Design and Implementation of Hybrid Cryptographic Technique using AES and RSA Algorithm

Jayashree Bodkhe[1], Vivek Kapoor[2]
[1] *Institute of Engineering & Technology, DAVV*
[2] *Institute of Engineering & Technology, DAVV*
(E-mail: jainiijay10@gmail.com)

***Abstract*—** The data security and network security is a crucial domain of research and development. On the other hand the computing changes their face and at the same ways the attackers and intruders are also aware about the traditional security techniques. Thus new kind of security is required to find that are not accurately from the traditional backgrounds. But the traditional cryptographic models are computationally cost effective, produce additional storage overheads, and also generate the less secure cipher for storage. Therefore in order to resolve the issues in cryptographic security a new methodology is required to develop. In this paper, we proposed a hybrid cryptography technique which includes the concept of symmetric key, asymmetric key and hash generation algorithm. In this, first the strong key is generated using MD5 algorithm and user personal 8 digit pin. This key is used for encryption of the original text. In addition of that for secure key exchange the concept of digital signature is used where the cryptographic key is encrypted using RSA algorithm by receiver's public key and its result i.e. encrypted key is signed by sender's private key. All the data i.e. cipher text, signed key and encrypted key is conveyed to receiver end. The receiver first validate the signed key by sender's public key and then recovers the cryptographic key using encrypted key by receiver's private key using RSA algorithm. After that the data is decrypted. Finally to validate the data, integrity check is performed. We have successfully implemented this hybrid approach in .NET environment. Our experimental results demonstrated the effectiveness and efficiency of our technique and ensure security by means of authentication, confidentiality and integrity.

***Keywords*—** *Data security, network security, hybrid cryptography, encryption algorithm, AES, RSA*

I. INTRODUCTION

In recent years a significant change in technology is observed. The new technology and applications are frequently consuming the network and their services. These applications not only carrying data on private networks but the applications are also utilizing the services of public network. But the use of public network is not much trustworthy and secure for private and confidential data exchange. Because a number of times applications requires the private and sensitive data such as banking information, private images and others. In this context the security in network communication and their data is a primary concern in network and data security [1] [2] [3].

There are a number of different approaches that exist for securing the data on network &among them the cryptography is a popular and classical approach. Additionally the key reason behind use of cryptography for security is their low cost implementation and freedom and flexibility to change the security according to needs. Therefore, in this paper key area of work is investigation and design of a secure hybrid cryptographic technique. That technique is combination of multiple cryptographic strategies to make the security more complex and easy to use.

II. BACKGROUND

The background study is an important part of our research paper. It provides the context and purpose of the study. Hence there is requirement of background study that contribute to prepare the proposed system.

A. What is Network Security?

The technology used in daily life is changing. Information technologies are transforming the ways we generate, gather, process, and distribute information. Computer networking is driving many of these changes; electronic transactions and records are becoming essential to everything from commerce to health care. The explosive growth of the Internet exemplifies this shift to a networked society [4].

In a broad way, Network security is any activity intended to protect the usability and integrity of your data and network. It includes both hardware and software technologies. Effective network security manages access to the network. It points a range of threats and stops them from entering or spreading on your network.

Network security blend multiple layers of defenses at the not only at boundary but also inside the network. Each network security layer implements policies and controls. Authorized users get access to network resources, but malicious actors are blocked from carrying out exploits and threats [5].

B. Goals of Network Security

The need for network security is a moderately new requirement. Security incidents are going up at an alarming

rate every year. As the complexity of the threats increases, so do the security measures required to secure networks.

We are addressing three very important goals of any computer-related system.

