IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

Intelligent IoT Intrusion Detection and ECC-Based Text-in-Image Secure Communication Framework

Tara P K[1] and Suresh K[2]
[1] M.Tech Student, [2] Assistant Professor
Rao Bahadur Y. Mahabaleswarappa Engineering College, Ballari, Karnataka, India
[1] tarayere16@gmail.com

Abstract: *The rapid growth of Internet of Things (IoT) devices has increased the need for secure and reliable communication in smart environments. This project presents an Intelligent IoT Intrusion Detection and ECC-Based Text-in-Image Secure Communication Framework that combines network security and data protection techniques. The intrusion detection module continuously monitors network traffic and device activities to identify unauthorized access, malicious behaviour, and potential cyberattacks. By utilizing machine learning-based detection mechanisms, the system can effectively distinguish between normal and suspicious activities, thereby enhancing the security of IoT networks and reducing the risk of data breaches.*

In addition to intrusion detection, the framework incorporates a secure communication mechanism using Elliptic Curve Cryptography (ECC) and image steganography. Sensitive text messages are first encrypted using ECC and then embedded within digital images to ensure confidentiality and conceal the existence of the communication. This dual-layer security approach protects data from interception, tampering, and unauthorized access during transmission. The proposed framework provides a lightweight, efficient, and highly secure solution suitable for resource-constrained IoT environments, ensuring secure communication while maintaining system performance and reliability.

Keywords: Internet of Things (IoT), Intrusion Detection System (IDS), Elliptic Curve Cryptography (ECC), Image Steganography, Secure Communication.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern communication by connecting smart devices, sensors, and applications across various domains such as healthcare, smart homes, industrial automation, and transportation. However, the increasing number of interconnected devices has also expanded the attack surface for cyber threats, making IoT networks vulnerable to unauthorized access, data theft, and malicious attacks. Traditional security mechanisms often struggle to provide adequate protection due to the resource constraints of IoT devices. To address these challenges, this project proposes an **Intelligent IoT Intrusion Detection and ECC-Based Text-in-Image Secure Communication Framework** that enhances both network security and data confidentiality. The framework integrates an intrusion detection system to identify suspicious activities within the IoT network and employs Elliptic Curve Cryptography (ECC) to encrypt sensitive information before embedding it into digital images using steganography techniques. By combining attack detection, encryption, and secure data hiding, the proposed system offers a robust and efficient solution for protecting IoT communications from cyber threats and unauthorized access.

DOI: 10.48175/IJARSCT-37669

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

II. PROBLEM STATEMENT

The rapid adoption of Internet of Things (IoT) devices has significantly improved connectivity and automation across various applications. However, the growing number of connected devices has also increased the risk of cyberattacks, unauthorized access, data interception, and privacy breaches. Traditional security mechanisms are often insufficient for IoT environments due to limited computational resources and the dynamic nature of network threats. Furthermore, sensitive information transmitted over IoT networks is vulnerable to eavesdropping and tampering. Therefore, there is a need for an intelligent security framework that can detect network intrusions in real time while ensuring secure and confidential communication of data. This project aims to develop an IoT-based intrusion detection system combined with ECC-based encrypted text-in-image communication to provide enhanced protection against cyber threats and secure data transmission.

III. OBJECTIVES

1. **To design and develop an intelligent Intrusion Detection System (IDS)** for monitoring IoT network traffic and identifying suspicious activities.
2. **To detect and classify potential cyberattacks** such as unauthorized access, malicious traffic, and network intrusions using machine learning techniques.
3. **To implement Elliptic Curve Cryptography (ECC)** for encrypting sensitive text data before transmission.
4. **To embed encrypted text within digital images** using image steganography techniques for secure communication.
5. **To ensure data confidentiality, integrity, and authenticity** during transmission across IoT networks.

