IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct. 2018 E-ISSN: 2347-2693

# IMPLEMENTING HYBRID CRYPTOGRAPHY ALGORITHM TO ENHANCE THE SECURITY IN CLOUD COMPUTING

**S. Rajendira Kumar[1*], A. Marimuthu[2]**

[1]Govt. Arts College, Coimbatore, India
[2]Dept. of Computer Science, Govt. Arts College, Coimbatore, India

[*]*Corresponding Author: rajendirakumarphdscholar@gmail.com*

**Available online at: www.ijcseonline.org**

Accepted: 10/Oct/2018, Published: 31/Oct/2018

***Abstract*-**Nowadays, both public and private sector organization have come to be increasingly dependent on Digital Statistics Processing. These Virtual data are going by means of an insecure channel from one location to any other location via networks and anyone can get that critical information without the knowledge of the sender. For protecting those crucial records, Cryptography plays a vital role in community protection. Many Cryptographic algorithms are applied by the Studies Community all around the world. Also they had some limitations and implemented for precise packages, Key size or Block size restricted to some minimum number of bits. This paper provides an implementation of Symmetric and Asymmetric Cryptography techniques and also it elaborates the Hybrid Cryptography techniques by fusing the Cryptographic algorithms. A comparison has been conducted for those Algorithms at different settings such as Sizes of data blocks, Throughput, Encryption Speed and Decryption speed. Finally, the Performance Metrics shows the better performance of the Hybrid Cryptographic Technique.

***Keywords*-** Cryptography, Encryption, Decryption, AES, RSA

## I. INTRODUCTION

In the digital world Data Communication and information security plays an important aspect in the recent past years. With the rapid growth and practice of internet for industrial purpose, safeguarding the potential data ensures the fact of data security and authenticity is very vital. At first, the internet designed for studies and academic purpose, no longer for business packages. The increase in the customers of the internet, the existing safety framework became insufficient for current packages and software program.

Cryptography is the technology of using Mathematical calculations to encrypt and decrypt the confidential data. It provides a manner of methodology to save the Sensitive data and transmit into some format, in order that it can't be examine by anyone besides the particular Recipient. This method is extensively used to safeguard a fact that traverses over open and unsecured networks. Many Cryptographic algorithms have been implemented by the Research groups in all around the Global, but all the algorithms had some obstacles and carried out for Precise programs, Key size or Block size constrained to 64, 128 and 256 bits.

## II. CRYPTOGRAPHY

Cryptography is otherwise called as a study of Secret Writing. It is the technological or artwork of encompassing the concepts and methods of converting an intelligible message into one form and then it remodel the message again to its original form. Cryptography offers for secure communication within the presence of malicious third parties called challengers or strangers. A cryptosystem defines a couple of information variations referred to as encryption and decryption [1]. Encryption is a technique, which is used to convert the plain text into the ciphertext using an encryption key. Decryption uses the decryption key to transform cipher textual content to plain text i.e. the secret data. The essential necessity in security is to cover statistics from beside the point public or malicious attackers. This requirement has given birth to distinctive kinds of cryptographic primitives such as Symmetric Cryptography and Asymmetric Cryptography, Hashing Techniques, DS i.e. Digital Signature, MAC i.e. Message Authentication Codes and so on.

### 2.1 SYMMETRIC CRYPTOGRAPHY

In symmetric encryption, a key is shared among the sender and the receiver that is saved as a secret key from the intruder. One of the popular symmetric algorithms i.e. Advanced Encryption Standard (AES) is gaining reputation due to its higher safety and performance than its ancestors. By way of a symmetric cipher, AES stakes a secret key to encrypt and decrypt any message and operates on fixed block [2]. AES may be constructed to apply 3 special key lengths and the resulting algorithms are named as AES-128,

© 2018, IJCSE All Rights Reserved 

AES-192 and AES-256 respectively to signify the key size in bits.

### 2.2 ASYMMETRIC CRYPTOGRAPHY

Nothing like the Symmetric Cryptography, Asymmetric Cryptography makes use of a couple of keys to encrypt and decrypt message. One of these keys is referred to as public key as it is disbursed to others and the second key is known as private key, such key is stored as secret. Generally the sender uses the public key to encrypt the plain data, which could only be decrypted by using the corresponding private key.

