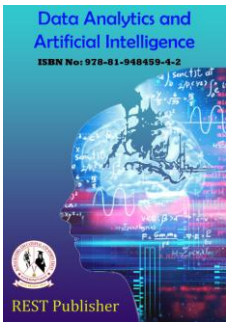
Data Analytics and Artificial Intelligence

Vol: 3(1), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/2/5



Medical Data Security in IOT Using DNA Cryptography and Insertion Method

E. Vidhya, R. Kiruba Kumari

Padmavani Arts and Science College for Women, Salem, Tamilnadu, India.

*Corresponding Author Email: vidhya11tamilarasi@gmail.com

Abstract. *The Internet of Things (IOT) system is a network system that communicates with other devices and systems via the web by using any one of the sensors, devices, applications, and other tools. To prevent unauthorized data transmission access, these systems and networks should include a suitable cryptography mechanism. The security of the shared resources on the data communication network is regarded as one of the key challenges. In this paper, the proposed scheme consists of two parts: (i) generating a key using an array of prime numbers based on the RSA algorithm, and (ii) devising a secure communication scheme based on DNA cryptography and Insertion Method. DNA cryptography is a cryptographic technique that uses DNA sequences to encode and decode source data using biological processes. It is an innovative way to protect data from hackers using DNA. The proposed scheme's security analysis shows that it is secure against the relevant threat models and provides a higher level of protection than previous related studies in the literature.*

Keywords: *IOT security, DNA encryption and decryption, Medical Data, Insertion Method.*

1. INTRODUCTION

The Internet of Things (IOT) is a new paradigm for modern, pervasive wireless communications that connects a wide range of physical devices to collect and exchange data via the Internet. Smart sensors, wearable or implantable health devices, and medical instruments that can remotely monitor a patient's health comprise a healthcare IoT network. Patient security and privacy are two major areas of concern in the healthcare IoT. Remote health care provider (end-user) authentication and authorization, as well as end-to-end data protection, are critical requirements in this regard to prevent eavesdropping on sensitive medical data or malicious task triggering [1]. Because humans are directly involved in healthcare IOT applications, reliable and secure data communication between healthcare sensors, actuators, patients, and careers is essential. Cryptography is defined as the technique of using functionality and arithmetic to store and transmit information in a programming code and to ensure data integrity so that only the intended recipient can peruse and translate the message. Due to resource constraints, security level requirements, and system architecture, cutting-edge security and protection mechanisms, such as existing cryptographic solutions, secure protocols, and privacy assurance, cannot be re-used in healthcare IOT systems [2]. To mitigate the above-mentioned risks, huge network protection infrastructures for short-range and long-range information exchange are required. Unlike symmetric encryption, which use the same secret key to encrypt and decrypt sensitive data, asymmetric cryptographic algorithms, also known as public-key cryptography or public-key encryption, encrypt and decrypt sensitive information sent to and received from senders and recipients utilizing mathematically linked public- and private-key pairs. The exclusion of a secret channel for the exchange of the public key is a significant advantage of asymmetric encryption methods over symmetric encryption. The receiver only needs to be assured of the public key's authenticity. Prime numbers are widely used in restricted environments for asymmetric cryptography key generation due to their greatness in generating a powerful encryption mechanism with small key sizes. Prime numbers boost device performance while lowering power consumption, making them ideal for a wide range of applications, including healthcare IOT. Deoxyribonucleic acid (DNA) cryptography, on the other hand, is a technique for hiding data in terms of DNA sequence. The cryptographic technique converts each letter of the alphabet into a different combination of the four bases that make up the genetic code [4, 5]. DNA cryptography, which is based on DNA information technology ideas, is a rapidly developing technology. Aside from their huge parallel processing capacity, DNA molecules have a huge storage capacity. A gram of DNA molecules contains 1021 DNA bases, or nearly 108 terabytes [6]. As a result, it is possible to conclude that a few grams of DNA can hold all of the world's largest data sets [7]. This article suggests a security scheme for medical IOT systems. This work

makes two major contributions. First, researchers will discuss with us comprehensive security solutions for medical systems. Researcher's use [19, 20, 5] DNA cryptography and prime number and Insertion Method techniques in this regard. Second, researchers examine the security characteristics of the proposed scheme. The scheme's security analysis demonstrates that it is secure against the relevant threat models and provides a higher level of security than previous related work in the literature.

