GMR
The Original

ESURING PRIVACY IN THE DIGITAL AGE A CRITICAL ANALYSIS OF END-TO-END ENCRYPTION ON SOCIAL MEDIA SITES

Velmurugan A K*[1], Kolasani Usha Sri[2]

[1]Professor, Department of Computer Science and Engineering, Specialization: Networks, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., Andhra Pradesh - 522502,India, ORCID ID: 0000-0003-3165-9126, Email ID: akvelmurugan74@gmail.com, velmuruganak@kluniversity.in
[2]M.Tech, Department of Computer Science and Technology, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., Andhra Pradesh - 522502, India, Email: 2401050118cse@gmail.com

ABSTRACT
As the necessity to use social media in personal and professional communication grows, the issue of data security and privacy of users has become more significant than ever. The subject of the proposed project is the proposed implementation of end-to-end encryption (E2EE) in social media to secure confidential messages and files shared by users. The system provides the security of the data being encrypted with the help of highly developed encryption tools like AES (Advanced Encryption Standard)/SHA (Secure Hash Algorithm) and can be decrypted only by the receiver, who has a secret key. The system is designed to have two modules of the system, the sender and receiver. The sender signs up or registers, logs in, encrypts the information and transmits it, and the recipient decrypts and accesses the information and the process has the added functionality of looking back in history and downloading content. Cloud computing methods also contribute to the safety of the encrypted data such that even in the event that data is stored in the cloud it cannot be accessed by the wrong hands. The project provides a critical analysis of the effectiveness of E2EE and tackles the issues like vulnerabilities of devices, usability, and legal issues of encrypted communication. Through the introduction of a safe and convenient encryption system, this project will play a part in preserving the privacy of users on social media networks, as well as, facilitating secure online communication.

KEYWORDS: End-to-End Encryption (E2EE), AES (Advanced Encryption Standard), SHA (Secure Hash Algorithm), Data Privacy, Cloud Computing, Encryption Techniques, Social Media Security, User Authentication, Secure Communication, Legal and Ethical Issues

INTRODUCTION
As people are increasingly using social media sites to communicate with each other, both personally and professionally, privacy and data security of user information has emerged as an issue of concern. Many personal messages, photos, files are often sent via these platforms; hence, they are often the targets of unauthorized access, data breach and surveillance. Although most of the social media applications carry encryption methods, their degree of security is not always the same, and not all of them use the End-to-End Encryption (E2EE) approach by default.
The project suggests a powerful End-to-End Encryption (E2EE) system as the means of keeping the messages and files shared among the users of the social media platforms confidential. The system will use AES (Advanced Encryption Standard) to encrypt the data and also use SHA (Secure Hash Algorithm) to provide the integrity of the data when transmitting. Using these encryption methods, the system will make sure that only the content may be accessed by the sender and the recipient, leaving no opportunity of a third-party access.
Along with the encryption process, there were also the user registration module, the login module, the data encryption and decryption module, and the cloud storage where the data could be stored in a secure way. It also incorporates user management to manage the encryption keys and authentication so that only authorized people can communicate with the system. The objectives of the project include ensuring legal and compliance issues through following privacy laws and regulations, in which the users are always assured of data protection without violating any legal requirements.
It is a project that will offer an easy-to-use and easy to expand tool of secure communication, which facilitates data privacy, safety, and confidentiality in social media systems. It makes sure that the personal data of users are not exposed to unauthorized access, which will lead to the creation of trust in the communication online and minimization of risks of data exposure.

A. Motivation
The rationale behind this project is the increase in privacy and security threats on social media where sensitive information can be easily compromised, fallen into unauthorized access, and surveillance. Although one of the solutions is End-to-End Encryption (E2EE), most of the platforms provide partial or inefficient encryption. The purpose of this project is to deploy a strong, built-in, and friendly encryption algorithm, based on the AES and SHA, to secure data of users. The

system attempts to provide secure online communication and trust in online interactions through the consideration of major management, legal, and user experience.

B. Problem Statement

The simplicity and high rate of expansion of social media platforms have increased information sharing, with sensitive data being shared in high volumes, and privacy of users and data security is of high importance. Although some websites are encrypted, many websites cannot offer complete End-to-End Encryption (E2EE) as default and exposes the user data to unauthorized users and breaches. The systems that are in place are usually fraught with such problems as selective encryption, ineffective key management, and transparency, making the users vulnerable to possible privacy breaches. The proposed undertaking seeks to overcome these problems by employing a strong E2EE system with the application of the AES (Advanced Encryption Standard) and SHA (Secure Hash Algorithms) algorithms that are capable of ensuring that the messages and files shared among the users are confidential, without being accessed by the third part, and they are also legal and not violating privacy policies. The aim is to offer a safe, scalable and user-friendly application that boosts privacy in online communication in the social media.