- ✓ **Confidentiality**
- ✓ **Integrity**
- ✓ **Availability**

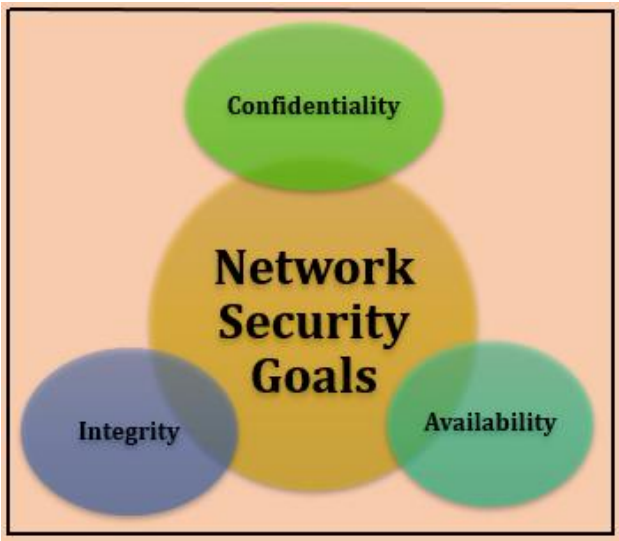

Fig 1: Goals of Network Security

The meaning of these three words (CIA) is quite wide-ranging. For different applications, the interpretation of CIA is different [6].

Confidentiality: Confidentiality refers to the protection of data from unauthorized revelation to a third party. Whether it is customer data or internal company data, a business is responsible for protecting the privacy of its data.

Integrity: Integrity refers to the assurance that data is not altered or damaged in an unauthorized manner. For example, integrity is maintained when the message sent is identical to the message received. Even for data that is not private, actions must be taken to guarantee the integrity of the data.

Availability: Availability is defined as the uninterrupted operation of computing systems. Applications need differing availability levels, depending on the business impact of downtime. For an application to be available, all components must provide continuous service. These components include application and database servers, storage devices, and the end-to-end network [7].

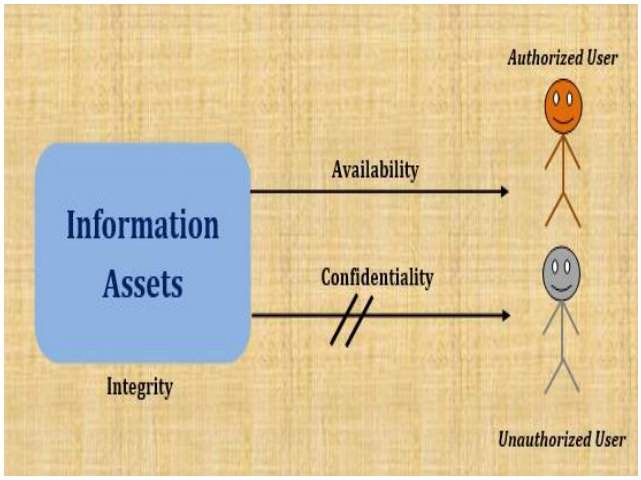

Fig 2: A graphical description of the CIA triad – Confidentiality, Integrity and Availability

For example, weaknesses in confidentiality may be caused both by revelation of sensitive information and by unauthorized use of a computer system. Integrity can be seen as a quality characteristic of information resources, while confidentiality and availability are characteristics of the relations between information resources and an authorized user (availability) and an unauthorized user (confidentiality), as depicted in Fig. 2 [8].

C. What is Cryptography?

Advances in computer and communication technologies have resulted in information exchange in almost all fields and the twenty first century is called information age. Cryptography is the art of using mathematics to encrypt and decrypt the data. Cryptography helps users to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anybody except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication [10] [9].

III. PROBLEM DOMAIN

A problem domain is the area of knowledge or application that needs to be examined to solve a problem. A problem domain is simply looking at only the topics of an individual's interest, and excluding everything else.

The proposed work is motivated from the research article [11]. In this article user offers an secure cryptographic technique for data encryption and verification at the client end. According to best of our knowledge there are three improvements we find which are addressed as:

1. RSA encryption algorithm is secure but for large data encryption process requires a significant amount of time and memory resources
2. DES algorithm is also not much secure as compared to similar kind of algorithm as it can be easily breakable by brute force attack.
3. Need to improve key generation methodology.

IV. PROPOSED WORK

This section introduces the functional aspects of the proposed system. In addition of that the core system design concept and the algorithm steps are explained in detail.

A. System Overview

Cryptography is an art of mathematical computation that helps to transform data from one readable format to human unreadable format and also help to recover the information from unreadable format when required. According to the need of security and scenario of application the implementation of different cryptographic techniques are available (i.e. symmetric key and asymmetric key). The aim of cryptography is to hide the confidential or private data from the unauthorized person and prevent them to recover the information. Therefore the entire cryptographic system design considers on three components.

