REVIEW OF CRYPTOGRAPHY ALGORITHMS WITH A HYBRID COMBINATION OF AES

[1]Rucha R Dhumne, [2] Dr S. S. Salankar
[1] Mtech Research Scholar, [2] Professor
[1,2] Department of Electronics And Communication Engineering
G.H Raisoni College of Engineering Nagpur. India

Abstract : Cryptography is the art and science of keeping information secure. Cryptosystem plays important role in securing confidential information. In Cryptography first information is store and then transmit data it in a secret form so that only the person who is intended can read and process it. Cryptography is of two types such as symmetric key cryptography and asymmetric key cryptography. In a hybrid cryptosystem, symmetric and asymmetric both the cryptographic algorithms are used. RSA, AES, ECC are some of the most widely used algorithms for hybrid cryptography. The major scope of work has been done using AES. This paper provides the survey of various cryptography algorithms used in hybrid cryptography, checking their efficiency, effectiveness and comparison with other related work.

***Keywords-symmetric* key, asymmetric key, cryptography algorithms, hybrid cryptography,AES.**

I. INTRODUCTION

As the use of digital data is increasing in transmission and processing, data protection is becoming much more important. To meet the safety requirement, cryptography is a common technique which provides security for transmitting electronic data like images, videos. There are two important parameters which are considered while sending information on the public are efficiency and safety. A cryptographic algorithm is widely used today because of its security advantages. Three main requirements of cryptography are authentication, confidentiality, and non-repudiation.

II. CRYPTOGRAPHY GOALS

There are three main goals of cryptography[2].

- Authentication: a process in which a user has to provide their identity to another who does not have personal knowledge of their identity
- Confidentiality: Confidentiality refers to keeping the information secret. The sender encrypts the message using a cryptographic encryption algorithm with a suitable key. The recipient decrypts the message using a cryptographic decryption algorithm with match key that may or may not be the same as the one used by the sender.
- Non-repudiation: Sender or receiver cannot deny a transmitting/received message. The sender of a message cannot later claim he/she did not send it[1].

The cryptographic algorithm has two types which are given below:

1. Symmetric key cryptography algorithm
2. Asymmetric key cryptography algorithm

2.1. Symmetric (Secret) Key Cryptography

Symmetric key cryptography is also called secret key cryptography as it is the oldest technique which is used by users. A secret key which is used by the user in this is called the private key. A secret key can be anything it has been a random letter, a number or else just a word. A secret key which is used to encrypt the data can able to change the content in a particular way so that only authorised receiver can see the original information. [1].

Some Asymmetric key cryptographic algorithms which are trending these days are given below:

1)DES (Data Encryption Standard)
It stands for elliptical curve cryptography, it is one of the most powerful and advances cryptographic standard used my modern systems. As the name suggests it uses elliptical curve theory to produce efficient keys used for public key algorithms. Systems like RSA invent their own keys rather than depending on other security systems. Like other cryptographic systems, it is also used for encryption and decryption of data and exchange of keys but the only difference which makes it more advance is the elliptical curve structure which keeps changing and makes it difficult for the attackers to decode the information. It is efficient and powerful but difficult to design. [13].
2)3-DES(Triple–Data Encryption Standard)
It stands for triple data encryption standard and is practically more advance than normal block cipher DES. In such systems, the data is subdivided by blocks. And then the algorithm is applied. In 3 Des the algorithm is applied thrice to each data blocks which further increase the length of the key and also give efficient encrypted output. This block cipher algorithm is an advanced version

of the DES system and is used widely where computerized cryptography is needed. Being more advanced, it also requires more processing power for generation of bits. [11].

3)RC4 (Rivest cipher 4):

RC4 is a stream cipher which is developed by Ron Rivest. It is also known as Rivest Cipher 4 used for ciphertext generation. In RC4 a bit-wise encryption/decryption is performed where the key length for this is 40-128 bits.RC4 popularly used in transport layer security. The key generation is basically done by the pseudo-random stream [9].

4)AES (Advanced Encryption Standard):

AES stands for advanced encryption standard. It is made by National Institute standard technology (NIST) in 1997 and invented by Vincent Rijmen. AES replace to DES algorithm because the size of the secret key of DES is only 56 bit. Due to the small size of the secret key DES insecure for many application and unknown person hacks the data easily. AS compare to DES, AES is stronger because the size of the secret key of AES is 128, 192, 256 bits are used for encryption and decryption purpose and block size of AES is 128 bits, which is higher than DES.