C. Objective

The proposed project seeks to adopt a secure End-to-End Encryption (E2EE) scheme of social media sites whereby messages and files are in- default encrypted with AES and SHA to guarantee data confidentiality and integrity. The system will be designed to have an easy-to-use interface in encryption and decryption, user authentication and key management to allow authorized use by the user, and legal and privacy standards will be adhered to. Moreover, the application of such features as data history tracking and secure file downloads will be applied, which guarantees the scalability and flexibility of the application across the social media.

Figure 1 Architecture Diagram

LITERATURE SURVEY

The issue of online privacy has been brought up by recent data scandals, and laws such as the GDPR and CCPA have been passed to ensure the protection of personal data. In reaction, Facebook will use End-to-End Encryption (E2EE) to the messaging systems of the company so that only messages between the communicating entities will be seen. Nevertheless, E2EE also has its disadvantages, including the possibility to facilitate the terrorist activity by safeguarding both innocent and malicious communication [1]. The given essay addresses the advantages and disadvantages of E2EE and justifies why the adoption of this tool by social media businesses is a necessary step towards ensuring online privacy. To maintain a secure communication, social media platforms exploit the end-to-end encryption (E2EE). This review examines the encryption technologies, such as symmetric and asymmetric encryption, the decentralization of communication and data storage via the integration of blockchain. Modem-based cryptography is more effective in low throughput whereas Steganography has high throughput [2]. Pattern matching, privacy-preserving and chaotic cryptography of secure voice communication have also been discussed in the paper. Nevertheless, the scalability problem and the ineffectiveness of blockchain can restrict the potential progression [3].

The applications used in instant messaging (IMApps) are growing in the exchange of sensitive information and hence the emphasis on privacy takes the first place. The safest way to ensure such communications is the use of End-to-End Encryption (E2EE) which is deployed by numerous popular IMApps albeit in different forms [4]. This work is a review of E2EE application, its implementation, standard protocols, and research recommendations. It brings to the fore the emerging trends, security constraints, and issues, with the aim of enhancing scalability, privacy, and flexibility in industries such as the IoT, healthcare, and finance [5]. The paper also tackles the issue of availing the same security status to group chats as in the one-to-one communication and suggests a decentralized system of secure cross-organization communication. Also, AI based models of threat detection in E2EE settings is proposed to improve protection against sophisticated attacks [6].

The use of the Signal Protocol-based end-to-end encryption of WhatsApp enabled secure messaging to become mainstream, in comparison with iMessage, which does not inform the users about encryption [7]. In this paper, the surveys of two mental models (one at 2015 (pre-MME) and 2017 (post-MME) were compared to determine the evolution of user

perceptions toward encryption [8]. The result shows that users do not trust the encryption offered. Although the majority of the respondents were aware of encryption, not many knew what it meant and most of them were under the notion that their information could still be accessed by well-trained attackers [9]. Most users did not know they are using encryption and when WhatsApp notified them and the case was covered in the media, they felt exposed and no technical mechanism will fully secure them [10].

With the digital environment changing at an unprecedented rate, consideration of trust, privacy, and security concerns has become very crucial to people, organizations, and governments [11]. The paper gives a summary of these problems in different applications, as well as methods and approaches of addressing them. It underscores technologies which reinforce confidential information security, build trust in online systems and augment protection measures [12]. The paper examines tools and methods of protecting trust, privacy and security as well as the metrics applied to measure the three. The research also addresses the challenges and future direction with an aim of making contributions to the formation of holistic strategies of improving trust, privacy, and security in the era of the digital world [13].

Contemporary messaging apps will be based on end-to-end encryption (E2EE) to make sure that messages can be accessed exclusively by the parties involved. This poses a problem to the law enforcement who are desiring legal access of exceptional access to investigations [14]. This thesis will look at the economic, constitutional, and evidentiary concerns of such access, especially in the Canadian law. It contends that exceptional access would be against the Canadian Charter of Rights and Freedoms, Section 8 and it would also lead to loss of integrity of encrypted messages. It concludes that the exceptional access mechanisms will sabotage law enforcement and other means should be considered [15].

