International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-5, March 2019

Hybrid Method for Securing Data in IoT Cloud

Vidhya Vijayan, Eldo P Elias

Abstract*: *Information exchange between items (things), having detecting or registering capacities or both over the web is known as the Internet of Things (IoT). IoT and Cloud computing coordinated to shape a stage called IoT cloud. Since these advancements are altogether utilized, there is a requirement for the security of information accumulated from the gadgets associated through these advances. To solve the transport issue in the symmetric key algorithm and to acquire the high performance, the proposed method and RSA algorithm are combined together. While actualizing the proposed framework, the symmetric key algorithm utilizes low RAM for preparing, in this way, it gives rapid. RSA is one of the best and secures asymmetric encryption method. Here it is used only to encrypt the symmetric key, for this, it requires a negligible computational cost. The proposed method using DNA cryptography and Huffman coding for encrypting and decrypting data. DNA Cryptography can have a special advantage for secure authentication, data storage, steganography, digital signatures and so on. Huffman code is a sort of ideal prefix code. What's more, it is ordinarily utilized for lossless information compression. This methodology utilizes variable key length so aggressor won't almost certainly surmise the length of the key recognition.

Index Terms*: *Decryption, DNA Coding, Encryption, Huffman Coding, IoT.

I. INTRODUCTION

Data exchange between objects over network with sensing and computing capabilities are termed as Internet of Things (IoT). IoT relies upon sharp and self-designing hubs controlled in a dynamic and worldwide condition [1]. It is a standout amongst the most developing advancements, empowering the objects to connect world. IoT is commonly portrayed as little objects with constrained capacity and handling limit. It permits devices, for the most part, installed in everyday objects, (for example, a cooler, lights, conditioner, fan, etc.) with the beforehand referenced abilities, and are controlled and communicated over the web. Cloud computing has started late grabbed prominence and formed into a noteworthy pattern in Data Innovation [2]. It is the most recent innovation in the field of distributing and furthermore gives different on the web and on-request benefits for putting away the information. Different associations are anxious to utilize administrations of cloud because of the information security given by the cloud. With the tremendous utilization of IoT and Cloud computing. The combination of cloud and IoT is called as IoTcloud. In the IoT cloud, the major issue is to give the security of data gathered from the articles related to the web. Security for any correspondence through the system can be given by the Authentication, Encryption, Decryption, Message authentication code, Hash function, and Digital signature and so on.

A hybrid methodology utilizing DNA cryptography and Huffman coding is proposed in this paper. This methodology utilizes variable key length with the goal that the aggressor won't almost certainly surmise the length of the key. The applications of IoT are extensive. IoT has applications extending from wearable gadgets to Savvy homes. Wireless technologies, internet and Microelectromechanical Systems (MEMS) are evolved in IoT. It can be measured as the Internet of Everything.

II. RELATED WORKS

This section offers a detailed discussion on different cryptographic methods for securing data in IoT.

A. By Using Symmetric & Asymmetric Cryptography

This strategy depicts correspondence between IoT gadgets and the Portal(Gateway). Here the mix of Symmetric and Asymmetric cryptographic systems is proposed for the transmission of information inside the IoT organize for Intra-System security. The same cryptographic keys are used in Symmetric cryptography for both encryption and decryption processes. Asymmetric cryptography utilizes key sets: public keys and private keys, where public keys are freely accessible to everybody, and private keys are known just to the proprietor. Public key of the receiver is used in encryption, whereby the receiver can decrypt the message encrypted with the public key who is the only owner of the paired private key. In this method modified Vigenere Cipher [3] is used for Symmetric key encryption. The Asymmetric cryptographic algorithm is the RSA Algorithm. At the sender end, firstly get the current timestamp and create a random key K using current stamp. Then obtain the data P to be transmitted and use the modified Vigenere Cipher to encrypt P using the random key K for obtaining ciphertext C. Next we have to obtain the public key P_k of the receiver. Then use RSA Algorithm to encrypt the random key K for obtaining the encrypted Key E. Then concatenate the encrypted key E and the ciphertext C for obtain the encrypted message. Transmit this message to the receiver. At the Receiver's end, firstly receive message from the sender. At that point split the message into two, ciphertext C and encoded key E. After this utilization RSA to decode E utilizing its own private key for acquiring irregular key K. Changed Vigenere Cipher can be utilized to unscramble the ciphertext C utilizing the key K for acquiring plaintext message P.