### 2.3 HYBRID CRYPTOGRAPHY

In the network security environment, many security algorithms were used each algorithm has its own way of execution, merits and demerits. The symmetric cryptographic algorithms are high speed compared than asymmetric cryptographic algorithms or public key cryptographic systems like RSA, Elliptic Curve Cryptography. The public key cryptographic algorithms are more secure than symmetric algorithms. Because, it has two keys one for encryption and another one for decryption. In this hybrid encryption technique, both the symmetric encryption key and asymmetric decryption key were fused to generate a common key for encryption/decryption.

## III. RSA (RIVEST-SHAMIR-ADLEMAN) ALGORITHM

The RSA algorithm was first published by Ronald Rivest, Adi Shamir, and Leonard Adelman in April 1977. At that time, the RSA algorithm has been actively implemented as an encryption algorithm in most common internet electronic communications. The basic idea behind the RSA Algorithm is based on the trouble in factorizing huge numbers which have 2 and only 2 numbers as factors i.e. Prime Numbers.

The RSA Cryptography system works on Public Key and Private Key. The Public Key is made accessible to everyone. With this Public Key, the sender can encrypt data into ciphertext but nobody else can decrypt it, the person who possesses the private key only can decrypt the ciphertext into plain text. Its miles theoretically viable however extremely tough to generate the private key from the general public key, this makes the RSA algorithm a very famous desire in data encryption. Among the most standard idea of Asymmetric Cryptography, RSA is the best one.

Standard encryption techniques use mathematical operations to convert a message which is represented as a number or a chain of numbers, into a ciphertext. Mathematical operations referred to as one-way process is specifically suited to this Conversion process. A one-way process is one which is relatively smooth to do in a single route or single direction; however a whole lot tougher to do in reverse.

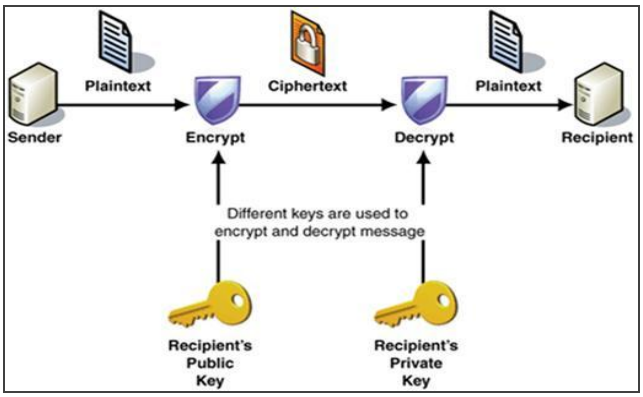


***Figure 1: An Overview of Cryptography Methodology using RSA***

The RSA system makes use of the one-way process of a more complex nature. Especially, the machine makes use of modular mathematics to convert a message into unreadable ciphertext. Modular arithmetic is often referred to as "clock" mathematics, because addition, subtraction, etc, work like telling time. The RSA system makes use of multiplication in modular mathematics. The RSA machine multiplies one range which is referred to as the base, by way of itself the number of times and the product are then divided with the aid of a modulus. The quantity of instances a base is improved via itself is referred to as the exponent and the process is referred to as modular exponent. The following were the operations used in modular arithmetic notation:

The message M is multiplied by way of itself e times and the product is then divided with the aid of a modulus n, leaving the rest as a ciphertext C:

$$C = M^e \bmod n \qquad \text{.....Equ(1)}$$

Now in the decryption operation, a special exponent, d is used to transform the ciphertext returned into the plain text content:

$$M = C^d \bmod n \qquad \text{.....Equ(2)}$$

The modulus n is a composite number, built through multiplying two high numbers, p and q, together:

$$n = p * q \qquad \text{.....Equ(3)}$$

Additionally, φ (n) is referred to as Euler's Phi-function and may be calculated with the aid of the use of the following equation:

$$\Phi(n) = (p-1)(q-1) \qquad \text{.....Equ(4)}$$

The encryption exponent e is selected such that:

$$gcd(e, \varphi(n)) = 1 \qquad \text{.....Equ(5)}$$

The decryption exponent d is calculated by using solving the subsequent equation:

$$d = e^{-1} \bmod \varphi(n), \qquad \text{.....Equ(6)}$$

Thus, the public encryption key is e, n and the private decryption key is d, n.