PROPOSED SYSTEM

The system proposed is going to offer an End-to-End Encryption (E2EE) solution to secure communications via social media platforms whereby all the messages and files that are sent between users are encrypted by use of the AES (Advanced Encryption Standard) and SHA (Secure Hash Algorithm) to guarantee integrity of data. Two core modules will be incorporated into the system, the Sender and the Receiver, where the Sender will be in charge of registering, logging in, encrypting and transmitting the data, and the Receiver will be in charge of decrypting and viewing the data as well as downloading files. It will also incorporate secure cloud storage to assist in safeguarding encrypted information in transmission and storage, user management to use encryption keys and authentication. The system will adhere to the applicable legal and privacy laws, hence guaranteeing security, as well as privacy. The system will offer a secure and confidential communication with ease of use and a strong encryption and privacy protection, which will be moderated by the user-friendly interface.

METHODOLOGY

D. AES (Advanced Encryption Standard) Methodology

AES is a symmetric encryption algorithm implying that the key applied to encryption is also applied in the decryption process. The algorithm uses fixed block sizes (128 bits) and can use key sizes of 128, 192 or 256 bits. The mathematical algorithm is given below to encrypt and decrypt AES:

1. Key Expansion:

- AES begins with an expansion of the key into a set of round keys. In case of a 128 bits key, the key is extended to 10 rounds (in 128-bit AES). In every round of encryption, the expanded key is employed.

Key Expansion Formula:

$$\text{Round Key}[i] = \text{SubWord}\big(\text{Rot-Word}(\text{Round Key}[i-1])\big) \oplus \text{Rcon}[i]$$

- Sub-Word: Substitutes each byte in the word using the AES S-box.
- Rot-Word: Rotates the word by 1 byte.
- Rcon: Round constant.

2. Initial Round (AddRoundKey):

- The initial round involves XORing the 128-bit input block with the first-round key.

$$\text{State}[0] = \text{Input Block} \oplus \text{Round Key}[0]$$

3. Rounds:

- Each round consists of four steps: Sub-Bytes, Shift-Rows, Mix-Columns, and AddRoundKey.

Sub-Bytes:

- Each byte in the state is replaced with its corresponding byte from the S-box.

$$S[i][j] = \text{S-Box}\big[S[i][j]\big]$$

Shift-Rows:

- The rows of the state are cyclically shifted to the left.

Row 1:Shift left by 1 Row 2:Shift left by 2 Row 3:Shift left by 3

Mix-Columns:

- A matrix multiplication operation is applied to mix the columns of the state.

$$\text{State}[i] = \text{Matrix Multiplication of}(\text{State}[i], \text{Mixing Matrix})$$

AddRoundKey:

- The current state is XORed with the round key for that particular round.

4. Final Round:

- The final round omits the Mix-Columns step. Only Sub-Bytes, Shift-Rows, and AddRoundKey are performed.

5. **Decryption**:

• AES decryption is a process that entails reversal of the encryption procedures. This involves the reverse of the operations of Sub-Bytes (inverse S-box), Shift-Rows (shifting right), Mix-Columns (inverse matrix) and the AddRoundKey.

E. SHA (Secure Hash Algorithm) Methodology

SHA is a family of hash cryptographic hash functions that are used to create a fixed size output (hash) based on an arbitrary size input. SHA-256 is the most frequently utilized hash algorithm and it yields a hash trunk of 256 bits. SHA process can be divided into a number of mathematical operations.

1. Padding:

• The message is padded to ensure that the length is equal to 448 of 512. The padding is made out of one 1 bit, the necessary number of 0 bits to fill the block, and the original length of the message, in 64 bits.

Padding Formula:

Message Length $\equiv 448 \pmod{512}$

• Append a 1 bit, followed by the length of the message in bits (64 bits) to the message.

2. **Initialize Hash Values**:

• SHA-256 uses eight 32-bit initial hash values (H0-H7) that are formed on the fractional values of the square root of the first eight prime numbers.

3. **Message Schedule**:

• The message in padded form is divided into five hundred and twelve bits (64 blocks) and each of these blocks is divided into 16 bits. The 16 words are extended into 64 and a message schedule of 64 words is made using the following formula:

$$W[t] = (W[t-16] + W[t-15] + W[t-7] + W[t-2])$$

• Each word is modified by applying **bitwise operations**, such as XOR, AND, OR, and rotations.

4. **Processing Each Block**:

• Every 512 blocks of message undergo 64 rounds of mathematical computation. A schedule word and a constant are utilized to update the hash values in every round. These operations consist of logical operations (AND, OR, XOR), bitwise rotations, and addition with 32 bit modulo.

