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

Design and Implementation of Hybrid Cryptographic Model based on Data Authentication, Integrity and Privacy Schemes

S.M. Bhat[1*], V. Kapoor[2]

[1] IT Department, Institute of Engineering & Technology, DAVV, Indore, India
[2] IT Department, Institute of Engineering & Technology, DAVV, Indore, India

[*]*Corresponding Author: sourabhbhat456@gmail.com, Tel.: +91-86003-45044*

Available online at: www.ijcseonline.org

Accepted: 03/Jun/2018, Published: 30/Jun/2018

Abstract— Information security is the one of the ultimate generous apprehension in each turf of today's period. In order to shelter the data broadcast over the ambiguous passage, formerly abundant cryptographic procedures are accomplished. But several limits present in the currently asymmetric and symmetric encryption procedures. The key transaction is a prime delinquent of symmetric cryptographic techniques though quicker in ciphering. Prolonged encryption interval is foremost delinquent convoyed with asymmetric methods but key transaction is simple & secure. Now, to incredulous these anomalies, in this paper a hybrid model is projected which agreements extreme security with decreased key maintenance problem and encryption time using unification of the together symmetric and asymmetric cryptographic procedures. To achieve the embryonic security services as authentication, integrity, and confidentiality in this hybrid model message digest, encryption methods and digital signature respectively is used and a digital envelope is also incorporated which involves all of this to transfer them confidently over the connection.

Keywords— Hybrid Cryptography, Information Security, Asymmetric cryptographic technique, Symmetric cryptographic technique, Digital signature, Digital envelope.

I. INTRODUCTION

In this practised work a hybrid model is actives which is the unification of asymmetric, symmetric cryptographic procedures and digital signature. This projected model agreements an boosted hybrid cryptographic scheme which conveyed tenable atmosphere with less reserve breakdown.

Hybrid cryptosystem: This cryptosystem (provide excessive security with minimized key maintenance) is the mishmash of both symmetric and asymmetric cryptography technique, taking pluses of both cryptography and left their downsides. Symmetric encryption process is faster than the asymmetric encryption, but sharing of the secret key is the problem accompanied with symmetric cryptography.

In the figure 1.1 a hybrid cryptosystem is presented which mainly comprises of symmetric, asymmetric techniques and digital signature.

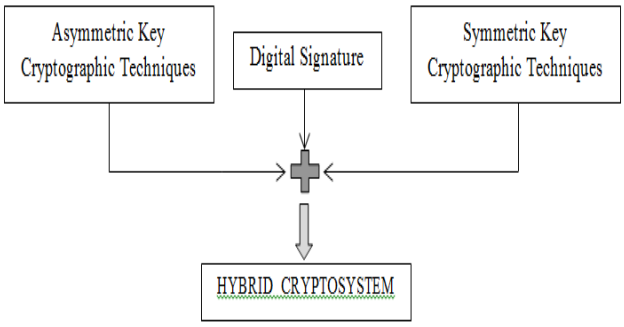

Fig 1.1:- Hybrid Cryptosystem

II. RELATED WORK

In the works pursuit, depiction of considerate on the certain research papers of different cryptographic procedures which are recycled for fortifying the information from the unreliable links.

This paper pointing on augmenting the security by enlightening the level of encryption in network as the encryption process is turn out to be a vivacious instrument

for obstructing the intimidations to information spreading and instrument to safeguard the integrity of data . This study's central intention is to expose the importance of security in network and provide the improved encryption method for currently implemented encryption procedures. In this study, author has projected a combination of MD5, DSA and RSA as a merging connection for wireless devices in the MANET networks.[1]

This novel method enciphers the image and implants the digital signature into the image. A digital signature is a scheme recycled to accomplish integrity of documents, digital forms and approve the authenticity. Steganography is also an encryption procedure that can be accomplished along with cryptography as extra shielded scheme escalating to shelter data. Here, the Java methodology is planned to shelter Images to cover objects used in steganography.[2]

