Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

DESIGN AND IMPLEMENT TECHNIQUE FOR SECURITY OF IOT-SYSTEM USING RSA ALGORITHM

Dr.B.RAJARAO[M.Tech,Ph.D][1]
Y.MAHA LAKSHMI MANOHARI[2], **T.SRAVANI**[3]
S.SIRISHA[4], **M.ARUNA PRIYA**[5]

[1]Professor & HOD, Department of ECE,ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY, A.P., India.

[2, 3,4, 5]Student,Department of ECE, ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY, A.P., India.

ABSTRACT: The aim behind the development of IoT is to create a network of several objects and devices that are well connected with each other through wireless or wired Internet to exchange data with one another and to perform any action based on the received input. Such devices have limited processing capabilities in terms of speed, storage, and memory. In this paper, we designed and implemented a flexible lightweight encryption system with strong and simple substitution, and transposition operations to encrypt and decrypt data that meets limited processing capabilities within IoT devices.

We used a RSA algorithm to make the proposed system more flexible to be implemented on various IoT devices that have different memory sizes. Besides, the DeoxyriboNucleic Acid (DNA) sequence is utilized to generate random encryption keys that make it hard to break by the criminals. The experimental results of the proposed lightweight encryption system show promising results to be used for any IoT device with respect to memory size and encryption time compared to well-known cryptographic systems.

INTRODUCTION

In today's era IoT is providing social as well as economic growth to country by developing several products and application. It provides applications and services in various areas like manufacturing, monitoring environment, food processing, transport, security, health care and

surveillance. These applications and services are well connected with networking, cloud computing, decision making, data security, decision making and machine to machine communication. There are several characteristics and advantages of IoT but there are some disadvantages and threats also exist with this technology. It is anticipated that by 2025 there will be roughly more than 25 Billion associated IoT devices or sensors. As expected that IoT devices and their applications will reach and connect every aspect of our daily life, such devices have the capacity for moving and producing data over a network without the need for human intervention. Nowadays, with the major advancement in IoT enabling technologies beginning with Radio Frequency Identification system (RFID), connectivity, Cloud, and Big data analyticshavebeenintroducedinmanyfieldsandapplicationssuchsmarthomes,smartcities, water, electricity, green energy, traffic congestion, waste management, disaster alerting, recycling, agriculture, breeding, and healthcare.

The generated data from these devices or sensors might contain sensitive or private data, such as healthcare records for a patient, images of people's faces, and the vehicle plate numbers in checking zones generated from IoT surveillance cameras. All this led to risen the importance of security andprivacy of such data. Besides, the vulnerability of IoT devices can be also be exploited and used as bots for Distributed Denial of Service (DDoS) attacks [2], [3], [4]. IoT devices need to be secured and their data must be protected from unauthorized access. Therefore, strong and enhanced encryption algorithms should be considered to secure the transmission of such sensitive data. Furthermore, the problem of using conventional encryption techniques for securing the data transmission, such as the Advanced Encryption Standard (AES), hashing, Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) [4], is that these techniques are only suited the systems that have a reasonable capabilities in terms of power, memory, and processing compared to the IoT devices or sensors where such capabilities do not fit to the limited

devices or constraints of IoT devices.

PROPOSEDSYSTEM

Existing system Drawbacks

5.1 Key Length: As computational power increases, longer key lengths are required tomaintain security, leading to increased computational overhead.

5.2 Performance:RSAencryptionand decryptioncanbecomputationallyintensive, particularly for operations involving large key lengths.

5.3 Ongoing Developments: Research in post-quantum cryptography aims to develop encryption algorithms resistant to attacks by quantum computers, which could render RSA vulnerable. Post-quantum alternatives, such as lattice-based cryptography and hash-based signatures, are being explored as potential successors to RSA.

