Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

Comparison of Encryption Techniques in Internet of Things

Mullapudi Chaitanya Krishna
School of Electronics Engineering
Vellore Institute of Technology
Vellore, India

Arjun Varma
School of Electronics Engineering
Vellore Institute of Technology
Vellore, India

Ashwath A
School of Electronics Engineering
Vellore Institute of Technology
Vellore, India

Vishnuvardhan A
School of Electronics Engineering
Vellore Institute of Technology
Vellore, India

***Abstract*— There are 20 Billion IoT devices in the world. The major difficulty facing the industry is the security and privacy of the data that is transmitted in IoT networks. This can be overcome with the use of Encryption during data transmission. Here we analyze the working of different Encryption and their use cases. A good Encryption technique will only reveal the content of the data transmitted to the intended recipient. We cover some popular and promising encryption techniques like Advanced Encryption Standard (AES), RSA and two fish algorithm and also the Hybrid encryption in Cloud computing.**

Keywords: Encryption, Internet of Things, Advanced Encryption standard, twofish encryption, Cloud computing

I. INTRODUCTION

Internet of Things (IoT) is a fast-emerging industry of interconnected devices. These devices share information with each other, and the protection of this information is of massive importance.

An IoT system consists of web-enabled smart devices that use embedded systems to collect, send and act on data they acquire from their environments. These IoT ecosystems collect data from the various sensors to an IoT edge device where it is then stored and analyzed locally or on the cloud. The large amounts of data that is gathered from the various sensors can then be used in the fields of machine learning and artificial intelligence. These IoT networks can therefore automate many processes with many different devices working together. Some of the major applications include Smart Homes and Smart manufacturing which will significantly improve our lives. It also can enable businesses to cut down on waste, improve service delivery and reduce labor costs.

The installed base of IoT devices is forecast to be 20 Billion by 2022. This gives us the ability to access information from anywhere at any time on any device. Since a large amount of these IoT devices will be in the hands of everyday people it is of extreme importance to protect their privacy. Since IoT devices involve billions of data points, it has an expanded attack surface which can compromise sensitive information about the user. For example, in 2016, a botnet infiltrated the domain name server provided Dyn and took down many websites for an extended period. This was one of the larges DDoS (distributed denial of-service) attacks that occurred after the hackers gained access by exploiting poorly secured IoT devices. This goes to show how since all IoT devices are connected, all an attacker must do is exploit one vulnerability to access all data. Which is why Encryption is the need of the hour to protect IoT networks from their biggest threats. Most industry experts believe that IoT security and IoT privacy are cited as major concerns for IoT industry. In simple terms, Encryption is the process of scrambling sensitive data into an unreadable format. This data is used to encrypt using a special encryption key. It can only be read using a special decryption key. This ensures that only the intended person can access this information. Without encryption, all the data that is sent in IoT systems can easily read by anyone who intercepts this transmission.

Some of the most popular encryption methods are

1. RSA
2. Advanced Encryption Standard (AES)
3. Twofish

Encryption ensures that data stored in servers can only be accessed when privacy and exclusivity of data are both guaranteed. Hence, it protects and isolates data between users, companies and other people involved or with access to the data. This also ensures people and companies build trust knowing that their sensitive data is safe. This is why Encryption should be used in every IoT device. Security is also the key for IoT to fulfil its full potential.

This data can then be analyzed with machine learning tools and other patters. This helps find patterns and conduct research etc. However, if all this data is readable it makes the whole IoT network very vulnerable. Encryption therefore ensures machine learning data sets can be very large while also ensuring privacy.

Another industry where encryption is of utmost importance are the wearable and healthcare industries. This ensures that sensitive medical data can be used to predict illnesses but also that it is not readable to everyone

This paper deals with some common encryption and compares and contrasts their different use cases.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

II. Related Work

A. *Binary-bit sequencing and multi-stage encryption algorithm:*

This is a new symmetric cryptography algorithm and uses the symmetric key provided by the user [1]. The same key will be used to encrypt the given information making use of the projected algorithm. In this technique we substitute the plain text with the cipher text by performing operation on the binary bit sequence of the plain text. The key provided by the user must be between 0 and 255. Overall simplified concept of the symmetric cryptography process is shown in Fig 3.

