International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S3, September 2019

Enhanced Data Security using Integrated Secret Key with Panagram Series

S. Yamuna Devi, R.Kavya, D. Monalisha, O.V Dhivya Bharathi, K. Ramya

Abstract:- ***In this fast moving world, communication among several systems via networks plays a vital role. It is significant to secure Data for a classified transmission. It becomes indispensable to protect information from unconstitutional users. The Existing system uses a common value shared between sender and the receiver. Parent string is arranged in ASCII order, therefore same cipher value is generated for a single character at every instance making brute force attack possible. The proposed system aims at the secured transmission of data in text format between the sender and the receiver. The system uses synchronous stream cipher for the secured transmission of data. The system uses algorithm that is integrated with a series of keys adding to which the message can be encrypted and by using this algorithm the cipher text is decrypted on the receiver end. A pangram is chosen as parent string, so that random cipher values are generated at every instance thereby making brute force attack impossible. The key value is generated by Tribonacci multiplication which uses a prime factor impossible for the hacker to trace the key using traffic analysis. The system remains secured as the secret key of the existing system is replaced with a series of hash value that are self generated by the built-in module in the sender and receiver.***

I. INTRODUCTION

Cryptography is essential in various wired and wireless network domains for securing emails, card data and corporate information. Some of the features of modern cryptography in information security are integrity and confidentiality of data, authentication.[1] [11]. Encryption of messages is essential in communication to avoid intruders from sneaking into our messages. Encryption includes the way toward changing over plain instant messages into cipher content. Decoding otherwise called decryption is the way toward reestablishing the plain content from the ciphered content. Cryptanalysis is the methods utilized for unraveling the content without the information about encryption. The significant targets of cryptography are classification, confirmation, non-revocation, get to control and availability[4].In order to perform encryption and decryption various cryptographic techniques are used such as AES, DES, 3DES, Blowfish and RSA. These techniques have different key size, block size, number of rounds and each method has different execution time and throughput.

II. LITERATURE REVIEW

A.H. Al-Hamami et Al., analyzed about Symmetric key cryptography technique in which sender and receiver shares same key for encryption and decryption. Symmetric key algorithm consists of two parts. Block cipher which is used for dividing data into blocks of data which are used for encryption and decryption. Example of block cipher is AES, triple DES which is popular techniques of symmetric algorithms. Stream cipher is the second part which works on a solitary bit at any given moment. Single-key encryption requires least assets and has diverse mystery key which is utilized for correspondence with each extraordinary gathering. On the off chance that the key is undermined, just the specific pair of sender and recipient is influenced leaving different interchanges unaffected [4].

R S Dhakar et al., concluded that Symmetric key cryptographic ciphers come in two varieties, stream and block ciphers. Padding bits are required to finish the somewhat filled blocks since the plain content are not generally in multiples of block size. In network applications block ciphers are used for transmission of huge size files which require high security. Cryptanalysis of block ciphers is difficult compared to stream ciphers. Block ciphers are used for providing better security. In SP network key and plain text are taken as an input and number of alternating rounds of S-Box substitution and permutation are applied to get a single cipher text block. The reverse process is done for decryption of the blocks[4].

R. Minni et al., in his work analyzed about public key cryptography. There are two types of keys, public and private key. The former being used for encryption and the latter for decryption. Private keys are known only to the concerned particular users whereas the public key is known to all users in the part of communication. The comparison of asymmetric and symmetric ciphers revealed that the former is slower and can be easily attacked by intruders but they make key exchange easier[6]. M.Thangavel et al., investigated the historical backdrop of RSA and its technique.

Manuscript published on 30 September 2019.
***** Correspondence Author (s)
S.YamunaDevi, Assistant Professor, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.(Email: yamuna.s@kce.ac.in)
R.Kavya,Student, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.(Email: kaavyasid19@gmail.com)
D.Monalisha, Student, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.(Email: monalishad98@gamil.com)
O.V DhivyaBharathi, Student, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.(Email: o.v.dhivyabharathi@gmail.com)
K.Ramya, Student, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, Tamilnadu, India.(Email: ramya.kandasamy98@gmail.com)

The RSA calculation has empowered a straightforward trade of the encoded correspondence between clients at various closures. Investigation of the exponent in the RSA calculation has uncovered that the security dimension of the RSA
calculation increments with exponent value. Subsequently, for high security levels, it is recommended to utilize high exponents in RSA algorithm [11].

F.Kong et al., explained the encryption and decryption using RSA and the cryptographic challenges with issues such as key distribution and speed of RSA. It proposes, RSA is slower just as its security depends on the trouble of considering expansive whole numbers. Sending a similar message with little exponent to various beneficiaries without paddinging empowers hackers to recuperate the plain content. It utilizes a similar key for encryption and marking which decreases the security[10].