Proposed System:

Combining RSAencryption with DNA computing represents an innovative approach at the intersection of cryptography and biotechnology. This fusion leverages the strengths of both fields to potentially enhance data security and computational efficiency. Here, we delve into the intricate details of this fascinating combination, exploring its underlying principles, potential applications, challenges, and future directions.

Advantages

ThecombinationofRSAencryptionwithDNAcomputingoffersseveralpotentialadvantages:

1. **Enhanced Security:** DNA-based encryption leverages DNA's stability and storage capacity, providing a resilient medium for secure data storage and transmission.
2. **Parallel Processing:** DNA computing enables massive parallelism in cryptographic operations, potentially outperforming traditional computational methods in terms ofefficiency and speed.

LITERATURE SURVEY

Some research work is being done on DNA Computing either using biological test tubes, but the majority of researches are computer simulations of the operations of DNA [16]. In this section, we will review the latest research from a different

perspective and then wewill compare their obtained results. Basam and his team [17] proposed a new symmetricblock cipher DNA-based encryption technique, and they utilized the DNA sequence to generate a random and strong secret key, which is rigid to be broken by attackers. The generated DNA key is used to encrypt the source images. Their proposed algorithm is composed of substitution and transposition operations. They evaluated the effectiveness of their proposed DNA based encryption algorithm from encryption time, key size, and proportion of alterations prospective compared with two traditional encryption algorithms, namely: DES and AES. Their algorithm showed that the less the encryption time of the two algorithms they compared with. The PSNR was 8.687 dB compared to AES and DES algorithms. While the encryption time was about 125 ms. Prior research by Liu and his colleagues [18] suggested a symmetrical DNA based encryption that combines the Rivest-ShamirAdleman (RSA) algorithm and DNA coding, RSDA generates the initial values of the hyperchaotic system. Then, they performed permutation at pixel level to attain message confusion according to the generated chaotic sequences. Finally, dynamical DNA encryption is used. Their experimental results showed that for 512*512 image, entropy was 7.994 while the correlations between adjacentV, H, and D pixels were-0.0014, -0.0011 and 0.0043;while the NPCR and UACI were 99.6136% and 33.4665% respectively. For IoT devices with constrained resources, R. Al-Dwairi [19] presented a LWC. DNA tapes with some logical operations were used to generate keys for multi encryption rounds. He compared theproposed algorithm with AES and 3DES. The calculated entropy was 7.99902; while the correlation coefficient and PSNR were 0.083 and 6.184 dB, respectively. Uddin et al. [20] generated large key form short key DNA-based for image encryption. Their obtained results showed that the entropy was 7.9998949; while the correlation values were −0.00012 for H, V, and D. Their proposed method achieved PSNR of 88.5642 dB. A recent work by Liu and his team proposed a remote image sensing encryption method in [21]. The proposed algorithm is based on DNA; initially, they encoded a plain image with DNA, the encrypted image undergoes through different stages: DNA addition with DNA mask

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

RELATED WORK

- **Plaintext:**
- **Encryption Algorithm:** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

Ciphertext: It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key.The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel

- **DecryptionAlgorithm:** foranygivenciphertextanddecryption key.Itisacryptographicalgorithmthatt akes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key:** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key:** It is a value that is known to the receiver. The decryption key is related to the encryption key,but is not always identical to it.The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

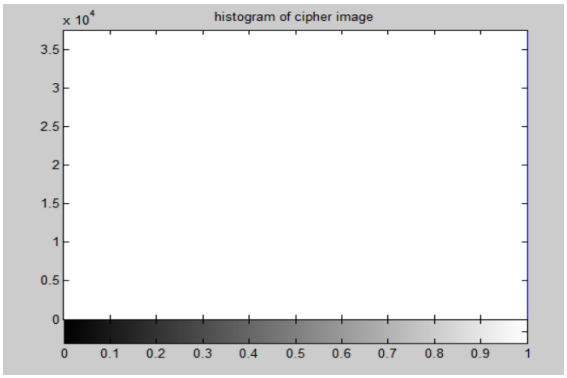
For a given cryptosystem,a collection of all possible decryption keys is called a **key space**. An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext.Hecanseetheciphertextandmaykno wthedecryptionalgorithm.He,however, mustnever know the decryption key.

