International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 11 Issue 3 Series I || March 2022 || PP 01-05

Comparative Analysis of Some Selected Cryptography Encryption Algorithms

Ayannusi A.O[1] Olusanya O.J[2] Oloyede E.O[3]
[1](Cisco Department, Ogun State Institute of Technology Igbesa, Nigeria)
[2](Cisco Department,Ogun State Institute of Technology Igbesa, Nigeria)
[3] (Cisco Department,Ogun State Institute of Technology Igbesa, Nigeria)

ABSTRACT : *Internet of things is comprised of smart machines interacting with other machines, objects environments, and infrastructure. As a result, the huge volume of data is being generated; so the necessity to protect such data have become greater by using cryptography technique. Cryptography is a method of transforming information into such form that it is not readable and understandable and then re-transforming that information back to its original form.*
The two most accepted and used cryptography techniques are symmetric and asymmetric. In this paper, extensive research on the various cryptographic algorithms will be examined and compared to determine the best combination with Rijndael algorithm in other to improve the security of the Internet of Things.
KEYWORDS *Cryptograph, Encryption, Symmetric, Asymmetric, DES, 3DES, RSA, Rijndael, Blowfish & IoT.*

Date of Submission: 01-03-2022 Date of Acceptance: 11-03-2022

I. INTRODUCTION

There are so many encryption algorithms that are present and in use in Information Technology today. Encryption is one of the most efficient data and information protection that are currently available. Encryption solutions implement cryptosystems that utilize one or more cryptography algorithms. Daily, new encryption techniques are discovered. Encryption is the method of transforming plain text into ciphertext. Most times, these solutions combine asymmetric and symmetric cryptography as different encryption algorithms have different strengths.

The Encryption algorithms can be group into asymmetric (public) and symmetric (private) keys encryption. In symmetric key encryption, only one key is used to encrypt and decrypt data [1]. There are so many examples of strong and weak keys of cryptography encryption algorithms like RC2, DES, 3DES, RC6, BLOWFISH, and AES.

Usually, the key distribution problem is solved using asymmetric key encryption or public key encryption. In the Asymmetric keys encryption algorithm, two keys are used, private and public keys [1]. Asymmetric encryption methods are 1000 times slower than symmetric techniques because they require more computational processing power.

[2], the symmetric algorithm includes a class of algorithms for cryptography that uses the same cryptography key for the sole purpose of encryption of plain old text and the decryption of the ciphertext. Symmetry encryption is the earliest encryption method. The key that is utilized shows a shared secret between the two individuals to uphold a private information contact. Accessing the same shared secret key by the two individuals is one of the major problems of symmetric key encryption when it is being compared to a public key encryption algorithm.

It is not a better option to use a private or symmetric key encryption algorithm where it makes use of a public network for sharing the key. The opportunity for snide insertions and alteration is greater in symmetric cryptography technique [2].

Security and privacy issues represents a very important component that would allow the widespread adoption of Interent of Things technologies and applications. With no measure in place that would guarantee the level of confidentialilty, auathenticity and privacy, people are unlikely to adopt internet of Things in a large scale. Though, cryptography algorithm play a critical role in information security.Choosing an appropriate or best cryptography algorithm can be a bit difficult or confusing . This paper, provides a comparison of various cryptographic algorithms and find the best available among others that would provide security to Internet of Things

II. RELATED WORK

In this section, various methodologies and techniques for the encryption technique used by various papers are delivered.

Cryptography is the technique and body of knowledge of securing information for art and the science of protecting information from the unsolicited person and transforming it to a form that is undisguisable by its intruder either through storing or when it is on transits. The main aim of cryptography is to keep data secure from unauthorized persons [3]. Also, cryptography is the study and practice of secure communication in the presence of a third party, it constructs and analyzes protocols that are useful in surmounting the effect of the enemies [2]. Confidentiality, authentication, integrity, non-repudiation, and access control are various goals of cryptography to avoid security issues [4].

Asymmetric cryptography algorithm is different from symmetric cryptography algorithm in the manner that they use pairs of keys; as opposed to the symmetric encryption algorithm that uses one key for both encryption and decryption, the asymmetric utilize the first key for encryption while the second key is used for decryption [2]. Asymmetric key cryptography otherwise regarded as public key cryptography has two mathematically connected keys which are employed. Generally, the secret key is also known as a decryption key whereas the encryption key is otherwise named a public key because it is transmitted to anybody that needs to transmit encrypted information [2].

A secret key sometimes can be a simple string of haphazard characters, a number, or a word. Secret key is used on the plain text to convert its information with plain text to change its content which is done by shifting each number in several places. The symmetric key algorithm has many advantages in the sense that it is efficient and secure, execution at a very high rate does not use much memory and processor time. Likewise, it suffers from key management and distribution problems, coupled with the fact that it cannot sign a message digitally [4]. The problem associated with symmetric is the key exchange and trust with parties that shared a private symmetric key. However asymmetric helps to solve this problem by encrypting the hash using a private key that is only known to an individual [5].

