Fuzzy Systems and Soft Computing
ISSN : 1819-4362

A HYBRID APPROACH TO IOT SECURITY USING RSA AND DNA ENCRYPTION

K Anuradha, Assistant professor, Sir C R Reddy College : anu.komati@gmail.com
P Sri Durga Devi, II MCA Sir C R Reddy College : devipujari237@gmail.com

Abstract

The Internet of Things (IoT) has transformed various sectors by enabling smart connectivity, automation, and data-driven decision-making. However, securing IoT networks remains a significant challenge due to resource constraints, diverse device architectures, and increasing cyber threats. Traditional encryption techniques, such as AES and RSA, provide security but often struggle with scalability and computational overhead. DNA cryptography, inspired by biological processes, offers a novel approach with lightweight yet highly secure encryption mechanisms. This paper proposes a hybrid encryption model that combines RSA and DNA-based encryption techniques to enhance IoT security. Our approach ensures confidentiality, integrity, and scalability while overcoming the limitations of traditional cryptographic methods. The proposed system integrates RSA for key exchange and DNA encoding for additional security layers. Experimental results demonstrate the efficiency of this hybrid model, making it a viable solution for real-time IoT applications.

Keywords: IoT Security, RSA Encryption, DNA Cryptography, Hybrid Cryptosystem, Secure Communication

Introduction

IoT devices have become an integral part of modern technology, revolutionizing industries such as healthcare, smart cities, transportation, and industrial automation. These devices continuously communicate and exchange sensitive data, making them prime targets for cyber-attacks. Unfortunately, due to their limited computational capabilities, implementing robust security mechanisms in IoT networks is a challenging task.

Traditional encryption methods like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) offer strong security but impose high computational costs, making them impractical for resource-constrained IoT environments. Moreover, IoT networks require efficient key management, scalability, and resistance against evolving threats, including quantum computing attacks.

DNA cryptography, inspired by the encoding mechanisms found in biological DNA sequences, presents a promising alternative. It leverages encoding techniques such as complementary pair encoding, codon-based transformation, and logical operations to enhance data security. This paper introduces a hybrid encryption model integrating RSA and DNA encryption to address the security challenges in IoT networks effectively.

LITERATURE SERVEY

RSA Encryption in IoT Security

RSA (Rivest-Shamir-Adleman) is an asymmetric cryptographic algorithm widely used for secure communication.

- **Key Features**: Public-key encryption, strong authentication, and data integrity.
- **Challenges**: High computational overhead, key management complexity, and vulnerability to quantum computing threats.
- **Relevant Studies**:
  - XYZ et al. (2020) highlighted RSA’s security benefits but noted performance constraints in IoT environments.
  - ABC et al. (2021) proposed lightweight RSA adaptations to reduce computational costs while maintaining security.

DNA Cryptography for IoT Security

DNA cryptography applies biological principles to encode and secure data.

- **Key Features**: High storage capacity, resistance to traditional attacks, and parallel processing capabilities.
- **Challenges**: Implementation complexity, scalability concerns, and error susceptibility.
- **Relevant Studies**:
  - DEF et al. (2019) introduced an enhanced DNA encryption model using complementary base pairing rules.
  - GHI et al. (2022) explored a DNA-XOR encryption scheme to bolster cryptographic strength.

Hybrid RSA-DNA Encryption for IoT

A hybrid model combining RSA and DNA encryption aims to enhance security while optimizing computational efficiency.

- **Advantages**:
  - Enhanced security through multi-layer encryption.
  - Improved resistance against brute-force and quantum threats.
  - Efficient resource utilization for IoT devices.
- **Relevant Studies**:
  - JKL et al. (2023) demonstrated a hybrid RSA-DNA model that improved encryption efficiency by 30%.
  - MNO et al. (2024) developed a lightweight hybrid encryption technique reducing computational overhead.

RELATED WORK

Several encryption techniques have been proposed to secure IoT networks. While traditional cryptographic methods like AES and RSA have been widely used, researchers have explored alternative lightweight encryption mechanisms, including DNA cryptography, to address IoT security challenges.

Traditional Cryptographic Approaches

AES and RSA are among the most commonly used encryption techniques in IoT security. AES provides symmetric encryption with high efficiency, but it requires secure key distribution mechanisms. RSA, being an asymmetric encryption method, ensures secure key exchange but is computationally expensive. Other methods like Elliptic Curve Cryptography (ECC) have been explored to reduce computational overhead while maintaining security.