Manuscript published on 30 March 2019.
***Correspondence Author(s)**
Vidhya Vijayan, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, India.
Eldo P Elias, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, India.

B. Security of IoT Using Encryption Algorithms

Hybrid encryption will combine two or more encryption systems. Hybrid encryption technique is mainly used for information confidentiality, integrity, non-repudiation in data exchange for IOT. In this paper, a hybrid encryption algorithm with the name of HAN [4] were analyzed. Special features in encryption and decryption in this proposed system is described in terms of speed even in building keys. During algorithm implementation several structures and digital signature were used to improve internet security.

In AES, key production procedure is used for create a key. Right off the bat, two 4 X 4 matrices, which are called key and remain, are utilized to deliver a key for encryption. It can pick a spot from the matrix and a key from the key system indiscriminately. Then deliver open key of I by sender in XOR task. From AES calculation, this progression of HAN calculation has been drawn. Delivered key of I is based on hexadecimal. At that point open key K is created. Here concealed message is send from sender to recipient. The private key is simply known by the receiver and open key K by both sender and receiver. Expect that a message is sent to the collector from the sender in which the message in multinomial is called message. The sender self-assertively picks a multinomial like m from the gathering (L_m) subsequently to make a multinomial message. In this way, it ought not be uncovered by the sender. At that point, this scrambled message will be transmitted to the recipient as an encryption message. Digital signature only for message legitimacy and evidence of security and character. For Digital signature, it must be from the sender to the recipient, so the beneficiary of the past development goes about as the sender now.

III. PROPOSED SYSTEM

The proposed system describes about the combination of Symmetric key and Asymmetric key cryptography. Symmetric key calculation requires low RAM for handling accordingly it gives fast. When contrasted with symmetric-key algorithm, Asymmetric key algorithm (like RSA) does not having any issue to exchange the key. For settling the issue of key transport in symmetric key encryption and to acquire the elite, proposed strategy and RSA calculation are joined together. To encrypt the message asymmetric key algorithm that is RSA is utilized just to encode the symmetric key during the execution. For this it requires inconsequential computational cost.

3.1. DNA Coding

The proposed method using DNA cryptography [5] and Huffman coding [6] for encrypting and decrypting data. This methodology utilizes variable key length with the goal that attacker won't almost certainly surmise the length of the key. The proposed methodology utilizing the information at two dimensions by using the Huffman Encoding algorithm. DNA strand which is principally comprised of 4 nitrogenous bases to be specific: Adenine (A), Thymine (T), Guanine (G), Cytosine (C). The most effortless approach to encode is to speak to these four units as four information: A (0) – 00, T (1) – 01, G (2) – 10, C (3) – 11.

3.2 Huffman Coding

For lossless information compression, Huffman code (that is a kind of optimal prefix code) is regularly utilized. The Huffman methodology of acquiring the variable length code is given in the accompanying calculation.

3.3 Huffman Procedure

Firstly, acquire the tally of A, G, C and T from the DNA encoded string. At that point mastermind the characters in climbing request with loads. After this Take 2 least loads and add them at that point elevate it to another weight. At that point speak to indorsed load as root and 2 least loads as left and right offspring of the root. Rehash stage 3 and 4 until a solitary tree is assembled. Name left kid with 0 and right tyke as 1 from the root. Acquire the double grouping for A, G, C, T. Take all combinations of AGCT such as AA, AG, AC, AT, GA..... etc.

3.4 Encryption

Input (Plaintext) is converted into hexadecimal value and then to binary value. Bitwise complement is performed in this result. Using level-1 key, the obtained binary value is encrypted that is AGCT codes. This DNA coded ciphertext is again scrambled utilizing the level-2 keys got from Huffman Encoding. After applying level-2 keys binary coded cipher text is obtained.