1. To improve the cipher generation process
2. To improve the key generation process
3. To validate the cryptographic data
4. To check the integrity of key by verifying signed key

The main aim of the proposed work is to investigate the different approaches of cryptographic technique and design and implementation of a new hybrid cryptographic approach that improve the security and data complexity. The proposed technique involve the good properties of AES, MD5 and RSA algorithms for providing integrity and security to data and managing the data confidentiality by verifying the digital signature. In addition of that the system incorporates the goodness of public key and private key cryptography for generation of improved and complex encryption and decryption key. This section provides the overview of the proposed system and basic characteristics of the system. In the next section detailed system design is explained.

B. Proposed Methodology

This section includes the explanation of the proposed hybrid cryptographic data model. Therefore entire process is explained stepwise as:

1) Key generation

The Fig.1 shows the process of cryptographic key generation process. In order to generate the cryptographic key the original text is processed using MD5 hash generation algorithm. That creates 128 bit hash code. On the other hand an 8 digit pin is accepted by user input. This 8 digit pin is converted into equivalent binary digits as demonstrated in table 1.

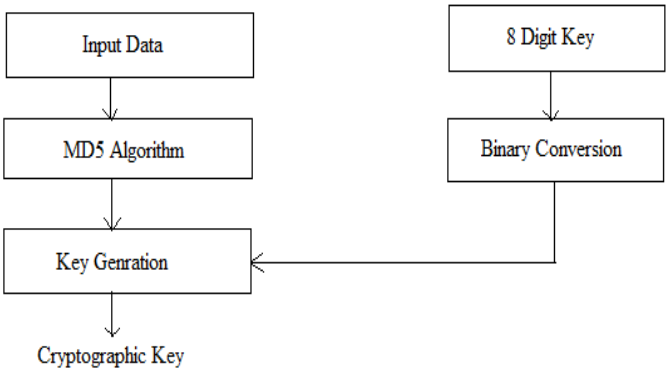

Fig. 1 Key Generation Process

TABLE 1 BINARY CODES

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9

The above given table is used to convert the 8 digits into 8 X 4 = 32 bit binary codes. On the other hand we have 128 bit binary hash code generated by MD5 algorithm. This 128 bit hash code string is replaced with 32 binary codes because 128 divisible by 32 therefore each 4^{th} bit of 128 bit string are replaced with 32 binary code respectively and a new key of128 bit is generated. This generated new key is termed here as the cryptographic key.

2) Data encryption

The Fig. 2 demonstrates the data encryption process. In this phase the 128 bit AES algorithm is used with the previously generated cryptographic key. The data (input file) and generated cryptographic key(new key) is fed as an input to AES algorithm to generate the cipher text.

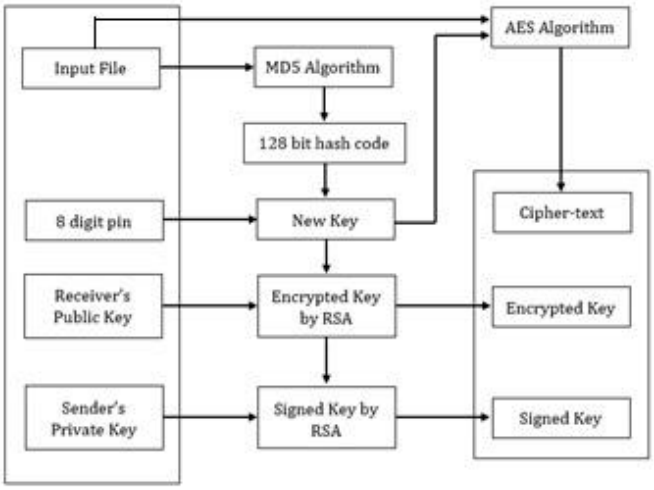

Fig. 2 Data Encryption

3) Key encryption

After data encryption, for transmission of secure cryptographic key, the generated cryptographic key is also encrypted as shown in Fig. 2. In this context RSA encryption algorithm is used. The RSA algorithm accepts the new key (Cryptographic Key) and a key pair. Therefore, receiver's public key is used to encrypt the cryptographic key and its result i.e. Encrypted Key is again signed by sender's private key. This will result in generation of signed key or digital signature of key.

