International Journal of Application on Sciences, Technology and Engineering
(IJASTE)
Volume 1, Issue 3, 2023. ISSN:2987-2499

CHAT SIMULATOR USING AES ENCRYPTION

Sukhwinderjit Singh[1], Hadian Satria Utama[2*], Joni Fat[3]

[1] Electrical Engineering Department, Universitas Tarumanagara, Jakarta, Indonesia
Email: sukhwinderjit.525190011@stu.untar.ac.id
[2] Electrical Engineering Department, Universitas Tarumanagara, Jakarta, Indonesia
Email: hadianu@ft.untar.ac.id
[3] Electrical Engineering Department, Universitas Tarumanagara, Jakarta, Indonesia
Email: jonif@ft.untar.ac.id

*Corresponding Author

Submitted: 11-03-2023, Revised: 12-03-2023, Accepted: 14-03-2023

ABSTRACT

Smartphones have become an integral part the lives of individuals and their priorities The present moment. The most visible uses are to chat and chat programs Most of these apps do does not provide the necessary protection and privacy information exchanged between users. Chat apps have become one of the most important and popular smartphone apps. It has the ability to exchange text messages, images and files that can freely communicate with each other. All messages must be protected and in this paper the encryption to used for secure all messages is by using AES encryption. AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely used to keep data confidential in Internet networks. AES uses a block cipher with a block length of 128 bits and can encrypt data with keys consisting of 128, 192, or 256 bits. AES is one of the strongest encryption algorithms available today. It has been adopted by many organizations, including governments, banks, and technology companies. AES security is based on mathematical complexity and is difficult to crack even on ultra-fast computers. The AES encryption process involves multiple steps such as replace, move, and merge. The original data is split into smaller blocks and encrypted with the provided key. The blocks then change periodically, complicating the data patterns an attacker might find.

Keywords: *AES Encryption, Android, Secured Chat Application*

1. INTRODUCTION

In today's digital age, messaging applications are the most commonly used means of communication. However, the advent of digital communications has increased the risk of unauthorized access to users' personal information and messages. Chat encryption is an important tool for protecting user privacy and protecting messages from prying eyes. Chat encryption works by encrypting messages so that only the intended recipient can read them. This process ensures that third parties such as Internet service providers, government agencies, and hackers cannot intercept and read your messages. Chat encryption also provides message integrity. This means that messages cannot be tampered with or altered in transit.Messaging has seen a number of high-profile data breaches and cyberattacks against his platform in recent years, raising user concerns about the security and privacy of their messages. As a result, chat encryption is becoming increasingly important to ensure user privacy and security online.This article examines the importance of chat encryption, the types of encryption methods available, and their effectiveness in protecting chat messages. We also discuss some challenges and limitations of chat encryption and how developers can overcome them to improve security and privacy in messaging apps.

With the rapid development of mobile phones, mobile devices have become an integral part of daily activities. In recent years, chat apps have evolved and made a big difference in social media

https://doi.org/10.24912/ijaste.v1.i3.931-940

because of their unique features that attract the audience [1].The traditional text message is quickly becoming obsolete, especially with the explosion of popular chat apps. WhatsApp, Telegram, Viber and various applications offer free text messages. It also does not mean that the options for sharing audio and images to different clients are mentioned. Chat apps have become a way of life [2], [3]. In recent years, data confidentiality, authentication, integrity, non-repudiation, access control and availability are the most important information security services in the security criteria considered in secure applications and frameworks. Despite this, mobile chat systems do not provide such security services. Both the mobile chat system client and the mobile chat system server are protected against both passive and active attacks. Passive threats are related to message body arrival and traffic investigation, while active threats combine message content manipulation, masking, replay and denial of service (DoS). Really, all the defined risks are suitable for mobile chat [2].