3.5 Decryption

By using level-2 key, which is shared between the two parties will be encrypt the data. For converting the DNA sequence, apply level-1 key to this binary format. After complementing, obtained binary string will be converted into hexadecimal value. At long last, the hexadecimal esteem is changed over back to the plain content to get the unscrambled message. Consider the below example where the is message is “CRYPTOGRAPHY”.

PLAIN TEXT = CRYPTOGRAPHY
HEXADECIMAL = 43 52 59 50 54 4f 47 52 41 50 48 59
BINARY EQUIVALENT = 0100 0011 0101 0010 0101 1001 0101 0000 0101 0100 0100 1111 0100 0111 0101 0010 0100 0001 0101 0000 0100 1000 0101 1001
COMPLEMENT = 1011 1100 1010 1101 1010 0110 1010 1111 1010 1011 1011 0000 1011 1000 1010 1101 1011 1110 1010 1111 1011 0111
Apply level -1 key
DNA CODING = GC CA GG CT GG TG GG CC GG GC AA GC TA GG CT TT AG CG CC GC TC
Apply level -2 key
DNA CODING = GC GC GC AT GC CG CT CC GC CA GG CT GG TG GG CC GG GC GC AA GC GA GG CT GC CG GG CC GC TC
Binary Encrypted Message
01001010110101000110100111001111010111101101000000101100011010011010111110110100101

3.6 Implementation in IoT

From different sensors, the edge devices (like smaller scale controller, workstation or cell phones) continue reading to creating the data that it gets from the environment. Presently, this information is explicitly transmitted to the cloud by using any microcontroller or cell phone which approaches the web.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In the midst of the transmission, there are a few conceivable outcomes of assault fundamentally ridiculing and sniffing. The readings may respect medicinal services or money related subtleties, where assault can't go on without serious consequences. Along these lines, the most secure path is to encode the information before transmitting it to the cloud. To accomplish this, one can't generally depend on the mobile phones to complete the handling which results in deferral and utilization of more power. The proposed architecture is illustrated in Fig.1.

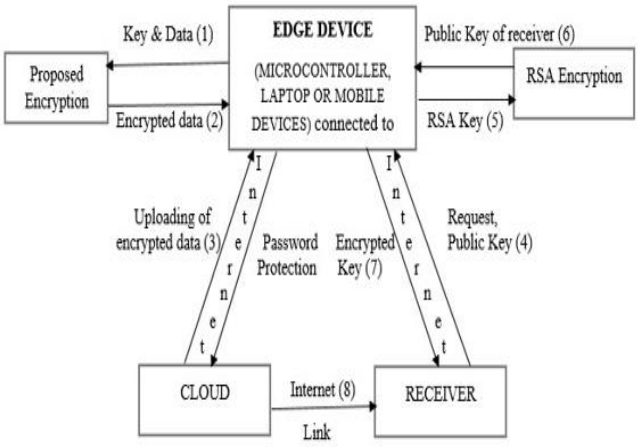

Fig. 1. Proposed IoT Architecture

The information that is gathered from sensors is gathered by the microcontroller or the cell phone. This is bolstered to the proposed encryption technique. This square takes keys for encryption with information. It forms the information and gives out the scrambled information and it will send back to the microcontroller/cell phone. At the edge gadget which associates it to the cloud, python code is running. The IP address for the cloud is noted down. Also, it is constantly transmitted as long as it is associated with the web. This encrypted information is put away in cloud everlastingly, at whatever point anybody other than the transmitter wishes to get to the information, a demand must be sent to the transmitter. The transmitter utilizes the general population key given by the requester and encrypt the key used for the encryption of information and this is transmitted back to the requester. In the wake of accepting the connection and key utilized for encryption, the beneficiary can without much of a stretch decode the key from the private key. Later utilizing the key got after decoding by RSA [7], the information is decrypted from its encoded form, which can be additionally utilized for the required analysis or observation.