After preparing the cipher text and digital signature the four components which are consumed on decryption end is transmitted to receiver namely:

Cipher Text

Signed key

Encrypted key

8 digit pin

4) Decryption Process

The decryption process of the system is explained using Fig. 3. To ensure that key has not been modified while transmission i.e. to check the integrity of key, initially, system accepts signed key and validate it by decrypting the signed key using sender's public key. This will help in establishing authentication. Once the signed key is validated, the encrypted key sent by the sender is decrypted by receiver's private key to recover the key. This will ensure the confidentiality of key.

The RSA algorithm validates the digital signature (signed key) and then only decrypts the encrypted key that will result in recovery of the cryptographic key (new key). The decrypted key (new key) is used with AES algorithm to decrypt the received cipher text to generate plain text (Input file). Now to check the integrity of decrypted data it is fed as an input to MD5 algorithm that will generate 128 bit hash code. Again from MD5 128 bit hash code and 8 digit pin entered by receiver a 128 bit new key is generated. The decrypted key and new generated key is compared to validate integrity of the data. If both the keys are same then data is accepted by system otherwise rejected.

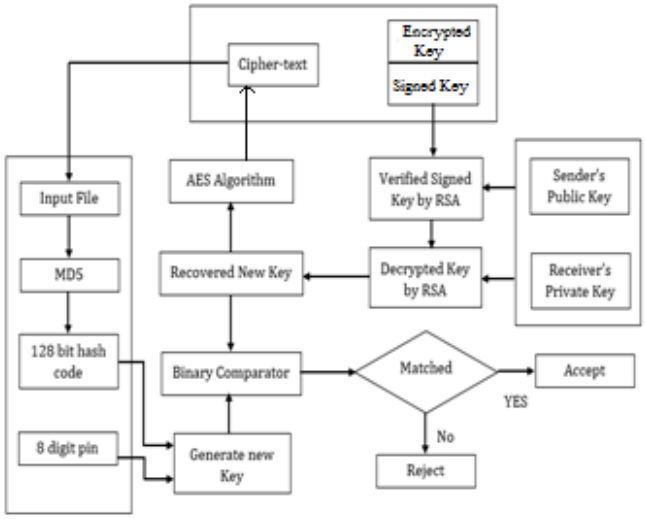

Fig. 3 Decryption Process

The design of the system is explained for encryption and decryption of the text files.

C. Proposed Algorithm

The table 2 shows the encryption process of the proposed cryptographic model and the table 3 contains the decryption process.

TABLE 2 ENCRYPTION ALGORITHM

Input: plain text T, eight digit pin P, receiver's public key RP_{key}, sender's private key SP_{key} Output: Cipher text C, encrypted key E_{key} digital Signature D or Signed Key
Process: H_{key} = MD5.GenerateHash(T) P^{32} = ConvertBinary(P) N_{key} = GenerateKey($H_{key,}$ P^{32},4) C = AES.Encrypt(T, N_{key}) E_{key} = RSA.Encrypt($N_{key,}$ RP_{key}) D = RSA.Sign($E_{key,}$ SP_{key}) Return C, E_{key}

TABLE 3 DECRYPTION ALGORITHM

Input : Cipher text C, digital signature D, sender's public key SPU_{key}, receiver's private key RPR_{key}, encrypted key E_{key}, 8 digit pin (P) Output : Plain text T, integrity decision Dc
Process: $Validate_{key}$ = RSA.Decrypt(D, SPU_{key}) N_{key} = RSA.Decrypt(E_{key}, RPR_{key},) T= AES.Decrypt(C, N_{key})

H_{key} = MD5.GenerateHash(T)

P^{32} = ConvertBinary(P)

N'_{key} = GenerateKey(H_{key}, P^{32},4)

If(N'_{key} = = N_{key})

Dc=Accept

Else

Dc= Reject

End if

Return T,Dc.

V. RESULTS ANALYSIS

The security is essential feature in the computational applications. The experimental evaluation and the system performance is computed and demonstrated in this section. Therefore some essential performance parameters are obtained and listed with their obtained observations.

