Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secured Data Transfer in Wireless Networks Using Hybrid Cryptography

K.Brindha, G.Ramya
Assistant Professor(Senior)
School of Information Technology and Engineering,
VIT University, Vellore, India

Rajpal Amit Jayantila
School of Information
Technology and Engineering,
VIT University, Vellore, India

Abstract—In today's life, use of Internet is vast for accessing the information from enormous resources. Many times it requires sending important and secure information. Main objective of paper is exploring way of encryption done; improve some aspects of the algorithm which is already existed and create way for the excellent security. Implementation of encryption of the information is done in such a way that it will be impossible for the attackers to read the resources sent on the web. Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are the methods used for the encryption. In this encryption, conversion of file containing text is done using AES algorithm and key will be encrypted using ECC algorithm. Result will be text (cipher) which is decrypted on the receiver's side. AES and ECC algorithm implemented together to perform hybrid cryptography.

Keywords— Advanced Encryption Standard, Elliptic Curve Cryptography, Encryption, Decryption, Hybrid

I. INTRODUCTION

The Advanced Encryption Standard is the strong symmetric key cryptographic algorithm which has been introduced due to the limitations of other algorithms like DES (Data Encryption Standard). The security of AES will be high due to the presence of large number of rounds or blocks. The output of one block acts as the input of the next block in both encryption and decryption. For the wireless networks, this significantly is merit given to their power needs. The elliptic curve cryptography is a type of symmetric key encryption method that is used for key exchange, digital signatures and also for encrypting the secure data. When compared to the other asymmetric key algorithms the system resource utilization like band width, memory, hard disk of this ECC is very much less. Therefore ECC is treated as the best suitable cryptographic algorithms for the wireless devices. The common equation that is used to represent the ECC is the $y^2 = x3 + a^x + b$ where the values of a, b are fixed.

II. RELATED WORK

The algorithm is designed combination of two "symmetric" cryptographic techniques.

These two primitives were achieved with the help of Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

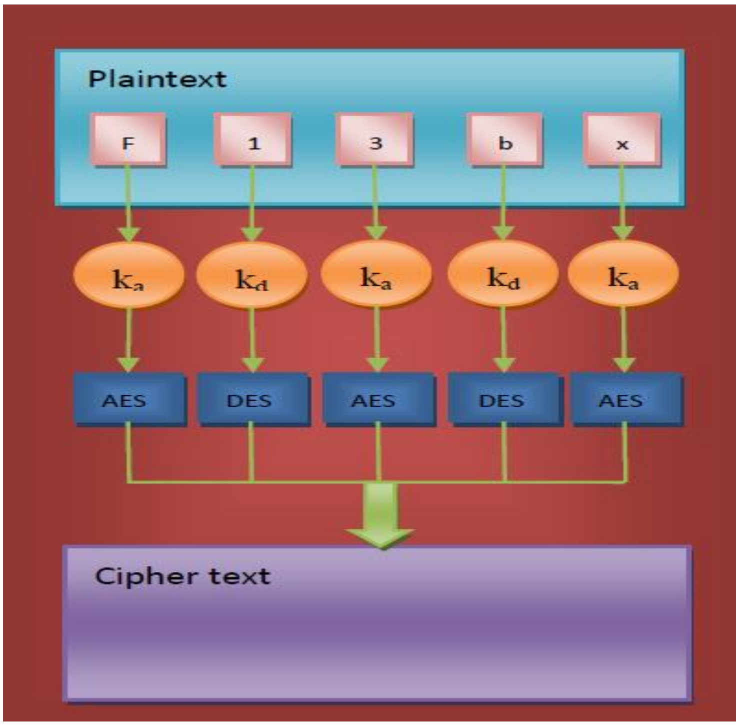

Fig. 2 Existing System

III. ALGORITHM

A. Advanced Encryption Standard (AES)

I. Derive the set of round keys from the cipher key.
II. Initialize the state array with the block data (plaintext).
III. Add the initial round key to the starting state array.
IV. Perform nine rounds of state manipulation.
V. Perform the tenth and final round of state manipulation.
VI. Copy the final state array out as the encrypted data (ciphertext).