2. RESEARCH METHOD

Encryption

Encryption is a method of changing the form of data into a string of hard-to-transform codes so that it cannot be read by third parties. Encrypted data can only be read by recipients with a specific key. This key can be obtained directly from the document or data author**.** In order to make the original communication unintelligible to those who lack the encryption key, encryption scrambles the message using a mathematical technique (cipher text). Cipher text is a term used to describe a message or piece of data that has been encrypted using a mathematical formula or encryption key to make it unintelligible from its original form (plaintext). Anyone without the key to unlock the ciphertext and restore it to unencrypted form will be unable to understand it. In other terms, it is a technique for encoding data or messages such that only authorized people can decipher their contents. Ciphertext, a crucial component of contemporary cryptography, is frequently employed to safeguard sensitive data during transmission or storage. The ciphertext is converted back into plain text using a piece of information known as the key. They can be divided into symmetric (private) and asymmetric (public) keys. encryption. Symmetric or private key cryptography uses only one key to encrypt and decrypt data. Asymmetric keys use two keys. private and public key. The public key is used for encryption and the private key for decryption (such as RSA or ECC). Public-key cryptography is based on mathematical functions, is computationally intensive, and is not very efficient for small mobile devices. Encryption algorithms are widely used and information security. They can be classified as Symmetric (private) and asymmetric (public) keys encryption. Symmetric key cryptography or secret key Encryption uses only one key for encryption and decryption data. Keys must be distributed before sending between entities. Keys play an important role. weak key is used in an algorithm, anyone can decrypt the data. The strength of symmetric key ciphers depends on their size There are many examples of the strength and weakness of the keys to be used RC2, DES, 3DES, RC6, blowfish, AES. RC2 uses a 64-bit key. DES. Use 64-bit keys. Triple DES (3DES) is three 64-bit key. AES uses different (128,192,256) bit keys asymmetric or public key cryptography [4]. Encryption has become an important aspect of modern communications and data storage as concerns about cyberattacks and data breaches grow. Encryption technology can be used to protect sensitive data and communications from unauthorized access. Encryption is used in various industries and applications to protect sensitive data such as online banking, e-commerce, and email communications. It is also used in the healthcare industry to protect patient data, and in government and military applications to protect sensitive information.Encryption algorithms have evolved over time, with newer, more robust algorithms being developed to combat increasingly sophisticated cyberattacks. Modern cryptographic algorithms use complex mathematical functions to encrypt data, making it virtually impossible to decipher without the proper key. Encryption strength depends on the length and complexity of the encryption key. Therefore, the longer the key, the greater the security.Encryption is also used in digital signatures to ensure the authenticity and integrity of electronic documents. Digital signatures use public key infrastructure (PKI) to verify the signer's identity and ensure that the document has not been altered since it was signed.Encryption technology is also used to develop secure messaging apps that provide end-to-end encryption. End-to-end encryption ensures that messages can only be read by the sender and recipient and cannot be intercepted or accessed by third parties, including app providers and government agencies. Email communication is protected by encryption as well. Today, encryption is often used by default in email systems to prevent messages from being intercepted and read by unwanted parties. Medical records and other sensitive data are protected using encryption as well. As the usage of electronic health records rises, it is crucial to make sure that patient data is shielded from unwanted access.

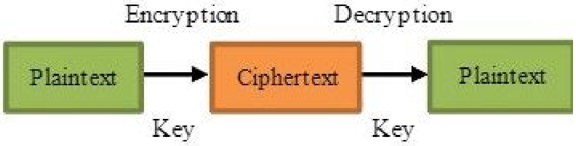


Figure 1. Common encryption scheme

Source: [5]

Symmetric Key Encryption

Symmetric-key cryptographic algorithms comprise a class of algorithms for encryption that use the same cryptographic key to encrypt plaintext and decrypt ciphertext. This is the oldest known encryption method. A private key can be something as simple as a number or a string. In practice, a key represents a shared secret between participants to maintain a secret connection.

The requirement that both parties have access to the private key is one of the main drawbacks of symmetric-key cryptography compared to public-key cryptography. Symmetric key encryption can use either stream ciphers or block ciphers. Stream ciphers encrypt the numbers/bytes of a message individually, while block ciphers take many bits as input and encrypt them as a unit [6]. The Advanced Encryption Standard (AES) is one of the most popular symmetric encryption methods. The block cipher algorithm AES encrypts data in discrete, fixed-size blocks. AES uses 128 bits as its default block size, but different block sizes can also be employed. AES is utilized in a variety of applications, such as online banking, e-commerce, and email communication. It is regarded as one of the most secure symmetric encryption algorithms.