5)Blowfish:

Blowfish is symmetric block cipher. Blowfish is unpatented and license-free. It can be effectively used for encryption purpose. The block size of blowfish is 64 bit, was designed in 1993 by Bruce Schneider. Blowfish is unpatented so is available free for all users [19].

6)SHA:

SHA or secure hash algorithm is a symmetric cryptographic hash function. It is developed by NIST along with NSA. In 1993 SHA was published as a federal information processing standard. It has following versions SHA-0,SHA-1,SHA-2,SHA-3[12].

2.2. Asymmetric (public) Key Cryptography

An asymmetric key is differing from the symmetric key algorithm because in this sender and receiver use different keys that cannot be derived from each other. A public key is distributed freely where the private keys are kept hidden. A public key used for encryption has to be shared by both sender and recipient . A public key which is used to encrypt the data can able to change the content in a particular way so that only authorized receiver can see the original information. An asymmetric cryptosystem is also referred to as public key cryptosystems [1].

Some Asymmetric key cryptographic algorithms which are trending these days are given below:

1)RSA (Rivest, Shamir and Adleman)

RSA is one of the most important cryptographic algorithm used for highly secure devices. This algorithm is widely complex to get through because it works in the factorization of two or more large prime numbers. It is a known public key asymmetric algorithm, as it consists of both private and public keys. Where one key is kept private and the other is known to both sender at the source and the receiver at the destination. It proves it's security by the amount of data it sends through the digital medium or via modern computers. It is a fast and efficient algorithm but yes difficult to built. Its name RSA is derived from the name of their makers Rivest, Adi Shamir and Leonard Adleman.[9].

2)Diffie-Hellman

When it comes to cryptography, it means two mutual parties will form a secure connection and transfer their key information via a key or data. This algorithm is based on such a simple principle where two parties exchange data which is nothing but a shared secret key. This key is used in symmetric algorithms like AES. The shared secret key is basically a small data or random numbers or password used to unlock the main data bytes. It is quite complex to hack this algorithm because of this difficult structure and mode of exchange. It is different from RSA but similar in solving numeric problems. It is named after it's makers Whitfield Diffie, Martin Hellman and Ralph Merkle. [10].

3)El-Gamal

E1-Gamal is introduced by taher E1-Gamal in 1985. Is the asymmetric public key cryptography which is based on Discrete Logarithm Problems.E1gamal is also used as a digital signature. Each time when the same plaintext is encrypted, it gives a different cipher text. The biggest disadvantage of Elgamal is having cipher text twice the size of the plaintext.

4)ECC

It stands for elliptical curve cryptography, it is one of the most powerful and advances cryptographic standard used my modern systems. As the name suggests it uses elliptical curve theory to produce efficient keys used for public key algorithms. Systems like RSA invent their own keys rather than depending on other security systems. Like other cryptographic systems, it is also used for encryption and decryption of data and exchange of keys but the only difference which makes it more advance is the elliptical curve structure which keeps changing and makes it difficult for the attackers to decode the information. It is efficient and powerful but difficult to design. [7].

III LITERATURE SURVEY

The aim of this paper, which we are already, mentioned that is to provide the survey for various algorithms used for cryptography and different implementation techniques of them. Sangapu Venkata Appaji [1], shows the detail case study of recent advancements on symmetric cryptography techniques from the year 2000 till 2013.

The review of papers that described the most recent algorithms that have been designed during the year 2014 until 2018 are given below.

3.1 During 2014

Prof. S. T. Bodkhe [2], shows how to increase the security of image for transmission over a network up to (16) times in consideration of security of a data or information. While using secret information we need more secure information hiding technique. Instead of one in a single information transmission, a number of spitted blocks gives secure information.

Dudhatra Nilesh, Prof. Malti Nagle [3], proposes the new cryptography algorithm for encryption of data along with the study of other highly used algorithms like AES, DES, Blowfish. The key length for this algorithm is 16 bit. The implementation is totally on the software platform and compares it with other algorithms on the basis of the throughput parameter. The author basically encrypts 128-bit data with the size of the 128-bit key with it.

