Secure Data Using Encryption And Decryption Of Data

Dr K Santhi
Department of Computer science and busniess systems
Panimalar Engineering College
Chennai,India

C Praveen
Department of Computer science and busniess systems
Panimalar Engineering College
Chennai,India

B Pravin
Department of Computer science and Panimalar Engineering College
Chennai,India

N Roshan
Department of Computer science and busniess systems
Chennai,India

***Abstract*—Applying cryptography to data encoding and decoding. The use of encryption to protect private data, conversations, or digital photos has become increasingly difficult as a result of recent developments in analysis. Analysing carrier data can rapidly reveal whether there is any hidden information there.. To facilitate communication between two private parties and public parties, this project provides a revolutionary cryptography technique. Both traditional and cryptographic approaches are used in the methodology presented in this study. The XChaCha20-Poly1305 algorithm is used in cryptography. We also use the mutual authentication technique to satisfy all criteria for cryptography, such as access control, confidentiality, integrity, and authentication. We can preserve the data more securely retain the data in this manner. Since the data is secured using the XChaCha20-Poly1305 algorithm. In order to prevent access by other network users to the already-available information. Only the sender and the recipient may extract the message from the data.**

Keywords- Cryptography, XChaCha20-Poly1305

I. INTRODUCTION

A. General

Digital communication-related Internet applications have seen substantial and continued growth. Consequently, providing secure communication sessions is required. Measures of network performance now heavily weigh the security of data sent over a worldwide network. The confidentiality and integrity of data must be maintained in order to prevent eavesdroppers from gaining access to and using transmitted data. Cryptography is a crucial technique that provides network security. The purpose of this project is to offer an innovative way to hide sensitive data by making use of the benefits of encryption.

B. Cryptography

One of the conventional approaches for ensuring the secrecy of interparty communication is cryptography. This technique, known as secret writing, is used to encrypt plaintext into ciphertext that may be sent between parties through an unsafe channel. The ciphertext may be unlocked using a working key to reveal the original plaintext. Nobody can retrieve the plaintext without the key. Confidentiality, anonymity, non-repudiation, key exchange, and authentication are just a few of the numerous elements in that cryptography play a crucial part.

C. Symmetric / Secret Key Cryptography

Secret key encryption is a method that is also referred to as symmetric-key, shared-key, single-key, and ultimately private-key encryption. Private key encryption and decryption are done on both ends using this method. The sender encrypts the original data, or plaintext, using a key, and the recipient uses a keyto decode a message and get the plaintext. Only those who are permitted to perform the encryption and decryption will have access to the key. However, while the method provides strong transmission security, it has a problem with key distribution. One can easily obtain all the data if they stole or discovered the key. An example of a Symmetric-Key is XChaCha20-Poly1305 Algorithm.

D. Asymmetric / Public Key Cryptography

This method, also known as an asymmetric cryptosystem or a public key cryptosystem, encrypts and decrypts data using two keys that are mathematically related to one another. When using the private key in this method, there is no way to access the data or even just find the other key. The decryption key is held secretly and is referred to as the private key because the encryption key is stored publicly. An example of Asymmetric-Key Algorithm is X25519. X25519 is an elliptic curve Diffie-Hellman key exchange using Curve25519. It allows two parties to jointly agree on a shared secret using an insecure channel.

This system's goal is to provide users with an interface where they may upload whatever files they want to transfer securely via networks in an encrypted format while encrypting them with a password. Using the same passphrase provided by the sender, the recipient may utilize this mechanism to decrypt the file they have received. If the recipient wants a file given to them securely across public networks, they can create a pair key from which they can share the sender with the public key in order to encrypt the information and distribute it without worrying about being attacked.

We utilize the XChaCha20 approach to encrypt and decode data instead of the conventional AES algorithm because the latter is more vulnerable to attack due to its widespread use in similar scenarios. In order to allow the user to choose the most appropriate technique for his needs, we have deliberately supplied both symmetric key (password) and asymmetric key (public/private) based encryption here in the same interface. In terms of asymmetric key encryption, the system can produce the key that must be used and can also keep the generated keys locally, eliminating the need to worry about losing the keys. As the system is hosted on the user's local host rather than a

public network, the files that are put into it are safeguarded there. Consequently, the system doesn't require a network connection to operate and carry out its features when utilized privately.

II. Literature survey

Ronaldo Serrano et al [1] Today's world, is more dependent on network communicationwhen it comes to application and usage of internet in online banking ,shopping,social network etc. The high the growth in networkingtechnology ends up in interchanging great amount of knowledge. Hence, whiletransmitting confidential information, there comes the requirement of datasecurityThe idea of encryption/decryptionalgorithms are used where the encryption is scrambling the plain message intocipher text and vice versa for decryption. This encoding/decoding isdone with the help of a secret key or code.Without the key an intruder cannotable to decrypt the messages (Heckerman, 1995). Hence cryptography plays avital role in securing the information. The cryptography isdivided into many types here we see two types namely symmetric andasymmetric cryptography. Symmetric key cryptographyis one where use of single key for both encryption and decryption.Whereas in public key cryptography one key act as public key forencryption and the other is private key to decrypt the message.