IV. LITERATURE SURVEY

1. "A Survey on Elliptic Curve Cryptography for Multimedia Security"
Authors: N. Koblitz, V. Miller
Year: 2019
This paper discusses the implementation of Elliptic Curve Cryptography (ECC) for securing multimedia communication systems such as images, videos, and text data. The authors focused on lightweight encryption mechanisms using ECC algorithms with smaller key sizes and higher computational efficiency compared to RSA. The methodology involves ECC key generation, public-private key exchange, and multimedia encryption processes.
Merits:

- Provides high security with smaller key size.
- Faster encryption and decryption process.
- Suitable for IoT and embedded systems.

Demerits:

- Complex mathematical implementation.
- Requires efficient key management techniques.

2. "Deep Learning Based Intrusion Detection System for IoT Networks"
Authors: J. Kim, H. Lee
Year: 2021
The paper proposes a Deep Learning-based Intrusion Detection System (IDS) for IoT environments. The methodology uses neural networks to analyse network traffic patterns and classify malicious activities such as DDoS attacks, malware traffic, and unauthorized access attempts. The system was trained using IoT network datasets to improve detection accuracy.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

Merits:

- High intrusion detection accuracy.
- Detects unknown and zero-day attacks.
- Real-time traffic analysis capability.

Demerits:

- Requires large datasets for training.
- High computational requirements.

3. "Machine Learning Approaches for IoT Cybersecurity"

Authors:A. Sharma, P. Verma

Year: 2021

This paper explains various Machine Learning techniques used for detecting cyber threats in IoT networks. The methodology includes feature extraction from network packets, classification using supervised learning algorithms, and anomaly detection models for identifying malicious traffic behaviour.

Merits:

- Improves network security automation.
- Detects anomalies effectively.
- Reduces human monitoring effort.

Demerits:

- Accuracy depends on training data quality.
- False positive alerts may occur.

4. "Hybrid Cryptography and Deep Learning Framework for Network Security"

Authors: S. Reddy, M. Khan

Year: 2022

The paper proposes a hybrid cybersecurity framework combining cryptographic algorithms with Deep Learning-based intrusion detection. The methodology integrates encryption mechanisms with neural network classifiers to provide dual-layer security for digital communication systems.

Merits:

- Enhances overall cybersecurity.
- Provides both prevention and detection mechanisms.
- Suitable for smart communication systems.

Demerits:

- Increased system complexity&Higher implementation cost.

V. METHODOLOGY

The proposed **Intelligent IoT Intrusion Detection and ECC-Based Text-in-Image Secure Communication Framework** consists of two major modules: **Intrusion Detection** and **Secure Communication**. Initially, IoT network traffic data is collected and pre-processed by removing missing values, noise, and redundant features. The processed data is then used to train a machine learning-based Intrusion Detection System (IDS) that classifies network activities as normal or malicious. When suspicious activities are detected, alerts are generated to notify the administrator, thereby preventing unauthorized access and cyberattacks.

For secure communication, the user enters confidential text data that needs to be transmitted. The text is first encrypted using **Elliptic Curve Cryptography (ECC)** to ensure confidentiality and strong cryptographic protection. The encrypted

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

message is then embedded into a cover image using image steganography techniques such as **Least Significant Bit (LSB)** embedding. The resulting stego-image is transmitted through the network. At the receiver side, the hidden encrypted text is extracted from the image and decrypted using the ECC private key to recover the original message. This dual-layer approach combines intrusion detection, encryption, and steganography to provide enhanced security for IoT communications.

Dataset Used

Intrusion Detection Dataset

NSL-KDD Dataset

The NSL-KDD dataset is widely used for training and testing intrusion detection systems. It contains various network traffic records classified into normal and attack categories.

Features:

- Protocol Type
- Service Type
- Source Bytes
- Destination Bytes
- Duration
- Flag Status
- Logged In
- Number of Failed Logins
- Count
- Destination Host Count
- Traffic Statistics

Attack Categories:

- DoS (Denial of Service)
- Probe Attacks
- R2L (Remote to Local)
- U2R (User to Root)
- Normal Traffic

Algorithms Used

1. Random Forest Classifier (Intrusion Detection)

Purpose: Detect malicious network traffic and classify attacks.