Hrushikesh S. Deshpande, [4], implements the efficient AES Algorithms on FPGA on the Xilinx ISE 14.1 platform. Author design AES-128 bit algorithm. This proposed architecture consists of a 128-bit symmetric key. This AES design is 3 step approach i.e Top, (1-to 9 round), Last round. Total 4 phase accepted for this algorithm which is proceeding sequential manner. The results of this encryption algorithm provide good performance with a less occupied area.

Ghada F. Elkabbany, Heba K. Aslan [5], proposed a fast parallel-pipelined implementation of AES. In this paper, the design of parallel AES on the multiprocessor platform is presented. This design is based on combining pipelining of rounds and parallelization of mix columns transformation. This analysis increases the degree of improvement of both encryption and decryption by approx 95%.

Saurabh Kumar[6], Shows the improved version of S-box architecture for better performance in the area of delay and power consumption. The implementation of this delayed version is done by programming of Xilinx FPGA with VHDL code also this architecture is implemented on ASIC which also gives better performances of about 16 per cent. The structure of S-Box is basically a multiplicative structure. This new version of S-box is comparing with the conventional structure on the basis of delay and area improvement.

3.2 During 2015

Ijaz Ali Shouka [7], shows the comparison between two most trendier hybrid cryptosystems i.e AES-ECC and AES-RSA which have been evaluated and compared through practical experimentations. According to the final results, a hybrid combination of RSA with AES shows the better performance level in case of encryption and decryption with the time of 0.994 seconds as we compare it with a hybrid combination of AES with ECC with the time of 7.225 sec.

Dr Amit Babiker[8] shows the study of various techniques and algorithm like ECC, AES, RSA used for the secured communication has been done for encryption of data if we choose a longer key length it consumes more power. According to the author according to the comparative analysis of the above mention algorithm, RC4 has the redeeming feature of being fast comparatively, than the above mention algorithms. ECC is based on elliptical curve cryptography, is hard to solve but there are many attacks that can be successfully broken ECC if the chosen implementation is poor for good security one must use safe curves. ECC structure is complex in the calculation so this hybrid structure leads to wastage of memory and which cause unnecessary wastage of electric power.

Akinyele Okedola[9], shows the Cryptosystem Performance Evaluation of RSA and RC4 using image and text File-This paper present a fair comparison between the two commons and used algorithm RSA and RC4 in the data encryption field. The major factor to determine the performance is the algorithm speed to encrypt/decrypt data blocks of various sizes. Rc4 seems to be faster in encryption and decryption and RSA is highly complex due to modular exponentiation is not usually acceptable for encryption of large files. RC4 is the simpler of two algorithms to implement. There are no computational optimization is likely not necessary.

3.3 During 2016

Aakash Gore[10], Shows the hybrid cryptography by combining Blowfish and Hash Algorithms (SHA). this proposed system implemented on an open shift public cloud. In this work, SHA and MD5 are used for message digest algorithm which uses for calculating a hash value. This proposed model improves the security issues related to cloud models and also gives file exchange protection. This work is on a hybrid algorithm which lies on symmetric and asymmetric cryptography on cloud computing.

Ankita Varma [11] shows a comparison between different cryptographic algorithms. This paper presents a comparative analysis of different algorithm like AES, DES, Blowfish, RSA, 3DES. Author compares these algorithms on various parameters. Results state that AES and Blowfish are the most secure and efficient algorithm. The speed and power consumption of these algorithms are better as compare to others. In the case of an asymmetric encryption algorithm, RSA is secure and can be used for application in wireless networks.

Table1: Comparative analysis of different cryptography algorithms

Algorithms	DES	AES	3DES	Blowfish	RSA
Year of use	1977	2000	1978	1993	1977
Key Size	56-bit	Up to 256-bits	Up 168-bits	32-bit	1024-bits
Power Consumption	Law	Law	Law as compared to DES, AES, Blowfish	High	Very High
No of rounds	16	Up to 14	48	16	No rounds
Size of Block	64-bit	128-bits	64-bits	64-bits	Min 512-bits
Avalanche Effect	Less than AES	Faster	Medium	Fastest Except when changing key	Slower

V. Kapoor [12], proposed a hybrid cryptography technique for improving network security. This hybrid technique uses algorithms like RSA, DES and SHA1. The implementation of the proposed techniques is provided using the JAVA technology and their performances like space, time and complexity is measure and compares with the traditional RSA cryptography. According to the obtained results, this technique provides efficient and complex cipher with less resource consumption. This process also reduces the key size and improving the complexity of the key generation process. Results state that this proposed technique found efficient and improved ciphertext during comparative performance analysis.