Important causes of using the symmetric key for encryption and decryption are:

1. 1.Process is easy going.
2. 2.Security is dependent on the key.
3. 3.Both the dispatcher and the respective recipients can use the similar keys and processes for encryption and decryption techniques.

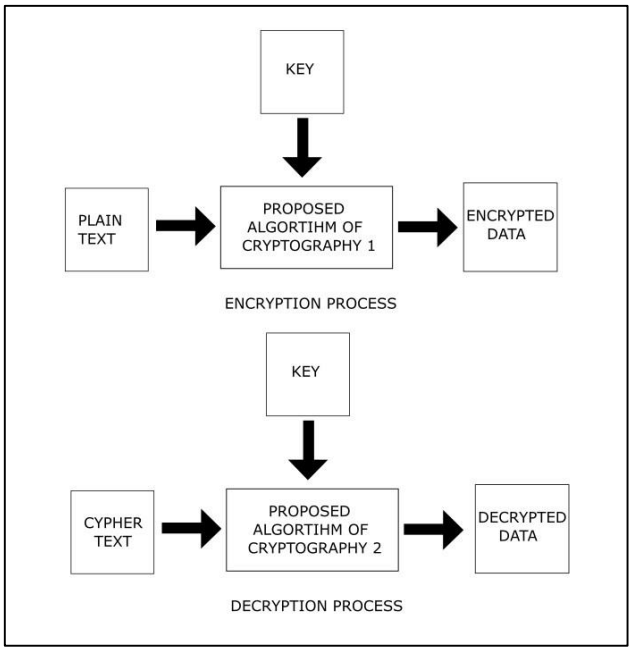

Fig 1. Block diagram of Binary-bit sequencing and multi-stage encryption algorithm [1]

Proposed Encryption Algorithm: Initially we need to define some character values that will used to replace the plain text. Defined characters = 2n/2. N is binary bit sequence.

1. Read the plaintext message from user.
2. Replace the plaintext by their ASCII values.
3. Read a secret key from the user.
4. Perform the XOR of ASCII values with the key provide by user.
5. Converting numerical values in the binary n bit sequence.
6. Converting the received n-bit sequence in the n/2-bits binary sequence.
7. Converting the n/2-bits binary sequence in the decimal format.
8. Changing all the decimal values with respective character from the character table.
9. Transmit the cipher text.

Proposed Decryption Algorithm:

1. Use the same character table used in the encryption process.
2. Reading the cipher text from user.
3. Replacing cipher text by their numerical values.
4. Reading the secret key from the user.
5. Managing the binary bit sequence.
6. Performing the XOR operation of binary bit sequence and secret key.
7. Performing reverse character substitution.
8. Processing the plaintext.

Advantages:

1. Algorithm uses minimum memory.
2. Algorithm works fast and is time efficient
3. Multistage encryption is used by this algorithm
4. Algorithm is quite simple and more secure.
5. It requires n! Attempts to crack, so algorithm is more robust.

Disadvantages:

On an average the encryption and decryption time is comparatively less than Rivest–Shamir– Adleman (RAS) algorithm but more than AES algorithm which concludes that AES is more efficient than Binary-bit sequence algorithm.

B. *Advanced Encryption Standard:*

The Advanced Encryption Standard (AES) is a fast and secure form of encryption that keeps attackers away from our data [2].

Important features of AES:

1. AES is a symmetric key block cipher.
2. AES gives whole specification and design details.
3. AES uses large key sizes.

Operations of AES:

AES does computations on bytes. AES uses 128 bits of a plaintext block as 16 bytes. These are arranged in four columns and rows. AES is variable dependent the length of key. An AES cipher specifies the number of repetitions of conversion rounds that exchange input that's called plaintext, and also the resulting output is termed cipher text.