The symmetry key always seems to have the benefit of not utilizing too much computing power, since only a single key is being used for symmetric encryption, symmetry encryption algorithm are always less complex as compared to asymmetric algorithms. It has the advantage of low error propagation which means an error in the encryption process affects only the character as each symbol is separately encoded [2].

The risk of getting to know the asymmetric key cryptography is much less as the private key does not have to be shared. However, an asymmetric algorithm is not as fast as a symmetric algorithm as it needs more computation for its operation [5]. In most technologies, a hybrid method is being employed by efficiently incorporating asymmetric and symmetric encryption techniques which are used for message sending purposes. The Symmetric encryption method which causes less overhead is used for key sharing to establish secure communication [2].

Asymmetric encryption algorithm total number of key required is smaller when compared to the symmetric case because one key is associated with one party. Also, the asymmetric key will not only be generally used to implement digital signature schemes that include non-repudiation; it may also provide a greater degree of security [5]. At the same time, comparing symmetric and asymmetric encryption, it is found out that asymmetric cannot only cause overheads, but it also has a low speed and needs extra processing power for encrypting and decrypting message content [3].

There are so many examples of weak and strong cryptography encryptions algorithms like RC2, DES, 3DES, RC6, BLOWFISH, and AES.

III. SUMMARY AND DEDUCTIONS FROM REVIEWED WORK

Simple and easy Evaluation methodology was used in this research, different types of the encryption algorithms and resources such as manuals, research papers, and source codes were also studied. On the premise of some criteria, each cryptographic algorithm was evaluated.

A symmetric key algorithm is a class of cryptography technique that makes use of an identical keys for encryption and decryption of ciphertext while asymmetric uses two keys: a public key is utilized for encryption and a private key is utilized for decryption. We have so many weak and strong cryptography encryptions techniques such as TWOFISH, AES, Elliptic Curve Cryptography, RC2, Rijndael, DES, RSA, Diffie- Helman, DES, and 3DES.

Data Encryption Standard (DES) is the predecessor of the Rijndael algorithm that was not only vulnerable to brute force attack, it is also vulnerable to cryptanalysis attack. Though it is still in use, it has proven insecure for big organizations and governments.

3DES is a better encryption algorithm to DES as it is three times the encryption level of DES and has an average safety time. However, it is slower than the other block cipher methods and also exposed to differential and related key attacks.

BLOWFISH is a symmetric and one of the topmost common public domain encryption algorithms that utilize 16 rounds like DES. Each round contains dependent permutation and data-dependent substitution for its operation. It is simple, fast, and compact block encryption cryptography that has a variable length that gives room for a tradeoff between security and speed. Blowfish suffers from weak keys which sometimes makes its reliability questionable.

IDEA is also a symmetric key encryption algorithm that bases its concept on substitution permutation structure. It has powerful impenetrable protection against differential cryptanalysis and at the same time make utilizes numerous group operations to improve its strength also uses multiple group operations to increase its strength against familiar attacks and is also susceptible to different classes of weak keys.

TWOFISH is a symmetry key block cipher encryption algorithm that contested for the Advance Encryption Standard but was not selected due to standardization. It employs 16 rounds-Feistel networks with extra whitening of the input and output. Twofish is known for its flexibility, fast and, has a variety of implementation tradeoffs. It was designed with a smart card in mind and can decrypt and encrypt at faster speeds. It performs well on a wide range of platforms and applications while retaining speed and efficiency when it is implemented on software and hardware.

MARS is a symmetric cipher key block technique that is built on a separate structure. It uses 128-bit plain text with 32 rounds and the variable key length including multiplication data-dependent rotation. It provides improved security and speed more than 3DES and DES but it is the most complicated out of all the AES candidates. Robustness which was its main design goal happened to be its main strength. However, MARS contains more fail-stop mechanisms than other finalists. Apart from the fact it is not suitable for smart card implementation and is relatively complex to analyze there are also no significant limitations in MARS.

SERPENT is a symmetric key method that is built on substitution- permutation network structure. It has 128 bits of plain text with 32 rounds and a separate variable key length of 128, 192, and 256. It uses two different modes of implementation which are standard and bit-slice mode. The main advantage of the serpent is its conservatory number of rounds nature and unlike MARS SERPENT has no fail-stop mechanism. There is no limitation except that the 32 rounds make it difficult to execute and slower on mini blocks.