Mukta Sharma [13], gives you the highlights of primary flow, history, implementation, significance and drawbacks of DES. In this proposed work DES Algorithm accepts 64-bit data blocks which are basically based on Feistel Network. The author says that we can make DES more vulnerable by reducing the key size of the algorithm but then it will not be able to use by military or government for protecting the confidential data.

3.4 During 2017

Flevina Jonese D'souza[14], presented work on some modification related to the AES system to protect the data encryption from cyber attacks. The modification is basically implementing a hybrid system with a dynamic key and dynamics-box generation. The system will have a data of 128 bit and the generated key will also be of 128 bit. The key will be generated through time function. The dynamics-box will be generated through xor operation with cipher bytes. The sender and receiver will be connected via the dynamic key. The decryption of the system is basically the inverse algorithm of the s-box from static to dynamic. They have also given a clear example for the encryption process and the result they got clearly prove that the proposed system of AES with a hybrid approach, will have enhanced the security of AES.

Vikrant Shende[15], proposed a hybrid combination of AES-RSA. This hybrid design is synthesized using Xilinx ISE platform. In this hybrid combination encryption is performed by AES algorithm and for encryption and decryption of that AES key, RSA is used. This technique decreases the complexity of the system, but makes RSA less secure. In the architecture designing of AES, a table lookup is used for optimization of purpose. The author shows that using this technique, less power is consumed and performance is faster in software and as well as in hardware.

Amal Hafsa[16], proposed the image encryption/decryption cryptography model for image security. This proposed system is used as an AES algorithm with the key length of 256-bits. This key is considered as the most secure key length against different attacks. For the implementation of this 256-bit AES, FPGA ALTERA board is used and the design of this system is mode using NIOS II softcore processor for the analysing of results MATLAB is used. This technique improves the speed and image securely [9]

Sheetal Jonwal[17], shows the improved version of AES Algorithm. This design is implemented on the Xilinx ISE design suite. For transmitting input/output data to the FPGA, MATLAB is used. For encryption of data 128-bit data is considered along with the 128-bit size of a key. This design used the SDK tool for implementation, which deals with hardware designs. The SDK bit gives provision to create a software platform in C language. This technique is used for optimizes area consumption. [10]

3.5 During 2018

S. Aruna Sankaraligam[18] presented a proposal of a hybrid model to ensure security, validity and integrity assurance of data during transmission. This model is an implementation of two cryptographic algorithms like SHA-1 and AES. Implementation of these hybrid techniques is basically on the internet of things. This proposed model gives you law power consumption and low cost. This paper also presents an overview of another model that why AES was preferred over other algorithms.

Marwan Ali Albahar, Olayemi Olawumi,[19] proposed work the researchers had implemented a hybrid cryptographic system consist of three major encryption technique such as AES, RSA and Twofish algorithm. This hybrid cryptosystem works primarily for Bluetooth modules by enhancing security and transmission capability. The system is also compared with the old modules and hence found to be more efficient for wireless data transmission with higher security and high data privacy. The encryption step is further processed by encryption through AES 128 bit key, which is connected parallel with the Twofish algorithm. When the key is generated, the key is then used to encrypt with the 1024 bit key of RSA. The same process is reversed in the case of decryption of the data. The encryption is done in such a way that the data transferring through the air should be highly protected. The system hence gives the confidentiality of messages transmitted over the network will be guaranteed.

Omar G. Abood [20], gives the survey of the most important cryptography algorithm like DES, AES, Blowfish, ECC etc. these algorithms are studies and analysed well to enhance their performance. The comparison between ciphers shows that the symmetric algorithm is faster than the asymmetric, where results also prove that AES is best in security, flexibility when compared to others.