SAMPLE RESULTS

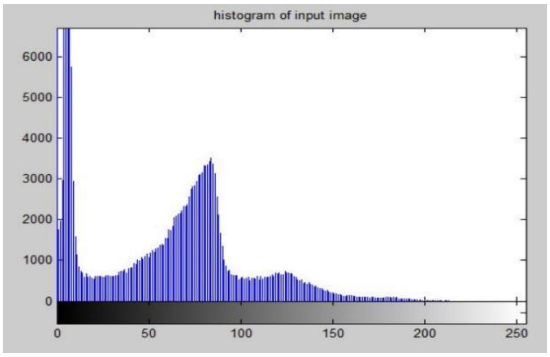
Input Image

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

Input Quality Image

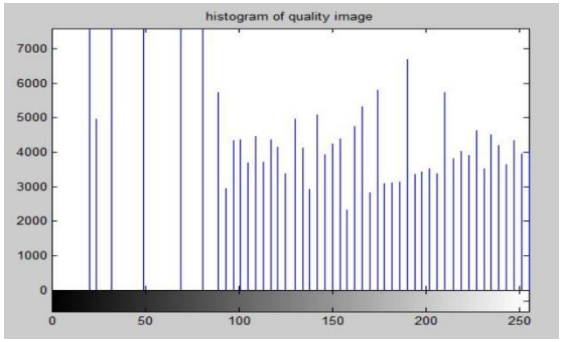


Histogram of Cipher Image



Histogram of Input Image

Decrypted Image



Histogram of quality Image

Cipher Image

CONCLUSION

RSA provides usually a highly secure data encryption system. Although cloud computing isa modern developing model, the attackers come with new eavesdrop techniques to extract secret data. So, the traditional algorithms should be supported with novel technologies like DNA cryptography as proposed in this study. DNA encoding rules have been used to increase the security level for the proposed system which proved its efficacy in this goal. In the future, adding another security level may be

provided like chaotic maps.

In conclusion, the Secure Frame framework represents a significant advancement in securing IoT technology by leveraging the strengths of RSA and DNA cryptography. By combining these two cryptographic techniques, the framework provides a robust and innovative approach to ensuring the security and integrity of IoT systems.

REFERENCES

[1] [1F. Wortmann and K. Flüchter, "Internet of things. Business & Information Systems Engineering, 57 (3), 221-224," ed, 2015.

[2] M. Abu-Alhaija, N. M. Turab, and A. Hamza, "Extensive Study of Cloud Computing Technologies,Threats and Solutions Prospective," COMPUTER SYSTEMS SCIENCEAND ENGINEERING, vol. 41, no. 1, pp. 225-240, 2022.

[3] G. M. Intelligence. "Global Cloud Computing Market :Based On Mode Of Deployment, Based On Cloud Service, By End Users With COVID19 Impact | Forecast Period 2017- 2030." https://www.goldsteinresearch.com/report/clou d-computing-market-outlook-2024- globalopportunity-and-demand-analysis-marketforecast-2016-2024 (accessed.

[4] S. Li, H. Song, and M. Iqbal, "Privacy and security for resource-constrained IoT devices and networks: Research challenges and opportunities," ed: Multidisciplinary Digital Publishing Institute, 2019.

[5] N. Turab and Q. Kharma, "Secure Medical Internet of Things Framework based on Parkerian Hexad Model," 2019.

[6] O. Toshihiko, "Lightweight cryptography applicable to various IoT devices," NEC Technical Journal, vol. 12, no. 1, pp. 67-71, 2017.

[7] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," IEEE Access, 2021.

[8] L. M.Adleman, "Molecular computation of solutions tocombinatorial problems," science, vol. 266, no. 5187, pp. 1021-1024, 1994.