2. RELATED WORK

To improve key generation, Roy et al. [8] devised a method based on DNA synthesis. This system optimises the encryption and decryption processes. To convert plain text to primary cypher text, a first-level key and an encryption algorithm are used. The idea of a second-level key is introduced, which improves the security of this technique. The second-level private key fortifies the cypher text by introducing primers and intron positions. After analysing the proposed method against brute force attacks, excellent results were obtained. Using a modern computer, the hacker would need more than a half-year to decrypt the cipher text. This method is extremely time- and space-complex.Shinde and colleagues [9] proposed a new DNA-based cryptography technique. To improve data security, the method combines traditional cryptographic techniques with novel approaches. The plaintext is converted first to an ASCII value, then to binary strings. The binary strings are then converted to hexadecimal values, and the MD5 algorithm is used to generate a 128-bit key. This key is encoded as a 32-character hexadecimal string that corresponds to 16 dynamic values. A mapping table is used to encode the binary values. After encoding, some mathematical and logical operations are performed. This method is both quick and effective. However, the security provided by this algorithm is insufficient for healthcare IOT systems.Gogte et al. [10] presented a new type of DNA cryptography system based on quantum cryptography for secure communication. Quantum cryptography is a new security technique that uses a quantum channel to communicate between two parties. Heisenberg's uncertainty principle and the no-cloning theorem serve as its foundations. First, a simulation of quantum key exchange and authentication is performed. Following that, a DNA-based algorithm is used. As input, the DNA encryption algorithm uses a symmetric encryption algorithm with a 128 bit key.Man-in-the-middle attacks, eavesdropping, replay attacks, packet sniffing, and spoofing are all prevented by this method. However, the technique is too complex to be used in resource-constrained e-health systems. Zhang et al. [11] proposed a DNA cryptographic algorithm. The technique is based on the joining of DNA fragments.The algorithm used by the authors combines DNA digital coding, DNA molecular keys, and some software techniques. This method is based on the symmetric key cryptography concept. In this case, the encryption mechanism is accomplished through the use of DNA digital coding. The implementation of the DNA molecular key is the main challenge of this algorithm.Ibrahim et al. [12] proposed using double DNA sequences to improve data hiding security. The scheme's main concept is to encrypt secret messages to ensure security and robustness. The encrypted message is hidden in another DNA reference sequence. A new data concealment algorithm based on DNA sequences has been proposed in general. In this scheme, data is hidden in repeated characters to reduce the rate of modification. However, if the attacker obtains the secret message using this method, the method is broken.

Proposed Scheme: In this section, the proposed work is described in detail. Figure 2 illustrates the architecture of the proposed system [DNA Based Cryptosystem and Insertion method].

3. SECURITY THROUGH DNA-BASED INSERTION METHOD AND PRIME NUMBERS

Researchers present our security scheme for medical data IoT systems in this section. The proposed scheme consists of (i) mutual authentication and authorization based on prime numbers and (ii) encryption based on DNA- Based Insertion method and prime numbers. Our scheme provides first-level security via the prime number algorithm, which requires a smaller key size and less computation overhead. The use of a low-computation DNA cryptosystem provides the second level of security. Figure 1 depicts the structure of a DNA-based cryptography technique.

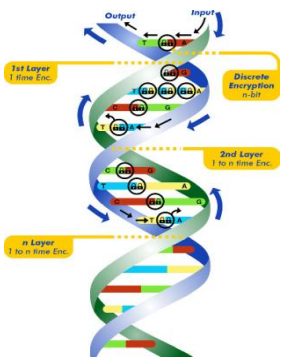


Figure 1 DNA Based Cryptography

Table 1. DNA Sequence to binary

Bases of DNA	Decimal	Digital coding
A	0	00
T	1	01
C	2	10
G	3	11

DNA-BASED CRYPTOGRAPHY WITH INSERTION METHOD

The DNA-INS algorithm is organized into three steps. They are as follows:

- Key Generation
- Encryption
- Decryption.

HR Key_gen(SSB):

Begin:

1. $SN \leftarrow random(n)$ // n-natural numbers
2. $kg \leftarrow read(SN)$ // Read the secret number
3. $SBN \leftarrow (kg)2$ // SN to binary number
4. $SSB \leftarrow (SBN \ \% \ m)$ //m=1,
5. return (SSB)

End:

Enc_alg(NDS):

Begin:

1. DNA _enc(BN):

Begin:

1. R←read(Medical Data) // Read Plaintext/ Image.
2. EI ←encode(R) // convert the image to string

Prime Number(P,Q):

Begin:

3. R=(P+Q)mod 26 //equation (1)
4. return (R)

End

1. End:
1. ST←split(R) //Split the plaintext or image string
2. AS ←ASCII(ST)
3. BN ← (AS)2 // ASCII to Binary numbers
4. return (BN)
5. End
6. ***Insert_enc(NBN):***
7. Begin:

1. $IN \leftarrow read(BN,SSB)$ // Read BN and SSB
2. $BD \leftarrow (BN\% \ k)$
3. $NBN \leftarrow insert(PB,DB)$ // Insert BD into PB
4. return (NBN)