Encryption:

In this algorithm the input information is taken for encryption. The transform this data into hexadecimal number and perform shift rows operation to remodel this hexadecimal number into rows and column for encryption. In Shift rows operation the initial queue is unchanged. Each byte of the subsequent string is shift individual near the gone. within the same way, third and fourth queue be shifted. In shift rows, transformation may be a permutation. Then perform mix column transformation to convert each column keen on an imaginative line. In column conversion make original column standards by applying expressions to convert the input column. An expression can contain variables, function, operator and column from the transformed input. and so adding some round key to every column to perform the addition of matrix. Finally, XOR the output of the addition of matrix with key.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

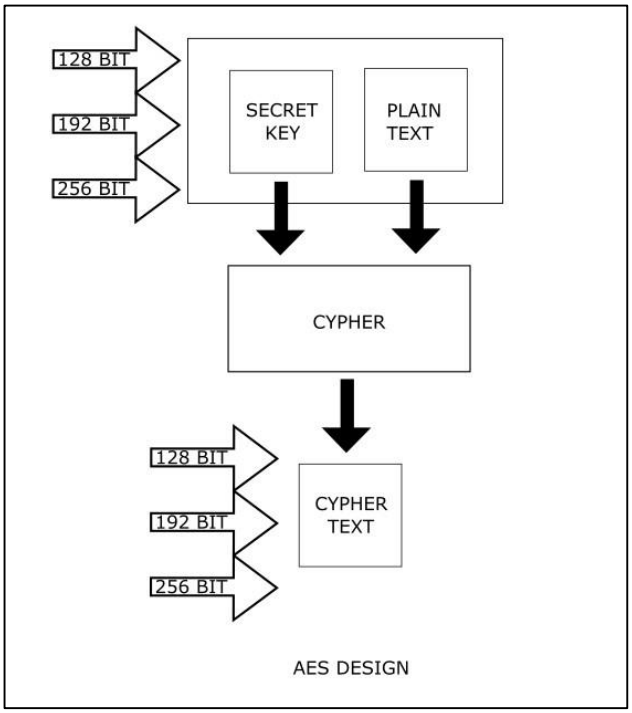

Fig 2. Block Diagram of AES [2]

Decryption:

In this algorithm firstly input file is taken for decryption. At the moment transform this data into hexadecimal number and then perform shift rows operation to remodel this hexadecimal number into rows and column for decryption. In shift rows, the initial queue is gone unchanged. Every byte of the following string be shift individual near the gone. Similarly, third and fourth queue be shifted. In shift rows transformation could be a simple permutation. After that do mix column transformation to convert each column keen on a original line. In column conversion make original columns standards by applying expressions to convert input column. An expression is able to contain variables, function, operator and column from the transformation input. then add some round key to every column to perform.

Advantages of AES:

1. As it is implemented in both hardware and software, it is most efficient security protocol.
2. It uses high length key sizes such as 128, 192 and 256 bits [3].
3. It is used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.
4. It is faster than traditional DES algorithm.
5. Exceedingly difficult to hack any personal information.

Disadvantages of AES:

1. It uses a remarkably simple algebraic structure.
2. Always every block is encrypted in the same way.
3. Difficult to implement with software.

C. An encryption-based secure framework

The solution for a security issue in Internet of Things (IoT) routing is to utilize straightforward protocol with a strength of scrambling data with the private key [4]. For this, arrangement should be done in the existing bundle structure.

ENCRYPTION PROCEDURE

1. let good_keys = {x>0| x belong to unique secret keys}
2. let bit_pattren = unique 7 bit pattern
3. secret_key = random(good_keys) 4. encrypted_pattren = encrypt(bit_pattren, secret_key) so that length(encrypted_pattren) = 7 and decrypt(encrypted_pattren, secret_key) = bit_pattren while decrypt(encrypted_pattren, wrong_key) != bit_pattren
5. encrypted_data = encrypt(data, secret_key)
6. make and send packet
7. exit

Fig 3. Encryption procedure [4]

This procedure can be followed with any routing protocol as it just includes a change to the information part of the client. These keys are likewise put away in each base node alongside the one of a kind ID of the bit. All the client's information in messages are scrambled utilizing an arbitrarily chosen key from the encryption key. On the off chance that the client information is to be encoded, then an atypical 7-bit design is additionally scrambled using a similar key. It can be each of the 1s (111111) or every one of the 0s (0000000) or combination of 0s and 1s. This example is used to limit information unscrambling at the base station as decoding huge information will take even more preparing time and figuring powers.

