
    etc_list.append(precision_etc)
    etc_list.append(recall_etc)
    etc_list.append(fscore_etc)

    accuracy_ann, precision_ann, recall_ann, fscore_ann = ann_evaluation(X_train, X_test, y_train, y_test)
    ann_list.append("ANN")
    ann_list.append(accuracy_ann)
    ann_list.append(precision_ann)
    ann_list.append(recall_ann)
    ann_list.append(fscore_ann)

    accuracy_cnn, precision_cnn, recall_cnn, fscore_cnn = cnn_evaluation()
    cnn_list.append("CNN")
    cnn_list.append(accuracy_cnn)
    cnn_list.append(precision_cnn)
    cnn_list.append(recall_cnn)
    cnn_list.append(fscore_cnn)

    metrics.clear()
    metrics.append(rf_list)
    metrics.append(etc_list)
    metrics.append(ann_list)
    metrics.append(cnn_list)


    return render_template("evaluations.html", evaluations=metrics)
```

Fig. 3 – Metrics Evaluation

5. Result:

The proposed AI-based security system for data encryption was implemented and evaluated through a simulation environment using Python-based frameworks. The system demonstrated effective integration of anomaly detection and dual-layer encryption, resulting in significant improvements in data security and reliability. The Modified Artificial Neural Network (MANN), trained using Modified Particle Swarm Optimization (MPSO), showed high

precision in classifying input data as normal or intrusive. It successfully filtered malicious inputs and forwarded only verified data to the encryption pipeline, ensuring that potentially harmful content was intercepted early in the process.

Following intrusion validation, the encryption phase employed a combined AES and RSA mechanism that achieved secure encoding and key protection without compromising processing efficiency. AES enabled rapid encryption of the data payload, while RSA safeguarded the key transmission, enhancing the confidentiality of the overall system. The subsequent steganography layer proved effective in obfuscating encrypted content within benign carrier files, offering an added layer of protection against data interception during network transmission.

Experimental evaluations revealed that the system maintained robust performance under varied input scenarios. It consistently produced encrypted outputs that were both computationally efficient and secure against pattern recognition and data leakage. The steganographic component was able to conceal encrypted information in such a manner that standard inspection techniques could not detect the presence of hidden data. These results validate the effectiveness of combining intelligent data analysis with strong cryptographic and concealment techniques for real-time applications in IoT and autonomous vehicle systems. The outcomes highlight the viability of the proposed architecture in ensuring data privacy, security, and integrity in highly dynamic and interconnected environments.

6. Requirements:

6.1. Hardware Requirements

- Processor : Any Update Processer
- Ram : Min 4 GB
- Hard Disk : Min 250 GB

6.2. Software Requirements

- Operating System : Windows family
- Technology : Python 3.8
- Front-end Technology : HTML, CSS, JS
- Back-end Technology : MySQL
- IDE : PyCharm IDE
- Web Framework : Flask

7. Conclusion:

TThe proposed system successfully integrates artificial intelligence with cryptographic techniques to enhance data security in autonomous and IoT environments. By employing MANN-based intrusion detection and dual-layer encryption, it ensures confidentiality, integrity, and resilience. The use of steganography further strengthens data protection by concealing encrypted content. Experimental results validate the system's effectiveness in mitigating cyber threats. This framework demonstrates practical applicability for secure, real-time data communication in intelligent networks.

Appendix A. Detailed Algorithm

Step 1: Import Required Libraries

Import essential Python libraries such as NumPy and Pandas for data manipulation. Use Scikit-learn for preprocessing and evaluation, and TensorFlow/Keras for deep learning model development.

Step 2: Dataset Collection and Organization

Use structured input data, either collected manually or from datasets. Organize the data into labelled CSV format, including features relevant to anomaly detection and encryption.

Step 3: Feature Extraction and Preprocessing

Load the dataset and inspect the attributes. Perform feature encoding for categorical variables and normalize numerical values to maintain consistency. Remove duplicates and irrelevant fields.

Step 4: Intrusion Detection Model Training

Train a Modified Artificial Neural Network (MANN) using Modified Particle Swarm Optimization (MPSO) for weight tuning. The model classifies input as either normal or intrusive based on trained patterns.

Step 5: Anomaly Classification

Evaluate the model on the testing dataset. If data is classified as normal, proceed to encryption; if classified as intrusive, discard or log the data for review.

Step 6: Hybrid Encryption

Encrypt valid data using AES for fast, symmetric encryption and protect the encryption key using RSA for secure key transmission.

