Comparative analysis of different algorithms on security of chat applications

Munmun Sharma,[1, a)] Anurag Mahish,[1, b)] Udit Kumar Singh,[1, c)]
Radhika Chandel,[1, d)] Sikant Kumar,[1, e)] Suneha Suman,[1, f)]
Isha Khughar,[1, g)] and Parnika Bhat[1, h)]

[1]*Lovely Professional University, Jalandhar Punjab 144001, India.*

[a)] munmun.sharma430@gmail.com
[b)] anuragmahish.18o1@gmail.com
[c)] uds290802@gmail.com
[d)] singhradhika92786@gmail.com
[e)] shikantchoudhary2000@gmail.com
[f)] ssuneha21@gmail.com
[g)] ishakhughar@gmail.com
[h)] bhatparnika@gmail.com

Abstract. This paper offers a review on security of currently available chat applications and comparative analysis of the existing techniques. Internet surfers and owners of smartphones frequently utilise chat software. As a result, privacy and confidentiality becomes topmost priority taking this in mind we have compared four mostly used encryption algorithms-Data Encryption Standard (DES), Triple DES (3DES), RC4 and Advanced Encryption Standard (AES). They have been tested in terms of their ability to prevent data from unauthorized access (data breach) , how long it takes to encode and decode the data taking size as variable. Different algorithms behave differently depending on the inputs.

Keywords: Encryption, Decryption, Ciphertext, Plaintext Peer-to-peer networks, Compression, Encoding, Security layer, Cryptography, DES, 3DES, RC$, AES.

INTRODUCTION

Internet, technological development and networks are constantly evolving around the world. The devices have been integrated into daily activities with the rapid development of mobile phones. Chat apps have evolved in recent times and provide various services such as exchanging text messages, photos, files and other things as well as real-time communication.

Reading private conversations from a privacy perspective is unbearably annoying. Most applications use only transport layer security to protect channels, and as a result, the service provider has full access to all messages sent and received over those channels. As a result, attackers can exploit these messages. To guarantee the privacy and security, data encryption from sender to receiver becomes necessary so that the data is protected from attacks and breaches in such a way that not even the service provider, can read them. In this article, we propose full security that ensures that only the sender and recipient can read messages without a third party, focusing on security, privacy and speed. In addition, messages between parties are transferred quickly. Cryptography is utilised throughout the world by secret services to convert data into unintelligible codes so that messages can be transmitted securely online or offline [1].

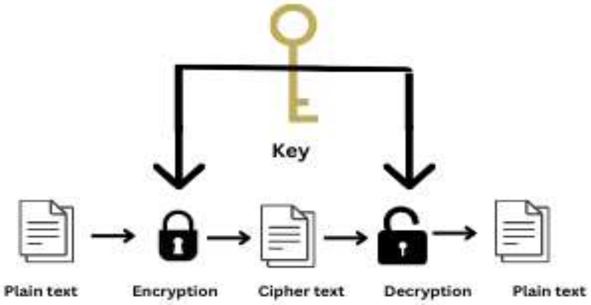


Fig 1. Encryption and decryption flow diagram.

Security Services

Six services are presented by ITU-T (X.800) to ensure appropriate and necessary security and to prevent data breaches and attacks [2].

Confidentiality. Data confidentiality is a measure that ensures the privacy of data in such a way that no one has access to the data except the subscribers or authorized users (having permission to know and control the data).
Integrity. Integrity is a system that prevents unauthorized people from changing (deleting, adding or modifying) data. It can protect all or part of the message.
Authentication. A procedure used for identification of user, service or a feature related to identity authentication. Access to the resource system requires authentication.
Indisputability. The certificate ensures that no contract or activity is later disputed, and the non-repudiation service protects the information from being contested by both the sender and the recipient. For example, using a digital signature, the sender of the information can show later that the information was delivered to the intended recipient.
Access control. A controlled process which is use to protect the access of unauthorized access to the services and systems.
Availability. This makes sure that the information is always available, continuously and without delay. An availability service is a service that ensures system availability. It keeps a check on the security issues caused by denial-of-service attacks [2].

RELATED WORK

Chaudhary et al. [1] In this paper, the endeavour is to make a web application for secure transmission of messages, starting with one client and moving onto the next. They utilised RSA calculations. They played out the transmission of the messages by utilising 1024-bit encryption. They additionally perceived how the size of the key influences the encryption and decoding processes, which expresses that the bigger the key, the better the security.