A. Encryption Time

The amount of time required to perform encryption using the selected algorithm is termed as the encryption of the cryptosystem. Therefore, encryption time of the proposed security algorithm is demonstrated using following formula:

Encryption Time = Algorithm End Time – Algorithm Start Time

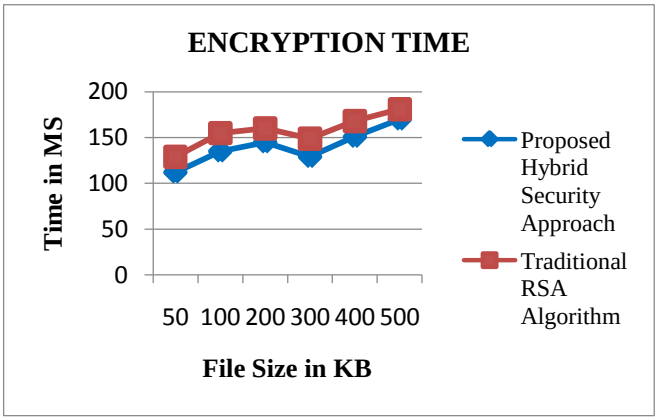

Fig. 4 Encryption Time

In order to show the performance of implemented proposed and traditional algorithm, the encryption time is depicted using Fig. 4 and Table 4. In this diagram the X axis contain different file size in kilo bytes (KB) values and Y axis shows the amount of time consumed for processing and encrypting selected input file for both algorithms. Additionally the performance of proposed security approach and traditional algorithm is demonstrated by blue and orange line respectively. According to the generated results the proposed system consumes less time for encrypting data file as compared to RSA algorithm. We noticed that on this results that the amount of time consumed is depends on the amount of data file provided for execution. As well as data size is increased therefore encryption time will also increases. Therefore, proposed hybrid approach is more efficient for delivering security of user sensitive information.

TABLE 4 ENCRYPTION TIME

Number of File Size	Proposed Hybrid Security Approach	Traditional RSA Algorithm
50	112	129
100	135	155
200	142	160
300	129	149
400	151	168
500	170	181

B. Decryption Time

The quantity of time required to recover the original data from the cipher-text is known as the decryption time of the proposed algorithm. Following are the formula shows the decryption time:

Decryption Time = Algorithm Start Time – Algorithm End Time

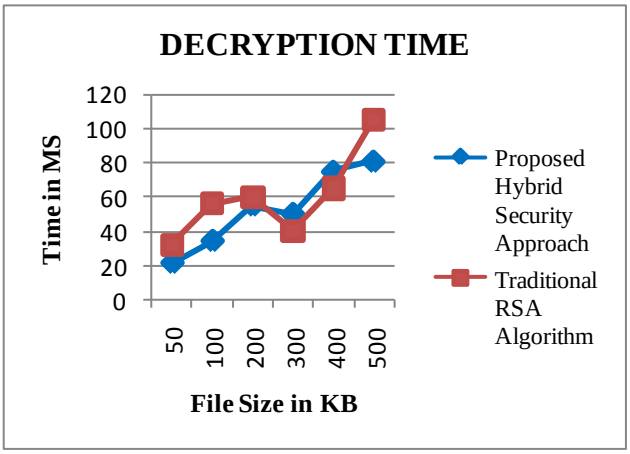

Fig. 5 Decryption Time

Hence, Fig. 5 and Table 5 show the obtained performance for both developed algorithm in terms of millisecond. To show the performance of hybrid cryptography approach and traditional RSA algorithm using blue line and orange line. In given figure 6, X-axis shows different amount of file size in kilo bytes (KB) and the Y-axis shows the amount of time consumed to decrypt the data file. According to the observations the encryption time is higher than the decryption time for data access, but the decryption time of the proposed algorithm is much adoptable. Additionally, RSA algorithm consuming much more time for decrypting cipher-text to recover original text. Therefore, our approach is much superior for data security.

TABLE 5 DECRYPTION TIME

Number File Size	Proposed Hybrid Security Approach	Traditional RSA Algorithm
50	21	32
100	34	56
200	55	60
300	50	40
400	75	65
500	81	105

C. Encryption Memory

The amount of main memory required to execute the algorithm with the input amount of data is known as the encryption memory. The total memory consumption of the algorithm is computed using the following formula.