Y. Li et al., in his work implemented an efficient RSA algorithm using two public key pairs and despite assigned the exponent value directly, he used mathematical logic because if an attacker has opportunity of getting e value they can directly find the d value and decrypt the message. The two open keys are sent independently, this makes the assailant not to get much learning about the key and unfit to unscramble the message[10].

III. EXISTING SYSTEM

RSA Algorithm

The algorithm for generating the public and private key is the mind boggling some portion of RSA cryptography. The Rabin-Miller fundamental test calculation is used to derive the prime numbers p and q. A modulus n is determined by augmentation of p and q.[11] The e figure shouldn't be a stealthily picked prime number as the open key is granted to everyone. The private key includes the modulus n and the private type d, which is resolved using the Extended Euclidean estimation to find the multiplicative inverse with respect to the totient of n. Consider modulo n, let's say that e is an integer that is co prime to the totient φ(n) of n. Further, say that d is the multiplicative inverse of e modulo φ (n).

n = modulus for modular arithmetic

φ (n) = n's totient

e = integer relatively prime to φ(n) .

This guarantees that e will possess a multiplicative inverse modulo φ(n)] d = an integer that is the multiplicative inverse of e modulo φ(n)[10].

IV. PROPOSED SYSTEM

Objective

- To overcome the difficulties faced by asymmetric cryptosystem
- To reduce the risk of assigning the same cipher value for a character at every instance
- To lessen the space and time complexity to encipher and decipher the data sent
- To create a more secured system where brute force attacks can't trace the data sent

Architecture diagram

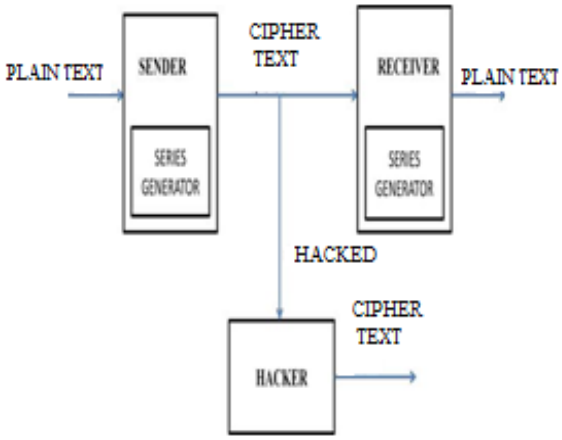

Fig.1.Architecture diagram

Description

The proposed system uses stream cipher technique where a single shift key is replaced by a series of hash values by which the encrypted text becomes harder to crack. The series of hash values are integrated inside the encrypting and decrypting programs so that it becomes nearly impossible for any hacker to get the knowledge of the encrypting algorithm and the key values. The system consists of a module in which an algorithm to generate a series of hash values in order to combine with the text data and form cipher text. The proposed system also has the parent string arranged in a random order so that even if the hacker manages to trace the hash value series, he will not be able to decipher the encrypted data without a properly ordered parent string similar to that in the encryption algorithm.

The computational steps for key generation are

1. Select a pangram as the parent string
2. Select a prime number p
3. Read the public factors a1 and b1 for a fixed value q from the sender
4. The fixed value has more than two set of factors
5. Calculate the private factors a2 and b2 for q at the receiver end
6. Encrypt the plain text, C=(a1*b1*p)+M where C=cipher text
7. Decrypt the cipher text, M=C-(a2*b2*p) where M=plain text

Advantages

- The system remains secured as the secret key of the existing system is replaced with a series of hash value that are self generated by the built-in module in the sender and receiver
- The cipher value given to a character is not the same at every instance whenever the character is repeated. So a hacker will not be able to trace the data by a brute force attack
- Parent string does not remain the same as that of the ASCII code order. So a hacker will not be able to crack the whole data that is sent using the ASCII code order of string arrangement

- The time and space complexity of the integrated secret key algorithm is less comparatively high with respect to other algorithms[7]

V. MODULE DESCRIPTION& RESULTS

Sender

The sender module acts as an encrypting client. In this module, a socket is created by specifying the IP address or by calling the local host address and a socket port. The sender program gets information at the sender end. It encrypts the information by calling a method encrypt(). At the sender end, the data given from the user is first encrypted and only then the cipher text is transmitted through network medium. The sender program gets information at the sender end. It encrypts the information by calling a method encrypt(). At the sender end, the data given from the user is first encrypted and only then the cipher text is transmitted through network medium.