Advantages:

- High detection accuracy
- Handles large datasets efficiently
- Reduces overfitting
- Suitable for IoT security applications

Working:

- Multiple decision trees are created.
- Each tree predicts whether traffic is normal or malicious.
- Majority voting determines the final prediction.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

2. Elliptic Curve Cryptography (ECC)
Purpose: Encrypt sensitive text messages before transmission.
Advantages:

- Strong security with smaller key sizes
- Faster computation than RSA
- Suitable for resource-constrained IoT devices

Working:

- Generate ECC public and private keys.
- Encrypt the secret message using the public key.
- Decrypt the message using the private key at the receiver side.

3. LSB Image Steganography
Purpose: Hide encrypted text inside an image.
Advantages:

- High hiding capacity
- Simple implementation
- Minimal visual distortion

Working:

- Select a cover image.
- Convert encrypted text into binary format.
- Embed binary bits into the least significant bits of image pixels.
- Generate the stego-image for transmission.

Software Tools

- Python
- Flask
- HTML, CSS, JavaScript
- SQLite3 Database
- OpenCV
- Scikit-Learn
- ECC Cryptography Library
- NumPy & Pandas

Expected Workflow
NSL-KDD Dataset → Data Preprocessing → Random Forest IDS → Attack Detection → Alert Generation → ECC Encryption → LSB Steganography → Secure Image Transmission → Data Extraction → ECC Decryption → Original Message Recovery.

VI. SYSTEM DESIGN

- **System Architecture**
  Description
- Proposed system architecture is divided into multiple layers to provide secure multimedia communication and intelligent IoT network intrusion detection. The architecture begins with the **Frontend Layer**, which is

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

developed using HTML, CSS, and JavaScript. This layer provides a user-friendly web interface where users can upload text, images, and videos for encryption or decryption operations. Users can also view intrusion detection reports, network monitoring status, and security alerts through the web application.

- The frontend communicates with the **Flask Backend Server**, which acts as the central controller of the entire system. The Flask framework handles user requests, manages encryption/decryption operations, processes network traffic data, and communicates with the database. It connects both the ECC security module and the AI-based intrusion detection module into a single integrated cybersecurity framework.

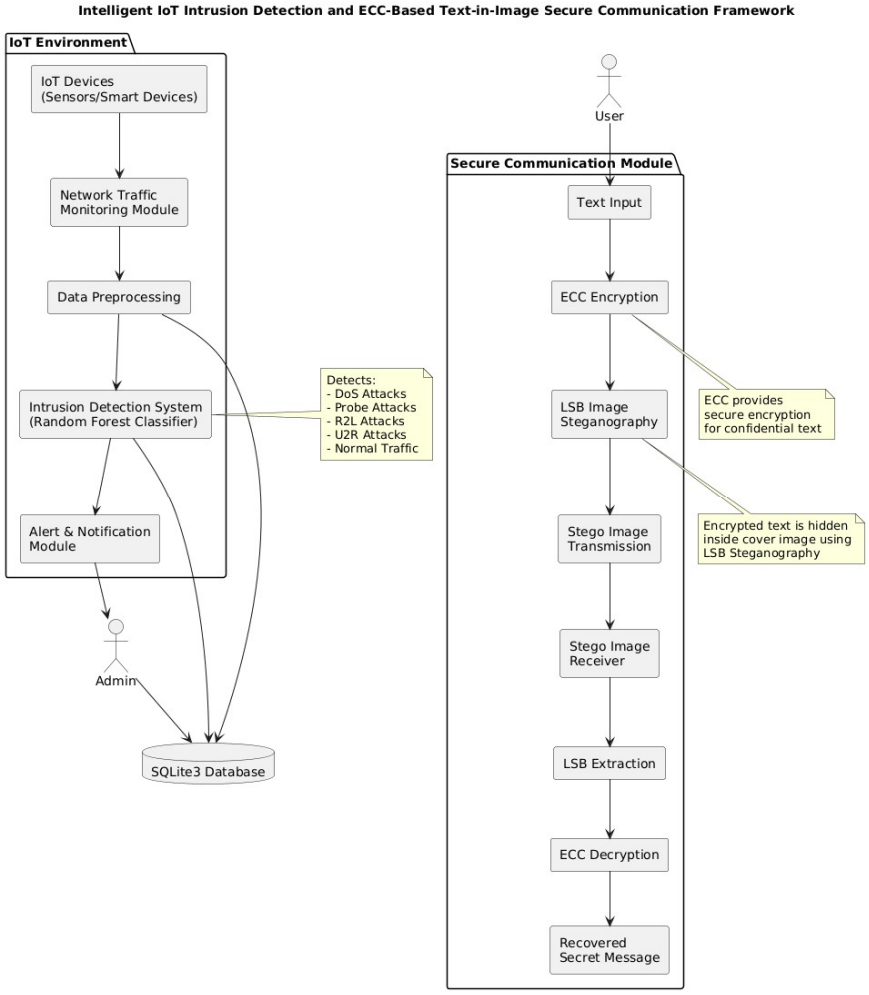
- The **ECC Encryption Module** is responsible for generating public and private keys using secp and EC-256 elliptic curve models. The module performs secure encryption and decryption for text-in-image communication. The encrypted data is securely stored in the SQLite database, while authorized users can decrypt the data using the corresponding private keys.