Symmetric encryption has several benefits, one of which is that it is typically faster and simpler than asymmetric encryption. Symmetric encryption techniques often operate faster and use less computer resources than asymmetric encryption algorithms since the same key is used for both encryption and decryption. They are therefore perfect for applications that demand real-time encryption and decryption, including streaming video or internet conversation.

One of the main disadvantages of symmetric encryption is the requirement to utilize the same key for encryption and decryption is one of symmetric encryption's primary drawbacks. This necessitates the sharing of the key between the sender and the receiver, which poses a security concern if the key is obtained by an intruder. The key needs to be kept a secret and secured against unauthorized access in order to maintain the encryption's level of security.

Asymmetric Key Encryption

Asymmetric encryption algorithms (public key algorithms) use different keys for encryption and decryption. Although some schools of thought believe that the decryption key cannot be derived from the encryption key, and that their implementation is based on digital certificates, the true meaning is that the decryption key cannot be derived from the encryption key. You can generate a decryption key from an encryption key by extracting the keys. Use software tools such as Open Secure Socket Layer (OpenSSL). One problem with private keys is exchanging them over the Internet while protecting them from theft. Anyone who knows the private key can decrypt the message. Your public key is available to anyone who wants to send or receive messages. The second private key should be kept secret only by its owner. This means you don't have to worry about sharing your public key over the internet. One problem with asymmetric encryption is that it is slower than symmetric encryption. Also, encrypting both requires more processing power (battery).

Decrypt the contents of the message. In it, everyone has a pair of keys instead of a single key. One key, called the public key, is known to everyone, and the other private key is known only to its owner. There is a mathematical relationship between these keys [7]. RSA (Rivest-Shamir-Adleman) is the most popular asymmetric encryption method for chat encryption. A public key and a private key are used by the public-key cryptosystem known as RSA to encrypt and decrypt data. The approach is based on the observation that the product of two huge prime integers is exceedingly challenging to factorize.

The fact that asymmetric encryption offers a higher level of security than symmetric encryption is one of its key advantages. Asymmetric encryption is less susceptible to attacks than symmetric encryption since the private key is never shared. For applications that need a high level of security, such online banking, e-commerce, and digital signatures, this makes it the best choice.

One of the main drawbacks of asymmetric encryption is that it is slower and more computationally intensive than symmetric encryption. This is because the algorithms used in asymmetric encryption are more complex and require more computing power. This can be a significant problem for applications requiring real-time encryption and decryption, such as: B. Online Communications or Streaming Media. Another drawback of asymmetric cryptography is that it is more complex to implement and maintain than symmetric cryptography. Because two keys are involved, asymmetric cryptography requires more careful management of keys to keep them secure and not compromised by an attacker. This can add complexity to your system and increase the risk of bugs and vulnerabilities.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES), also known as Reijndael, is used. Safe information. AES is an analyzed symmetric block cipher. Widely used today. AES, symmetric key encryption It uses an algorithm with a key length of 128 bits. high security, mathematical robustness, resistance to all known attacks, high cryptographic speed, It is license-free worldwide and compatible with a wide range of hardware and software. AES algorithm properties. The DES and 3DES encryption algorithms have gaps, but the AES algorithm has no such gaps so far [8]. AES (Advanced Encryption Standard) is a common symmetric encryption technique that encrypts data in fixed-size blocks of 128 bits using a 128-bit, 192-bit, or 256-bit private key. The number of permutation and permutation rounds used in the encryption process depends on the key size. Data is encrypted with a unique round key for each round. Due to its protection against known threats, AES is considered a secure encryption algorithm. Applications include Internet communications, data storage, financial transactions, and more. The decryption process is the inverse of the encryption process by using the same key and the opposite action as the encryption process. AES has a number of important characteristics that lead to its widespread use. Due to its resilience to many attacks, such as differential and linear cryptanalysis, it provides a high level of security. With options for software optimization, hardware acceleration, and parallel processing, AES is also quite efficient. It is a flexible option for protecting a diverse range of applications due to its compatibility, flexibility, and simplicity. The security of AES lies in its ability to combine confusion and diffusion to maintain confidentiality. Confusion is achieved through the use of permutation operations that introduce nonlinearities and make it difficult to discern the relationship between plaintext and ciphertext. Spreading is achieved by a permutation operation that distributes the effect of each input bit over the entire output, thus distributing the effect of individual bit changes. AES has been extensively analyzed and compared to other encryption algorithms. This section provides a comparative analysis of AES and DES, triple DES, and other symmetric encryption algorithms. Evaluate a variety of criteria, including security, performance, key length, and suitability for a particular application, to understand the advantages of AES and justify its continued use. An efficient and secure implementation of AES requires careful consideration of key management, modes of operation, padding schemes, optimization techniques, and other factors. This section provides insight into these implementation considerations, including guidance on choosing appropriate key sizes, using secure modes of operation (CBC, CTR, etc.), and integrating cryptographic libraries with hardware support.