The order of operation in decryption is:

1. *Perform initial decryption round:*
   XorRoundKey
   InvShiftRows
   InvSubBytes
2. *Perform nine full decryption rounds:*
   XorRoundKey
   InvMixColumns
   InvShiftRows
   InvSubBytes
3. *Perform final XorRoundKey*

The same round keys are used in the same order.

B. Elliptic Curve Integrated Encryption Scheme (ECIES)

Alice has the domain parameters D = (q, FR, a, b, G, n, h) and public key Q. Bob has the domain parameters D. Bob's public key is Q_B and private key is d_B. The ECIES mechanism is as follows.

Alice performs the following stepsA does the following

Step 1: Selects a random integer r in [1, n – 1]
Step 2: Computes R = rG
Step 3: Computes $K = hrQ_B = (K_x, K_y)$, checks that $K \neq \boldsymbol{O}$
Step 4: Computes keys $k_1||k_2 = KDF(K_x)$ where KDF is a key derivation function, which derives cryptographic keys from a shared secret
Step 5: Computes $c = ENC_{k1}(m)$ where m is the message to be sent and ENC a symmetric encryption algorithm
Step 6: Compute $t = MAC_{k2}(c)$ where MAC is message authentication code
Step 7: Sends (R, c, t) to Bob

To decrypt a cipher text, Bob performs the following steps

Step 1: Perform a partial key validation on R (check if $R \neq \boldsymbol{O}$, check if the coordinates of R are properly represented elements in F_q and check if R lies on the elliptic curve defined by a and b)
Step 2: Computes $K_B = h.d_B.R = (K_x, K_y)$, check $K \neq \boldsymbol{O}$
Step 3: Compute $k_1, k_2 = KDF (K_x)$
Step 4: Verify that $t = MAC_{k2}(c)$
Step 5: Computes m = $ENC_{K_1^{-1}}(c)$

We can see that $K = K_B$, since $K = h.r.Q_B = h.r.d_B.G = h.d_B.r.G = h.d_B.R = K_B$

IV. SYSTEM ARCHITECTURE:

A. Sender side:

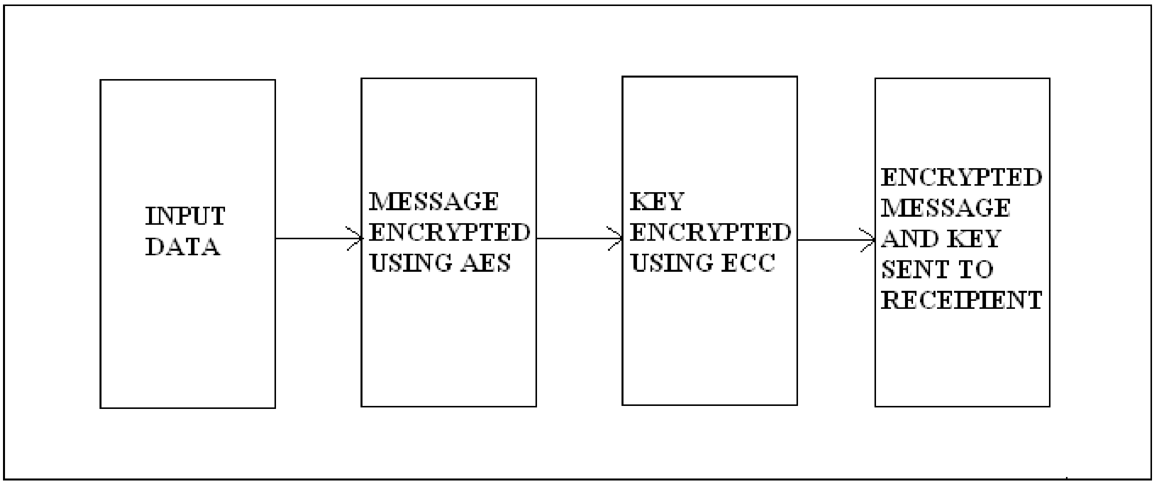
INPUT DATA
MESSAGE ENCRYPTED USING AES
KEY ENCRYPTED USING ECC
ENCRYPTED MESSAGE AND KEY SENT TO RECEIPIENT

