IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125282

A Secured Communication System Using Cryptographic Techinques

Pardeshi Pooja[1], Bhavsar Vaishnavi[2], Wadkar Pooja[3], Khandekar Nikita[4], Prof. Dalvi A.S.[5]

Student of Department of Computer Engineering, S.N.D College of Engineering & Research Center, Yeola[1]

Student of Department of Computer Engineering, S.N.D College of Engineering & Research Center, Yeola[2]

Student of Department of Computer Engineering, S.N.D College of Engineering & Research Center, Yeola[3]

Student of Department of Computer Engineering, S.N.D College of Engineering & Research Center, Yeola[4]

Professor, Department of Computer Engineering, S.N.D College of Engineering & Research Center, Yeola[5]

Abstract: The field of cryptography deals with the procedure for conveying information securely. The goal is to allow the intended recipients of a message to receive the message properly while interrupt eavesdroppers from understanding the message. Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data classified and for verifying data indignity. The dynamite growth of the Internet has made an expanded familiarity with intrigue uncertainty issues. Even though security is the measure worries over the internet, numerous applications have been created and structured without considering fundamental destinations of data security that is confidentiality, authentication, and protection. Cryptography plays a huge role to ensuring confidentiality of the users credentials like passwords, IDs etc. Again security of any cryptosystem should be hardly breakable

I. INTRODUCTION

Enhancing the privacy, eligibility and reliability of the work requires a lot work to strengthen the current methods from constant trials to break them and to improve new ways that are resistant to most kinds of attacks if not all. The data change is made very snap, quick and exact utilizing the internet. In any case, one of the primary tests with sending data over the internet is the “security risk”. Security is a significant factor in the open system and cryptography assumes a significant job in this field. Cryptography is old and made sure about the system of information out in the open system. There is a complex cryptographic relationship between individuals and government or authority like military always has a tendency to communicate data with full security. . This system is a basic yet groundbreaking yet key circulation is the main issue that should be addressed. While asymmetric key encryption utilizes two mathematically related keys: Public Key and Private Key for encryption. The public key is accessible to everybody except the data once encoded by the public key of any client must be decrypted by the private key of that specific client as either sender or receiver.

II. LITERATURE SURVEY

The encryption step performed by a Caesar cipher is regularly joined as a component of progressively complex plans, for example, the Vigenère cipher, and still has present day application in the ROT13 framework. Similarly as with all single letters in order substitution ciphers, the Caesar cipher is effortlessly broken and in present day practice offers basically no correspondence security. In adjustment of Vigenere cipher by irregular numbers, punctuations and scientific images was introduced. In proposed technique numbers, punctuations furthermore, scientific images were utilized for key instead of characters to make it increasingly hard for animal power assault. It was inferred that if irregular numbers are utilized for key what's more, to spread the range then just skilled people can recognize the message recognize the message. Another algorithm by combining Vigenere substitution cipher with Stream cipher was proposed in which repeated bits of plaintext consistently encrypted with the diverse segment of the catchphrase or binary key. The letters in odd location were encoded with stream cipher and the letters in even location with Vigenere cipher, each letter of a given text is supplanted by a letter some fixed number of positions down the letters in order. For instance, with a move of 1, M would be supplanted by N, N would become O, and so on. This technique is named after Julius Caesar, who utilized it to speak with his authorities. Accordingly, to cipher a given text we need a whole number worth, known as a move which demonstrates the quantity of position each letter of the the text has been descended. To improve the quality of the encryption algorithm they proposed a hybrid model. The proposed model is a blend combination of AES and DES algorithmic cryptographic. The two algorithms are symmetric key procedure and itself they are especially able for encryption. Reconciliation of AES and DES would give a solid degree of security at encryption end. A critical improvement in results has been seen with the proposed arrangement.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125282

ALGORITHM DETAILS

In its encryption process, the method employs both Vigenere Cypher and Polybius Square Cypher.

- Vigenere will be used to operate on the ciphertext first. The process will begin with a key chosen at random.
- The resulting ciphertext is then used as Input for the Polybius Square Cypher process at the end of the process.
- This process will make the final ciphertext more difficult to decrypt using existing cryptanalysis techniques.
- A software program will be written in Python to demonstrate the effectiveness of the algorithm, and cryptanalysis will be performed on the ciphertext.

Vigenere Cipher:

There are 26^n potential keys when a Vigenere cipher with n keys is utilized. For instance, there are 456,976 potential keys with a key length of 4. The length of the key increases exponentially with the amount of computing power needed to crack a Vigenère cipher using brute force. With a key length of 10, there are more than 141 trillion potential keys, for instance.

Polybius Cipher:

If we assume that the plaintext consists only of uppercase letters (A-Z), then there are 25 possible plaintext symbols. Each symbol can be represented by a pair of numbers, where each number ranges from 1 to 5 (since the grid is a 5x5 matrix). Therefore, there are a total of 25^2 = 625 possible pairs of numbers that can be used to represent the plaintext symbols. Therefore, the actual number of valid pairs of numbers in the Polybius cipher will depend on the specific grid used for encryption. For a standard 5x5 grid with the letters of a keyword as the first row and column, there are a total of 600 valid pairs of numbers that can be used to represent the plaintext symbols.

