International Journal for Modern Trends in Science and Technology, 6(8S): 122-124, 2020

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTSTCIET23
Available online at: http://www.ijmtst.com/ncracse2020.html

Securing Data in IoT Devices using DNA Cryptography

Naga Saranya Cherukupalli[1] | Sesha Shayee Maruvada[1]

[1]Department of Computer Science, GITAM Institute of Science, Visakhapatnam, AP, India.

To Cite this Article
Naga Saranya Cherukupalli and Sesha Shayee Maruvada, "Securing Data in IoT Devices using DNA Cryptography", *International Journal for Modern Trends in Science and Technology*, 6(8S): 122-124, 2020.

Article Info
Received on 16-July-2020, Revised on 15-August-2020, Accepted on 25-August-2020, Published on 28-August-2020.

ABSTRACT

IoT (Internet of Things) is one of the most trending technology which introduces the most significant improvements to various aspects of the human environment likewise health, commerce and transport. The heterogeneity of various technologies which the IoT combines increases the complexity of the security processes, since each technology is characterized by different vulnerabilities. The data that is generated by the multiple interactions between users and the systems make harder their management and the functionality of the access control system. The data that is collected from different sensors used in applications has to be stored and transmitted. The data that gets transferred is not much secured, where in the middle the hackers can attack, collect the data and tamper it. The data that is encrypted by using different cryptographic algorithms are also been cracked and hacked by the hackers. To reduce this hacking and tampering of data we are proposing an enhancement to the cryptographic algorithms through DNA Cryptography, the latest technology in the cryptographic methods. To receive or to send the necessary data the machine learning algorithms is been used, the natural process of DNA formation has been used to encrypt information and then retrieve them by decrypting it which is also called as DNA sequencing. The structure of DNA in this sequencing is such that the data that has to be transmitted or stored is encrypted by using the strong four bases Adenine(A), Cytosine(C), Guanine(G) and Thymine(T). In this DNA Cryptography, the strands that are present will be holding the data in the form of DNA and is encrypted by using this {A,C,G,T} code.

Keywords— *IoT, security, hackers, tampering, cryptographic algorithms, DNA Cryptography, Adenine, Cytosine, Guanine, Thymine*

I. INTRODUCTION

IoT (Internet of Things) is that the system of reticular computing devices, mechanical and digital machines given distinctive identifiers and also the ability to transfer the information over a network while not requiring human-to-human or human-to-computer interactions. The definition of the Internet of Things has evolved thanks to the convergence of multiple technologies, machine learning, wireless device networks, automation and others contribute to alter the IoT. By 2020, the Internet of Things (IoT) is foreseen to come up with an extra $344B in revenues, also on drive $177B in price reductions. By the tip of 2019, there'll be square measure around 3.6 billion devices that square measure actively connected to the web and used for daily tasks. With the introduction of 5G that may open the door for additional devices, and information traffic. because the applications growing chop-chop, the protection and also the privacy remains a vital challenge that must be self-addressed. Cryptography is that the security technique used for securing the data and communication through the codes. “Crypto” means that “Hiding” and “graphy” means that “Writing”; the term Cryptography means that “Hiding the Data”. DNA (Deoxyribose Nucleic Acid) cryptography is one among the foremost chop-chop rising technologies in cryptanalytic systems. It's modelled as polymers of the humans from the biological sciences. DNA Cryptography is one of the most emerging technology in the DNA Computing. Adelman in 1994 showed the whole world the solutions for the key issues like Hamilton problem and NP problem by this technology. DNA (Deoxyribose Nucleic Acid) may be outlined as hiding data in terms of DNA sequencing. The strands of the DNA square measure the long polymers of several the connected nucleotides. These nucleotides encompass four chemical element bases and 5 carbon sugar and a phosphate cluster. The data that's to be received or transmitted by this DNA sequencing is encrypted by the robust four bases known as Adenine(A), Cytosine (C), Guanine(G) and Thymine (T) with every given of 2 bytes as A=00,C=11, G=10 and T=01. A gram of polymer contains 1021 polymer bases = 108 Terabytes of Data. In this paper, we would like to propose that the data to be collected or send through network can be secured by using this DNA Cryptographic encoding and decoding techniques.