The process of the RSA algorithm is divided into three steps, they are:

a. **Key generation:** wherein the elements of the modulus **n**, such that, the prime numbers **p** and **q**, are selected and multiplied together to create **n** and **φ(n),** an

© 2018, IJCSE All Rights Reserved 

encryption exponent **e** is selected, and the decryption exponent **d** has calculated the usage of **e** and **φ(n)**. The generated public key used for encryption will be {**e, n}** and the generated private key used for decryption will be {**d, n}.**

b. **Encryption:** wherein the message **M** is elevated to the power **e**, after which is decreased by **modulo n**, so the ciphertext **C** may be calculated as **C= $M_e$ mod n**.

c. **Decryption**: wherein the ciphertext **C** is elevated to the power **d**, after which is decreased **modulo n**. So the plaintext **M** is redeveloped using the components, **M= $C_d$ mod n**.

## IV. AES (ADVANCED ENCRYPTION STANDARD) ALGORITHM

The Advanced Encryption Standard (AES) is a system security standard that comes to be in effect by replacing DES. The AES Symmetric cryptography system is a symmetric block cipher that encrypts and decrypts 128-bit blocks of Information. The standard key lengths utilized by AES algorithm are 128, 192, and 256 bits[5]. Advanced Encryption Standard (AES) algorithm is not only for protection however also for extraordinary speed. Using AES algorithm both hardware and software implementation are still faster it may be implemented on numerous systems in particular in small gadgets. It is carefully examined for lots of applications which need security [6].

In AES Symmetric Cryptography, the symmetric block cipher defined the block length as well as the key length, which can be independently specified to be 128, 192, 256 bits. These three options will be applicable for key size, but the block length is limited to 128 bits.

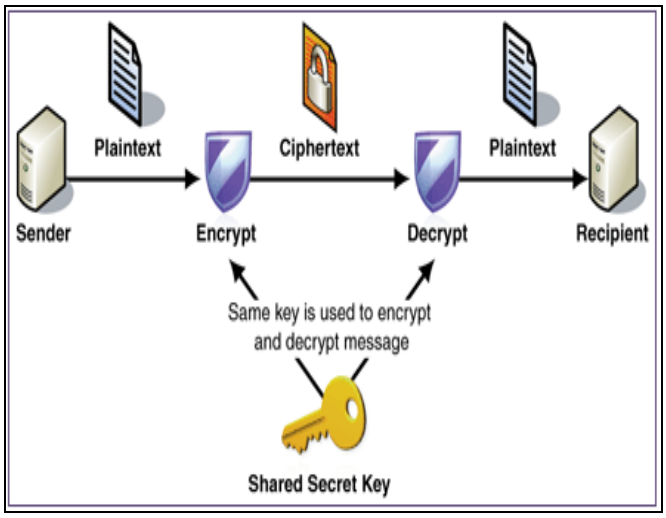


***Figure 2: An Overview of Cryptography Methodology using AES***

[8]In AES Symmetric Cryptography algorithm, four different exclusive stages are used:

I. SUBSTITUTION BYTES

The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, it was interpreted as two hexadecimal digits. S-Box is used to perform byte-to-byte substitution of the data in the block

II. SHIFT ROWS

Within the encryption, the transformation is referred to as Shift Rows. It executes an easy permutation operation.

III. MIX COLUMNS

The Mix Columns transformation functions on the column level; it converts each column of the state to a brand new column. It substitutes process by means of arithmetic operations.

IV. ADD ROUND KEY

Add Round Key executes one column at a time. With each state column matrix, this function adds around a keyword. The operation in Add Round Key is matrix addition. The last step consists of XOR and the output of the previous three steps with four words from the key schedule. A simple bitwise XOR operation with the data of the block which in progress and the portion of the expanded key. Such key is used in add round key stage.