Encryption Memory = Total Memory – Free Memory

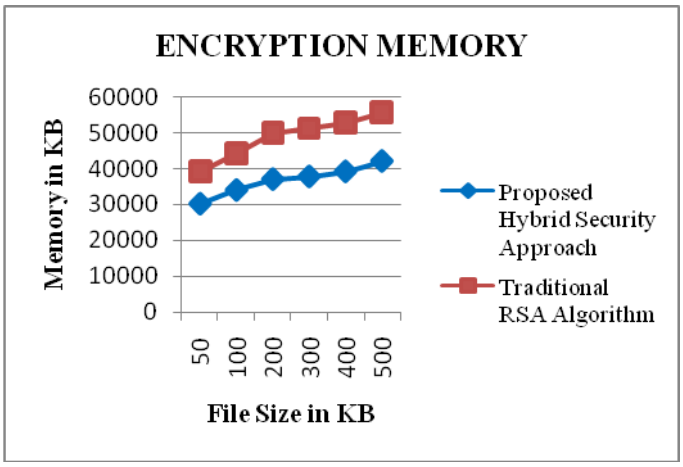

Fig. 6 Encryption Memory

The Fig. 6 and the Table 6 show the encryption memory consumption for algorithm in terms of kilobytes (KB). In this figure the amount of main memory consumed is given on Y axis and amount of file size are reported on X axis. According to the obtained results the proposed algorithm consumes fewer resources as compared to the other traditional RSA algorithm.

TABLE 6 MEMORY CONSUMPTION

Number File Size	Proposed Hybrid Security Approach	Traditional RSA Algorithm
50	30262.44	39226.65
100	34054.74	44362.25
200	37079.78	49865.77
300	37819.06	51231.23
400	39221.25	52889.41
500	42103.62	55694.22

D. Decryption Memory

The amount of main memory required to recover the original file from the cipher text is known as the decryption memory consumption or the space complexity of the decryption algorithm. Decryption memory of the proposed and traditional algorithm can be calculated using following formula:

Decryption Memory = Total memory – Free Memory

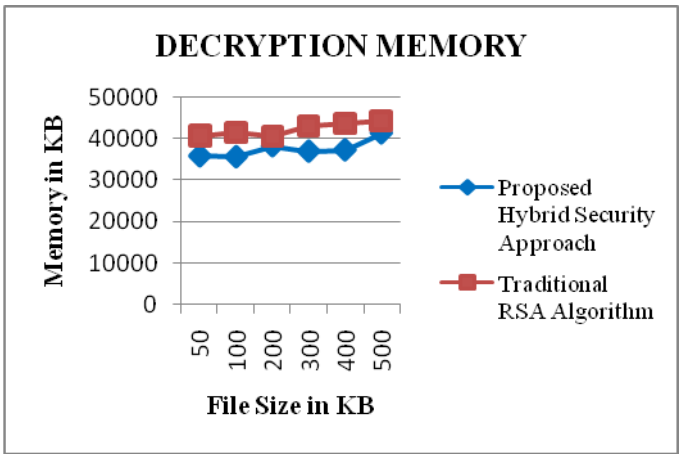

Fig. 7 Decryption Memory

The Fig. 7 and Table 7 show the amount of main memory consumed during the data decryption process. In this figure, X-axis depicts number of file size in KB used for decryption and the Y-axis shows the amount of main memory consumed. According to the obtained performance the amount of main memory is vary depending on file size. Additionally table 7, show comparison of proposed and traditional algorithm.

TABLE 7 DECRYPTION MEMORY

Number File Size	Proposed Hybrid Security Approach	Traditional RSA Algorithm
50	35765.07	40594.12
100	35565.26	41526.02
200	38224.71	40520.36
300	36908.93	42963.21

400	37215.55	43654.01
500	41321.84	44226.51

VI. CONCLUSION AND FUTURE WORK

This chapter provides the summary of entire work performed. Therefore the summarization of work is provided using conclusion of work additionally the future extension of the work is also included in this chapter.