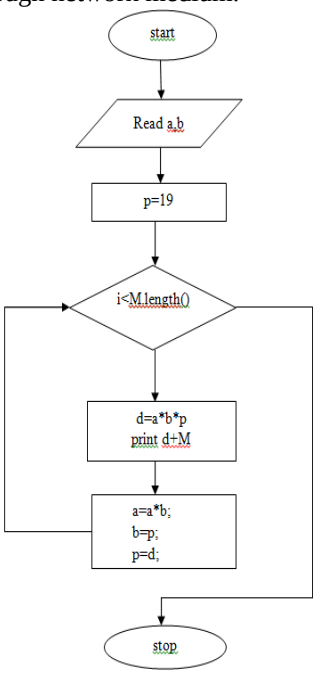

Fig. 2. Data flow diagram for sender

The following steps are involved at the sender side

- Select a pangram as the parent string
- Select a prime number p
- Read the public factors a1 and b1 for a fixed value q from the sender
- The fixed value has more than two set of factors
- Encrypt the plain text, C=(a1*b1*p)+M where C=cipher text

The sender here is the client who sends the message. The parent string is declared. A prime number is selected and assigned to a variable. Read the plain text from the user. Determine the position of each character in the parent string. Calculate the key value by calling the function func() and adding the result to character position. Replace the plain text using the position generated from key value. Assign the newly generated text to the variable cipher text. This is the encrypted message.

Encryption is carried out using the function encrypt(), where the client is required to enter two non prime factors of a fixed value. The two factors are then multiplied with the given prime number, the result of which is added to the plain text's position in order to obtain the cipher text's position. The same procedure is followed for the succeeding characters with the help of swapping as with a series called Tribonacci series.

The tribonacci numbers are a generalization of the Fibonacci numbers defined by $T_1=1$, $T_2=1$, $T_3=2$ and the recurrence equation $Tn=Tn-1+Tn-2+Tn-3$ for $n \geq 4$ [9].

They represent the n=3 case of the Fibonacci n-step numbers.

The first few terms using the above indexing convention for n=0, 1, 2,…,n are 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149,... (OEIS A000073; which however adopts the alternate indexing convention $T_0=T_1=0$ and $T_2=1$).

The first few prime tribonacci numbers are 2, 7, 13,149, ...(OEIS A092836), which have indices 3, 5, 6, 10, 86, 97,...(OEIS A092835) and no others with $n \leq 291217$.

Utilizing Brown's criteria, it is demonstrated that the Tribonacci numbers are complete; that is, each positive number can be composed as the aggregate of particular tribonacci numbers. Also, every positive number has a special Zeckendorf-like extension as the total of unmistakable tribonacci numbers and that whole does not contain three sequential tribonacci numbers. The Zeckendorf-like development can be registered by using greedy algorithm.

VI. CONCLUSION

In this system, encryption and decryption are done using stream cipher technique. Unlike the existing system, this system does not have risk of letting its data getting traced by brute force attacks possibly traffic analysis. The series of hash values are generated from a separate algorithm to ensure more security. The system remains secured as the secret key of the existing system is replaced with a series of hash values that are self generated by the built-in module in the sender and receiver. The system stands by the main advantage that even if the system is hacked by any hacker, it remains difficult for the hacker to trace the actual original data that is transmitted from the sender to the receiver.

REFERENCES

1. S.RadhaKrishnan and R.ShanthiPriya, "Eco-friendly materials used in traditional buildings of chettinad in Tamilnad, India", American Journal of Sustainable cities and society, Issue 3,vol 1.January 2014.
2. Luisa Maria Gil-Martin, Maria Jose Gonzalez Lopez and Alejandro Luis Grindlay, "Toward the production of future heritage structures:Considering durability in building performance and sustainability- A philosophical and historical overview", International Journal of Sustainable Built Environment(2012)1, 269-273.
3. Wankhede H.A and Wackchaure P.N, "Sustainable materials and Construction Techniques of Ancient India", Imperial journal of Interdisciplinary Research (IJIR),Vol-2,Issue-7,2016.
4. Marie D.Jackson and Eric N.Landis(September 2014), "Mechanical resilience and cementitious processes in Imperial Roman architectural mortar".
5. Waclaw Celadyn(2014), "Durability of Buildings and Sustainable architecture".
6. K.Van Belen and D. Van Gemert, "Modelling lime mortar carbonation", Materials in Structures,1994

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

7. S.Jeyalakshmi and S.Muthupandi, “Behavioural Study on partial replacement of lime and natural admixtures in conventional mortar”, International Advanced Research Journal in Science, Engineering and Technology,Vol.5,Issue 3,March 2018.
8. Dr.M.Vijaya Sekhar Reddy and K.Asha Latha (Jan-Apr 2018), “Effective utilization of Herbocrete- A natural admixture in cement mortar to assess the strength properties”, International Journal of Institutional & Industrial Research ISSN:2456-1274, Vol. 3,Issue 1,Jan-April 2018,pp 31-36.