In AES, every stage is reversible easily without the knowledge of the key. Encryption and Decryption process was not the same in AES. While decryption, the first three stages were adopted as it is. Such that, substitute byte, shift row, mix column stages. For the Add round Key stage, XOR of the same round key to the block, because the decryption algorithm used the inverse function. This is an important significance of the specific structure of the AES. Thus this scheme is more effective and safe.

The steps involved in the AES Algorithm to encrypt 128-bit block were explained:

1. Assigning the round keys from the cipher key.
2. Prepare the state array and add the preliminary round key to the starting state array.
3. Accomplish round = 1 to 9, Execute typical Round. Typical Round will perform the following operations which might be described above.
   a. Sub Bytes b. Shift Rows c. Mix Columns
   d. Add Round Key, using K(round)
4. Perform Final Round. Final Round will perform the following operations which might be described above.
   a. Sub Bytes b. Shift Rows c. Add Round Key, using K(10)
5. In Encryption, each round comprises of the following four steps:
   a. Sub Bytes b. Shift Rows c. Mix Columns
   d. Add Round Key

© 2018, IJCSE All Rights Reserved 

6. Decryption involves reversing all the steps taken in encryption using inverse functions like
   a. Inverse shift rows, b. Inverse substitute bytes,
   c. Add round key, and d. Inverse mix columns.
7. Equivalent ciphertext was given to the Final round step as an output

## V. HYBRID CRYPTOGRAPHY (AES- RSA)

AES algorithm always makes use of secret keys; such keys need to be produced by way of a secure random number generator. As there are no acknowledged attacks on complete AES whilst used as a block cipher, it is possible to brute forcing the AES secret key to guessing a 128, 192 or 256-bit number [7].

RSA's key size isn't always directly related to its protection margin. So RSA is appreciably less secure and very slower than any form of AES. Moreover, to generate padding the data, RSA encryption additionally requires access to a secure random number generator.

Hybrid Cryptography is implemented by combining the symmetric cryptography and asymmetric cryptography i.e. AES and RSA algorithms. The methodology used in this hybrid cryptography is to generate a secret key using AES symmetric algorithm, and to encrypt the plain text with the secret key, after which need the RSA public key to encrypt the AES secret key and the encrypted AES secret key is decrypted by using the RSA private key, finally from the decrypted data, by using the AES secret key to obtain the plain text. Thus a combination of AES and RSA are pretty secure for data communication.

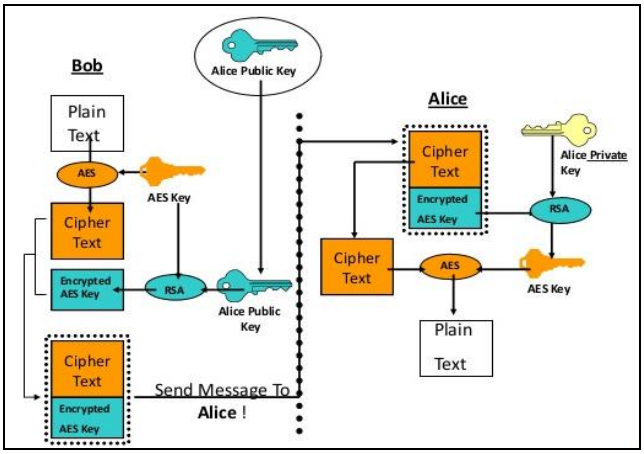


***Figure 3: An Overview of Cryptography Methodology using Hybrid Cryptography (RSA & AES)***

## VI. IMPLEMENTATION AND EXPERIMENTAL RESULT

The proposed system was designed and developed using Java coding and implemented in the Android application. A cloud Storage is created in the Firebase, a Google Cloud Service and the files used in the Proposed Hybrid Cryptography application was stored in the Cloud Firebase storage space.


