Special Issue | August 2017 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

All India Seminar on

Futuristic Trends in Telecommunication Engineering & Telecom Panorama – Fundamentals and Evolving Technology, with Particular Reference to Smart City on 5th – 6th August 2017

Organized by

The Institution of Engineers (India) Jabalpur Local Centre

17. Secure IoT (SIT) Performance Evaluation with Respect to DNA Based Encryption Imaging Technique

Nikita Asrani
M.Tech Research Scholar
Gyan Ganga Institute of Technology and Science, Jabalpur (M.P) INDIA
Email: Required

Vipul Awasthi
Assistant Professor
Gyan Ganga Institute of Technology and Science, Jabalpur (M.P) INDIA
Email: Required

Vinod Kapse
Principal
Gyan Ganga Institute of Technology and Science, Jabalpur (M.P) INDIA
Email: Required

Abstract The Internet of Things (IoT) being a promising technology of the future is expected to connect billions of devices. The increased rate of communication is able to generate mountains of data but the security of data can be a threat in itself. The devices in the architecture are essentially smaller in size and low powered. Conventional encryption algorithms are generally computationally expensive due to their complexity and requires many rounds to encrypt, essentially wasting the constrained energy of the gadgets. However, less complex algorithms may compromise the desired integrity. In this Paper we propose a light weight encryption algorithm named as Secure IoT (SIT).

1. INTRODUCTION

The Internet of Things (IoT) is turning out to be an emerging discussion in the field of research and practical implementation in the recent years. IoT is a model that includes ordinary entities with the capability to sense and communicate with fellow devices using Internet [18]. As the broadband Internet is now generally accessible and its cost of connectivity is also reduced, more gadgets and sensors are getting connected to it. Such conditions are providing suitable ground for the growth of IoT. As there is a great deal of complexities around the IoT, since we wish to approach every object from anywhere in the world. The sophisticated chips and sensors are embedded in the physical things that surround us, each transmitting

valuable data. The process of sharing such large amount of data begins with the devices within themselves which must securely communicate with the IoT platform.

This platform integrates the data from many devices and apply analytics to share the most valuable data with the applications. The IoT is taking the conventional internet, sensor network and mobile network to another level as everything will be connected to the internet. A matter of concern that must be kept under consideration is to ensure the issues related to confidentiality, data integrity and authenticity that will emerge on account of security and privacy [19].

2. APPLICATIONS OF IoT:

With the passage of time, more and more devices are getting connected to the Internet. The houses are soon to be equipped with smart locks [18], the personal computer, laptops, tablets, smart phones, smart TVs, video game consoles even the refrigerators and air conditioners have the capability to communicate over Internet. This trend is extending outwards and it is estimated that by the year 2020 there will be over 50 billion objects connected to the Internet [21].

The earth will be blanketed with millions of sensors gathering information from physical objects and will upload it to the Internet. It is suggested that application of IoT is yet in the early stage but is beginning to evolve rapidly. An overview of IoT in building automation system is given. It is suggested that various industries have a growing interest towards use of IoT. Various applications of IoT in healthcare industries are discussed and the improvement opportunities in healthcare brought in by IoT will be enormous. It has been predicted that IoT will contribute in the making the mining production safer and the forecasting of disaster will be made possible. It is expected that IoT will transform the automobile services and transportation systems. As more physical objects will be equipped with sensors and RFID tags transportation companies will be able to track and monitor the object movement from origin to destination, thus IoT shows promising nature in the logistics industry as well. With so many applications eyeing to adapt the technology with the intentions to contribute in the growth of economy, health care facility, transportation and a better life style for the public, IoT must offer adequate security to their data to encourage the adaptation process.

Evaluation Parameters

To test the security strength of the proposed technique, the algorithm will be evaluated on the basis of the following criterion. Key sensitivity, effect of cipher on the entropy, histogram and correlation of the image. The algorithm will be tested for computational resource utilization and computational complexity. For this we will observe the memory utilization and total computational time utilized by the algorithm for the key generation, encryption and decryption.

1) Key Sensitivity: An encryption algorithm must be sensitive to the key. It means that the algorithm must not retrieve the original data if the key has even a minute difference from the original key. Avalanche test will be used to evaluate the amount of alterations occurred in the cipher text by changing one bit of the key or plain text. According to Strict

Avalanche Criterion SAC [22] if 50% of the bits are changed due to one bit change, the test is considered to be perfect. To visually observe this effect, we will decrypt the image with a key that has a difference of only one bit from the correct key.

2) Execution Time: One of the fundamental parameter for the evaluation of the algorithm is the amount of time it takes to encode and decode a particular data. The proposed technique is for the IoT environment, must consume minimal time and offer considerable security.

