BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Yelahanka, Bengaluru-64

DEPARTMENT OF ELECTRONICS & TELECOMMUNICATION ENGINEERING

Course Name: Network Security	**Course Code:** 18EC821	**Sem:** VIII ETE
Course Coordinator: Dr. Siddiq Iqbal	**Batch:** 13	**Academic Year:** 2023-24

CO5: Perform in a **group** to make effective **presentation** on the topics related to applications of network security. **POs:** 9,10,12 **PSOs**-1

Poster Presentation on

"Secure Data Communication Using Padding Key Encryption Cryptography Algorithm"

Presented by: S Varsha (1BY20ET048), **Sagar Kothawar** (1BY20ET049), **Sharmila S** (1BY20ET053)

Abstract

Secure data communication is the most important and crucial problem by message transmission networks. The proposed Padding Key Encryption (PKE) algorithm is used to encrypt the data; it generates the secret key in an unreadable format. The receiver decrypts the data using the private key in a readable format. In the proposed PKE algorithm, the sender sends data into plain text to cipher-text using a secret key to the authorized person; the unauthorized person cannot access the data through the Internet; only an authorized person can view the data the private key.

Introduction

Cryptography is one of the safest data communications technologies; it encrypts and decrypts the given data for secure communication via networks. Rivest-Shamir-Adleman (RSA) is one of the most widely used public-key encryption methods. An RSA-enabled modular multiplier and modular layer requirement. Encryption not only protects against theft or data fraud, but it can also use for user authentication.

Methodology

1. The pre-processing stage prepares the data for analysis by sorting it and identifying message lengths.
2. The Padding Key Encryption (PKE) algorithm adds an extra bit to maintain the secret key.

   Algorithm Steps

   Step 1: Sender send plain text data M_E

   Step 2: initialize the message M_E

   Step 3: Sender encrypts the message using access private secret presentation key (s_k)

   Step 4- Remove the uncovered text region

   Step 5: Change the message forums to cipher ASCII and to attain odd prime factor o_n. $L_m = \sum ASCII\ values + o_n$

   Step 6: Loop for 256 sign ASCII for cipher conversion

   Step 7: Convert the message into cipher text (C_t) C_t= M_E mod l
3. The proposed PKE algorithm cipher-text encryption used to convert the cipher content.
4. The proposed PKE algorithm facilitates high-speed encryption and decryption using secure and private keys.
5. Decryption ensures that the receiver receives plaintext and facilitates conversion.

   Algorithm Steps:

   Step 1: Cipher text to input for decryption

   Step 2: access the private returned secret key P_K.

   Step 3: process encrypted message as ASCII values

   Step 4: Modulate ASCII formatted with binary message to return encrypted message

   Step 5: Encrypted content to decrypt content $M_E = C_t \ mod \ l$

   Step 6: return the original plain message.

Simulation and Results

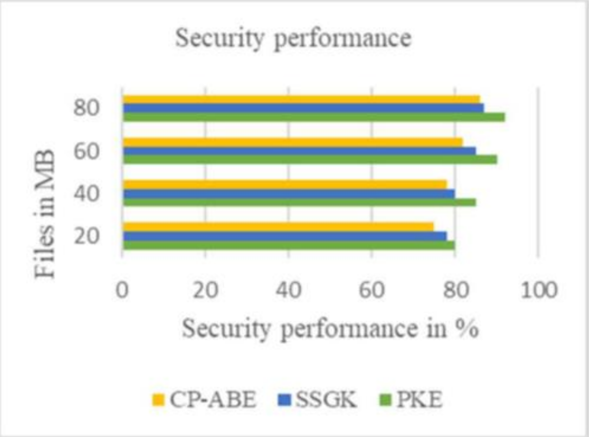

FIG. I. Analysis of security performance

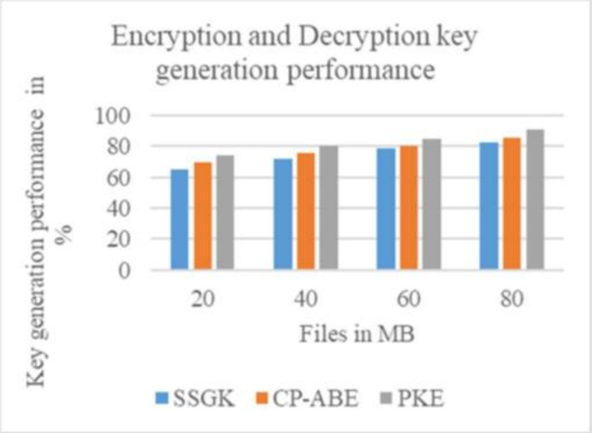

FIG. II. Encryption and Decryption key generation performance

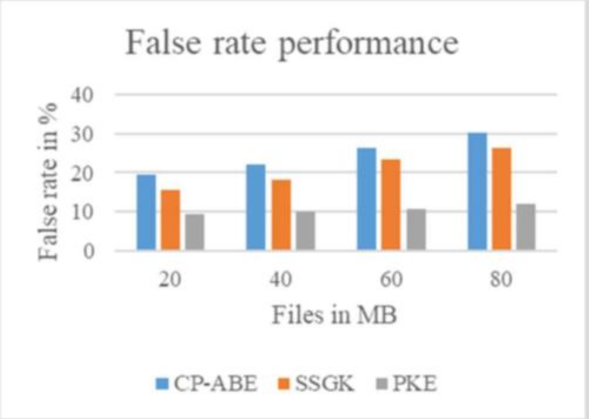

FIG. III. Evolution of False rate performance

Conclusion

The proposed PKE algorithm results provide a security performance is 92%, encryption and decryption key generation performance are 91%, the encryption time complexity is 33 sec, and decryption time complexity is 35sec.

References

[1] J. Feng, Laurence. T, R. Zhang; S. Zhang, "A Tensor-Based Optimization Model for Secure Sustainable Cyber-Physical-Social Big Data Computations," IEEE Transactions on Sustainable Computing June 2020

[2] L.Kuang, T. Yang, "An Integration Framework on Cloud for Cyber-Physical-Social Systems Big Data," IEEE Transactions on Cloud Computing, April 2020