In this paper, security etiquette is deliberate to advance the asset of confidence algorithms for online transaction using federation of both asymmetric and symmetric cryptographic procedures. This protocol deals three cryptographic facilities such as confidentiality, integrity and authentication. These services are conquered by using ECC method (for ciphering), Dual-RSA cryptographic method (for authentication), and Message Digest MD5 (for integrity).[3]

This study mentions to numerous features of cryptographic procedures and many matters connected to cryptography. The projected effort is presenting the certain of the vital concerns of cryptography along with their results. DES cryptographic scheme is used for encryption drive as well as RSA is used for asymmetric ciphering and hash method SH1 is charity in this paper.[4]

Author is using cryptographic primitives such as integrity, authentication and privacy to secure e-commerce transaction over the internet. In this paper acclaim encryption arrangement that is spreads the Diffie-Hellman key trading by consuming truncated polynomial in discrete logarithm problem to upswings the complexity of this scheme over the treacherous channel, also adding the MD5 algorithm, the AES scheme and the Modification of Diffie-Hellman procedure.[5]

Diffie-Hellman is revised to offer confirmation and avoid intuitive root generation stage to achieve speed and authentication to avoid key transaction with unauthenticated operator. RSA is cryptography arrangement placed on asymmetric key cryptography perception. In this paper amalgam cryptography planning is anticipated to undertake secret data substitution. RSA uses random prime numerals P and Q which swollen an catch value N is interchange to the receiver area.[6]

This paper studied as the information security can be interpreted into three key primitives: integrity, availability and data safety. In order to augmenting the virtues of the cryptographic schemes, we suggest a hybrid approach that cables three cryptographic processes.[7]

Secure Electronic Medical Records (SEMR), which delivering several services as, authentication and privacy. In this paper effort, author offers an execution of a fusion model that chains the HECC algorithm MD5 algorithm and AES algorithm in the digital envelope. The consequence reveals that the premium supplementary digital envelope is used in amalgam cryptographic based scheme for EMR.[8]

Author advises software implementation that encompasses a digital envelope which related with the MD5 scheme, AES scheme and the HECC scheme. The consequence elucidates that HECC is the distinguished additional asymmetric key method rather than ECC and RSA.[19]

It is alleged in author portrayal that DE delivers a countless docility to switch secret keys as often as the both receiver and sender would like, which will distribute more ruthless for an antagonist to discover the key which is individual used for a insignificant time interim.[10]

Author demonstrate the policy of a hybrid ECC-AES centered cryptographic organization which can be hastily mounted even in unreality of public key frames and linked certificate organization. It licenses protected exchange of data with connected ECDSA digital signature. Confirmed etiquettes were charity in an sole manner, curiously manipulating the straight ensconcing of the AES session key into an elliptic arc and the code in C++ has been fabricated.[11]

In this proposed paper, author reports a probe whether it is comprehendible to build an amalgam signcryption arrangement in identity-based background. Author responses the probe evidently in this paper with an example of identity-based signcryption key encapsulation procedure and it can be elongate the notion of signcryption key encapsulation procedure to the identity-based background. It is publicised that an identity-based signcryption planning can be contrived by correlating an identity-based signcryption key encapsulation procedure with a data encapsulation process.[12]

III. RATIONALE

- Due to manifestation of countless figuring impetus processors which is hewing varied environments for secret key encryption with the insignificant size of the key because spread reckoning procedures can discontinuity slighter size of key merely.
- Another exertion is the key transaction in secret key encryption procedure over the unsafe network. A shortcoming of consuming asymmetric scheme is sluggish swiftness encryption scheme.
- Entire widespread secret-key encryption schemes are considerably quicker than any currently surviving symmetric encryption scheme.

- Public key cryptography scheme is not feasible in case of massive data. Plentiful hybrid patterns are prepared to overwhelm these circumstances.
- Also authentication and integrity are the excessive anxieties of each field.