3) Memory Utilization: Memory utilization is a major concern in resource constrain IoT devices. An encryption algorithm is composed of several computational rounds that may occupy significant memory making it unsuitable to be utilized in IoT. Therefore; the proposed algorithm is evaluated in terms of its memory utilization. Smaller amount of memory engagement will be favorable for its deployment in IoT.

4) Image Histogram: A method to observe visual effect of the cipher is to encrypt an image with the proposed algorithm and observe the randomness it produces in the image. To evaluate the generated randomness, histogram of the image is calculated. A uniform histogram after encryption depicts appreciable security.

5) ***Image Entropy:*** The encryption algorithm adds extra information to the data so as to make it difficult for the intruder to differentiate between the original information and the one added by the algorithm. We measure the amount of information in terms of entropy, therefore it can be said that higher the entropy better is the performance of security algorithm.

6) ***Correlation***: The correlation between two values is a statistical relationship that depicts the dependency of one value on another. Data points that hold substantial dependency has a significant correlation value. A good cipher is expected to remove the dependency of the cipher text from the original message. Therefore; no information can be extracted from the cipher alone and no relationship can be drawn between the plain text and cipher text. This criterion is best explained by Shannon in his communication theory of secrecy systems [23].

3. CURRENT STATE OF LITERATURE

Today is the era of digital communication. Security and privacy is important for communication. Cryptography is a process, well known for hiding the message. Its known as time back. Steganography is derived from two words, stegano means secret and graphy means secret writing. In this paper, we are discussing only about steganography using DNA. Adleman is known to be the father of DNA computation [1]. He has done chemical reactions and shown how DNAs can be used for computations. We are going to discuss about the works Done using theoretical DNA computing. Catherine Taylor [2], proposed an idea in which information is encoded into DNA strands, and then converted into microdots. A microdot is a highly reduced photograph of a typewritten page. Developed DNA based doubly stegano graphic method. First done DNA encryption and then reduced it to a microdot. Simple substitution cipher is used for encryption. Because of the huge possibilities of DNA nucleotides, it acts as a complex background for storing secret message. Random key is used for encryption. Disadvantage is its Expensive.

Andre Leier et.al. [3] proposed cryptography using DNA binary strands. They proposed two different DNA based cryptographic techniques. In method 1, initially mix the binary encoded plaintext with dummy strands in equimolar International Journal of Science and Research (IJSR) ISSN (Online):

2319-7064 Index Copernicus Value (2015): 78.96. Here decryption is done using Polymerase Chain reaction (PCR). In method 2, encryption is same as before. Here they used gel image of dummy pool as the key. Decryption is done by graphical method. Method 2 has the advantage of easy encryption, but resolution of gel is a problem. Jiechen [4], used the random nature of DNA for making the cryptographic system unbreakable. Here they used carbon nanotubes as a medium for message transmission. Plaintext messages are converted to cipher text by adding message with one time pads. Here DNA sequences act as one time pads. But this method is expensive.

Pak Chung Wong et.al [5], proposed an idea of DNA memory prototype. Today, we

use magnetic media and silicon chips to store our data. All these storage media can easily be destroyed by people or natural disasters. So, they proposed an alternate storage mechanism. Here they initially Encode meaningful information as artificial DNA sequences. Then transform the sequences to living organisms, allow the organism to grow and multiply. Extract the information back from organisms. Success of this method depends on finding good storage medium to ensure adequate protection for the encoded DNA strands. Host with embedded information must be able to grow and multiply. Advantage is that it has enormous potential capacity. Disadvantage is that mutation of organism may affect the integrity of embedded messages [7].Monica Borda [8], published a paper on DNA secret writing. Steganography using DNA hybridization has five steps, plaintext message given in ASCII is converted to binary. Evaluate required length for DNA OTP. If each bit is encoded with 10 nucleotide, OTP of length>10*n. The encrypted message is placed between two primers hidden in a microdot, Perform decryption using PCR.

Qiang Zhang et.al. [9], published a paper on Image encryption using DNA addition combining with chaotic maps. Here initially encode the original image to obtain DNA sequence matrix. Divide this matrix to equal blocks and then carry out DNA sequence addition operation. Find the DNA sequence complement using 2D logistic maps. Decryption done as reverse of above. Deepak Kumar [10], proposed the idea of secret data writing using, DNA sequences. Here DNA OTP method is used for defining the new security algorithm. DNA coding is necessary because we cannot process the DNA molecules as in form of alphabets, so change alphabets to ASCII. Almost same as Monica Borda's algorithm.

Amal Khalifa [11], proposed a steganography algorithm to exchange data secretly. Its implemented in mainly 2 levels. In first level, encryption is done using DNA based play fair cipher. In second level, encrypted message is hidden to some reference DNA using substitution. The performance of presented algorithm is also analyzed with respect to robustness against attacks as well as hiding capacity.