8. End:
1. $NDS \leftarrow DNACode(NBN)$
2. return NDS

9. End:

Enc_alg(NDS):

Begin:

2. DNA _enc(BN):

Begin:

5. R←read(Medical Data) // Read Plaintext/ Image.
6. EI ←encode(R) // convert the image to string

Prime Number(P,Q):

Begin:

7. R=(P+Q)mod 26 //equation (1)
8. return (R)

End

2. End:

10. ST←split(R) //Split the plaintext or image string
11. AS ←ASCII(ST)
12. BN ← (AS)2 // ASCII to Binary numbers
13. return (BN)
14. End
15. ***Insert_enc(NBN):***
16. Begin:
5. $IN \leftarrow read(BN, SSB)$ // Read BN and SSB
6. $BD \leftarrow (BN\%\ k)$
7. $NBN \leftarrow insert(PB, DB)$ // Insert BD into PB
8. return (NBN)
17. End:
3. $NDS \leftarrow DNACode(NBN)$
4. return NDS
18. End:

The first process is the key generation process, which is detailed in algorithm 1. The first step in this process is to generate a secret key at random. The secret key is encoded in binary numbers and stored in the SSB variable. The encryption process is the second step, which is described in Algorithm 1. The initial stage in this process is to generate a DNA sequence. The user reads the plaintext or image using the DNA encryption method called DNA enc(). The first stage in this process is to encrypt information using the Prime number. The Medical image is shifted with a user-defined random value to generate a new plaintext NPT. The new plaintext is converted to their corresponding ASCII values, which are then converted to binary numbers. Table 1 is used to translate binary numbers into a DNA sequence. The second step is the Insertion encryption process, Insert_enc (NBN). In this step, the plaintext binary numbers BN and the secret binary numbers SSB are read by an Insertion-Based encryption method. The plaintext binary numbers and the secret binary numbers are split by a user-defined value. The secret binary numbers are inserted into plaintext binary numbers with a user-defined position k using algorithm 1 insert () function. A new set of binary numbers is generated. Based on table 1, the new binary numbers are converted to a fake DNA sequence called NDS. An NDS is sent through a public channel by the sender and received by the receiver. The third process is decryption, which is the inverse of encryption as stated in algorithm 1. The initial stage in this process is to transform the fake DNA sequence NDS into a new binary number NBN. The second stage is the Insertion-Based Decryption Algorithm Insert_dec (). In this step, using the Extract () function, the secret binary numbers SSB are extracted from the new binary numbers NBN and returned as plaintext binary numbers SE1. The SE1 is converted to the ASCII character AS. DNA_dec() reads the new plaintext. The NPT is shifted by a user-defined value, resulting in the PT or IM. Finally, the receiver receives the original plaintext or image.

4. SECURITY ANALYSIS OF THE PROPOSED SCHEME

Security analysis for analysis the security strength of encryption and decryption algorithm. The security analysis contains some of the common attacks. The explanations of each attacks is given below.

Brute-Force Attack: The proposed scheme selects DNA sequences at random from a pool of available DNA sequences. As a result, predicting the DNA sequence used in this study is impossible. In other words, an attacker cannot use a predictive model to determine the used DNA sequence. The attacker will be unable to capture the network unless he knows the DNA sequence. When multiple DNA sequences are assigned to each sensor, the DNA sequence pool is formed by randomly selecting DNA sequences from a pool of thousands. Each DNA sequence in the pool is distinct from the rest of the pool's DNA sequences. There are no methods for predicting which DNA sequences are present in the pool at the moment.

Histogram Analysis: A histogram is a statistical representation of the plaintext and cipher text. Here, variance is one of the main analyses of histogram analysis technique for measuring uniformity in both plaintext and cipher text. The variances in the original text are much higher than the variances in the cipher text. It means high non-uniformity in the histograms of the original text and high uniformity in the histograms of the cipher text. So, high uniformity validates high randomness of the original text in the cipher text. In addition, the high randomness of the text supports strong security in the encryption process.

Information Entropy Analysis: The results of entropy of the existing systems and proposed scheme. From these tables, it can be easily identified that the hybrid system has higher entropy values than the existing schemes. This validates high randomness in the hybrid cipher text, and hence, the chances of hacking are decreased. This shows that the hybrid system can resist information entropy attacks

Key Sensitivity Analysis: Key sensitivity analysis determines the sensitivity of the key in the algorithm. That means that it deals with the changes in results made by a small change in the key. The encrypted data are completely different by lightly changing the encryption keys. However, in the existing schemes, the encrypted data are not completely

different, when there are small changes in the secret key. This means that the secret keys are extremely sensitive in the proposed scheme.