SYSTEM ARCHITECTURE

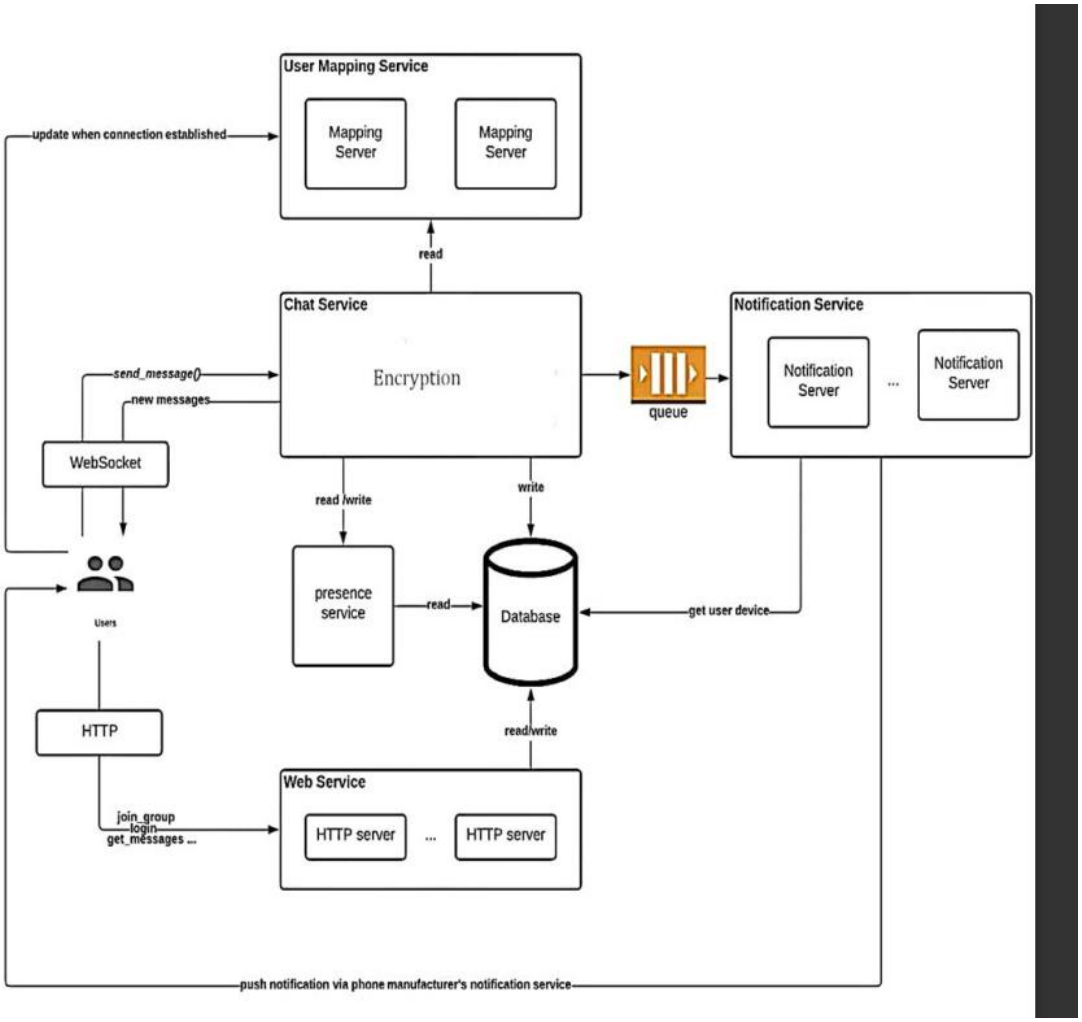

Fig. Architecture Diagram

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125282

Encryption:

Once the concept is outlined, we started with software development planning. We started the design process. We planned and drew some sample mockup user interface and build the project architecture. The inception stage helped us determine the product functionality.

Decryption:

Decryption is an opposite systematic procedure of encryption. It transforms the encrypted ciphertext into a message plaintext. In cryptography system decryption procedure execute at the receiver side. The process of decryption algorithm requires a couple of steps such as - a Decryption algorithm and a key.

CONCLUSION

Cryptanalysis, frequency analysis, pattern prediction and brute attack on proposed technique are also much difficult due to use of multiples tables for encryption. In spite of the fact that there are numerous cryptographic strategies yet this space still requires genuine consideration of research network for the improvement of data security. Cryptography is the generally utilized technique for the security, privacy, confidentiality and reliability of data. Single classic ciphers are cryptographic techniques that are viewed as least complex and most vulnerable because of numerous impediments, restriction, and smooth system. . If we know about all type of attack then it will be comparatively easy to improve the cryptographic tchniques or encryption techniques. Each cryptographic technique is unique in its own way, which might be suitable for different network security applications.

REFFRENCES

[1] A Secured Communication System Using Cryptographic Techinques, Pardeshi Pooja*1, Bhavsar Vaishnavi*2, Wadkar Pooja*3, Khandekar Nikita*4, Students of S.N.D College Of Engineering & Research Center,Yeola 2022

[2] Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher, Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma, School Of Computing Science And Engineering, North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020.

[3] An Overview on Security Issues in Modern Cryptographic Techniques, Bappaditya Jana*1, Chaibasa Engineering College, Techno India Group, Jharkhand India*1, Moumita Chakraborty*2, techno India Banipur, West Bengal, India*2,Tamoghna Mandal*3, Malay Kule*4, *3,4Indian Institute Of Engineering Science And Technology, Shibpur, West Bengal, India.