Sheena Anees [12], proposed highly secure DNA based audio steganography. Here a highly secure method to hide the messages, is proposed.

Prasenjit Das [14], proposed DNA based image steganography. Proposed algorithm uses images as primary cover media for message transfer between two interested parties.

Fasila K.A. et al [15], proposed the idea of multi phase crypto system. Here a hybrid cryptography based on RGB colors is proposed. Convert the plaintext to matrix form, pass it through a number of manipulation steps. Security is further enhanced by using a strong key which is encapsulated using DNA steganography method.

Sreeja C.S et al [16], proposed a DNA symmetric algorithm based on the pseudo DNA cryptography and central dogma of molecular biology. The suggested algorithm uses splicing and padding techniques along with complementary rules which make the algorithm more secure as it's an additional layer of security than conventional cryptography techniques.

Shweta et al [17], proposed paper on cascaded DNA cryptography and steganography. Initially it performs DNA cryptography and then its hidden in a random frame of video.

4. CONCLUSION

In this paper we reviewed a light weight encryption algorithm named as Secure IoT (SIT). This method has various advantages like speed, minimal storage requirements and minimal power requirements. We surveyed number of research article and decided to analyze DNA based encryption imaging technique.

REFERENCES:

[1] Leonard M Adleman, "Computing with DNA", Scientific American, pp.: 34–41, August 1998.

[2] Catherine Taylor Clelland, "Hiding Messages in DNA Microdots", Nature, pp.: 533–534, June 1999.

[3] Andre Leier, "Cryptography with DNA Binary Strands", Bio Systems, pp.: 13–22, April 2000.

[4] Jie Chen, "A DNA-based, biomolecular cryptography design", In Circuits and Systems, ISCAS '03, Proceedings of the 2003 International Symposium on, pp.: 822–825, vol.3, May 2003.

[5] Pak Chung Wong, "Organic Data Memory using DNA Approach", In Communications, pp.: 95–98, January 2000.

[6] Venkatraman S, Ajith Abraham, "Significance of Steganography of Information Technology", Coding and Computing, pp.: 347 – 351, April 2004.

[7] X.Wang, Q. Zhang, "DNA computing - based cryptography", Fourth International Conference, In Bio-Inspired Computing,

[8] M. Borda, O. Tornea, "DNA secret writing techniques", In Communications (COMM), 8th International conference on, pp.: 451–456, June 2010.

[9] Qiang Zhang, "Image encryption using DNA addition combining with chaotic maps", Elsevier, Mathematical and Computer Modelling, The BIC- TA Special Issue International Conference on Bio-Inspired Computing Theory and on Applications. 2009.

[10] D.Kumar and S.Singh, "Secret data writing using DNA sequences", Emerging Trends In Computer Communications (ETNCC), 2011.

[11] Khalifa, A. Atito. "High-capacity DNA- based steganography", In Informatics and Systems (INFOS), 8th International Conference on, pp.: 76 –80, May 2012.

[12] M. Shyamasree, S. Anees. "Highly secure DNA-based audio steganography". In Recent Trends in Information Technology (ICRTIT), pp.: 519–524, July 2013.

[13] P.Vijaya Kumar, V. Vijayalakshmi, "Enhanced level of security using DNA computing technique with hyperelliptic curve cryptography", Network Security, 2013.

[14] P. Das, N. Kar "A DNA based image steganography using 2d chaotic map", In Electronics and Communication Systems (ICECS), pp.: 1 – 5, Feb 2014.

[15] F. K. A., D. Antony, "A multiphase cryptosystem with secure key encapsulation scheme based on principles of DNA computing", In Advances in Computing and Communications (ICACC), pp.: 1–4, Aug 2014.

[16] S. C. S, M. Misbahuddin, and M. Hashim N. P., "DNA for information security: A survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology" (ICCCT), 2014, pp.: 1–6, Dec 2014.

[17] Shweta and S. Indora. "Cascaded DNA cryptography and steganography", In Green Computing and Internet of Things (ICGCIoT),

2015 International Conference on, pp.: 104–107, Oct 2015.

[18] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions", Future Generation Computer Systems, vol. 29, issue 7, pp.: 1645–1660, 2013.

[19] R. Want, S. Dustdar, "Activating the internet of things [guest editors' introduction]," Computer, vol. 48, issue 9, pp. 16–20, 2015.

[20] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, L. Kerr, "Security in the industrial internet of things," 2016.

[21] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp.198, 2015

[22] A. Webster and S. E. Tavares, "On the design of s-boxes," in Conference on the Theory and Application.

[23] C.E. Shannon, "Communication theory of secrecy systems," Bell system technical journal, vol. 28, no. 4, pp. 656–715, 2016.