It says that even incrementing the key size to 2048 bits RSA, which when endeavoured to break by a great PC would take around 300 trillion years, We can see that using the RSA algorithm with 1024 bits of key encryption for transmission of messages at a normal system level and applying a brute force attack would be more than sufficient.

Kuliya et al. [4] have done a survey on the current available chat systems and the security features adapted by these applications. A large percentage of people said that the current systems require improvement in their security and privacy implementations. This paper primarily talks about the system architectures used to develop the chat applications and how to increase their security layer. The author has also proposed a new chatting system architecture in which the messages can only be decrypted by the message receiver using his decrypting pin.

Taqa, A.; Zaidan et al. [5] Author in this paper talks about usage of H.264 and approach of selective frame steganography. H.264 - advanced video coding (AVC) also written as H.264 / AVC is very common format for compression of video as over 90% of video enterprise uses it. H.264 is applied in Blu-ray and many other streaming services like live television and on-demand. In spite of this fact that it calls for royalty bills to organisations sometimes who owns the patent for it.

Alanazi et al. [6] This paper shows the study of the comparison between AES, 3DES, and DES. Our choice of algorithm depends on our need of usage. When security is considered, AES provides more security, faster speed and higher efficiency over 3DES in some hardware implementations as described in paper. These algorithms are presented in nine different factors like possible keys, length of it, which cypher type is used, size of block decided for implementation, cryptanalysis resistance, security of system, ACSII character keys that are possible and total time to examine and check possible keys at rate of 50 billion seconds. These results states that AES is better for most situations than other two.

Abomhara et al.[7] to save you detection; hidden information after which take within the relaxation of the vicinity. The use of steganography can be mixed with encryption as an additional step to cover or guard statistics.

Almost all virtual materials which include text, pics, movies, and tracks can be used to cover information via steganography. Hidden information can be hidden in nearly any shape of digital content. The records intended to be hidden via steganography, additionally referred to as mystery textual content, are typically encrypted without being embedded in an otherwise simple-looking report or records movement.

Jeeva et al. [8] This observe offers a honest overall performance evaluation among various encryption algorithms, along with symmetric and uneven strategies utilized in 3DES, RSA, DSA, AES, DES and RC2. Both symmetric key encryption and uneven key encryption have had their parameters in comparison. The parameters are supplied, such as the styles of assaults on protection flaws, key duration, tunability, and computing velocity. This results in the provision of advanced symmetric key encryption and uneven key encryption answers.

Jha et al. [9] This paper concluded that the quick encryption algorithm NTRU's primary benefit is quick encryption and decryption, which chat applications require. It is also vital to keep in mind security precautions with dependability issues to preserve the speed and reliability within them. All results fit the NTRU. The suggested system operates faster. Decryption takes less time now. It turned out that the throughput factor was lower, which is good for battery consumption. Future research at this NTRU may be of high quality. It is comparable to the RSA and AES standard encryption techniques used by the Android operating system's Chat application.

Sharma et al. [10] in their paper have proposed to combine the compression techniques (RLC, HC, LZW, AC) with the encryption techniques (RC4, CC, DES) for improved security and reliable data transfer via the internet. Though the author concluded that the bigger the file size, the better the encryption ratio, and Huffman encoding has the best result, this data is only based on when the files are large text files, and that data has many repeating characters. The encryption and compression techniques we choose are dependent on the type of data and file size we are using.

Karabey et al. [11] In this study, a straightforward chat application has been enhanced with identity authentication and encryption to enable customers to communicate instantaneously over a secure internet channel. According to their paper, lot of methods was applied to save a user from any cyberattack such as(PKI), a trusted third party user with secret key to access the information of a sender and a receiver while transfer the information over the internet.

The Advanced Encryption Standard (AES) proposed by Rijndal selected these algorithms which have the block size of 128 bit with different key lengths such as 128, 192, or 256 bits. Proposed System Model: in this model two chat rooms used for both client and server TGT (TICKET GRANTING TICKET) have the session key, expiration date, and the user's IP address; once the TGT's validity period expires, these TGTs were no longer valid for the connection.

Verma et al. [12] According to this paper, they used different algorithms to compare between AES, DES, 3DES, Blowfish and RSA. These algorithms compared with symmetric and asymmetric encryption. AES and Blowfish are more secure algorithms for asymmetric encryption from symmetric encryption, RSA is more secure and has a good speed that can be used for wireless networks. These algorithms are good for speed and security.