IV. PROBLEM DOMAIN

With the antiquated cryptographic pattern two parties principally derive to a treaty to segment a secret key and preserve it covertly amid them. If they are in diverse spaces, they must assurance a contributor or certain other sheltered communication networks to constrain the exposure of the secret key during transmission. Anyone who snoop the key in passage can far along read, alter all data encrypted or genuine with that key.

In a cryptographic structure, the strain is that it can't accomplish this whole delinquent in a solo stage like integrity, confidentiality and authentication. In a existing arrangement the intruder outburst on a system modestly, brute force assaults fluently happen because of the requirement of security escalation. Predictable scheme takes additional interval in encryption and decryption since of this our scheme may perform ailing and yield complications. Hacking is the utmost substantial crisis in the prevailing scheme. Using endorsed methodology we will be tenacity these whole unruly.

V. PROPOSED SOLUTION

The leading objective of the projected prototype is to procure the primeval goals of the cryptography that is authentication, confidentiality, and integrity. A proficient, secure hybrid model is to be instigated using consolidation of the cryptographic procedures that darns the performance of the fashionable cryptographic security measures.

In this projected model, symmetric encryption of documents (accomplished confidentiality), digital signature offer authentication and linking the hash values gives integrity and digital envelope offer additional safekeeping over the link

VI. METHODOLOGY

Encryption Process:-

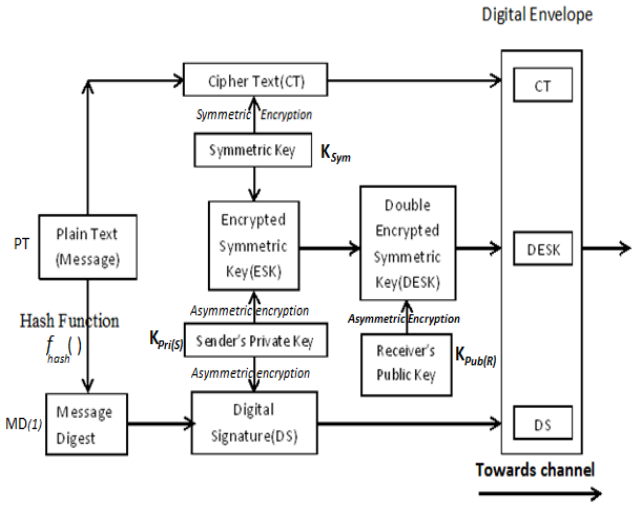

Fig 1.2 :- Sender Side Scenerio of Hybrid Model

Sender Side Process :-

- Symmetric Encryption :-
  [Psym , PT]----------> CT
- One way Hashing Scheme
  [F hash() , PT]----------> MD(1)
- Asymmetric Encryption
  I. [Kpri(s) , MD(1)]----------> DS
  II. [Epri(s)) , Ksym]----------> ESK
  III. [Kpub(R) , ESK]----------> DESK
- Digital Enveloping
  [CT , DESK , DS]---------> DE

In the figure 1.2 Source side consequences is exposed which is designated in followings stages:-

- Plain Text (PT) is encoded using symmetric key (Ksym) to acquire cipher text (CT).
- Message digest is designed by smearing one-way hashing procedure on input data and this message digest is encoded consuming sender's private key (Kpri(s)) to acquire the digital signature (DS).
- Firstly symmetric key (Ksym) is encoded using sender private key (Kpri(S)) and then this encrypted symmetric key (ESK) is encoded using receiver's public key (Kpub(R)) to acquire double encrypted symmetric key (DESK).
- A digital envelope DE is prepared for the transmission of entire three CT, DS, DESK over the passage steadily.