Aparna et al. [2] spoke about When sensitive data is kept and exchanged online, where it is no longer contained by physical borders, security becomes a top priority. By sending incomprehensible information that only the authorised receiver may view, cryptography is a crucial, effective, and efficient component to ensuring secure communication between the various organisations. A secure communication method that offers increased security, precision, and efficiency requires careful consideration while choosing a cryptographic algorithm. The most popular symmetric encryption algorithms, such as Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Blowfish, Advanced Encryption Standard (AES), and Hybrid Cubes Encryption Algorithm, are examined in this paper for their security-related features and processes(HiSea).

Ezeofor at al [11] discussed the examination of network data encryption and decryption methods employed in communication networks. Information sharing in network communication systems often takes place on networked computers, mobile phones, and other internet-connected electronic devices. Unsecured data can be read, manipulated, or falsified by anybody with access to it as it moves over various networks and is vulnerable to many different forms of attacks. Data encryption and decryption techniques are used to thwart such an assault. A Visual Basic simulation programme that encrypts and decrypts data was created, written, and tested in order to evaluate the performance of each encryption and decryption method used in communication networks. During data encryption, various data block sizes were recorded and plotted against overall response time.

SandipThitme et al. [12] spoke about Terabytes of data are produced every day in the internet and mobile phone age. Data security while communication via the internet is a significant concern. An essential component of the online data security system is cryptography. Information is rendered unreadable to unauthorised parties via cryptography. For real users, cryptography offers confidentiality and preserves integrity. Numerous cryptographic methods have been created during the previous year. However, each user requires a cryptographic method with the best level of performance and security. Several algorithms have a trade-off between cost and performance. Any cryptographic method that best fits the criteria can be selected by the user. We suggested a recent examination of several encryption and decryption strategies in this publication.

Information security has developed into a significant concern, according to Jiankuo et al. Recently, there has been a lot of research and development into data encryption and decryption due to the desire for better, more difficult-to-crack encryption and decryption. To meet these goals, cryptography is essential. AES, DES, RSA, and other encryption and decryption methods have recently been suggested by several academics. However, the majority of the suggested algorithms had issues with lack of resilience and a large increase in packet latency in order to preserve the security on the communication channel between the terminals.BjörnHaase et al[4] discussed the system's files and data are encrypted using a variety of well-known algorithms, including DES, RES, and AES. It is not impossible to break these algorithms and attack the files and information, even though they are sufficiently secure and difficult to breach. The encryption system uses the same set of algorithms that have been used to safeguard data throughout the internet. Due to recurring patterns in security flaws and weaknesses, this widespread use of comparable algorithms has been shown to be vulnerable to attack. As a new system that requires efficient and sufficient training before performing some operations, Chrome was previously using the AES algorithm to secure its service. This means that attackers now must deal with the difficulties of discovering new loopholes in their system, unlike AES, DES, and RES, which were previously broken through by sufficient research.

.

III. Design And Methodology

We utilise the XChaCha20 approach to encrypt and decode data instead of the conventional AES algorithm because the latter is more vulnerable to attack due to its widespread use in similar scenarios. In order to allow the user to choose the most appropriate technique for his needs, we have deliberately supplied both symmetric key (password) and asymmetric key (public/private) based encryption here in the same interface. In terms of asymmetric key encryption, he system can produce the key that must be used and can also keep the generated keys locally, eliminating the need to worry about losing the keys. As the system is hosted on the user's local host rather than a public network, the files that are put into it are safeguarded there. Consequently, the system doesn't require a network connection to operate and carry out its features when utilized privately.

The system was developed to be user-friendly and incorporates the entire functionalities on a single page with several modules built right into it. The modules are distinguished into tabs, from which one can choose the mode he need to accomplish his task properly. One may access all of the system's encrypting features in a single location rather than having to navigate through multiple pages. Fig1 represents the Architecture diagram.