Sabah et al. [13] According to this paper, most of the chat applications used Transport Layer Security (TLS) because this infrastructure message can be accessed by attackers. So, there is a need for a good encryption technique for providing end-to-end security and privacy. The author in their work has employed XSalsa20 for encrypting the body of the message and the Poly1305 algorithm for further authenticating it by generating a MAC (). This process improves the security and performance of their chat application.

Nisha et al. [14] According to this paper, RSA is nowadays the most popular cryptographic method; if RSA is to remain the best, its several drawbacks must be taken into account, and work must be done to make RSA quantum resistant. Studies on quantum encryption techniques that are resistant to quantum computers are more important than ever since they will soon replace the existing encryption systems. The creation of qCrypt is a start, but it is not sufficient. Hence, additional study on encryption systems that can withstand quantum effects is required.

Ali et al.'s [15] study created an end-to-end encrypted, secure messaging app for Android-powered smartphones. With public key cryptography techniques, this is accomplished. The key which is being utilised for the data encryption using symmetric techniques was produced by the implemented application using the Elliptic Curve Diffie Hellman Key Exchange (ECDH) algorithm. Users can send messages, talk on calls, and send images using this application.

Sivakumar et al. [16] This essay demonstrates how important it is to make sure that data is safe and free from damaging as more and more data is kept on computers or transmitted over computers. If data is encrypted, even if it is taken, it will be illegible and essentially useless. Due to the rapid development of electronic data interchange, encryption is crucial for the secure and reliable transmission of sensitive data through network. The latest technologies has made cryptography more complicated to increase the security of data. In the meantime, a large number of new cryptography algorithms are being created in the cyber world. The document presents a survey of all those various algorithms.

Natanael et al. [17] This paper outlines ECC for building a chat application which uses end-to-end encryption for Android. Singh1 presented a chat application type that encrypts and decrypts text using the ECC method. This study establishes the ECC algorithm's applicability and demonstrates its competitive performance in terms of speed and accuracy. To achieve better outcomes, the ECC application still needs some improvement to be done. So, in the future, the implementation and use of ECC method optimisation in the encryption of photos and videos will be possible.

Maganti Manasa et al. [18] According to this paper, different messenger applications have different techniques to secure the data of any individual, and these messenger applications use different algorithms. Here, for WhatsApp, they used AES-256 and Curve25519 encryption with 256 bits; for Hike, they used AES-256, RSA 2048, and AES-128 encryption with 128 and 256 bits; for Kakao Talk, they used AES-128 encryption with 128 bits; and for Telegram, they used AES-256 encryption with 256 bits. When the features of these applications are considered, then the speed and the time complexity of these algorithms also matter.

Zhimao Lu et al. [19] This study focuses on the methodical analysis of problems like key management and security functions and provides an overview of the AES algorithm, thorough application, and comparison with other current approaches. In this research, they suggested to reduce the execution cycle and modify the beginning key in order to address the issues of key sharing in the AES algorithm and also less speed of RSA.

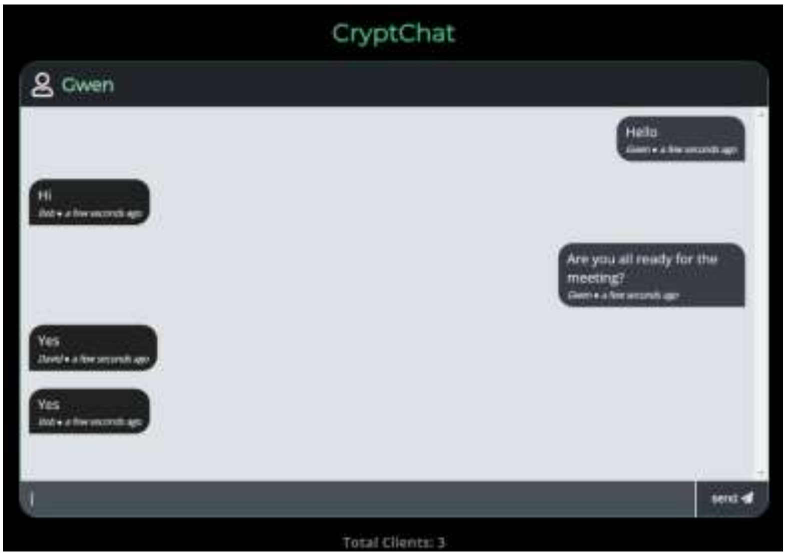
The authors of this study have additionally updated the AES algorithm by including two new features: introducing a modified key and reconfiguring the Sub Bytes function. By combining the Modified AES algorithm and the RSA algorithm, they have developed a sophisticated, complex encryption technique. AES is the main piece of information used in the complex encryption algorithm (hybrid encryption). It is more secure in terms of data security because RSA provides the AES encryption key. Data is encrypted with the newly proposed hybrid encryption technique, making it safer than AES.