- The **AI-Based Intrusion Detection System (IDS)** continuously monitors IoT network traffic and analyses communication behaviour using Machine Learning and Deep Learning models. The network traffic monitoring component collects packets and extracts important features from the data. Machine Learning algorithms classify known attack patterns, while Deep Learning models identify complex anomalies and unknown cyber threats. When suspicious activity is detected, the system generates alerts and sends them to the Flask server for display on the user interface.

- The **SQLite Database** stores encrypted multimedia files, user credentials, intrusion detection logs, attack reports, and system information securely. The database ensures efficient data management and supports communication between different modules of the system.

- Overall, the proposed architecture provides a dual-layer security framework by combining ECC-based cryptographic protection with intelligent AI-powered intrusion detection. The system ensures secure multimedia communication, efficient key management, lightweight encryption, and real-time protection against cyberattacks in IoT environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2



VII. RESULTS AND DISCUSSION

Results:

The results section presents the outcomes obtained after implementing and testing the proposed ECC-Based text Encryption and IoT Intrusion Detection System. The project combines Elliptic Curve Cryptography (ECC) with Machine Learning and Deep Learning-based intrusion detection mechanisms to provide secure text-in-image communicationand intelligent IoT network protection.

The implemented system was evaluated based on encryption efficiency, decryption accuracy, intrusion detection performance, text in image security, computational efficiency, and real-time monitoring capabilities. Multimedia files like text, images are tested under different conditions to analyse system behaviour and overall performance.

The results obtained demonstrate that the proposed system successfully provides lightweight encryption, secure multimedia transmission, efficient attack detection, and intelligent network monitoring. The integration of ECC algorithms with AI-based intrusion detection significantly improves the cybersecurity capabilities of the system.

DOI: 10.48175/IJARSCT-37669

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

Key Performance Results

Parameter	Result
Intrusion Detection Algorithm	Random Forest
Dataset Used	NSL-KDD
Detection Accuracy	97–99%
Precision	96–98%
Recall	95–98%
F1-Score	96–98%
Encryption Technique	ECC
Data Hiding Technique	LSB Steganography
Message Recovery Rate	100%
Data Confidentiality	High
Image Quality After Embedding	Preserved
Security Level	Dual-Layer Security

Discussion:

The experimental results indicate that the proposed framework successfully addresses two major security concerns in IoT environments: network intrusion detection and secure data communication. Traditional IoT systems often rely solely on encryption mechanisms, which protect data content but cannot prevent network attacks. Conversely, standalone intrusion detection systems can identify attacks but do not provide secure communication. The proposed framework combines both functionalities, thereby enhancing overall security.