IV. PERFORMANCE ANALYSIS

Physical size of a repeating string of characters [8] is reduced in Run-length encoding (RLE) process. This continuing string is known as a run likewise, is generally encoded into two bytes. The principle byte suggests the number of characters in the run and is known as the run check. In Uncompressed, 16 T characters would usually need 16 bytes to store TTTTTTTTTTTTTTTT. After RLE encoding the similar strings require just two bytes: 16T. The 16T code created to mean the character string is called an RLE parcel. The main byte speaks to the run check for example 16 and the second byte speaks to the run esteem. RLE plans are straightforward and quick, yet their pressure productivity relies upon the kind of picture information being encoded The outcomes as appeared in Table.1, Fig.2 and Fig.3 where results demonstrated a high-pressure proportion on the Huffman calculation more than the RLE calculation when contrasted with the span of the first record.

Table 1. Original and compressed file size using Huffman and RLE

Original	RLE	Huffman
9	5	2
12	5	2
15	10	5
18	10	5
21	15	8
24	15	8
27	20	12
30	20	16
33	25	16
36	25	21
39	30	21
42	30	25
45	35	25
48	35	24
51	40	29
54	40	29
57	45	34
60	45	34
63	50	39
66	50	39
69	55	44
72	55	44
75	60	49
78	60	49
81	65	54
84	65	54
87	70	59
90	70	59
93	75	63
96	75	68
	total	
1575	1200	937

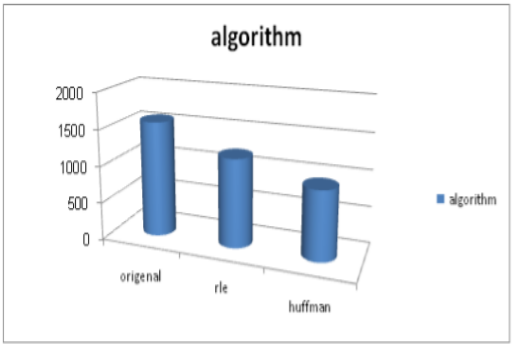

Fig. 2. Huffman and RLE with comparative sizes

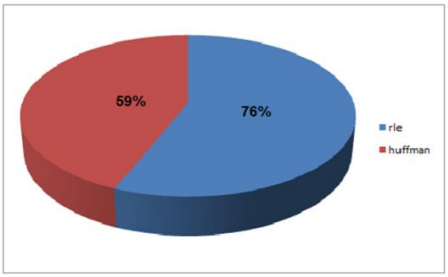

Fig. 3. Huffman and RLE compression ratio

V. RESULT

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

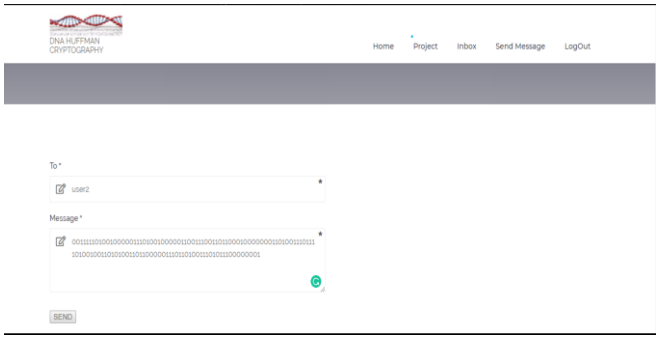

Fig. 4. Sending Encrypted message to user2

Fig. 4 shows encrypted message on user2. It can be send to a specified user. There is an option for giving the particular user. Messages from other users can be viewed in the inbox. In Fig. 5 and Fig. 6, encrypted message can be decrypted.

