A Novel Hybrid Cryptosystem for High-Security Text Encryption

Dr. Anjali R. Mehta, Dr. Ramesh V. Iyer, Dr. S. Priyadarshini
Department of Mathematics, Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India;
Department of Applied Mathematics, Anna University, Chennai, Tamil Nadu, India;
Department of Science and Humanities, PSG College of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

The recent information technology industry has facing more security vulnerabilities. The attackers are the major threats in hacking the third party data. To prevent from those attackers, a high secured approach is required to transmit the data over the internet. The proposed approach is aimed to offer a high secured way of text contents with combined cryptographic approaches. The proposed research work implements data security and cryptographic key security.

Keyword: *Hybrid, Hybrid Cryptography, AES, RSA, HTSecure.*

I. INTRODUCTION

Data transfer is the frequent and unavoidable thing in this modern era. For example: sharing email addresses, sharing web user accounts and bank related transactions. The unsecured way of data transfer can allow the third parties to access the data without any authentication. To avoid unauthorized access over the internet, more number of security approaches are proposed by the researchers. The cryptography is the powerful data security approach than the other innovations like steganography and etc. The attackers can able to trace the hidden data while using the steganography approaches. But the cryptographic approaches are usually can't be traced easily. Cryptography is the method of converting readable data into other format called encryption and reversing the conversion is called decryption. Encryption is made at the side of sender and receiver should decrypt the encrypted content.

The cryptographic approaches are summarized into the following types called symmetric and asymmetric algorithms. Symmetric key algorithms need a single secret key for encryption and the decryption. These algorithms are also called as private Key algorithms. Asymmetric algorithms are the combination of two different keys called public and private key.

The asymmetric algorithms are usually designed to perform the encryption with public key. The decryption is performed with the private key.

The Advanced Encryption Standard (AES) is the familiar and widely used algorithm which can offer highest data security and unbreakable from the symmetric cryptographic algorithms and the RSA cryptographic algorithm is the highest data security algorithm from the asymmetric key algorithms.

HTSecure approach is the primary goal of this research work. The HTSecure is the methodology which is aimed to offer highest text security with hybrid cryptographic approach. The proposed research work is aimed to provide a platform to perform the combined cryptographic approach based on the encryption and decryption. This proposed work combines the topmost symmetric algorithm AES and topmost asymmetric algorithm RSA. The new approach of combining symmetric and asymmetric algorithms is the powerful way than using the algorithms individually.

The HTSecure approach is aimed to provide very faster performance than using a single algorithm. Also the combined approach is aimed to provide a highest level of data security than the existing approaches.

The earlier cryptographic systems are explained with the following figures:

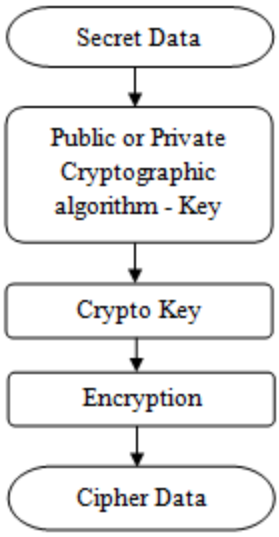

Figure 1: Usual Encryption

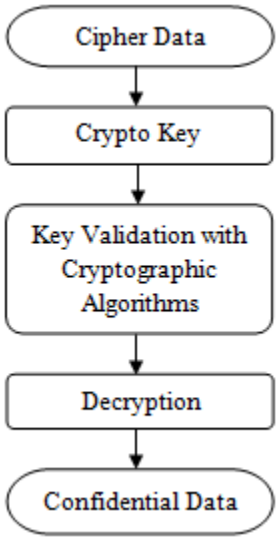

Figure 2: Usual Decryption

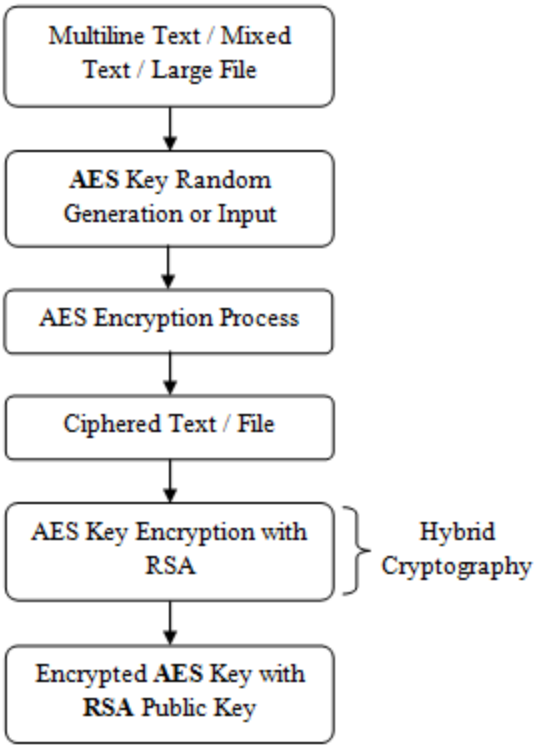

Figure 3: Encryption Flow Model in HTSecure Approach

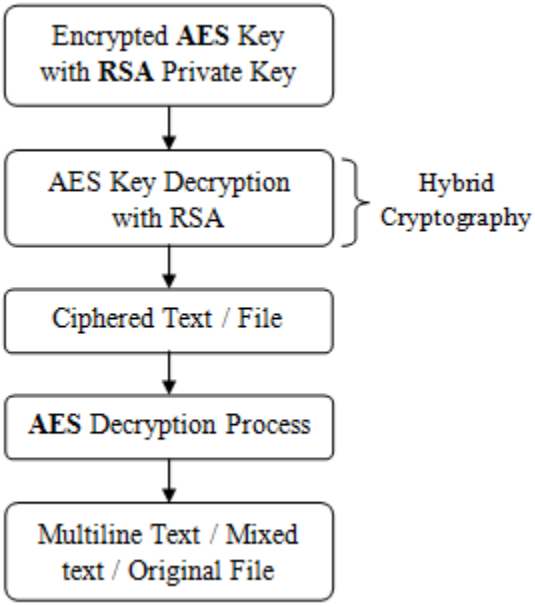

Figure 4: Decryption Flow Model in HTSecure Approach

II. RELATED WORK

Bhavik Rana, Sunil Wankhade., [1] in this proposal, the author's combines multiple cryptographic algorithms to provide high security for a single line secret text. The Authors implements a hybrid approach with multi layered

architecture. The proposed paper implements DES (Data Encryption Standard), IDEA (International Data Encryption Algorithms) and AES (Advanced Encryption Algorithm). A single line text is encrypted with the sequence of above and algorithm and decrypted with the reverse order of above algorithms.

Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, [2] in this paper, the authors analyzed the existing cryptographic algorithms and its applications. The authors proposed that the hybrid approach of cryptography offers high security than the usual cryptography with a single algorithm.

Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi.,[3], has proposed a linear block cipher algorithm. The approach demonstrates the hybrid approach of data and key management. The authors encrypt the data using AES and the AES symmetric key is also encrypted with the AES public key. The decryption is quite similar than the encryption like the private key is used to decrypt the public key and the public key decrypts the actual data.

Eman Salim Ibrahim Harba.,[4], in this proposal, the author proposed a hybrid based approach. The author implements an environment with AES, HMAC and RSA cryptographic algorithms. The encryption and decryption of data is done with the help of AES and HMAC. The private and public keys are secured with the help of RSA. The author concluded that the proposed approach is the highly advantage one. Also the author said, the proposed approach is fast and need very low RAM requirements.

Ch.Vijayalakshmi, L.Lavanya, Ch.Navya.,[5], has proposed a new novel cognitive authentication protocol called CoGAuth. This approach is developed to overcome the issues in the security over cognitive radio networks. The proposed approach employs hierarchy level of keys. The keys are classified into temporary keys, session keys and partial keys. The authors also utilize the AES and RSA algorithm mixed with COGAUTH approach.

The proposed approach is aimed to provide high security in CR based networks and CR devices.

III. RESEARCH OBJECTIVES:

The proposed research work is aimed to address the shortcomings of related works and to provide an efficient and effective approach in securing the data from unauthorized access. The related works are concluded that the hybrid cryptographic approach is better than using a single cryptographic algorithm. Also most of the attackers are easily track the secret keys and the data when using single crypto algorithms. The related approaches are implemented for single line text entries. The existing research work were implemented the hybrid cryptography with the help of AES, DES and IDEA algorithms.