A. Conclusion

The cryptography is a classical area of research and development. Additionally the domain requires the systematic development and enhancement on classical approaches. The cryptographic techniques are advantageous because the techniques are easily acceptable for securing data with less amount of cost, additionally modifiable and extendable according to the application needs. Therefore the proposed work is focused on design and development of new hybrid cryptographic data model. The proposed technique involves the concept of cryptography and digital signature for securing data in unsecured network and will help in achieving integrity, confidentiality authentication of key respectively.

The entire cryptographic model works on two major phases first the encryption and seconds the decryption. During the encryption of the data a modified key is generated using MD5 hash algorithm and 8 digit users Pin. That new generated key is used for encryption of data using AES algorithm. In order to transmit the key securely to receiver, the key is also encrypted using RSA algorithm. Here the RSA algorithm accepts the receiver's public key and sender's private key for encryption and generating digital signature of cryptographic key respectively. The encrypted key, digital signature(Signed key), cipher text and 8 digit pin is transmitted to the receiver. At the receiver end first the digital signature is validated using RSA algorithm by sender's private key. Once the key is validated the encrypted key is decrypted by receiver's public key to recover the cryptographic key. After the recovery of the cryptographic key AES algorithm is used to decrypt the cipher text. After decryption of data again key generation process is followed to generate the key using MD5 algorithm and 8 digit pin. Finally the integrity check is performed by comparing the recovered key and again generated key. If both the keys are similar then data is accepted otherwise data is rejected.

The hybrid cryptographic proposed technique is implemented using .NET technology. After successfully implementation of the propose approach the performance analysis of the system is also conduced based on time and space complexity. The table 8 includes the performance based summary of the technique.

TABLE 8 PERFORMANCE SUMMARY

S. No.	Parameters	Remark
1	Encryption time	The proposed technique is efficient due to less fluctuation of the encryption
2	Decryption time	The proposed technique consumes less amount of time as compared to the encryption of files
3	Encryption memory	The technique requires less memory for encryption of data
4	Decryption memory	The technique acceptable due to less memory resource requirements

According to the demonstrated performance of the system as listed on table 8 the proposed technique is efficient and implementable for different real world applications. Therefore the proposed technique is acceptable for future extension of the work.

B. Future Work

The proposed technique is an efficient and secure technique. In the near future the following work is feasible for extending the proposed approach.

1. The proposed technique basically aimed to secure data across the network, thus it can be extendable for secure cloud data also in un-trusted data hosting scenarios.

2. The proposed work approach only considers the data integrity therefore that technique can also extendable for managing the data ownership over the cryptographic data.

REFERENCES

[1] Stallings, William. Cryptography and network security: principles and practice. Pearson Education India, 2003

[2] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." In Information and communication technologies, 2005. ICICT 2005. First international conference on, pp. 84-89. IEEE, 2005.

[3] Denning, Dorothy E., and P. J. Denning. "Data security." ACM Computing Surveys (CSUR) 11, no. 3 (1979): 227-249.

[4] Herdman, R. "Information security and privacy in network environments." The Office of Technology Assessment (OTA) (1994).

[5] S. Feruza Y. and Tao-hoon Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007.

[6] Oscarson, Per. "Information security fundamentals, graphical conceptualisations for understanding: research group VITS, Department of Business Administration, Economics." Statistics and Informatics, Örebro University, Sweden (2003).

[7] Chaeikar, S. Shojae, M. Jafari, and Hamed Taherdoost. "Definitions and criteria of CIA security triangle in electronic voting system." Information Technology (IJACSIT) 1, no. 1 (2012).

[8] "Introduction of Computer and Network Security", Lecture Notes (Syracuse University), available online at: http://www.cis.syr.edu/~wedu/Teaching/IntrCompSec/LectureNotes_New/Introduction.pdf

[9] Gutmann, Peter, "Cryptographic Security Architecture: Design and Verification", Springer Science & Business Media, 2003.
[10] "Chapter 2: Literature Survey", online available at: http://shodhganga.inflibnet.ac.in/bitstream/10603/2189/8/08_chapter%202.pdf
[11] R. Yadav and V. Kapoor, "A Hybrid Cryptography Technique for Improving Network Security", International Journal of Computer Applications (IJCA), Volume 141 – No.11, May 2016.