Decryption process:-

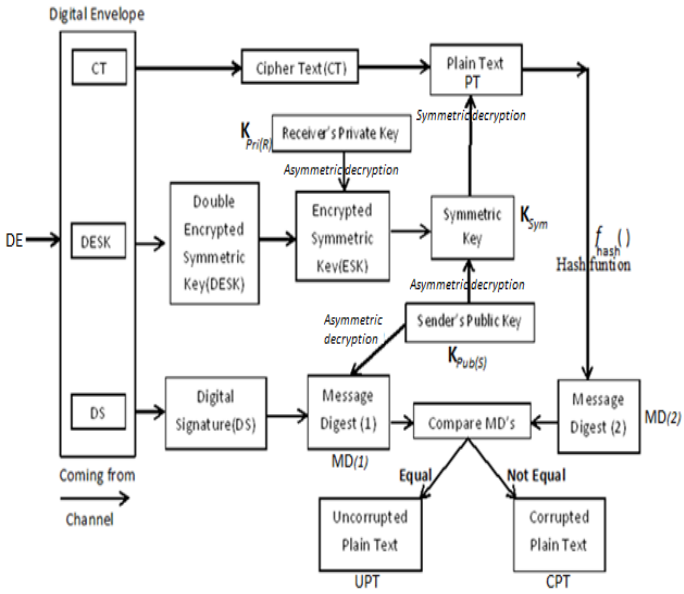

Figure 1.3 :- Receiver's Side Scenerio of Hybrid Model

Receiver Side Process :-

- Open Digital Envelope
  DE ----------> [CT , DESK , DS]
- Asymmetric Decryption Scheme :
  I. [Kpri(R) , DESK]-------> ESK
  II. [Kpub(S) , ESK]--------> Ksym
  III. [DS , Kpub(S)]----------> MD(1)
- Symmetric Decryption Scheme
  [Ksym , CT]----------> PT
- One way Hashing
  [F hash() , PT]----------> MD(2)
- Matching the Message Digest
  [MD(1) , MD(2)]----> CPT or UPT

In the figure 1.3 Receiver side consequences is revealed which is described in subsequent certain phases:-

- Entering digital envelope (DE) from the passage is comprised of CT, DESK, DS.
- The doubled encrypted key is first encoded with receiver's private key and acquire encrypted symmetric key is more encoded with sender's public key and lastly acquire symmetric key.
- This symmetric key is recycled to decode the cipher text (CT) to plain text. This plain text (PT) is altered into message digest by means of hashing algorithm md5 and acquire message digest (2).
- The digital signature is attained from digital envelope is decoded by means of sender's public key to acquire message digest (1).
  Message digest (1) is equated with Message digest (2). If both are matching than unspoiled plain text (UPT) is obtained and when both are dissimilar then corrupted plain text (CPT) is achieved

VII. IMPLEMENTATION WORK

In the implementation phase,

- The AES algorithm is used for symmetric technique
- The RSA algorithm is used for asymmetric technique
- The MD5 algorithm is used for hashing technique

Using Java technology on Notepad++ and NetBeans 7.0 the java code is successfully implemented the part of main code is shown in fig 1.4.

```
    public static void main(String[] args)
        throws IOException, GeneralSecurityException, Exception{

        StartEncryption startEnc = new StartEncryption();
        Server_Connect();
//ReceiveRSAValues();
ServerSocketClose();

 Client_Connect(reciver_ip);
        // SendCipherValue();
 File originalKeyFile = new File("OneKey\\secretKey");
// File encryptedKeyFile = new File("D:\\study\\workspace\\
SecurityProject\\src\\EncryptedFiles\\encryptedSecretKey");
 File encryptedKeyFile = new File("EncryptedFiles\\encryptedSecretKey\\temp.txt");
 //  File encryptedKeyFile = new File("EncryptedFiles/encryptedSecretKey");
 new EncryptKey(startEnc.getPublic("KeyPair/publicKey_Bob", "RSA")
                                    ,originalKeyFile, encryptedKeyFile, "RSA");

        File originalFile = new File("resource\\input.txt");
        File encryptedFile = new File("EncryptedFiles\\encryptedFile");
        long startTime = System.currentTimeMillis() % 1000;
        new EncryptData(originalFile, encryptedFile,
                startEnc.getSecretKey("OneKey/secretKey", "AES"), "AES");
                long endTime=System.currentTimeMillis() % 1000;
System.out.println("Time consumed in Encryption is "+(endTime-startTime)+" milliseconds");
                //CalculatePerformance();
```