These algorithms are implemented to encrypt and decrypt the single line text in sequential manner. This approach may collapse or made loss of actual data while encryption or decryption. If the same approach is implemented for a large and very large text file, then it consumes a very high processing time.

The HTSecure approach is proposed with modernized utilities in securing data from unauthorized access. The proposed approach is the new way of applying hybrid cryptographic approach in text, multi text, mixed text and large text files. The proposed approach is implemented as a hybrid crypto approach for text and document files. The approach is a common platform which is implemented with AES and RSA cryptographic algorithms. The architecture is planned to provide a fastest approach in hybrid cryptography than the existing approaches. The approach is also aimed to provide the enhanced cryptographic key security.

IV. SYSTEM MODEL

The HTSecure approach is aimed to provide an unique architecture to perform both encryption and decryption with hybrid approach. The approach is implemented with GUI (Graphical User Interface) based forms with the help of Microsoft Visual Studio.

The proposed approach allows the sender to upload text / document / rich text file into the processing drive. After the successful upload, the sender has to input the secret key to encrypt the file contents using the AES crypto

algorithm. The architecture loads and encrypts the file contents with AES algorithm and it's Key. After the successful encryption the framework allow the user to save the encrypted file in any storage device.

The proposed work inputs a secondary key from the sender. The secondary is utilized to encrypt the actual AES key. The AES key is encrypted with the secondary key with the help of RSA algorithm. The encrypted AES key is maintained in the memory heap. The receiver has to feed the encrypted key at first with its secondary key.

The framework validates and verifies the secondary key before the decryption of AES Key. The RSA decryption algorithm decrypts the actual AES key when the secondary key is validated successfully. After the decryption of encrypted AES key, the encrypted file will be decrypted with the help of AES decryption algorithm.

The framework allows the sender to upload and send the encrypted file with its encrypted password via internal email utility which is offered by the framework.

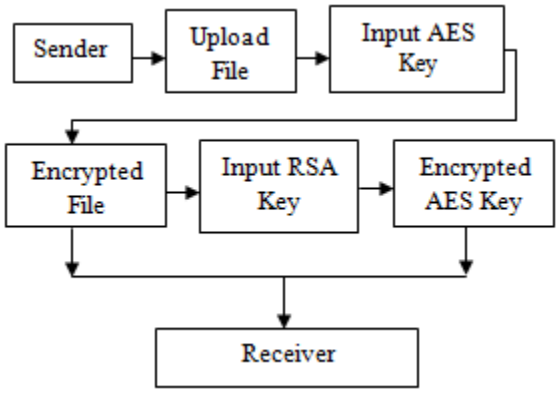

Figure 5: Sender Process Model

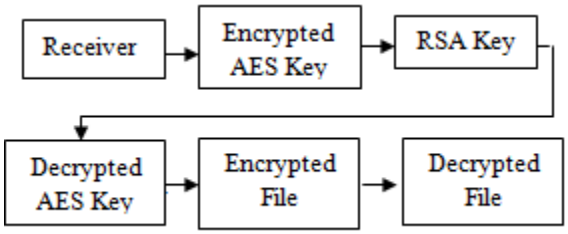

Figure 6: Receiver Process Model

The above figures demonstrate the sender side and receiver side processes with this hybrid cryptographic approach (HTSecure).

V. PROPOSED ALGORITHM

The Primary Steps for the Encryption:
Begin
Step1: Input Large Document / Text Files
Step 2: User Input – AES Secret Key
Step 3: File Encryption Process using AES
Step 4: File Creation Process – Encrypted File
Step 6: User Input - RSA Key (Secondary Key)
Step 7: AES Key Encryption process using RSA
Step 8: Encrypted AES Key
Stop

The Primary Steps for the Decryption:
Begin
Step 1: Input Shared File / Encrypted File
Step 2: Input Encrypted AES Key
Step 3: Input RSA Key (Secondary Key)
Step 3: AES Key Decryption process using RSA
Step 4: Decrypted (Actual) AES Key Verification
Step 5: Decryption of Encrypted File using decrypted AES Key.
Step 6: Decrypted File (Original File)
Stop