Planning

System designed to use AES encryption, the chat simulator enables real-time communication between users while maintaining the confidentiality of exchanged messages. Developing a chat simulator using the Python programming language gives developers flexibility and ease of use. The command line interface (CLI) used by the chat simulator allows users to interact with the system through text commands. This is especially useful for systems that require fast and efficient communication. Wireshark network protocol analyzer is a powerful tool that has been used to capture and examine network traffic and verify the effectiveness of encryption. Wireshark is an open source network packet analyzer that can capture and analyze network traffic in real time. Analysis of network traffic confirmed that messages exchanged between users were indeed encrypted using the AES encryption method. This gives users peace of mind that their messages are safe and will not be intercepted by unauthorized persons.

Implementing an AES encrypted chat system is especially important in scheduling systems where sensitive information is shared between team members. An AES-encrypted chat system allows team members to communicate securely and share sensitive information without fear of being intercepted by unauthorized persons. This provides a safe environment for team members to collaborate and work on projects while maintaining the confidentiality of shared information. In summary, implementing an AES encrypted chat system provides a secure environment for real-time communication between users. Using the Python programming language and CLI provides flexibility and ease of use for developers and users. Using the Wireshark network protocol analyzer ensures the effectiveness of your encryption and gives you confidence that your messages are safe. Implementing an AES encrypted chat system is especially important for scheduling systems where confidential information is shared between team members.

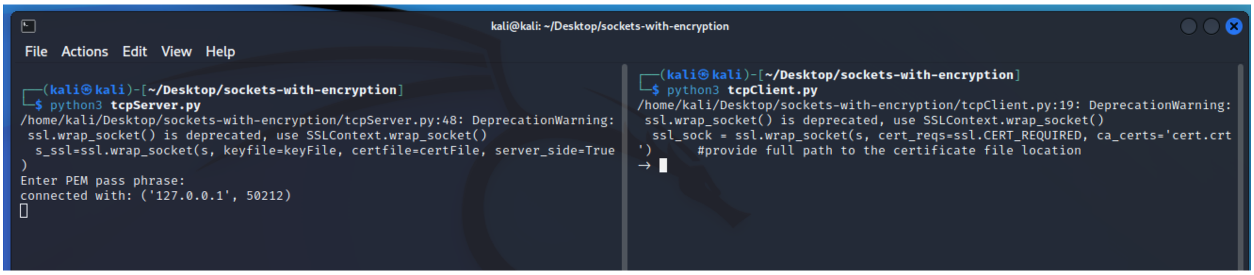
RESULTS AND DISCUSSIONS

Python programming language is used to create a chat simulator that enables real-time communication between users. The chat messages were encrypted using AES encryption with a 256-bit key size. Wireshark, a network protocol analyzer, was used to record and examine the network traffic in order to confirm the efficacy of the encryption. The study's findings showed that the chat simulator's use of AES encryption is successful in protecting conversation communications. All of the data was encrypted using a secure key, rendering the encrypted messages unreadable or unintelligible to any third party who intercepted the transmission. All of the network traffic that Wireshark was able to collect was encrypted; there was no readable text to be seen. These results attest to the efficacy of AES encryption in protecting messages. Wireshark's use as a tool for encryption functionality testing offers another level of confidence that the encrypted messages are actually secure. When it comes to analyzing network traffic, Wireshark is a powerful tool that is capable of spotting any malicious behavior or attempts to intercept the information. Our study's Wireshark analysis proved that the chat messages were successfully encrypted and that no outside entity was able to view the chat's content. As a symmetric encryption technique, which uses the same key for both encryption and decryption, AES encryption has the potential to present several difficulties. As a result, it could be difficult for users to exchange the key safely. In order to solve this problem, secure key exchange methods like the Diffie-Hellman key exchange might be used. And for the results of the test are shown on below. As the field of cryptography continues to evolve, new challenges and research opportunities arise. This section discusses future directions for AES, including: B. Post-quantum cryptography and integration of AES with other cryptographic primitives. We also discuss potential challenges, such as advances in cryptanalysis and future needs, and the results of the encrypted messages are below.