Fig 1.4: Implementation Work

VIII. RESULTS

In the final results as the output encryption time, decryption time, input data size, encrypted data size, decrypted data size are obtained.

Encryption Time:- It is the one of most important performance parameter of the cryptosystem which deals with the performance in form of encryption time at the sender side. With the help of taking different ranges of output, which is mentioned in table 1.

Table 1: Encryption Time

SIZE OF INPUTS DATA	***ENCRYPTION-TIME***
1 KB	15 mS
269 KB	31 mS
538 KB	42 mS
1070 KB	46 mS
2139 KB	47 mS
4277 KB	62 mS
6455 KB	63 mS
8466 KB	78 mS
12910 KB	94 mS
16932 KB	110 mS

In the fig 1.5 Encryption Time, the for various data size of input, corresponding encryption time of process is shown.

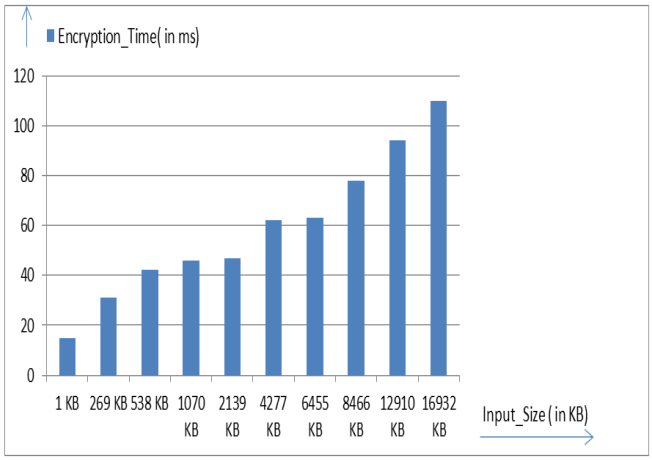

Fig 1.5 Encryption Time

Decryption time:-

It is the most significant parameter of performance of receiver side cryptosystem. At the receiver side, for the various data size of inputs individual decryption time is calculated which is shown in table 2.

Table 2 Decryption Time

SIZE OF INPUTS DATA	***DECRYPTION-TIME***
1 KB	15 mS
269 KB	31 mS
538 KB	32 mS
1070 KB	47 mS
2139 KB	63 mS
4277 KB	78 mS
8466 KB	93 mS
8553 KB	93 mS
12910 KB	109 mS
16932 KB	125 mS

In the figure 1.5, a relationship chart between different inputs data size and corresponding decryption time is mentioned.