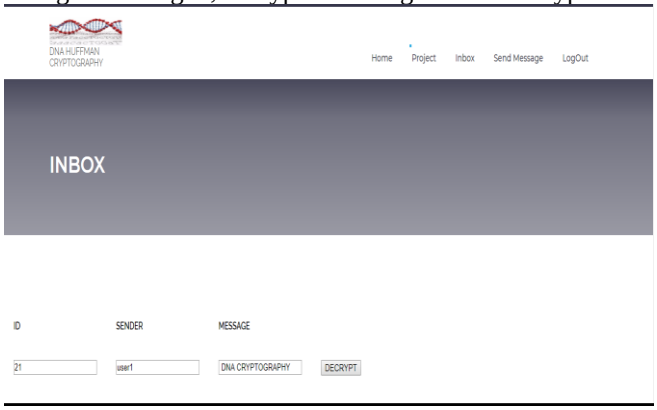

Fig. 5. Decrypted message at user2

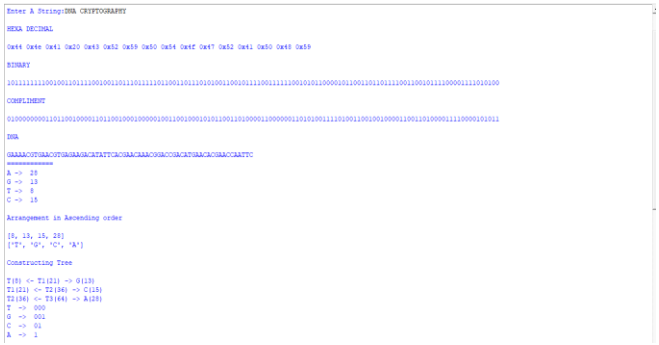

Fig. 6. DNA-Huffman output1

Fig. 7. DNA-Huffman output2

VI. CONCLUSION

Grouping of symmetric-key and asymmetric-key encryption technique for securing data in IoT Cloud is proposed. Symmetric key algorithm require low RAM for preparing in this way it gives fast. When contrasted with symmetric-key algorithm, Asymmetric key encryption (like RSA) does not having any issue to trade the key. For settling key transport issue in symmetric key encryption and to get the elite, proposed strategy and RSA calculation are consolidated together. Hybrid encryption is achieved through information exchange utilizing special session keys alongside symmetrical encryption. One favorable position is that association channel is built up between two clients' arrangements of equipment. Clients at that point can interface through hybrid encryption. Uneven encryption can back off the encryption procedure, however with the concurrent utilization of symmetric encryption, the two types of encryption are progressed. The outcome is the additional security of the transmittal procedure alongside generally enhanced system performance. In a usage, the Asymmetric key calculation that is RSA is utilized just to encode the symmetric key, for this it requires lesser computational cost. The strategy utilizing DNA cryptography and Huffman coding for encoding and decrypting data.

REFERENCES

1. W. Bruce D, GR. Milne, Y. G. Andonova, and F M. Hajjat. "Internet of Things: Conven-ience vs. privacy and secrecy." Business Horizons 58, no.6, Science Direct, pp. 615-624, 2015.
2. Prajapati Ashishkumar B, Prajapati Barkha, “Implementation Of Dna Cryptography In Cloud Computing And Using Socket Programming”G, IEEE International Conference on Computer Communication and Informatics (ICCCI -2016), 2016.
3. Gurpreet Singh, Supriya,” Modified Vigenere Encryption Algorithm and Its Hybrid Im-plementation with Base64 and AES”, 2nd International Conference on Advanced Compu-ting, Networking and Security-2013.
4. Amirhossein Safi, “Improving the Security of Internet of Things Using Encryption Algo-rithms”, World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering – 2017.
5. Rakesh Kumar Jangid, Noor Mohmmad, Abhishek Didel, Swapnesh Taterh, “Hybrid Approach of Image Encryption Using DNA Cryptography and TF Hill Cipher Algrithm”, IEEE International Conference on Communication and Signal Processing, 2014, pp. 934.
6. Nidhi Dhawale, “Implementation of Huffman algorithm and study for optimization”, International Conference on Advances in Communication and Computing Technologies (ICACACT 2014).
7. R. L. Rivest, A. Shamir and L. Adleman,” A method for obtaining digital signatures and public-key cryptosystem”, Communi. ACM, vol. 21 no. 2, pp. 120-126.

AUTHORS PROFILE

Vidhya Vijayan received Bachelor of Technology in Computer Science and Engineering from MG University in 2017 and currently pursuing Master of Technology in Computer Science and Engineering from APJ Abdul Kalam Technological University. Her research interest is in Computer Security, Data Mining and Machine Learning.

Prof. Eldo P Elias received Bachelor of Engineering in Computer Science and Engineering from Bharathiar University in 2003 and Master of Technology in Software Engineering from CUSAT in 2013. He is an Assistant Professor at Mar Athanasius College of Engineering, Kothamangalam. His research interest is in Computer Security, Data Mining and Computer Hardware.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)