Table 1. Result of AES Encryption on chat simulator

Plain Text	Encrypted Text
hi	e.v_..`.:.s. D.........w..G.\S..!(.R.
good	2."$L8w...l9..<P~.'nb9.n^93.1.].9~
test	2"$L8wl9.<P~'nb9n^.9331.].9~)0DP.m.&.- `.B.#+...65...qZ.
nice	2."$L8w...l9..<P~..'...nb.......9...n..... ^.9...331.].9~)...0....D.P.m..&B.#+...65...qZ5..+0b. _ F.Z. b'.\..C..
best	2."$L8wl9<P~'nb9n ^933.1]9~) 0D.P.m..&B.#+6qZ 5+0b_F.Zb'.\C.8I.14..}\!....1.H."G.;v.s.<B
ur	2."$L8wl9<P~'nb9n^933 .1.].9~) -0D.P.m..&-`B.#+65. qZ5+0b_ F.Zb'.\C8I.14..}\! 1.H."G ;v.s.<BH`8W; h^kjT

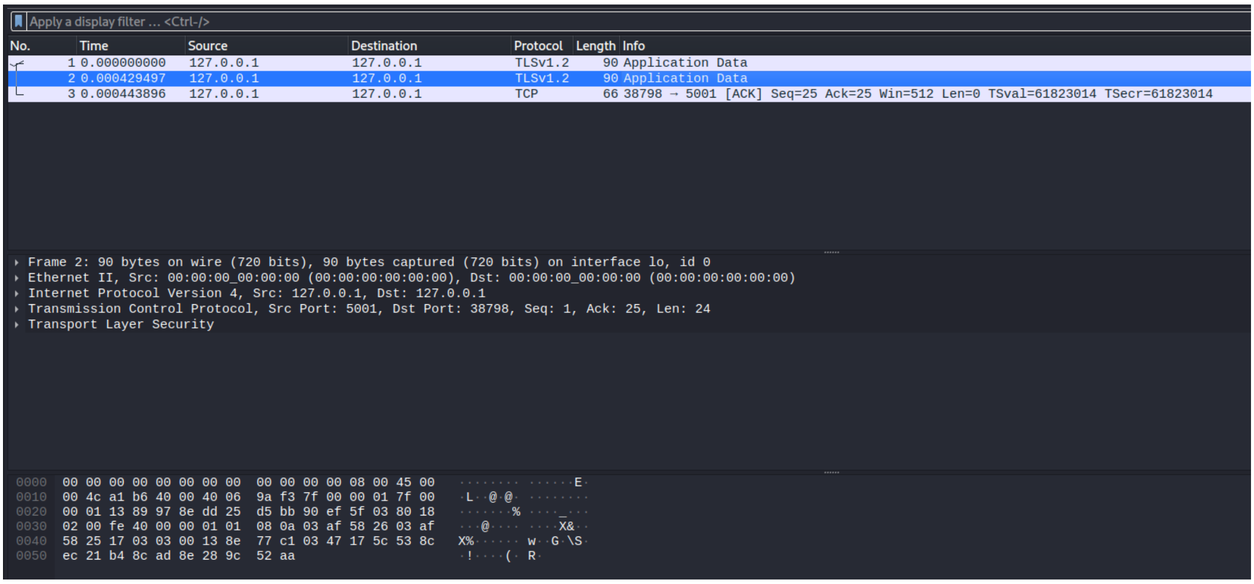
bye	2"$L8wl9<P~'nbn^9331.]9~) - 0DPm&`B.#+65qZ5+0b_F.Zb'\C8I.14..}\! 1H"G;v.s.<. BH.`8.W;..h^kjT{1FYQ (33.rq&B]]


kali@kali: ~/Desktop/sockets-with-encryption
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/sockets-with-encryption]
└─$ python3 tcpServer.py
/home/kali/Desktop/sockets-with-encryption/tcpServer.py:48: DeprecationWarning:
 ssl.wrap_socket() is deprecated, use SSLContext.wrap_socket()
  s_ssl=ssl.wrap_socket(s, keyfile=keyFile, certfile=certFile, server_side=True
)
Enter PEM pass phrase:
connected with: ('127.0.0.1', 50212)
```