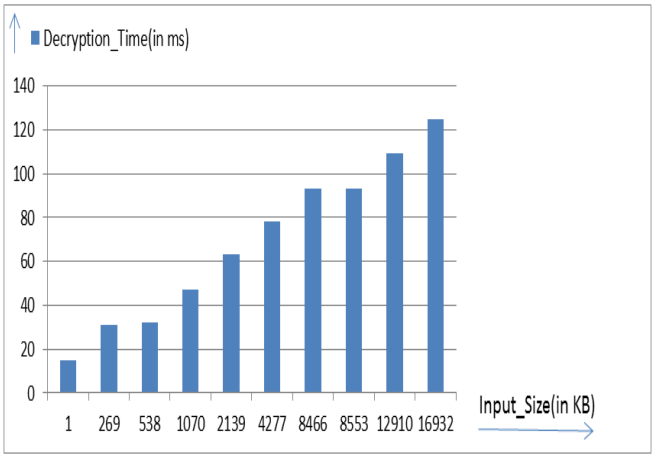

Fig 1.5 Decryption Time

IX. CONCLUSION

Today's modest and digitalised atmospheres with ever more oppressed from fiscally encouraged hackers and disgruntled workforces are producing too much ultimatum for efficacious, spontaneous, governing and risk-alleviating means to accomplish and confident keys all over their existence, so that the right of entry must be contracted only to the accredited operators. To avert vindictive attacks, solicitation and user access to these monies and schemes must be appraised, be able to and highly meticulous. For pledging the accomplishment of key safety targets a vigorous hybrid cryptographic scheme along with authentication based administration

organisation and a secure key encryption centred scheme is projected.

A sturdy cryptosystem composed with a secure key encryption scheme with authentication centred supervision structure can endorse entirely security targets. The alliance of dissimilar cryptography processes convey a maximized proficiency, altering or compensating each other's blemishes.

REFERENCES

[1] K. Kaur, Er. Seema *"Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices"* International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 5, pp.914-917 , Sept-Oct 2012.

[2] S. Sharma, V. Kapoor *"A Novel Approach for Improving Security by Digital Signature and Image Steganography"* International Journal of Computer Applications , Volume 171 – No. 8, August 2017.

[3] S. Subasree, N. K. Sakthivel "Design of New Security Protocol Using Hybrid Cryptographic Algorithm" IJRRAS 2 (2) February 2010.

[4] Dr. V. Kapoor, R. Yadav *"A Hybrid Cryptography method to Support Cyber Security Infrastructure"* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 11, November 2015.

[5] A.M.S. Rahma, R.N. Farhan, H. J. Mohammad *"Hybrid Model For Securing E-Commerse Transaction"* International Journal of Advances in Engineering & Technology, Vol. 1, Issue 5, pp. 14-20, Nov 2011.

[6] S. Deshmukh, Prof. R. Patil *"Hybrid cryptography method using modified Diffie-Hellman and RSA"* International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014,.

[7] G. Mateescu, M. Vladescu *"A Hybrid Approach of System Security for Medium and Small Enterprises: combining different Cryptography method"* Federated Conference on Computer Science and Information Systems pp. 659–662, 2013.

[8] M. Gobi, Dr. K. Vivekanandan *"A New Digital Envelope Approach for Secure Electronic Medical Records"* International Journal of Computer Science and Network Security, VOL.9 No.1, January 2009.

[9] Md. G. Rashed, S. Ullah *" Secured message data transactions with a Digital Envelope (DE) - High level cryptographic method"* International Conference on Engineering Research, Innovation and Education 2013, Bangladesh, 11−13 January 2013.

[10] R. Ganesan, M. Gobi, K. Vivekanandan *"A Novel Digital Envelope Approach for Secure E-Commerce Channel".* International Journal of Network Security, Vol.11, No.3, PP.121–127, Nov. 2010.

[11] L.M. Bottasso "A public-key cryptography tool for personal use: A true-world implementation of ECC for secure file exchange". E-Business and Telecommunications (ICETE), 12th International Joint Conference on 2016, July 2015.

[12] *F. Li, M. Shirase, T. Takagi "Identity-Based Hybrid Signcryption"* Availability, Reliability and Security, 2009. ARES '09. International Conference on March 2009.

Authors Profile

Mr. Sourabh Bhat pursed Bachelor of Engineering from Savitribai Phule Pune University in 2016 and pursuing Master of Engineering from DAVV University in year 2016-2018.

Dr. Vivek Kapoor acknowledged the B.E. degree in 1996 and M.TECH degree in Computer Science in 2003, Ph. D. degree in Computer Science in 2013. At present he is Asst. Prof. in IT department in IET DAVV university. His research concern comprises Data Mining, Information Security, Genetic Algorithm in Financial Engineering.