Fig.4.1 System Architecture – Sender Side

B. Receiver Side:

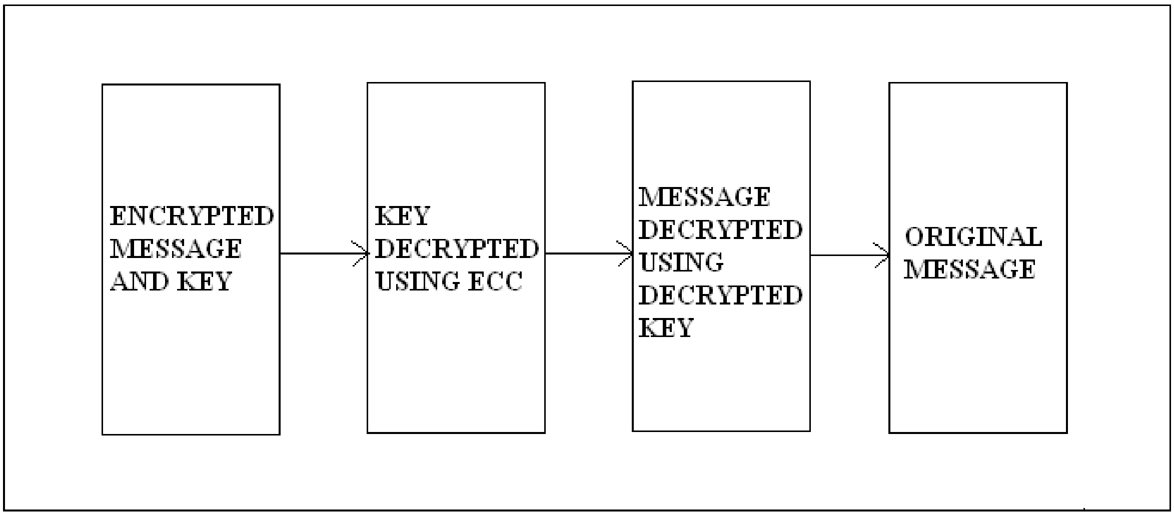
ENCRYPTED MESSAGE AND KEY
KEY DECRYPTED USING ECC
MESSAGE DECRYPTED USING DECRYPTED KEY
ORIGINAL MESSAGE

Fig. 4.2 System Architecture – Receiver Side

V. CONCLUSION

Secured Data Transfer in Wireless Networks Using Hybrid Cryptography provides the hybrid cryptography method. For better communication advanced algorithms are used which will be very hard to crack. The future recommendations of this project can include the selection of the appropriate encryption algorithms in such a way that all the network resources are utilized effectively and all the resource limitations of the sensor network are satisfied. In future if time permits I can implement this hybrid algorithm in a real scenario to check its effectiveness.

REFERENCES

[1] Dinghu Qin, Junli, Wanggen Wan. "*Research and Realization based on hybrid encryption algorithm of improved AES and ECC*," International Conference on Audio Language and Image Processing, pp.396-400., 2011.

[2] Abdul kader, Diaasalama and MohivHadhoud. "*Studying the Effect of Most Common Encryption Algorithms," "International Arab Journal of e-technology*," Vol.2. No.1.

[3] K. Ramesh Babu, Wang Tianfu. "*Design of a Hybrid Cryptography Algorithm," "International Journal of Computer Science & Communication Networks*," Vol. 2(2), 277-283, 2011.

[4] Jailin.S, Kayalvizhi.R, Vaidehi.V. "*Performance Analysis of Hybrid Cryptography for Secured Data Aggregation in Wireless Sensor Networks*," "IEEE-International Conference on Recent Trends in Information Technology", June 3-5, 2011.