***Figure 4: Login Framework Designed for Hybrid Cryptography***

© 2018, IJCSE All Rights Reserved 

Figure 4 shows the Login screen for the proposed framework. The user can register the Username, Email ID and Password in it, which is used to prevent the clash among the users as well as to maintain the individual user's data in the cloud data storage separately. Figure 5 shows the framework for Encryption. The user has to select the file to be upload to the Cloud Storage and by selecting the encrypt option the file will be encrypted using the key mentioned in the below text box. The final encrypted file will be uploaded to the cloud storage space in firebase. The list of files encrypted will be shown in the Encrypted files tab displayed in the framework. By selecting the file the decrypt button will be displayed. If the user wants to see the file, then by clicking the decrypt button the file stored in the cloud will be extracted and decrypted in the framework and displayed to the user. Figure 6 shows the storage segments available in the firebase cloud storage space. It shows separate folders for the data files and the key used for the encryption and decryption.

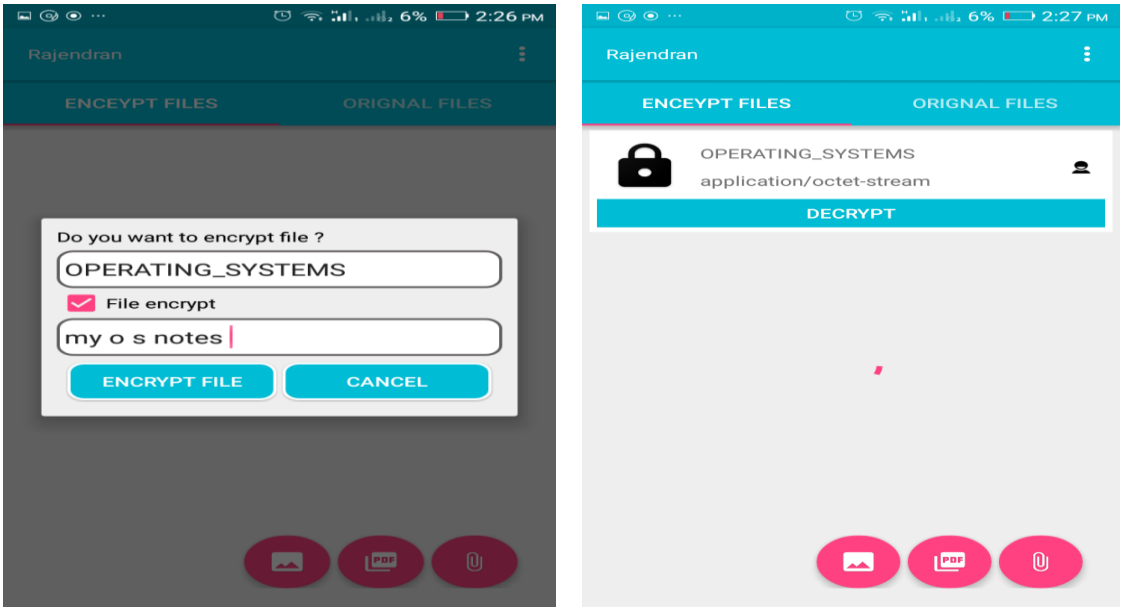


*Figure 5: Encryption Tab in Hybrid Cryptography Framework*

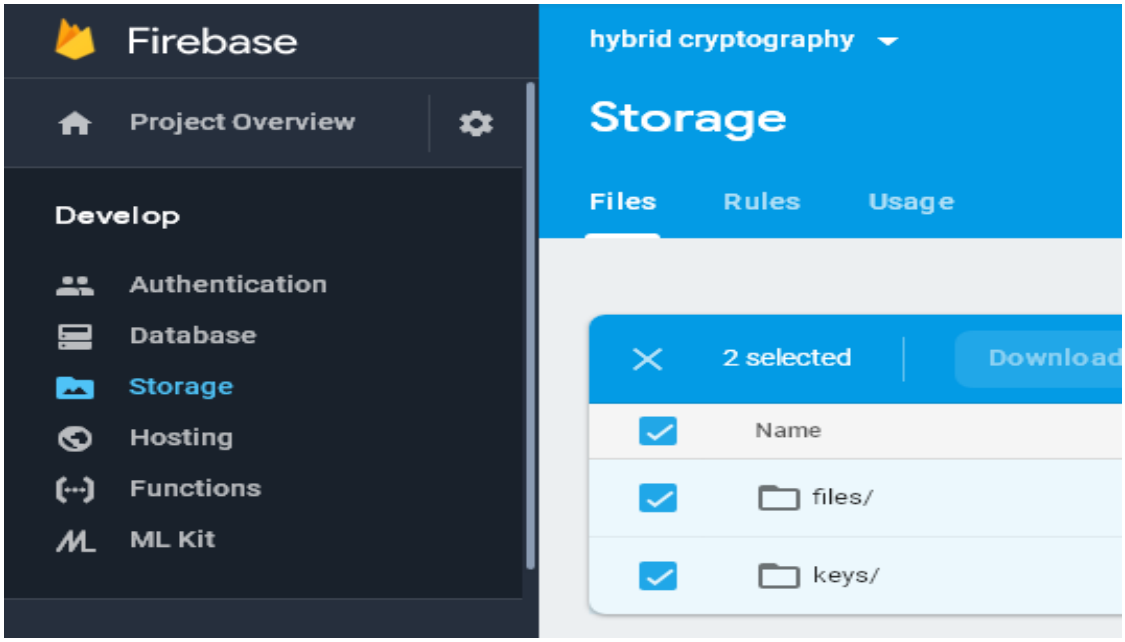


*Figure 6: Storage space in the Firebase for Hybrid Cryptography Framework*

© 2018, IJCSE All Rights Reserved 

Figure 7 shows the files that uploaded and stored in the Firebase cloud storage and detailed information about a particular file stored in the Firebase Cloud Storage using the proposed Hybrid Cryptography Algorithm Application.

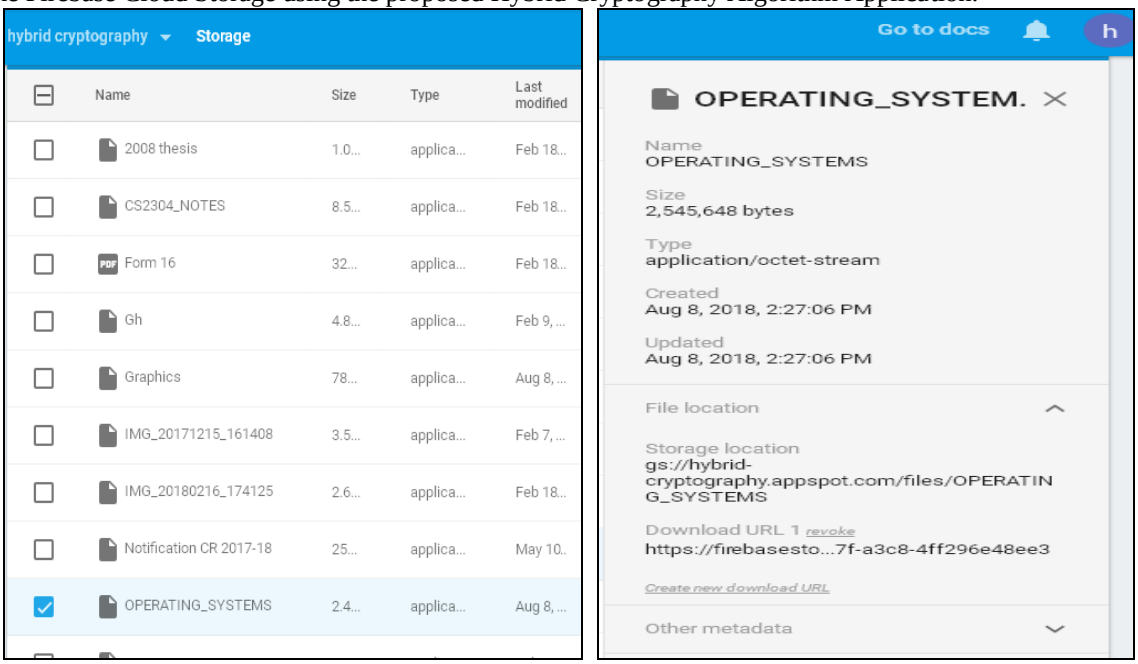


***Figure 7: List of files stored in the Cloud using the Hybrid Cryptography Application***

A comparison has been accomplished for those cryptography algorithms in completely different settings for each and every algorithm. The Performance metrics used in the comparison were different sizes of Information Blocks, Throughput, and Run Time for Encryption and Decryption process. Table 1 shows the Throughput Comparison for the Cryptography Algorithms that selected in the paper.