DECRYPTION PROCEDURE

1. let good_keys = {x>0| x belong to unique secret keys}
2. let bit_pattren = unique 7 bit pattern
3. secret_key = get_next_secret_key(unique ID of sender)
4. decrypted_pattren = decrypt(encrypted_pattren, secret_key)
5. if decrypted_pattren = null then drop packet and exit
6. if decrypted_pattren = bit_pattren then goto step 7 else goto step 4.
7. data = decrypt(encrypted_data, secret_key)

process data

Fig 4. Decryption Procedure [4]

The data is sent utilizing typical routing strategies. The base station first tallies if the received message is scrambled or not which is found on the main piece of client data. In encrypted bundle, the 7-bit design is unscrambled using all the keys and the decoded string is coordinated against putting away piece design and a match is discovered at that point by utilizing coming about mystery key whatever is left of the messages are decoded.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

D. RSA Algorithm:

As the applications of Internet of Things become more and more popular the security requirements become a major factor. There emerges the need of encryption techniques to protect the data communicated between various IoT devices. Comparison of major algorithms is done in the paper to ensure that. There are two types of encryption techniques namely symmetric key and asymmetric key encryption.

The Symmetric key technique has a concept of a private or secret key which will be used to encrypt the information while sending. At the receiver's end, the same key is being used to decipher the message [5]. In Asymmetric key encryption, there is a pair of keys for each receiver called public and private keys. The public key is known to everyone and is used in the process of encoding the data and the only receiver which has the paired private key can decode the message.

RSA is short for Rivest Shamir Adleman which uses Asymmetric key encryption technique to send and receive messages.

The Algorithm:

Key Generation:

1. Two prime numbers considerably large, p and q are taken.
2. The product n = p*q is calculated.
3. Euler's totient function is applied for n-$\phi(n)$ = (p - 1) * (q - 1). An integer e is chosen such that it is co-prime to and lesser than $\phi(n)$.
4. d is computed such that it satisfies the relation- d * e $\cong$ 1 (mod $\phi(n)$).
5. n and e are served as the public key and d is the private key known to the receiver.

Encryption:

1. The message to be sent is transformed to a number m [6]. Encoding will be done to produce the cypher text c as- c = me (mod n).

Decryption:

1. The private key is used on the received cypher text to decrypt the message- m = cd (mod n).
2. With m known, the two initial prime numbers can also be retrieved.

Advantages:

1. Although it uses complex mathematics, it is safe and secure.
2. Sharing of the public key is simple and easy as it is known to everyone.
3. It has a wide range of industry usage.

Disadvantages:

1. When the input message to be encrypted becomes large, the algorithm would be very slow.
2. The encrypted message containing the public key is vulnerable to attacks.
3. The generation of the keys is comparatively slow.

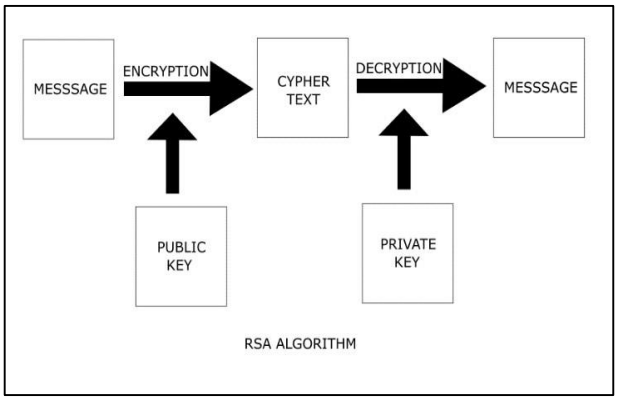

Fig 5. Block diagram of RSA Algorithm [5]

E. Twofish Algorithm:

The Block cypher is a finite state algorithm which is operated on 'blocks' or combination of bits. The initial bit stream is encrypted by the use of a function which takes another sequence of bits called the key to decrypted by the inverse of the function used to encrypt.

The Twofish cypher is a block cypher which makes use of the symmetric encryption process having the input bit size of 128 bits and the key size up to 256 bits [7]. Bruce Schneier first came up with the idea of the Twofish cypher, deriving it from Blowfish and Square.

The Algorithm:

G-Function:

1. It splits the input word into 4 bytes.
2. Each byte is transformed using separate Sboxes which has different keys.
3. The resulting vector of length four, is multiplied by an MDS matrix.