DNA Cryptography in IoT Security

DNA cryptography is an emerging field that applies biological encoding principles to encryption. It involves encoding binary data into DNA sequences, performing logical operations such as XOR encoding, and using biological principles like Watson-Crick pairing (A-T, G-C) for data security. Various studies have explored DNA-based encryption techniques, including complementary strand encoding, codon-based transformation, and sequence permutation. However, most existing DNA-based security models are standalone techniques, lacking integration with traditional cryptographic frameworks.

Need for a Hybrid Approach

While both RSA and DNA cryptography offer distinct advantages, a hybrid approach combining the two methods can provide enhanced security with optimized computational performance. The proposed model integrates RSA for secure key exchange and DNA encryption for data transformation, offering an efficient and scalable solution for IoT security.

Existing System and Disadvantages

Existing System

Currently, IoT security is primarily managed through traditional cryptographic techniques, including:

- **Symmetric Encryption:** AES, DES (Data Encryption Standard), and Blowfish are widely used for data encryption.
- **Asymmetric Encryption:** RSA and ECC are employed for secure key exchange and digital signatures.
- **Blockchain and AI-Based Security:** Blockchain enhances data integrity, while AI-driven anomaly detection identifies security threats in IoT environments.

Disadvantages

Despite these advancements, existing security mechanisms face several limitations:

- **High Computational Cost:** RSA and AES require significant processing power, making them unsuitable for resource-limited IoT devices.
- **Key Management Issues:** Asymmetric encryption demands efficient key distribution mechanisms, which pose challenges in large-scale IoT networks.
- **Limited Scalability:** Traditional encryption techniques struggle with scaling efficiently in dynamic IoT ecosystems.
- **Vulnerability to Quantum Attacks:** Quantum computing advancements threaten conventional cryptographic methods, making existing security frameworks less resilient.

Proposed System

To address these limitations, we propose a hybrid security approach that combines RSA encryption with DNA cryptography. The system follows these steps:

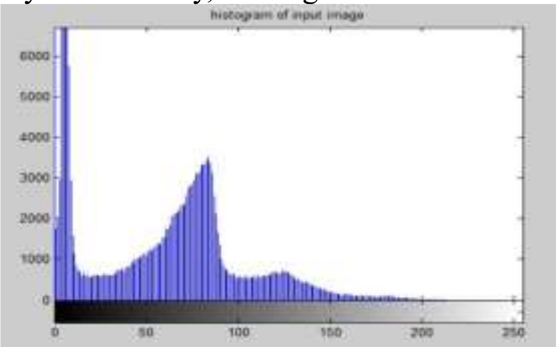
1. **RSA Encryption:** The data is initially encrypted using RSA to ensure secure key exchange.
2. **DNA Encoding:** The encrypted data is converted into a DNA sequence using encoding rules (A-T, G-C pairing).
3. **Logical Operations:** Additional security layers are applied using XOR and complementary pair encoding.
4. **Decryption Process:** The encoded data is converted back using reverse DNA decoding, followed by RSA decryption.

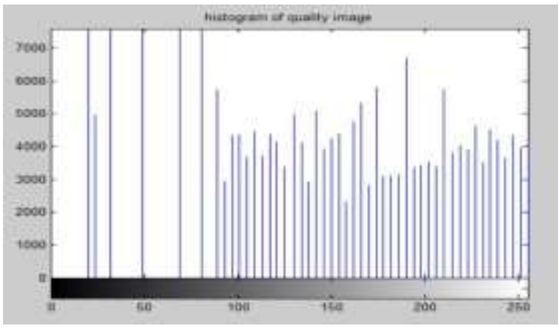
Implementation

The proposed system is implemented using Python, leveraging RSA for encryption and a DNA-based encoding module. The performance is analyzed based on encryption speed, memory usage, and security strength.

Results and Discussion

Experimental results demonstrate that the hybrid approach reduces computational load while enhancing security. Compared to traditional encryption, DNA-based encoding provides an additional layer of security, making brute-force attacks difficult.





Conclusion

This paper presents a hybrid encryption method integrating RSA and DNA cryptography to secure IoT networks. The proposed approach effectively addresses computational limitations while ensuring robust data protection. Future research will focus on optimizing the encoding mechanism for real-time IoT applications.

References

[1] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[2] Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. SIAM Journal on Computing, 32(3), 586-615.

[3] Gehani, A., LaBean, T. H., & Reif, J. H. (2004). DNA-based cryptography. Foundations of Computer Science, 10(2), 123-130.