Ratik Tiwari et al. [20] In this paper's backup, security WhatsApp and other messaging apps are now so secure that they probably don't need extra security, but storing messages in a backup file and then uploading that backup to a server is still weak and needs some improvements. This weakness can be overcome by providing additional security, using the individual backup packet method in series with effective AES encryption for the data. In total, they evaluated Android app development, encryption algorithms, industry standards for securing chats and backups, and innovative possibilities.

METHODOLOGY

In this paper we have created CryptChat that is NodeJS based chat application to implement encryption and decryption on the data send from one user to another.

To safeguard data security and user privacy, the CryptChat app in Fig. 2 delivers encrypted data across the network rather than the original, unencrypted message when a user sends a message and then this encrypted data is decoded before the message is received by another user to whom data(chat/message) has been sent.



Hello
Gwen • a few seconds ago

Hi
Bob • a few seconds ago

Are you all ready for the meeting?
Gwen • a few seconds ago

Yes
David • a few seconds ago

Yes
Bob • a few seconds ago

Fig. 2. Chat application interface

System specification used to build this app are: -

- System Type: x64-based CPU
- Memory: 8GB
- Windows Specification: Windows 10

Technologies used are: -

- Visual studio code
- GitHub
- NodeJS based libraries

Programming languages used are: -

- HTML
- CSS
- JavaScript
- NodeJS
- MySQL

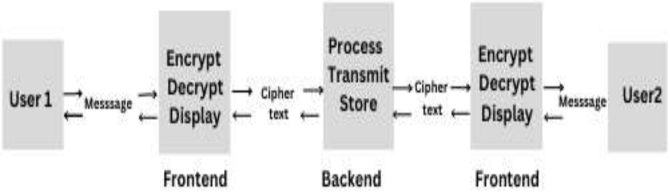


Fig 3. Data flow diagram in chat application.

RESULT AND ANALYSIS

The implementation results show the data and messages sent are received successfully 100% with encryption and decryption maintaining the privacy of user and security of data. Here, we have created tables showing the encryption and decryption time of a message on basis of the size of the data(message) using most popular algorithms DES, Triple DES, AES and RC4.

By analyzing the result set we understand that AES algorithm is the best for efficiency and safety from all others. As RC4 is faster than AES for small file sizes but it is vulnerable and can be easily decrypted whereas AES is faster than rc4 while encrypting large file sizes and also it is much more secure than rc4. des was enhanced for security in the Triple DES but it lacks in speed so overall AES beats all others in speed and security but still we use each algorithm according to the need.

TABLE 2: Time Performance Result of DES

File size	**Encryption time**	**Decryption time**
Tiny (1 Byte)	2ms	2ms
Small (<=25 Bytes)	1ms	1ms
Medium (<=150 Bytes)	1ms	1ms
Large (<=500 Bytes)	2ms	2ms
Huge (>500 Bytes)	12ms	24ms

The DES Encryption algorithm is fast because it uses small key size which is very easily decrypted by hacker which is why we needed a better encryption algorithm than DES.

TABLE 3: Time Performance Result of Triple DES

File size	Encryption time	Decryption time
Tiny (1 Byte)	6ms	4ms
Small (<=25 Bytes)	2ms	1ms
Medium (<=150 Bytes)	1ms	3ms
Large (<=500 Bytes)	2ms	4ms
Huge (>500 Bytes)	26ms	34ms

The Triple DES is a modified version of DES algorithm where a large key size was used to make it tougher to decrypt by hackers but it was relatively very slow for practical use.

TABLE 4: Time Performance Result of AES

File size	Encryption time	Decryption time
Tiny (1 Byte)	2ms	3ms
Small (<=25 Bytes)	0ms	1ms
Medium (<=150 Bytes)	1ms	1ms
Large (<=500 Bytes)	2ms	1ms
Huge (>500 Bytes)	10ms	19ms

AES was currently the best algorithm which provides both speed and security. It is faster than both DES and Triple DES and also secure which makes it the best choice for practical use.