5. CONCLUSION

Researchers presented a novel security scheme for medical data IoT systems using DNA cryptography techniques, the insertion method, and prime numbers in this paper. To the best of our knowledge, previously proposed security schemes for medical systems in general are insufficient to meet the essential security requirements of medical IoT systems. The majority of previously proposed solutions were not secure against the most common healthcare IoT system attacks. The proposed scheme was specified and designed by using (i) the prime number architecture to mutually authenticate and certify medical sensors and end-users (i.e. health carers), and (ii) the DNA-based Insertion method cryptographic technique to encrypt and decrypt medical data using patient DNA sequences. Researchers proved that our proposed scheme is safe against the relevant attacks and offers a higher level of security than comparable work in the literature. Researchers find that the proposed scheme has the appropriate features for use in e-health systems based on the security analyses presented in this paper. Researchers believe that our scheme is applicable to any IOT application that requires secure and efficient communication, not just healthcare IOT systems. Our future work will concentrate on analyzing the proposed scheme's effectiveness in terms of communication cost, delay, and memory usage.

REFERENCES

[1]. Hummen, R., Shafagh, H., Raza, S., Voig, T., Wehrle, K.: Delegation-based authentication and authorization for IP-based Internet of Things. In: IEEE International Conference on Sensing, Communication, and Networking, pp. 284–292 (2014)

[2]. Hung, X., Khalid, M., Sankar, R., Lee, S.: An efficient mutual authentication and access control scheme for WSN in healthcare. J. Netw. 6(3), 355–364 (2011)

[3]. Adleman, L.M.: Molecular computation of solutions to combinatorial problems. Science 266(5187), 1021–1025 (1994).

[4]. Akiwate, B., Parthiban, L.: A dynamic DNA for key-based cryptography. In: IEEE International Conference on Computational Techniques, Electronics and Mechanical Systems, pp. 223–227 (2018)

[5]. E.Vidhya, R. Rathipriya, Two Level Text Data Encryption using DNA Cryptography, International Journal of Computational Intelligence and Informatics, December 2018

[6]. Rafiul, M., Rokibul, K., Akber, A., Morimoto, Y.: A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem. In: International Conference on Networking, Systems and Security, pp. 1–8 (2017)

[7]. Pradeeksha, A., Sathyapriya, S.: Design and implementation of DNA based cryptographic algorithm. In: IEEE International Conference on Devices, Circuits and Systems, pp. 299–302 (2020)

[8]. Zebari, D., Haron, H., Zeebaree, S., Zeebaree, D.: Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. In: IEEE International Conference on Advanced Science and Engineering, pp. 312–317 (2018)

[9]. Chakraborty, R., Rakshit, G., Roy, B.: Enhanced key generation scheme based on cryptography with DNA logic. Int. J. Inf. Commun. Technol. Res. 1(8), 370–374 (2011)

[10]. Gehlot, L., Shinde, R.: A survey on DNA-based cryptography. Int. J. Adv. Res. Comput. Eng. Technol. 5(1), 107–110 (2016)

[11]. Gogte, S., Nemade, T., Nalawade, P., Pawar, S.: Simulation of quantum cryptography and use of DNA based algorithm for secure communication. J. Comput. Eng. 11(2), 64–71 (2013)

[12]. Fu, B., Zhang, Y., Zhang, X.: DNA cryptography based on DNA fragment assembly. IEEE Int. Conf. Inf. Sci. Digital Content Technol. 1, 179–182 (2012)

[13]. Abdelkader, H., Ibrahim, F., Moussa, M.: Enhancing the security of data hiding using double DNA sequences. In: Industry Academia Collaboration Conference (2015)

[14]. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. A8, 203–209 (1987)

[15]. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). https://doi.org/10.1007/3-540-39799-X_31

[16]. E.Vidhya, R. Rathipriya, Comparative Study of Hybrid RSA-ECC and Hybrid DNA-Insertion for Large Dataset, International Journal of Grid and Distributed Computing [web of science].

[17]. Aumasson, J., Henzen, L., Meier, W.: QUARK: a lightweight hash. J. Crypt. 26(2), 313–339 (2013)

[18]. Vijayakumar, P., Vijayalakshmi, V., Zayaraz, G.: DNA computing-based elliptic curve cryptography. J. Comput. Appl. 36(4), 1–4 (2011)

[19]. E.Vidhya, R. Rathipriya, Key Generation for DNA Cryptography Using Genetic Operators and Diffie-Hellman Key Exchange Algorithm, International Journal of Mathematics and Computer Science, 15(2020), no. 4, 1109–1115.

[20]. E.Vidhya, R. Rathipriya, hybrid Dna Cryptography Method Using Different Key Generation Techniques, Advances and Applications in Mathematical Sciences, 21(2021), no. 1, 251-167.