***Table 1: Throughput Comparison for the Cryptography Algorithms***

| Data size | RSA | AES | Hybrid |
|---|---|---|---|
| **118** | 7 | 5 | 1.2 |
| **153** | 7.3 | 4.9 | 1.6 |
| **196** | 7.5 | 5.1 | 1.7 |
| **259** | 7.6 | 5.6 | 1.8 |
| **312** | 7.8 | 5.9 | 1.8 |
| **412** | 8 | 5.7 | 1.9 |
| **468** | 8.2 | 5.9 | 2 |

Figure 8 shows the Graphical view of Throughput Comparison for the given block of Data size. Among these data's Hybrid Cryptography algorithm shows less Run Time while comparing with the other algorithms like, RSA and AES.

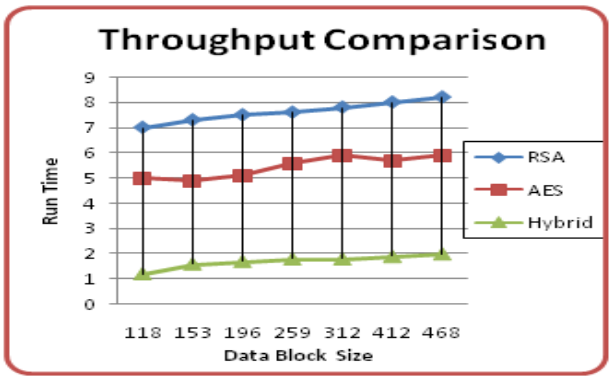


***Figure 8: Throughput Comparison Hybrid Cryptography***

Table 2 shows the Encryption Time for the different blocks of Data size for the Cryptography Algorithms like, RSA, AES and Hybrid Algorithm.

***Table2: Encryption Time vs Data size for the Cryptography Algorithms***

| Data size | RSA | AES | Hybrid |
|---|---|---|---|
| **118** | 6.7 | 3.6 | 2.3 |
| **153** | 6.9 | 3.9 | 2.6 |
| **196** | 7 | 4 | 2.8 |
| **259** | 7.2 | 4.2 | 3 |
| **312** | 7.3 | 4.6 | 3.1 |
| **412** | 7.5 | 4.8 | 3.5 |
| **468** | 7.9 | 5 | 3.8 |

© 2018, IJCSE All Rights Reserved 

Figure 9 shows the Graphical view of Encryption Time comparison for the given block of Data size. Among these data's Hybrid Cryptography algorithm shows less Encryption Time while comparing with the other algorithms like, RSA and AES.

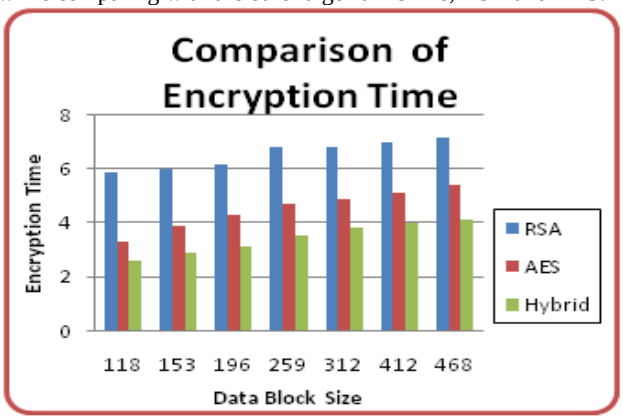


***Figure 9: Encryption Time Comparison***

Table 3 shows the Decryption Time for the different blocks of Data size for the Cryptography Algorithms like, RSA, AES and Hybrid Algorithm.