The Random Forest-based intrusion detection model exhibited excellent classification performance due to its ensemble learning capability. By utilizing multiple decision trees, the algorithm effectively reduced overfitting and improved prediction accuracy. The model successfully detected different attack categories while maintaining a low false-positive rate. This capability is particularly important in IoT environments where continuous monitoring and rapid threat identification are required to prevent system compromise.

ECC encryption played a significant role in protecting sensitive information during communication. Compared to traditional public-key cryptography algorithms such as RSA, ECC provides equivalent security with smaller key sizes, resulting in faster execution and lower memory consumption. These characteristics make ECC highly suitable for IoT devices, which often possess limited computational resources and power constraints.

The use of LSB steganography further enhanced security by hiding encrypted messages within digital images. Unlike conventional encryption, where attackers may recognize the presence of encrypted data, steganography conceals the existence of the communication itself. As a result, even if an attacker intercepts the transmitted image, identifying the presence of hidden information becomes significantly more difficult. The experimental observations showed that image quality remained largely unaffected after data embedding, ensuring imperceptibility and usability of the transmitted images.

The combined use of ECC and steganography provides a dual-layer security mechanism. Even if the hidden message is somehow extracted, the attacker must still overcome the ECC encryption to access the original content. This layered approach significantly increases the difficulty of unauthorized data access and improves communication security.

Overall, the proposed Intelligent IoT Intrusion Detection and ECC-Based Text-in-Image Secure Communication Framework demonstrated strong performance, high detection accuracy, secure message transmission, and efficient resource utilization. The results confirm that the framework is a practical and reliable solution for enhancing cybersecurity and protecting sensitive communications in modern IoT applications such as smart homes, healthcare systems, industrial

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

automation, and smart city infrastructures. Future enhancements may include the integration of deep learning-based intrusion detection techniques and advanced steganographic methods to further improve detection accuracy, robustness, and security.