RC6 is the most elegant, simple, and easiest to understand out of all the AES candidates. It is the strengthened version of RC5 and works with 20 rounds. Feistel structure work on 32 bit with modular multiplication, XOR with addition. Its main advantage is its simplicity and speed which makes it suitable for its current design. The main problem is its sole point of failure and issues relating to the number of rounds it uses. Full arbitrariness, weak keys, and the fact that it does not measure up to 17 rounds of the algorithm are the other limitations it possesses.

Rijndael algorithm is the adopted AES by NIST to replace DES after it was discovered that it is vulnerable and can be easily cracked. Rijndael is a symmetric block cipher algorithm that utilizes 128, 192, and 256 key sizes. It makes no use of the Feistel network rather, its operation is built on substitution and permutation network. It is more protected, fast, hard to crack, and very efficient than DES.

Rijndael has the advantage of not being susceptible to any attack apart from brute force attack. It performs and works comfortably on a broad variety of hardware frameworks from 8-bit smart cards to great performance computers. It also performs well on software and the fact that it can operate on low RAM devices make it stand out from all other encryption algorithms. However, its limitation is that the inverse cipher is less suited to be implemented on a smart card than the cipher itself. Though when compared with others it is still faster and better.

RSA is the most popular public key algorithm that was developed by Rivest, Shamir, and Adleman. It can encrypt information without necessarily have to exchange the private key separately. RSA is too slow for encrypting a large volume of data but it is widely used for key distribution. RSA has the disadvantage that it is not efficient for both hardware and software implementation.

Elliptic Curve Cryptography (ECC) is public key cryptography. It is a situation where a user that is involved in communication has a pair of keys, a private and public key, and a set of undertakings connected with the keys to the cryptographic process. Elliptic curve cryptography (ECC) can offer a similar degree and sort of security as RSA though with considerable concise keys it can be implemented on smart cards. It is also becoming increasingly important for wireless communication. It is the most suitable public key cryptography scheme for use in a constrained environment. And again, its efficiency and security make it an attractive alternative to conventional cryptosystems like RSA and DSA.

Diffie-Hellman key exchange requires two different keys and these two numbers are known to both senders and receivers. A Diffie-Hellman protocol has a Certificate Authority which is used to prevent man-in-the-middle attacks.

EAP- CHAP provides a fundamental structure for authentication and operates efficiently over a protected line. It helps by solving the authentication and authorization problem. However, CHAP requires that the secret be available in plaintext form

Para meter	DES	TWO FISH	Mars	Serpent	RC6	BLOW FISH	Rijndael	ECC	RSA	Diffie-Helman
Key Used	Same key Key used For Encryption & decryption	Same key Key used For Encryption & decryption	Same key Key used For Encryption & decryption	Same key Key used For Encryption & decryption	Same key Key used For Encryption & decryption	Same key Key used For Encryption & decryption	Same key Key used For Encryption & decryption	Difference key Used for encryption and decryption	Difference key Used for encryption and decryption	Key Exchange
Types of encry yption	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric	Asymmetric
Key Length	56 bits	128, 192 & 256	Variable 128 to 448 bits in multiples of 32-bit	128, 192 & 256	128, 192 & 256	32 bits to 448 bits	128, 192 & 256	Shorter key length	>1024 bits	Key Management
S Speed	Fast	Fast	Fast	fast	fast	fast	faster	fast	Not so fast	slow
tType of s structure	Permutation & Substitution	Feistel	Heterogeneous	Substitution permutation network structure	Feistel	Permutation & Substitution	Feistel	Modular arithmetic (Elliptic curve)	Multiplication of prime numbers	
Number of Rounds	I6 rounds	16 rounds	32rounds	32 rounds	20 rounds	16 rounds	10, 12 & 14	Nil	Nil	Nil
Security against attack	Brute force attack	No known attack	No known attack	No known attack	Differential Attack	Dictionary attack	Brute force Attack & Side channel		Timing attack	Eaves dropping
I Implement aaction	suitable For hardware but slow in software	Efficient in Software Implemen tation	Suitable for Hardware & Software Implementation		More efficient In software Than hard Ware implem entation	Suitable for Hardware & software	Very efficient For hardware And software	Efficient in Software Implemen tation	Not sufficient for hardware & software	Nil
LLow Ram & constrai I ned ddevices	Not suitable For low RAM And constrained devices	suitable For low RAM And constrain ed devices	suitable For low RAM And constrained devices	Not suitable For low RAM And constrained devices	Suitable for low RAM And constrain ed devices	Not suitable For low RAM And constrained devices	Suitable for low RAM And constrain ed devices	Suitable for low RAM and constrained devices	Not suitable For low RAM and Constrainedevices	Nil
Block size	64	64	64	64	128	64	128		Variable	
S Security	Not secure enough	secure	secure	secure	Good Security	Highly secure	Excellent secure	Well secure	Very secure	secure

Table 1 showing the comparison among different encryption techniques

IV. DISCUSSIONS AND SUMMARY

The block size plays an important role in encryption and decryption. A higher block size produces higher security with all other factors being equal. As a result, the Rijndael block of 128 bit is twice bigger than all other symmetric encryption algorithms under consideration. Another important evaluation is the number of rounds that is utilized for encrypting and decrypting procedure. The addition in the number of rounds will invariably enhance the security level. BLOWFISH and DES have 16 rounds of procedure a while Triple DES has three times of DES (48 rounds). Rijndael has a separate amount of rounds depending on the key size. MARS and are the best participant when we consider the number of rounds as they both have 32 rounds.