Step 7: Steganographic Embedding

Embed the encrypted data into a cover file (such as an image or text document) using steganographic techniques to conceal its presence during transmission.

Step 8: Secure Storage

Store the final secure file in a cloud environment protected by access controls and user authentication mechanisms.

Step 9: Prediction Function

Deploy a real-time prediction pipeline that accepts new data inputs, processes them through the trained MANN model, and automatically encrypts and stores valid inputs.

Appendix B. Survey Questionnaire

The following questionnaire was used to gather feedback on the botnet detection system:

- How intuitive was the process of uploading and submitting input data to the system?
- Was the user interface for encryption and result retrieval clear and easy to use?
- Were the results (normal/intrusive, encrypted output) understandable and clearly presented?
- Did the system provide appropriate feedback or error messages for invalid inputs?
- Do you feel the system offers a reliable and secure approach for protecting sensitive data?
- Would you recommend this system for use in real-time IoT or autonomous environments?
- How satisfied were you with the overall speed and responsiveness of the platform?
- Were you confident in the system's ability to prevent unauthorized access or attacks?

References

[1] J. Anitha Ruth, H. Sirmathi, and A. Meenakshi, "Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks," IET Information Security, vol. 13, no. 4. Institution of Engineering and Technology (IET), pp. 321 329, Jul. 2019. doi: 10.1049/iet-ifs.2018.5295.

[2] O. Alabi, A. J. Gabriel, A. Thompson, and B. K. Alese, "Privacy and Trust Models for Cloud-Based EHRs Using Multilevel Cryptography and Artificial Intelligence," Internet of Things. Springer International Publishing, pp. 91–113, 2022. doi: 10.1007/978-3-030-80821-1_5.

[3] J. Jain, "Artificial Intelligence in the Cyber Security Environment," Artificial Intelligence and Data Mining Approaches in Security Frameworks. Wiley, pp. 101–117, Aug. 10, 2021. doi: 10.1002/9781119760429.ch6.

[4] Z. Wang, L. Shi, N. Chen, and J. Chen, "Research on computer network security evaluation based on image recognition and neural network," Journal of Electronic Imaging, vol. 32, no. 01. SPIE-Intl Soc Optical Eng, Sep. 15, 2022. doi: 10.1117/1.jei.32.1.011214.

[5] S. Gadde, J. Amutharaj, and S. Usha, "A security model to protect the isolation of medical data in the cloud using hybrid cryptography," Journal of Information Security and Applications, vol. 73. Elsevier BV, p. 103412, Mar. 2023. doi: 10.1016/j.jisa.2022.103412.

[6] M. U. Bokhari, Q. M. Shallal, and Y. K. Tamandani, "Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning," IETE Journal of Research, vol. 65, no. 2. Informa UK Limited, pp. 227–235, Jan. 28, 2018. doi: 10.1080/03772063.2017.1419835.

[7] P. Garikapati, K. Balamurugan, and T. P. Latchoumi, "K-means partitioning approach to predict the error observations in small datasets," International Journal of Computer Aided Engineering and Technology, vol. 17, no. 4. Inderscience Publishers, 10.1504/ijcaet.2022.126601. p. 412, 2022. doi:

[8] B. Tadele Bekele, J. Bhaskaran, S. Dufera Tolcha, and M. Gelaw, "Simulation and experimental analysis of re-design the faulty position of the riser to minimize shrinkage porosity defect in sand cast sprocket gear," Materials Today: Proceedings, vol. 59. Elsevier BV, pp. 598–604, 2022. doi: 10.1016/j.matpr.2021.12.090.

[9] E. Altayef, F. Anayi, and M. Packianather, "A new enhancement of the k-NN algorithm by Using an optimization technique," 2022 2nd International Conference

on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, Apr. 28, 2022. doi: 10.1109/icacite53722.2022.9823537.

[10]M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover Internet of Things, vol. 1, no. 1. Springer Science and Business Media LLC, Feb. 24, 2021. doi: 10.1007/s43926-020-00001-4.

[11]Y. Alkali, I. Routray, and P. Whig, "Study of various methods for reliable, efficient and Secured IoT using Artificial Intelligence, SSRN Electronic Journal. Elsevier BV, 2022. doi: 10.2139/ssrn.4020364.

[12] P. Nirmala, S. Ramesh, M. Tamilselvi, G. Ramkumar, and G. Anitha, "An Artificial Intelligence enabled Smart Industrial Automation System based on Internet of Things Assistance," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). IEEE, Jan. 28, 2022. doi: 10.1109/accai53970.2022.9752651.

[13]S. D. Putra, A. D. W. Sumari, A. S. Ahmad, S. Sutikno, and Y. Kurniawan, "Cognitive Artificial Intelligence Countermeasure for Enhancing the Security of Big Data Hardware from Power Analysis Attack," Advanced Sciences and Technologies for Security Applications. Springer International Publishing, pp. 61–86, 2020. doi: 10.1007/978-3-030-35642-2_4.

[14] H. Sharma and N. Kumar, "Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey," Physical Communication, vol. 57. Elsevier BV, p. 102002, Apr. 2023. doi: 10.1016/j.phycom.2023.102002.