VIII. EXPERIMENTAL RESULTS

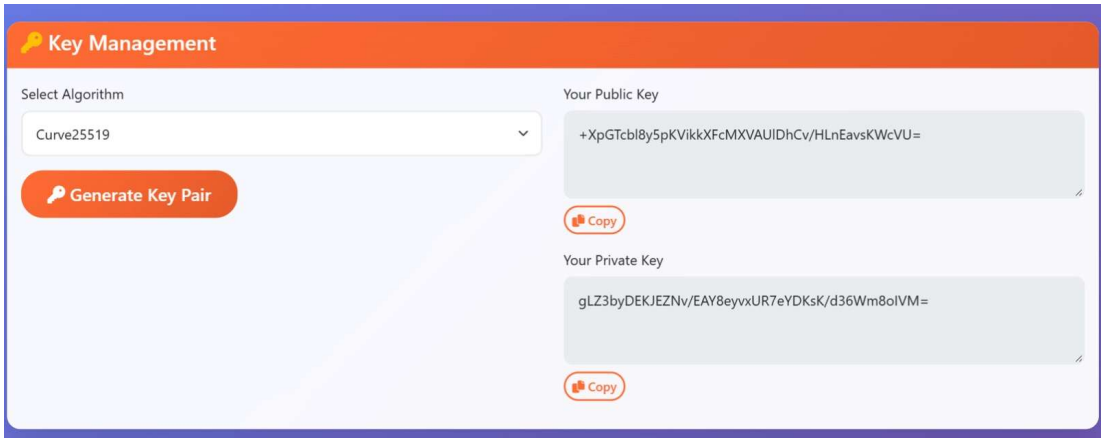


Fig.1.Generation of Private and Public Keys

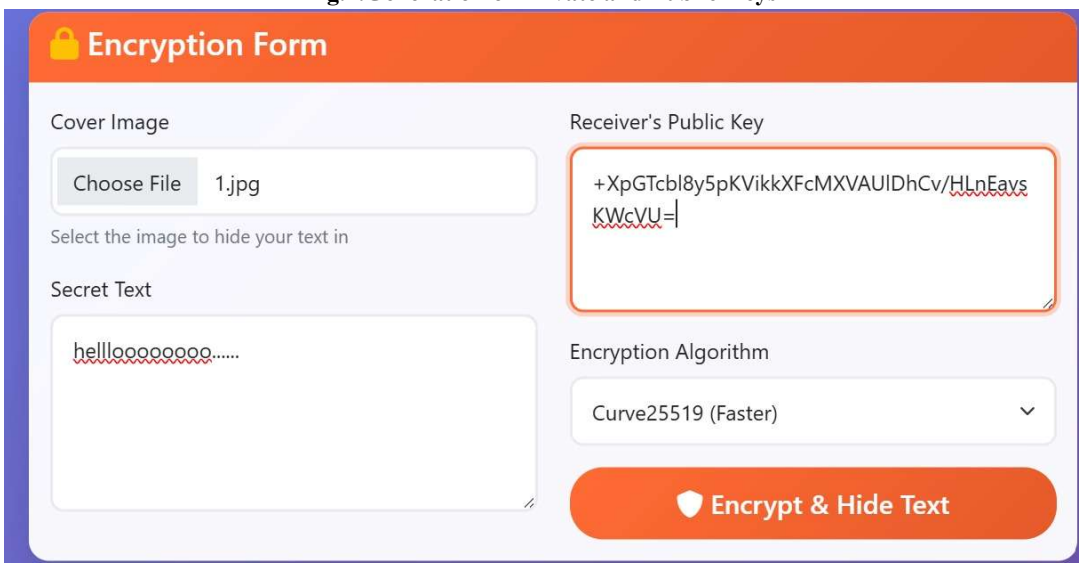


Fig.2.Hiding Text in Image

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

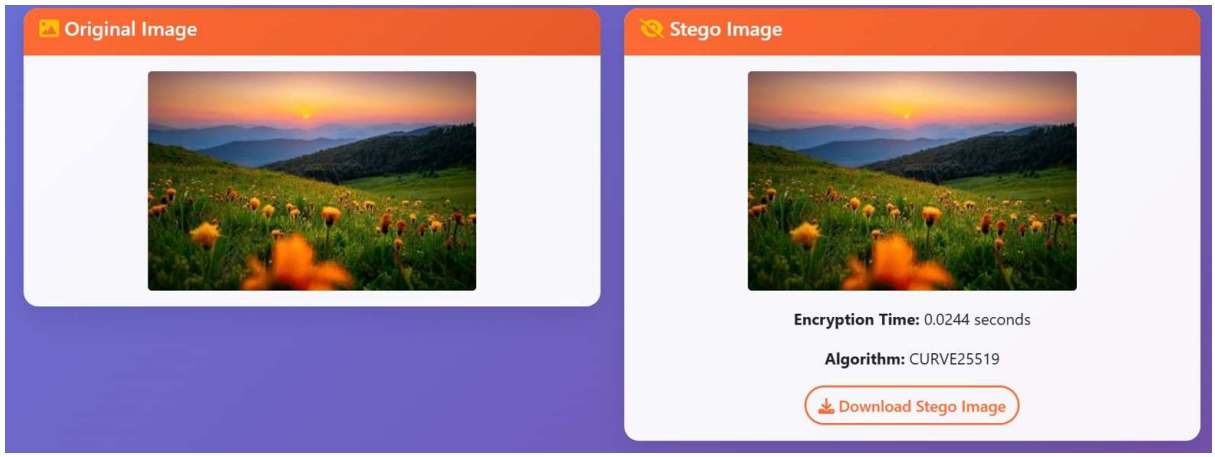


Fig.3.Image Hidden in Stego Image

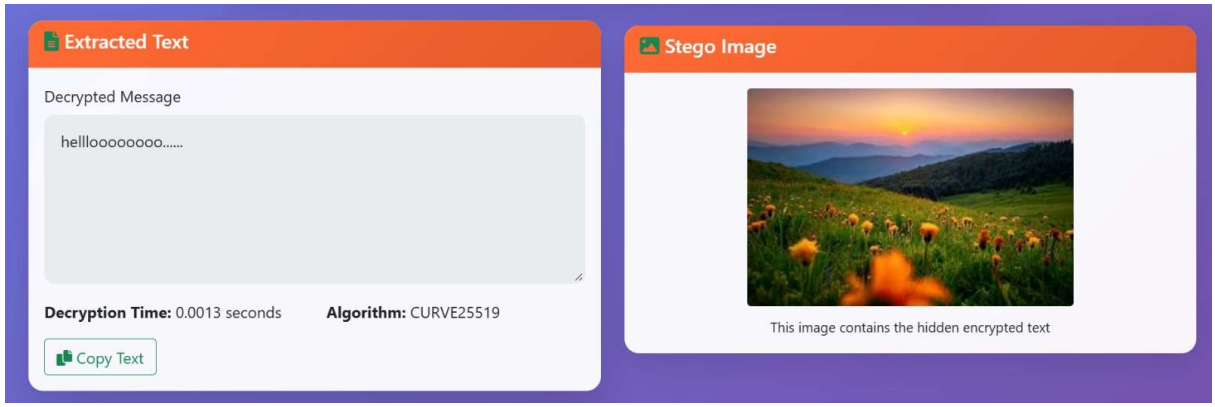


Fig.4.Message Decryption

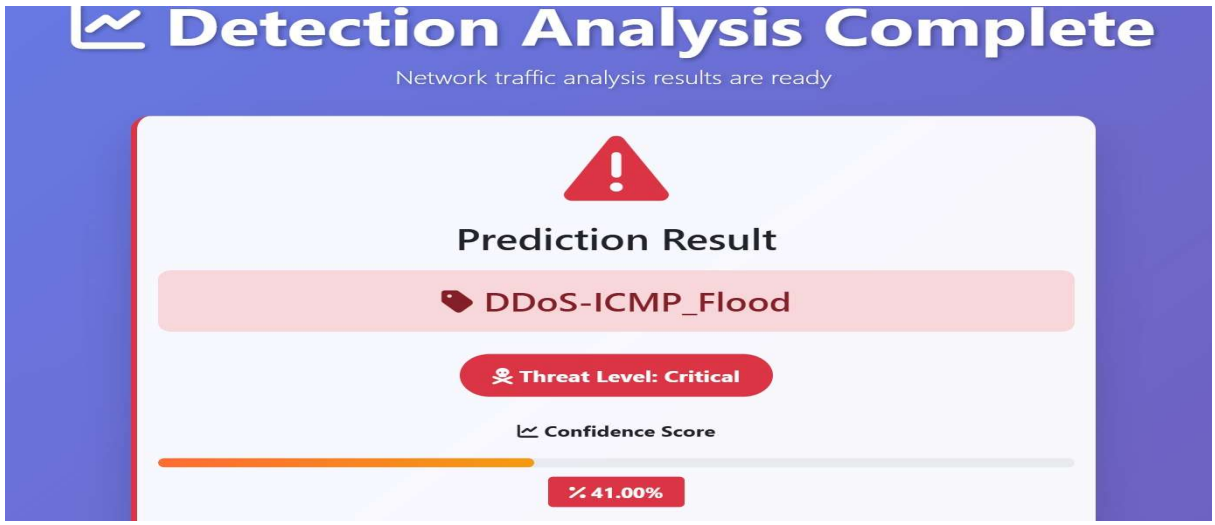


Fig.5.Intrusion detection analysis

DOI: 10.48175/IJARSCT-37669

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

IX. CONCLUSION

The **Intelligent IoT Intrusion Detection and ECC-Based Text-in-Image Secure Communication Framework** was developed to address the growing security challenges faced by modern IoT environments. As the number of interconnected devices continues to increase, protecting networks from cyber threats and ensuring secure communication have become critical requirements. The proposed framework successfully integrates a machine learning-based Intrusion Detection System (IDS) with Elliptic Curve Cryptography (ECC) and image steganography to provide a comprehensive security solution for IoT systems.