The major issue with the symmetric key algorithms is brute force attacks. With a longer key length, the feasibility of this attack is reduced, DES has the weakest key of 56 bits. IDEA has 12 bits which are still average, TDES has 168 bits with good resistance against attack. RC6 and Rijndael have a variable key length of 128, 192, and 256 that produces a higher key combination. BLOWFISH uses 488 bits which is the longest and strongest as a brute force attack is concerned. RSA does not need a key exchange which invariably increases the security but reduces the speed of the algorithm. The symmetric algorithms like Rijndael, BOWFISH, RC6 are much faster than asymmetric like RSA.

From the table above, it shows that symmetric algorithm RC6, BLOWFISH, RIJNDAEL TWOFISH are deemed as secure and efficient based on high security and less limitation. The comparison of symmetric with that of the asymmetric RSA, Diffie-Helman, and ECC are more secure than any symmetrical cryptography algorithms.

In addition, it can also be seen from the above table that Rijndael and ECC are not only both efficient and suitable for hardware and software implementation they are suitable for low RAM and constrained. Though DES, TWOFISH, BLOWFISH are efficient and suitable for hardware and software implementation, they are not efficient for low RAM and constrained devices. MARS is also suitable for hardware and software implementation and equally efficient in low RAM and constrained devices but it has a small block size compare to Rijndael which makes Rijndael more secure than MARS.

V. CONCLUSION

Internet of thing is all about physical "things" Hackers or attackers that have access to the Internet of Things devices will not only just perform the usual digital attacks such as moving money, stealing data, or shutting down websites; but also, they can cause damage by interfering with infrastructures like traffic signals and electrical grids thereby putting lives at risk by tampering with elevators, airplane and healthcare devices. Because of the worldwide connectivity and the sensitivity of applications, security is a big requirement when it comes to the Internet of things.

This paper uses an analytical approach on various symmetric algorithms like DES, MARS, TDES, SERPENT, BLOWFISH, TWOFISH, Rijndael, etc. and asymmetric encryption algorithms such as RSA, ECC, and Diffie-Hellman. The paper helps in highlighting their advantages, strengths, and limitations. Asymmetric cryptography algorithms are better in terms of providing security to information but they take more time for processing and require more memory, invariably, they are slower than symmetric encryption cryptography algorithm. For better security and optimization, the hybrid of asymmetric and symmetric when combine would produce a good result

In practice, our proposed approach would be the combination of Rijndael and Challenge Handshake Authentication Protocol (CHAP). Using this hybrid would allow the respective strengths of these two kinds of encryption and provide more effective robust, reliable security for the internet of things. Rijndael, on one hand, would be used for encryption and decryption while Challenge Handshake (CHAP) on the other hand will provide authentication that would help in solving the problem of the internet of things because of their effectiveness in low RAM and constrained devices like smart cards and the internet of things.

VI. RECOMMENDATION

For further research, this work can also be extended by implementing the hybridized cryptography encryption algorithm on the internet of things devices like a raspberry pie with low power and memory consumption

REFERENCES

[1]. Yogesh Kumar, Rajiu Munjal, Harsh Sharma (2011) Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and counter measures. International Journal of computer science and management studies. Vol, 11 issue 03, Oct 20111 (ISSN): 2231 -5268.

[2]. Swapna B Sasi, Dila Dixon Jesmy Wilson (2014) A general comparison of symmetric and Asymmetric cryptosystems for WSNs and an overview of location based Encryption Technique for improving security. IOSR Journal of Engineering (IOSRJEN) Vol 04, issue 03.

[3]. Tannu Bala, & Yogesh Kumar (2015). Asymmetric Algorithms and symmetric Algorithm. A Review. International journal of computer Application. International Journal on Advancement in Engineering Technology

[4]. Ritu Tripathi & Sanjay Agrawal (2014). Comparative study of symmetric and Asymmetric Cryptography Techniques. International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348-4853

[5]. Thornsteison book page 99 Tuesday, July 29, 2021 (Asymmetric Cryptography

Ayannusi A.O, et. al. "Comparative Analysis of Some Selected Cryptography Encryption Algorithms." *International Journal of Engineering Science Invention (IJESI)*, Vol. 11(03), 2022, PP 01-05. Journal DOI- 10.35629/6734