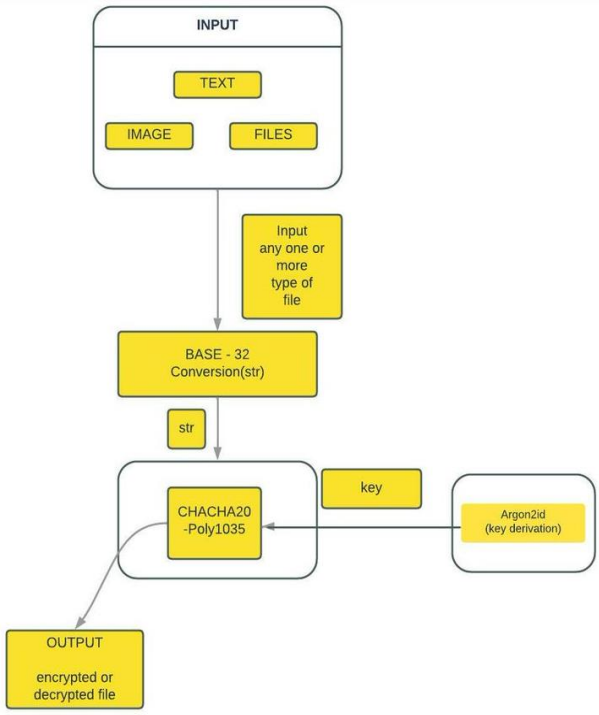

Fig1. Architecture diagram

A. Encryption panel

The tab where we will encrypt the file is the encryption panel module. This module comprises of selecting files, selecting an encryption method, setting an encryption password, and downloading the encrypted file.

1). Selecting the files: During this step, the user will browse the file that they want to encrypt. One or more files can be chosen by the user to be encrypted at once. The user will begiven two options for file encryption after selecting the files, and they can choose whichever one best fits their needs.

*2). Encryption methods:*The system will utilize the password the user enters to encrypt the files if they choose the password approach. The password must adhere to security standards or security concerns may occur or else they may use the password generation button to generate a password automatically for their file. We provided with a security description based on the password the user inputs after the password component.

On the other method, the system itself will develop a set of keys to be utilized in the encryption process and offer the user with a key generation procedure. The only sources of keys that the system will accept are those produced by the system itself.

3). Encrypted file: The files will be rendered unreadable by all types of extension readers after encryption, and if they are attempted to be opened in a word processor, they will display a complex mixture of symbols and characters that displays a cypher text that has no discernible meaning.

4). Downloading encrypted files: After the files have been successfully encrypted, you will be given the option to save the password locally in the system in case they forget to do so, removing the main flaw of the majority of current systems which is key loss. If the encryption is asymmetric, the system will provide a link that the receiver may use to load the decryption panel that is included with the encrypted file'spublic key, eliminating the need for the recipient to share their public key.

B. Decryption panel

The decryption panel module is the place where we will decrypt the file. Selecting files, recognizing the decryption technique, choosing a decryption password, and downloading the encrypted file are all included in this module.

1). Selecting the decrypting file: After choosing the file, the system recognizes the type of encryption mechanism used and provides alternatives depending on it for the user to input the key. The user will browse the file that they want to decode locally so that it won't be accessible to public networks. When choosing an encrypted file to decode, if the file is not in a recognized format, the programme will identify it as damaged and prompt the user to obtain another carefully encrypted file. When the uploaded file is acknowledged and ready to be decrypted, it will request the password or key needed to do so, preventing access by any other third parties that we might not desire.

*2). Downloading the decrypted file:*The receiver can have the original file safely decrypted and view it when the user enters the right key to the decrypted file. The system will decrypt the file and instantly provide the option to download it locally into the system.

C. Algorithm

1). The ChaCha20 Algorithm

ChaCha20 is a stream cipher which is are finement of the Salsa20 algorithm, and it uses a 256-bit key. It successively calls the ChaCha20 block function, with the same key and nonce, and with successively increasing block counter parameters.

```
chacha20_encrypt(key, counter, nonce, plaintext):
for j = 0 upto floor(len(plaintext)/64)-1
key_stream = chacha20_block(key, counter+j, nonce)
block = plaintext[(j*64)..(j*64+63)]
encrypted_message += block ^ key_stream
end
if ((len(plaintext) % 64) != 0)
j = floor(len(plaintext)/64)
key_stream = chacha20_block(key, counter+j, nonce)
block = plaintext[(j*64)..len(plaintext)-1]
encrypted_message +=
(block^key_stream)[0..len(plaintext)%64]
end
returnencrypted_message
end
```

2). The Poly1305 Algorithm

Poly1305 is a one-time authenticator which takes a 32-byte one-time key and a message and produces a16-byte tag. This tag is used to authenticate the message**.**

```
clamp(r): r &= 0x0ffffffc0ffffffc0ffffffc0fffffff
poly1305_mac(msg, key):
r = (le_bytes_to_num(key[0..15])
clamp(r)
s = le_num(key[16..31])
accumulator = 0
```

```
p = (1<<130)-5
fori=1 upto ceil(msg length in bytes / 16)
n = le_bytes_to_num(msg[((i-1)*16)..(i*16)] | [0x01])
a += n
a = (r * a) % p
end
a += s
return num_to_16_le_bytes(a)
end
```

We utilise the XChaCha20 approach to encrypt and decode data instead of theconventional AES algorithm because the latter is more vulnerable to attack dueto its widespread use in similar scenarios. In order to allow the user to choosethe most appropriate technique for his needs, we have deliberately supplied bothsymmetric key (password) and asymmetric key (public/private) basedencryption here in the same interface. In terms of asymmetric key encryption,the system can produce the key that must be used and can also keep thegenerated keys locally, eliminating the need to worry about losing the keys. Asthe system is hosted on the user's local host rather than a public network, thefiles that are put into it are safeguarded there. Consequently, the system doesnotrequire a network connection to operate and carry out its features when utilised
privately.