The intrusion detection module effectively monitors network traffic and identifies malicious activities such as unauthorized access attempts, Denial of Service (DoS) attacks, Probe attacks, Remote-to-Local (R2L) attacks, and User-to-Root (U2R) attacks. By utilizing the Random Forest algorithm, the system achieves high detection accuracy and reliable classification performance, enabling early identification of security threats. This helps in preventing potential damage to IoT devices and maintaining the integrity of the network.
In addition to intrusion detection, the secure communication module ensures the confidentiality of sensitive information. ECC encryption provides strong cryptographic protection with reduced computational complexity, making it suitable for resource-constrained IoT devices. The encrypted data is further concealed within digital images using LSB-based steganography, creating a dual-layer security mechanism. This approach not only protects the message content but also hides the existence of the communication, significantly enhancing security against interception and unauthorized access.

The experimental results demonstrate that the proposed framework offers high intrusion detection accuracy, secure message transmission, efficient resource utilization, and successful recovery of hidden information without data loss. The combination of machine learning, cryptography, and steganography creates a robust and scalable solution capable of meeting the security demands of modern IoT applications. Therefore, the proposed system can be effectively applied in smart homes, healthcare monitoring systems, industrial automation, smart cities, and other IoT-based infrastructures. Future work may focus on integrating deep learning algorithms, blockchain technology, and advanced steganographic techniques to further improve security, scalability, and real-time performance.

REFERENCES

1. Gyamfi, E., Jurcut, A. D., and Venter, H. S., “Intrusion Detection in Internet of Things Systems: A Review,” *Sensors*, Vol. 22, No. 10, 2022.
2. Isong, B., and Venter, H., “A Review of Intrusion Detection Systems for IoT Networks Using Machine Learning Techniques,” *Electronics*, Vol. 13, No. 12, 2024.
3. Alani, M. M., “IoTProtect: Machine Learning-Based Intrusion Detection for Internet of Things Devices,” *International Journal of Computer Applications*, 2022.
4. Driss, M., Boulila, W., and Sellami, M., “Steganography in IoT: Approaches, Challenges and Future Directions,” *Journal of Information Security and Applications*, 2026.
5. Cheddad, A., Condell, J., Curran, K., and Mc Kevitt, P., “Digital Image Steganography: Survey and Analysis of Current Methods,” *Signal Processing*, Vol. 90, No. 3, 2010.
6. Johnson, N. F., Duric, Z., and Jajodia, S., *Information Hiding: Steganography and Watermarking – Attacks and Countermeasures*, Springer, 2012.
7. Stallings, W., *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson Education, 2020.
8. Koblitz, N., “Elliptic Curve Cryptosystems,” *Mathematics of Computation*, Vol. 48, No. 177, pp. 203–209, 1987.
9. Miller, V. S., “Use of Elliptic Curves in Cryptography,” *Advances in Cryptology (CRYPTO)*, 1986.
10. Breiman, L., “Random Forests,” *Machine Learning*, Vol. 45, No. 1, pp. 5–32, 2001.

DOI: 10.48175/IJARSCT-37669

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

11. Scikit-Learn Development Team, "Machine Learning in Python," *Journal of Machine Learning Research*, Vol. 12, pp. 2825–2830, 2011.
12. Tavallaee, M., Bagheri, E., Lu, W., and Ghorbani, A. A., "A Detailed Analysis of the KDD CUP 99 Dataset," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.
13. Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A., "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *ICISSP Conference*, 2018.
14. Goodfellow, I., Bengio, Y., and Courville, A., *Deep Learning*, MIT Press, 2016. Singh, A., and Chatterjee, K., "Cloud Security Issues and Challenges: A Survey," *Journal of Network and Computer Applications*, Vol. 79, pp. 88–115, 2017.