```
┌──(kali㉿kali)-[~/Desktop/sockets-with-encryption]
└─$ python3 tcpClient.py
/home/kali/Desktop/sockets-with-encryption/tcpClient.py:19: DeprecationWarning:
 ssl.wrap_socket() is deprecated, use SSLContext.wrap_socket()
  ssl_sock = ssl.wrap_socket(s, cert_reqs=ssl.CERT_REQUIRED, ca_certs='cert.crt
')      #provide full path to the certificate file location
→
```

Figure 2. Chat simulator display based on CLI



```
No.   Time          Source       Destination  Protocol  Length Info
    1 0.000000000   127.0.0.1    127.0.0.1    TLSv1.2      90 Application Data
    2 0.000429497   127.0.0.1    127.0.0.1    TLSv1.2      90 Application Data
    3 0.000443896   127.0.0.1    127.0.0.1    TCP          66 38798 → 5001 [ACK] Seq=25 Ack=25 Win=512 Len=0 TSval=61823014 TSecr=61823014
```

```
› Frame 2: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface lo, id 0
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 5001, Dst Port: 38798, Seq: 1, Ack: 25, Len: 24
› Transport Layer Security
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  00 4c a1 b6 40 00 40 06  9a f3 7f 00 00 01 7f 00   ·L··@·@· ········
0020  00 01 13 89 97 8e dd 25  d5 bb 90 ef 5f 03 80 18   ·······% ····_···
0030  02 00 fe 40 00 00 01 01  08 0a 03 af 58 26 03 af   ···@···· ····X&··
0040  58 25 17 03 03 00 13 8e  77 c1 03 47 17 5c 53 8c   X%······ w··G·\S·
0050  ec 21 b4 8c ad 8e 28 9c  52 aa                     ·!····(· R·
```

Figure 3. Wireshark captures "hi"

3. CONCLUSIONS AND SUGGESTIONS

Chat Simulator with AES Encryption is a great example of how chat encryption can be implemented to enable secure and private communication over the internet. The simulator uses Advanced Encryption Standard (AES), a widely used symmetric encryption algorithm for secure communications.

In this chat simulator, the encryption process is implemented using AES in Cipher Block Chaining (CBC) mode. CBC is a block cipher mode that concatenates cipher blocks to provide additional security. In this mode, each block of plaintext is XORed with the previous block of ciphertext before encryption. One of the main benefits of using AES encryption in CBC mode is protection against attacks such as replay and man-in-the-middle attacks. In a replay attack, an attacker intercepts an encrypted message and resends it to the recipient, making it appear as if it was sent by the original sender. In a man-in-the-middle attack, the attacker intercepts the communication between her two parties, modifies the message, and then forwards it to the intended recipient. Her

AES in CBC mode can prevent both of these attacks by making the encryption of subsequent blocks unpredictable to the attacker.

A chat simulator with AES encryption is an example of how symmetric encryption can be used for secure communications. Symmetric encryption algorithms are fast and efficient because they use the same key for both encryption and decryption. In this chat simulator, keys are generated using a secure random number generator and shared between sender and receiver. This ensures that only the sender and recipient can read the message.

Symmetric encryption is fast and efficient, but it has one major drawback. The key is that the key must be shared between the sender and receiver. This means that if the key is intercepted or compromised by an attacker, the messages can be easily decrypted to read the content of the chat. To prevent this, chat simulators with AES encryption use a key exchange algorithm to securely exchange keys between the sender and receiver.

In summary, Chat Simulator with AES Encryption is a great example of how chat encryption can be implemented to enable secure and private communication over the internet. The simulator uses Advanced Encryption Standard (AES), a widely used symmetric encryption algorithm for secure communications. By using AES in CBC mode and implementing a secure key exchange algorithm, Chat Simulator provides a secure and efficient way to exchange messages over the internet. Chat encryption is an essential tool for protecting the privacy and security of your online communications, and our chat simulator with AES encryption is a great example of how this can be achieved.