TABLE 5: Time Performance Result of RC4

File size	Encryption time	Decryption time
Tiny (1 Byte)	5ms	2ms
Small (<=25 Bytes)	1ms	0ms
Medium (<=150 Bytes)	0ms	1ms
Large (<=500 Bytes)	1ms	1ms
Huge (>500 Bytes)	8ms	13ms

RC4 Encryption algorithm data shows that it works better than AES for small files in encryption speed but it is vulnerable to threats and is easily hackable by intruders.

CONCLUSION

In this paper, we introduced a specification for preserving the safety and confidentiality of the chat application. We compared four widely used algorithms, 3DES, RC4, AES and DES, for their decryption and encryption times based on different file sizes. We introduced a secure chat application, CryptChat, which uses the AES algorithm for encryption. However, because the chat application does not ensure data integrity, data can be tampered with during transmission. To tackle this problem, we can use parity bits to maintain the integrity of the data. For better results, this web app can be further optimised.

REFERENCES

1. Chaudhary, S., Dabas, S., Singh, V., & Raj, M. S. (2020). Crypto chat Encryption Messaging Application.
2. https://www.tutorialspoint.com/what-are-the-services-of-network-security-in-computer-network
3. https://www.proofpoint.com/us/threat-reference/encryption
4. Kuliya, M., & Abubakar, H. (2009). Secured Chatting System using Cryptography. *International Journal of Creative Research Thoughts (IJCRT)*, *8*(9).
5. Taqa, A., Zaidan, A.A. and Zaidan, B.B. (2009) New Framework for High Secure Data Hidden in the MPEG Using AES Encryption Algorithm. International Journal of Computer and Electrical Engineering, 1, 566-571. https://doi.org/10.7763/IJCEE.2009.V1.87
6. Alanazi, H.O., Zaidan, A.A., Jalab, H.A., Shabbir, M. and Al-Nabhani, Y. (2010) New Comparative Study between DES, 3DES and AES within Nine Factors. Journal of Computing, 2, 152-157.
7. Abomhara, M., Zakaria, O., Khalifa, O.O., Zaidan, A.A. and Zaidan, B.B. (2010) Enhancing Selective Encryption for H.264/AVC Using Advance Encryption Standard. International Journal of Computer and Electrical Engineering, 2, 223-229.
8. Jeeva, A., Palanisamy, D.V., & Kanagaram, K. (2012). COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS
9. Jha, S. and Dutta, U., 2015. Review on SMS Encryption using MNTRU Algorithms on Android. *Int J Comput Sci Inf Technol*, *6*, pp.3855-3858.
10. Sharma, R., & Bollavarapu, S. (2015). Data security using compression and cryptography techniques. *International Journal of Computer Applications*, *117*(14).
11. Karabey, Işıl, and Gamze Akman. "A cryptographic approach for secure client-server chat application using public key infrastructure (PKI)." *2016 11th international conference for internet technology and secured transactions (ICITST)*. IEEE, 2016.
12. Verma, A., Guha, P. and Mishra, S. (2016) Comparative Study of Different Cryptographic Algorithms. International Journal of Emerging Trends & Technology in Computer Science, 5, 58-63.
13. Sabah, Noor & Kadhim, Jamal & Dhannoon, Ban N. (2017). Developing an End-to-End Secure Chat Application. 17.
14. Nisha, Shireen, and Mohammed Farik. "RSA Public Key Cryptography Algorithm." *A Review. International Journal of Scientific and Technological Research* 6 (2017): 187-191.
15. Ali, Ammar, and Ali Sagheer. "Design of secure chatting application with end to end encryption for android platform." *Iraqi Journal for Computers and Informatics* 43, no. 1 (2017): 22-27.
16. Sivakumar, R., Balakumar, B., & Pandeeswaran, V.A. (2018). A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security.
17. Natanael, D., & Suryani, D. (2018). Text encryption in android chat applications using elliptical curve cryptography (ECC). *Procedia Computer Science*, *135*, 283-291.
18. Maganti Manasa, Dasari Veera Reddy, AmanapuYaswanth, G.V.S Raj Kumar (2019). Encryption Techniques for Different Messenger Applications
19. Zhimao lu., Houmed Mohamed (2021) A Complex Encryption System Design Implemented by AES
20. Ratik Tiwari, Azhar Ahmed, (2022).: PROVIDING ENCRYPTION FOR CHAT BACKUPS