***Table 3: Decryption Time vs Data size for the Cryptography Algorithms***

| Data size | RSA | AES | Hybrid |
|---|---|---|---|
| **118** | 5.9 | 3.3 | 2.6 |
| **153** | 6 | 3.9 | 2.9 |
| **196** | 6.2 | 4.3 | 3.1 |
| **259** | 6.8 | 4.7 | 3.5 |
| **312** | 6.8 | 4.9 | 3.8 |
| **412** | 7 | 5.1 | 4 |
| **468** | 7.2 | 5.4 | 4.1 |

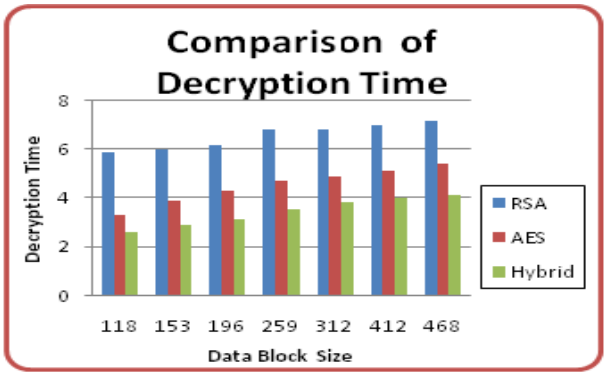


***Figure 10: Decryption Time Comparison***

Figure 10 shows the Graphical view of Decryption Time comparison for the given block of Data size. Among these data's Hybrid Cryptography algorithm shows less Encryption Time while comparing with the other algorithms like, RSA and AES.

## VII. CONCLUSION

In this paper, Symmetric and Asymmetric Cryptography have been combined that AES is used to encrypt the plaintext with encryption speed and its low RAM necessities. RSA algorithm is used to safeguard the encryption key by preventing it from getting stolen by generating Private key and a Public key. Then the Keys and the encrypted information are sent to the Receiver and get decrypted with Private key. Based on the Experimental results, it shows the performance of the Hybrid Cryptography is comparatively higher than the Standalone AES and RSA Cryptography Algorithm implementation with high security and in the future Quantum theory can be applied and implemented for more secure in the information.

## REFERENCE

[1]. Kruti H. Patel, Shrikant S.Patel, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", International Journal for Scientific Research & Development, Vol. 4, Iss. 1, 2016.

[2]. Amit Jain, Avinash Panwar, Divya Bhatnagar, "A Comparative Study of Symmetric Key Encryption Algorithms", International Journal of Advances in Engineering Research, Vol. 8, Iss. 2, 2014.

[3]. Vijay M, Sujatha R, "Intrusion Detection System to Detect Malicious Misbehavior Nodes in Manet", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Iss. 1, 2014.

[4]. Vishnu Priya R, Yuvarani G, "Attribute based LZ4 Encryption with Efficient Signature Verifiable Decryption", International Journal of Science Technology and Management", Vol.5, Iss.03, 2016.

[5]. Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology, Network, Vol. 13, Iss. 15, 2013.

[6]. Ashutosh Bhargave, Niranjan Jadhav, Apurva Joshi, Prachi Oke, Prof. Mr. S. R Lahane, "Digital Ordering System for Restaurant Using Android", International Journal of Scientific and Research Publications, Vol. 3, Iss.4, 2013.

[7]. Arpit Agrawal, gunjan Patankar, "Design of Hybrid Cryptography Algorithm for Secure Communication", International Research Journal of Engineering and Technology, Vol.3, Iss. 1, 2016.

[8]. Ritu Pahal, Vikas Kumar, "Efficient Implementation of AES", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Iss. 7, 2013.

[9]. Pavithra S, Ramadevi E, "Throughput Analysis of Symmetric Algorithms", International Journal of Advanced Networking and Applications", Vol. 4, Iss. 2, 2012.

[10]. Abraham Lemma, Maribel Tolentino, Gebremedhn Mehari, "Performance Analysis on the Implementation of Data Encryption Algorithms used in Network Security", International Journal of Computer and Information Technology, Vol. 4, Iss. 4, 2015.

[11]. S.Rajendirakumar, Dr.A.Marimuthu, "Cryptographic Algorithms used in Cloud Computing – An Analysis and Comparison", International Journal for Research in Applied Science & Engineering Technology, Vol 6, Iss. 1, 2018.

© 2018, IJCSE All Rights Reserved 