IV. Conclusion

Data encryption and decryption systems are used to improve informationsecurity to secure data that, thereby providing enhanced level of assurance suchthat the data that are encrypted cannot be viewed by unauthorized parties in theevent of theft, loss or interception. This system replaces the existing dataencryption and decryption system by adding some functionality such as digitalsignature

References

[1] "ChaCha20–Poly1305 Authenticated Encryption with Additional Data for Transport Layer Security 1.3" Ronaldo Serrano , Ckristian Duran , Marco Sarmiento , Cong-Kha Pham and Trong-Thuc, Hoang Department of Computer and Network Engineering, The University of Electro-Communications (UEC), Tokyo 182-8585, Japan; Published in October 2021.

[2] "ARGON2id IP Core" byAparna R, R. Nandakumar, Dr. Anil Kumar C.D, PG Scholar & Dept. of Electronics and Communication Engineering, GEC Idukki, kerala, India Scientist/Engineer & Dept. of Electronics and Communication Engineering, NIELIT, Calicut, Kerala, India Professor, Dept. of Electronics and Communication Engineering, GEC Idukki, kerala, India, Published in Volume: 06 Issue: 06 | June 2019.

[3] "Towards High-performance X25519/448 Key Agreement in General Purpose GPUs" by Jiankuo Dong, FangyuZheng B, Juanjuan Cheng, Jingqiang Lin, Wuqiong Pan and Ziyang Wang state Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China Published in 2018 IEEE Conference on Communications and Network Security (CNS).

[4]]"Making Password Authenticated Key Exchange suitable for resource-constrained industrial control devices" by BjörnHaase and BenoîtLabriqueEndress + Hauser Conducta GmbH & Co. KG, Dieselstr. 24, 70839 Gerlingen, Germany,Published in 2017..

[5] "A Coq proof of the correctness of X25519 in TweetNaCl" by Peter Schwabe MPI-SP, Germany &Radboud University, The Netherlands BenoîtViguierRadboud University, The Netherlands Timmy WeerwagRadboud University & Open University of the Netherlands FreekWiedijkRadboudUniversity,TheNetherlands,Published in 2021.

[6] [6] "A. ChaCha20-in-Memory for Side-Channel Resistance in IoT Edge-Node Device" by Aamir, M.; Sharma, S.; Grover, Open J. IEEE Circ. Syst., Published in 2021.

[7] "ChaCha20-Poly1305 Crypto Core Compatible with Transport Layer Security 1.3" by Serrano, R.; Duran, C.; Hoang, T.-T.; Sarmiento, M.; Tsukamoto, A.; Suzaki, K.; Pham, C.-K. In Proceedings of the International SoC Design Conference (ISOCC), JejuIsland,Korea, Published in 6–9 October 2021.

[8] "ChaCha20-Poly1305 Authenticated Encryption for High-speed Embedded IoT Applications" by De Santis, F.; Schauer, A.; Sigl, G. In Proceedings of the Design, Automation & Test in Europe Conference Exhibition (DATE), Lausanne, Switzerland, Published in 27–31 March 2017;

[9] "Argon2: new generation of memory-hard functions for password hashing and other applications"byBiryukov, Alex, Daniel Dinu, and Dmitry Khovratovich. IEEE European Symposium on Security and Privacy (EuroS&P). IEEE Published in 2016.

[10]"A Survey on the Cryptographic Encryption Algorithms", by MuhammedFaheemMushtaq The Islamia University of Bahawalpur,SapieeJamelUniversitiTun Hussein OnnMalaysia,ZahraddeenAbubakarPindarUniversitiTun Hussein OnnMalaysia,Mustafa Mat Deris Telkom University, International Journal of Advanced Computer Science and Applications Published in 2017.

[11]"Analysis of Network Data Encryption & Decryption Techniques in Communication Systems "by Ezeofor C. J.1, Ulasi A. G. Published in 2Vol. 3, Issue 12, December 2014.

[12]"A Recent Study of Various Encryption and Decryption Techniques", by SandipThitme, Vijay Kumar Verma Published in Volume 1, Issue 3, pp. 92-94, 2016.