IV. CONCLUSION

From the literature survey, it is concluded that all cryptography algorithms have their own advantages and disadvantages. Many algorithms are available these days for encryption and decryption purpose. Some are very secure for network security but they require more time for encryption and decryption. Whereas some are taking less time, they are easy to crack. Hybrid Cryptosystem is introduced in which symmetric and asymmetric both the cryptographic algorithm used over their advantages. Combinations like AES-RSA, AES-ECC and DES-RSA were discussed in some of the papers. Some have more power consumption due to a longer key length whereas some have complex computation which increases the power and memory. The study indicates that maximum use of AES can be done in the hybridization of various algorithms due to its advantage of higher security and low power consumption on the other hand RC4 has the feature of being fast comparatively, than the above mention algorithm also it does not have complex computation with lead to wastage of memory. To remove the drawbacks of existing systems to increase the security, speed, memory and electric power, an AES and RC4 algorithms can be designed as a hybrid encryption model and compared with existing algorithm AES as future work.

REFERENCES

[1]S. Appaji and D. Acharyulu, "Recent Advancements on symmetric cryptography techniques-A comprehensive Case Study", *Global Journal Of Computer Science And TECHNOLOGY: Graphics & Vision*, vol. 14, no. 2, p. 13, 2014.

[2]M. Qamruddin Khizrai and P. Bodkhe, "Image Encryption using Different Techniques for High-Security Transmission over a Network", *ISSN*, vol. 2, no. 4, p. 8, 2014.

[3]Dudhatra, N. (2014). The New Cryptography Algorithm With High Throughput. *2014 International Conference on Computer Communication and Informatics (ICCCI-2014)*, p.5.

[4] Deshpande, H., Karande, K. and Mulani, A. (2014).Efficient Implementation of AES Algorithm on FPGA. *International Conference on Communication and Signal Processing*, p.5.

[5]Elkabbany, G., Aslan, H. and Rasslan, M. (2014). A Design of Fast Parallel-Pipelined Implementation of AES:Advanced Encryption Standard. *International Journal Of Computer Science & Information Technology (IJCSIT)*, 6(6), p.21.

[6]S. Kumar and V. Sharma, "Law latency VLSI Architecture of S-BOx for AES Encrption",p.4,2014.

[7]I. SHOUKAT and A. AL-DHELAAN, "Practical Evaluation of Hybrid Cryptosystem", *Recent Advances in Computer Science*, p. 8, 2015.

[8]S. Mohammed Koko and D. Babiker, "Comparison of Various Encryption Algorithms and Techniques for improving secured data communication", *IOSR Journal of Computer Engineering*, vol. 17, no. 1, p. 8, 2015.

[9]A. Okedola and Y. Asafe, "RSA and RC4 Cryptosystem Performance Evaluation Using Image and Text File", *ISSN*, vol.6,no.5,p.6,2015.

[10]Gore, A. (2016). Hybrid Cryptosystem using Modified Blowfish Algorithm and SHA Algorithm on Public Cloud. *International Journal of Computer Applications*, 155(3), p.5.

[11]Verma, A., Guha, P. and Mishra, S. (2016). Comparative Study of Different Cryptographic Algorithms. *International Journal of*

Emerging Trends & Technology in Computer Science (IJETTCS), 5(2), p.6.

[12]Kapoor, V. and Yadav, R. (2016). A Hybrid Cryptography Technique for Improving Network Security. *International Journal of Computer Applications*,141(11), p.6.

[13]Mitchell, C. (2016). On the Security of 2-key Triple DES. *IEEE*, p.8.

[14]F. D'souza, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach",*International Conference on Computing,Communication and Automation*, p. 6, 2017.

[15]V. Shende and M. Kulkarni, "FPGA based hardware implementation of hybrid cryptographic algorithms for encryption and decryption", *ICEECCOT*, p. 8, 2017.

[16]A. Hafsa and A. Sghaier, "Image Encryption/Decryption Design Using NIOS II Soft Core Processor", *ICMIS*, p. 4, 2017.

[17]S. Jonwal and P. Shingare, "Advanced Encryption Standard (AES) implementation on FPGA with hardware in loop",*ICEI*,p.4,2017.

[18]S. Sankaralingam and G. Usha, "A hybrid cryptographic an algorithm based on AES AND SHA1 in RFID", *International Journal of pure and applied mathematics*, vol. 118, no. 11, pp. 835-840, 2018.

[19]M. Alabahar and O. Olawumi, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption", *Scientific Research Publishing*, vol. 9, p. 8, 2018.

[20]A. Omar, "A survey on Cryptography Algorithms", *International Journal of Science and Research Publications*,vol.8,no.7,2018.