VI. RESULT AND DISCUSSIONS

The Proposed research work HTSecure is the newest approach which can solve all the issues in the existing research approaches in cryptography. The proposed approach proposes a combined approach of symmetric and asymmetric cryptographic algorithms to offer high data security and key security. Preventing the data from unauthorized access is very important. So the cryptographic approaches are introduced. Also, preventing the cryptographic key from the attacker is most important. This is the major theme of this research approach. The approach is implemented as a GUI application. The results and its performances are shown as below:

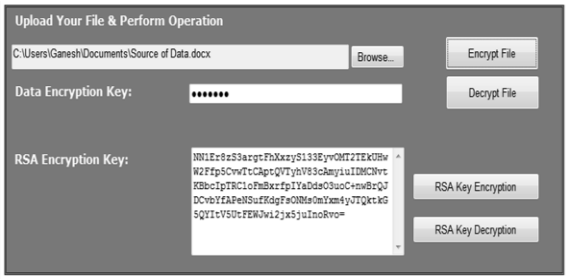

Figure 7: AES and RSA Hybrid Crypto Execution

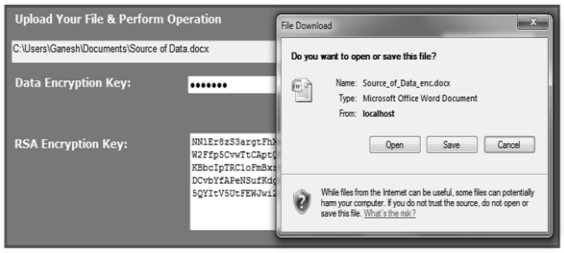

Figure 8: Encrypted File - Creation

Figure 9: Decryption of AES Key from Encrypted RSA Key

Figure 10: Decrypted AES Key

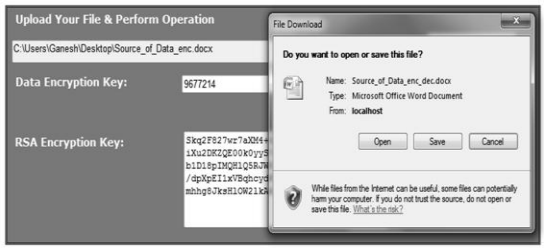

Figure 11: Decrypted File - Creation

Performance analysis

Table 1 – Time to Generate Keys

Algorithm	Time In Seconds
RSA & DES Approaches	8 Sec
Triple DES Approach	10 Sec
Proposed Approach (RSA & AES)	4 Sec

Table 2 – Encryption and Decryption Processing Time Measurement

No. Of Bits	Triple DES Approach	RSA & DES	Proposed Approach
100	250 MS	265 MS	220 MS
300	310 MS	335 MS	290 MS
500	350 MS	370 MS	330 MS
1000	435 MS	450 MS	385 MS

VII. CONCLUSION

The HTSecure approach is the unique framework which combines AES and RSA cryptographic algorithms to provide efficient data security and cryptographic algorithm key security. Based on the analysis of its performance, the proposed approach is very efficient than the existing approaches.

The hybrid cryptographic approach is tested with large and very large files. The approach performs the hybrid encryption and decryption in very less amount of time for any type of file than the existing approaches. This method of hybrid approach is very efficient and it offers very highest security for both data and its cryptographic key. The AES and RSA are unbreakable algorithms also performs the encryption and decryption process in fast and efficient

manner. The proposed approach is very easier to implement in any social media, data sharing networks, and communication services.

REFERENCE

1. *Bhavik Rana, Sunil Wankhade. "Hybrid Cryptographic Algorithm for EnhancingSecurity of Text", International Conference on Emanations in Modern Technology and Engineering (ICEMTE-2017), Volume: 5 Issue: 3*
2. *Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav. "Hybrid Key Cryptography: A Tool for Security". Vol. 6, Issue 3, March 2017 (IJIRSET)*
3. *Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi. "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm". Vol. 19, No. 2, March (2014).*
4. *Eman Salim Ibrahim Harba. "Secure Data Encryption through a Combination ofAES, RSA and HMAC". Engineering, Technology & Applied Science Research. Vol. 7, No. 4, 2017*
5. *Ch.Vijayalakshmi, L.Lavanya, Ch.Navya. "A Hybrid Encryption Algorithm Based On AES and RSA". Vol. 4, Issue 1, January 2016 (IJIRCCE).*