One possible suggestion is to include two-factor authentication (2FA) in your chat system. To do this, the user must provide her second identity, such as a fingerprint or SMS code, in addition to the password. 2FA adds a layer of security to chat systems and can make it more difficult for attackers to access sensitive information. The other options are by implementing two-factor authentication adds another layer of security to your chat system. Users must provide a second form of identity in addition to their password. B. A verification code sent to your mobile device or email. This greatly reduces the risk of unauthorized access to your chat system, even if a user's password is compromised or end-to-end encryption is used.

End-to-end encryption (E2EE) ensures that only the sender and intended recipients can read the message. This is accomplished by encrypting the message on the sender's device and decrypting the message on the recipient's device before sending. Even if the message is intercepted by a third party, the contents of the message cannot be read. Popular chat apps like WhatsApp and Signal use E2EE by default. Conduct regular security audits.

It is important to regularly review the security measures in place in your chat system to identify any weaknesses or vulnerabilities. Regular security scans can help you stay ahead of potential threats and keep your chat system secure. Restrict access to sensitive data.

Limit access to sensitive data to only those who need it to do their jobs. This can be achieved through role-based access control. In this case, users are only allowed access to the data they need to do their job. It also limits the amount of data stored on user devices to reduce the risk of a data breach if the device is lost or stolen.

Another suggestion is to regularly review and update the encryption algorithms used by your chat system. As technology continues to advance, new vulnerabilities and weaknesses may be discovered in current encryption algorithms. Keeping your system up-to-date with the latest encryption technology can help mitigate these risks and keep your chat system secure.

Additionally, it is important to educate users about the importance of using strong passwords and not sharing them with others. Weak passwords can be easily guessed or cracked, giving attackers easy access to sensitive information. You can further improve the security of your chat system by choosing strong, unique passwords and encouraging users to change them regularly.

ACKNOWLEDGEMENT

We would like to thank the Department of Electrical Engineering and the Mechatronics Laboratory of Universitas Tarumanagara for their great contributions to this research.

REFERENCES

[1] Sabah, N., Kadhim, J. M., & Dhannoon, B. N. (2017). Developing an End-to-End Secure Chat Application Image processing View project image processing and Artificial intelligence View project Developing an End-to-End Secure Chat Application. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 17, Issue 11). https://www.researchgate.net/publication/322509087

[2] H. Ali, A., & Sagheer, A. M. (2017). Design of an Android Application for Secure Chatting. *International Journal of Computer Network and Information Security*, *9*(2), 29–35. https://doi.org/10.5815/ijcnis.2017.02.04

[3] Ali, A. H., & Sagheer, A. M. (2017). Design of Secure Chatting Application with End to End Encryption for Android Platform. *Iraqi Journal for Computers and Informatics*, *43*(1), 22–27. https://doi.org/10.25195/2017/4315

[4] Vashishtha, J. (2012). Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard). In *IJCEM International Journal of Computational Engineering & Management* (Vol. 15). www.IJCEM.orgIJCEMwww.ijcem.org

[5] Sari, C. A., Rachmawanto, E. H., & Haryanto, C. A. (2018). Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security. *Scientific Journal of Informatics*, *5*(2), 2407–7658. http://journal.unnes.ac.id/nju/index.php/sji

[6] Salama, D., Elminaam, A., Mohamed, H., Kader, A., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms Higher Technological Institute 10th of Ramadan City. In *International Journal of Network Security* (Vol. 10, Issue 3).

[7] Ajagbe, S. A., Adesina, A. O., & Oladosu, J. B. (2019). EMPIRICAL EVALUATION OF EFFICIENT ASYMMETRIC ENCRYPTION ALGORITHMS FOR THE PROTECTION OF ELECTRONIC MEDICAL RECORDS (EMR) ON WEB APPLICATION. *International Journal of Scientific & Engineering Research*, *10*(5). http://orcid.org/0000-0002-7010-5540http://www.ijser.org

[8] Singh, S., & Attri, V. K. (2015). Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, *8*(5), 259–266. https://doi.org/10.14257/ijsip.2015.8.5.27