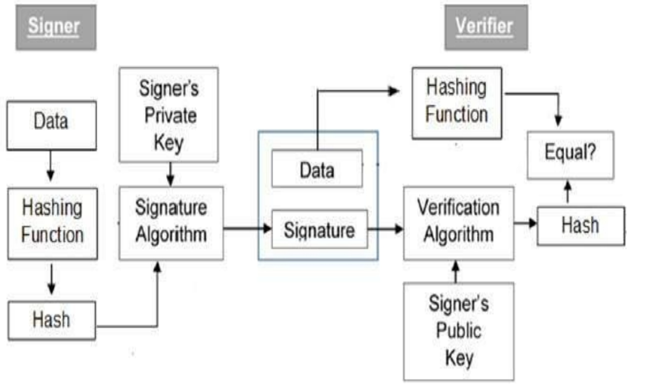
II. Related Works

Securing the data in IoT has been a major issue since years. Many researches have been created and plenty of proposals had been given by upon the security. Existing researches has given varied cryptographic algorithms upon securing the data. Insight, hackers are still attacking to tamper the data. There is no strong authentication and data protection. The data collected and transferred is not secured properly. Integrity and confidentiality of data is not authenticated. The data stored in the IoT devices are also not secured. DNA Cryptography can currently be used as the strong algorithm for data security as its cracking time and key generation are designed that it is time taken to decode the ciphered data, and is quite not possible for a life time. So, it ought to be the primary alternative for the cyber security researchers for securing knowledge and data. The study created here is comprehensive and also the data given here can mostly facilitate to the researchers for doing additional work in this line of thinking. The current work will facilitate to implement and apply DNA methodologies to cryptography. The main aim of my research work is to “Secure the data that's collected from the IoT devices”. To imply that the data to be sent or received is in additional secured method and to associate algorithmic rule that is more secured to store the data. To ensure that the hackers might take life time to crack the code for meddling the data. The crypto logical algorithms that can be tampered by the hackers are to be enhanced by this DNA cryptography.

III. Proposed Methodology

Upon many attacks has been done and still going on the data, here in my research work I propose a methodology for securing the data in more secured way by using the digital signatures using DNA cryptography. Digital signatures is one of the cryptographic technique that binds a person/entity to the digital data. The digital signature is a public-key cryptographic technique which adopts the scheme of both public and private keys. This public-key cryptographic algorithm is implemented by the DNA cryptography in the form of DNA sequencing. This DNA sequencing can store the data and is transferred in more secured way. The data from the IoT sensors is collected through the machine learning algorithms and is secured by this digital signature algorithm by DNA Cryptography and is stored and sent in more secured way.

The following figure represents the digital signature algorithm:



IV. Conclusion

IoT (Internet of Things) is a simple concept, taking all the things in the world and connecting them to the internet. The real power of Internet of things is, it can send information and receive the information from the things and act upon it. IoT has become very popular and it has been used in various applications like farming, Health and Safety, Disaster management, etc. The proposed methodology ensures the security of the data from tampering and also reduces most of the hacking.

REFERENCES

[1] https://searchsecurity.techtarget.com/definition/cryptography

[2] https://www.information-age.com/iot-and-data-breaches-123483531

[3] https://tools.cisco.com/security/center/resources/secure_iot_proposed_framework#4

[4] https://www.infosys.com/insights/iot/security-iot.html

[5] https://www.telit.com/blog/how-to-prevent-iot-breach-with-secure-modules/

[6] https://www.electronicdesign.com/industrial-automation/article/21805420/8-critical-iot-security-technologies

[7] https://securityaffairs.co/wordpress/33879/security/dna-cryptography.html

[8] https://www.researchgate.net/publication/279978777_DNA_Cryptography, Ahsan Omer ,Hitec University · MS Program in Electrical Engineering, BSEE

[9] Volume 4, Issue 3, March 2016, International Journal of Advance Research in Computer Science and Management Studies, A Review on Image Encryption Using DNA Based Cryptography Techniques

[10] https://resources.infosecinstitute.com/dna-cryptography-and-information-security/#gref

[11] https://arxiv.org/ftp/arxiv/papers/1904/1904.05528.pdf

[12] https://link.springer.com/chapter/10.1007/978-3-642-04292-8_49, DNA Cryptographic Algorithms O. Tornea and M.E. Borda Communications Department, Technical University of Cluj-Napoca, Romania

[13] https://www.researchgate.net/publication/328261954_Study_on_Security_issues_in_Internet_of_Things

[14] https://www.aranca.com/knowledge-library/articles/business-research/ai-a-key-element-in-bridging-the-security-gap-for-iot-devices

[15] https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[16] https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.html.

[17] https://reader.elsevier.com/reader/sd/pii/S235286481730247X, Machine learning for internet of things data analysis: a survey,Mohammad SaeidMahdavinejad, Mohammadreza Rezvan, MohammadaminBarekatain, Peyman AdibiPayamBarnaghiAmit P.Sheth