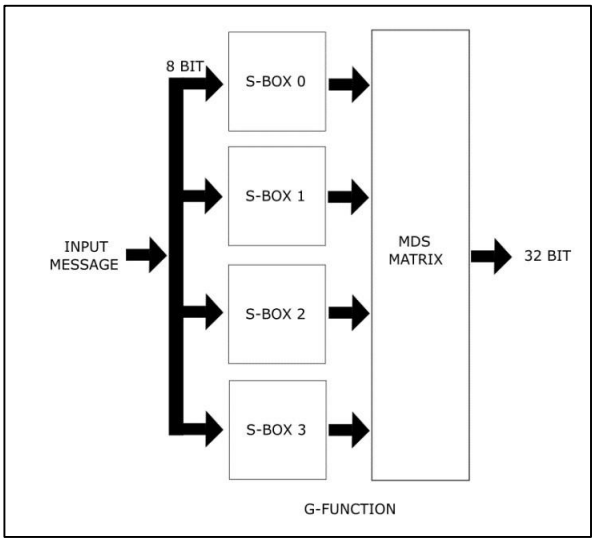

Fig 6. Block diagram of G-Function [7]

Encryption:

1. The input text is divided into four 32-bit words and is XORed and given as input to the g-function in cyclic order.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

2. The PH Transform is used to combine the results of the g-function and the order is swapped for the next sequential round.

Decryption:

1. The sub-keys are reversed and the same procedure is done to decrypt the message.

Advantages:

1. It overcomes the downsides of the algorithms it is derived from.
2. The algorithm is not broken till now.

Disadvantages:

1. As in [8], it is much slower compared to the previous algorithms.
2. The algorithm is not standardized.

F. Hybrid Encryption in Cloud Computing

Cloud computing is a computing process where user store, process and manage the data by remote servers on the internet instead of local server on own computer [9]. It also provides various models to provide security and protect the information from other people. There are many type of Hybrid encryption combining suitable other encryption techniques. A hybrid encryption scheme by integrating RSA and Diffie Hellman to get data security for the services of cloud is one of its kind. The idea of this integration is to exploit secret key cryptography that includes encoding, decoding process speed and public key cryptography which is management of key. Diffie Hellman is an aged encryption technique used internet protocol security.

Methodology:

Hybrid cryptography strategy embrace the integration of both symmetric and asymmetric algorithms for increasingly incredible outcome. Every cryptography strategy involves the scramble and decryption process. In encryption, first information is changed into non-understandable format, which shouldn't be understood easily by any person. To obtain first information from figure, information decoding process is utilized. In this investigation two-time encryption and decoding process is performed in light of fact that the utilization of asymmetric and symmetric process.

Security Issues

1. Data Confidentiality: Due to security reasons users want the information to be read by right people. So, for this, unknown accessing and using information must be stopped.
2. Data Authenticity: Security necessity guarantees the personality of node with which correspondence happens is certified.
3. Data Integrity: The Security necessity in which messages ought not to get altered while exchanging among sender and beneficiary.
4. Data Authorization: Security necessity to guarantee that data dispersal should just from approved sensors.
5. Non- repudiation: It manages re-transmitting of message through a node. A node ought not to preclude retransmitting from claiming officially sent a message.
6. Data Freshness: It manages keeping up and scattering up and coming data by sensor nodes.

Related Work

1. In this paper the authors have proposed a hybrid cryptography method using two symmetric cryptography techniques Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) for security of sensitive data in military data, Banking trades, etc [10].
2. In this, the author used AES and Blowfish algorithm for application in military, bank, in network companies, big websites those control big data base, etc [11].
3. In this, they have proposed hybrid encryption system with Blowfish and RSA for secure storage for healthcare data on cloud because it minimizes the time for encryption and decryption compared to other symmetric techniques [12].

III. CONCLUSIONS

In this paper we have discussed about the importance of various types of encryption.

Table 1. Summary of all encryption methods

Encryption method	Conclusion
Binary-bit sequencing and multi-stage	• Uses minimum memory • Works fast and more secure but it takes more time compared to AES algorithm
AES	• Faster than the traditional DES algorithm making it difficult to hack any personal information • Difficult to implement with software
RSA	Safe and secure and sharing public key is simple and easy but when the message to be encrypted is large, the algorithm would be slow
Townish	• Overcomes the downsides of Blowfish and square algorithms from which it was derived, and this algorithm has not broken till now • Slower than the previous algorithms

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 10, October-2020

Encryption time comparison (ms)			
Plain text size	RSA	AES	Binary Bit
100 bytes.txt	45	63	2
1 kb.txt	62	64	8
2 kb.txt	78	65	24
5 kb.txt	192	112	110

Decryption time comparison (ms)			
Plain text size	RSA	AES	Binary Bit
100 bytes.txt	141	2	2
1 kb.txt	156	2	4
2 kb.txt	169	3	7
5 kb.txt	172	8	69

Fig 7. Time comparison of encryption methods

REFERENCES

[1] I. Hussain, M. C. Negi and N. Pandey, "Proposing an Encryption/ Decryption Scheme for IoT Communications using Binary-bit Sequence and Multistage Encryption," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 709-713, doi: 10.1109/ICRITO.2018.8748293.

[2] Deepika Khambra, Poonam Dabas, " Secure Data Transmission using AES in IoT", International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Volume 6, Issue 6, June 2017 , pp. 283-289 , ISSN 2319 - 4847.

[3] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[4] S. Chaudhry, "An Encryption-based Secure Framework for Data Transmission in IoT," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 743-747, doi: 10.1109/ICRITO.2018.8748523.

[5] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, 2017, pp. 1-4, doi: 10.1109/ICIOTA.2017.8073643.

[6] L. Kumar and N. Badal, "A Review on Hybrid Encryption in Cloud Computing," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoTSIU.2019.8777503.

[7] T. Zhou, "Study on Several Fast Algorithm of Modular Exponentiation in RSA," 2011 International Conference on Network Computing and Information Security, Guilin, 2011, pp. 374-377, doi: 10.1109/NCIS.2011.82.

[8] Pil-Joong Kang, Seon-Keun Lee and Hwan-Yong Kim, "Study on the design of MDS-M2 Twofish cryptographic algorithm adapted to wireless communication," 2006 8th International Conference Advanced Communication Technology, Phoenix Park, 2006, pp. 4 pp.-695, doi: 10.1109/ICACT.2006.206060.

[9] S. A. M. Rizvi, S. Z. Hussain and N. Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes," 2011 International Conference on Communication Systems and Network Technologies, Katra, Jammu, 2011, pp. 76-79, doi: 10.1109/CSNT.2011.160.

[10] M. Jain, and A. Agrawal, "Implementation of Hybrid Cryptography Algorithm", International journal of Core Engineering & Management, Volume 1, Issue 3, pp. 1-8, June 2014.

[11] Ali E. Taki El_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, pp. 669-673, December2013.

[12] P. Chinnasamy, P. Deepalakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography", ICICCT, 2018.

[13] Ritambhara, A. Gupta and M. Jaiswal, "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT)," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017, pp. 422-427, doi: 10.1109/CCAA.2017.8229877.

[14] M. S. Mehmood, M. R. Shahid, A. Jamil, R. Ashraf, T. Mahmood and A. Mehmood, "A Comprehensive Literature Review of Data Encryption Techniques in Cloud Computing and IoT Environment," 2019 8th International Conference on Information and Communication Technologies (ICICT), Karachi, Pakistan, 2019, pp. 54-59, doi: 10.1109/ICICT47744.2019.9001945.

[15] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766407.

[16] E. P. Yadav, E. A. Mittal and H. Yadav, "IoT: Challenges and Issues in Indian Perspective," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 2018, pp. 1-5, doi: 10.1109/IoT-SIU.2018.8519869.

[17] I. B. Aris, R. K. Z. Sahbusdin and A. F. M. Amin, "Impacts of IoT and big data to automotive industry," 2015 10th Asian Control Conference (ASCC), Kota Kinabalu, 2015, pp. 1-5, doi: 10.1109/ASCC.2015.7244878.

[18] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55, doi: 10.1109/WFIoT.2018.8355182.

[19] J. Han, Y. Jeon and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 1116-1118, doi: 10.1109/ICTC.2015.7354752.

[20] R. Chow, "The Last Mile for IoT Privacy," in IEEE Security & Privacy, vol. 15, no. 6, pp. 73-76, November/December 2017, doi: 10.1109/MSP.2017.4251118.