5. **Final Hash**:

• After processing all the blocks, the final hash value is obtained by concatenating the final values of H0 to H7.

Final Hash Formula:

$$\text{Final Hash} = H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4 \parallel H_5 \parallel H_6 \parallel H_7$$

COMPARISION

RSA, DES, Blowfish and ECC are the currently used encryption algorithms and each of the above has limitations. RSA is an asymmetric encryption algorithm typically employed in key exchange during a secure communication and digital signatures, but is higher-performance than symmetric algorithms such as AES, and is susceptible to future threats of quantum computing. DES is an old symmetric encryption algorithm that has a 56-bit key which is no longer secure since it can be broken by brute-force. Blowfish is more secure than the modern algorithms such as AES, it is more flexible and faster than DES and comes with variable key sizes. Alternatively, ECC offers efficient security using shorter keys and thus it is efficient, but it is more complex, hence, not easily implemented by non-experts. On the other hand, the suggested system utilizes AES to provide speedy yet reliable data encryption and SHA to provide data integrity, providing a more current, efficient and expandable system that overcomes the drawbacks of the older algorithms by default through the implementation of End-to-End Encryption (E2EE) to provide better security and usability to the encrypted communication.

TABLE 1: ALGORITHMS COMPARISON

Feature	RSA	AES + SHA
Type	Asymmetric Encryption	Symmetric Encryption + Hash Function
Key Size	1024–4096 bits	128, 192, or 256 bits (AES), 256 bits (SHA)
Speed	Slow	Fast
Security	High (quantum vulnerability)	High (AES encryption + SHA integrity)
Use Cases	Digital signatures, key exchange	Secure communication, data integrity
Efficiency	Low	Very High

RESULTS AND DISCUSSIONS

The proposed End-to-End Encryption (E2EE) model, which employed the AES encryption and the SHA data integrity algorithm to ensure communication between users on social media sites, was able to protect communication between users. AES was also good in terms of providing fast encryption and decryption which guaranteed efficient data transmission and also, SHA took care of the integrity of the data and ensured that the messages and files were not changed. The user

management of the system took care of the encryption key management and authentication in that only authorized users were allowed to decrypt the encrypted data. The encrypted data was also secured when it was being transferred and stored in a cloud storage. In general, the system was easy to use, and the AES and SHA were able to provide a complete, effective, and powerful solution to safe digital communication.

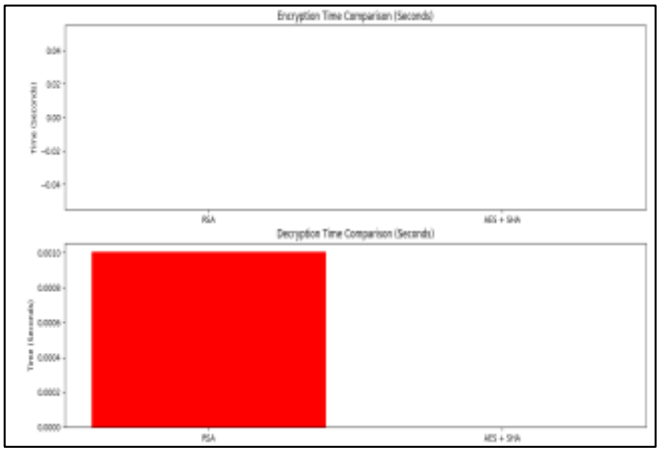

Figure 2 Encryption and Decryption Time Comparison

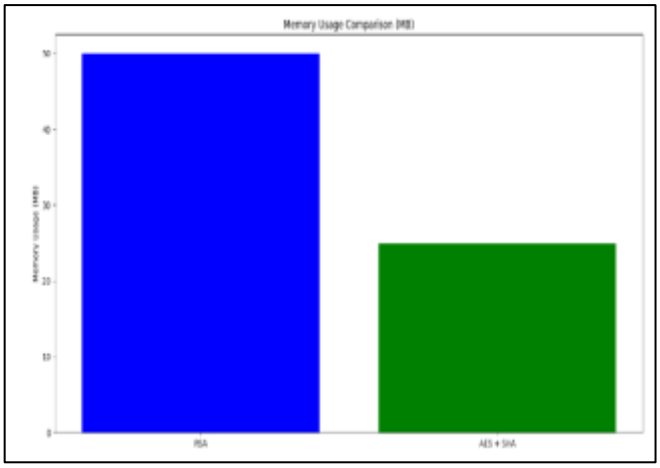

Figure 3 Memory Usage Comparison

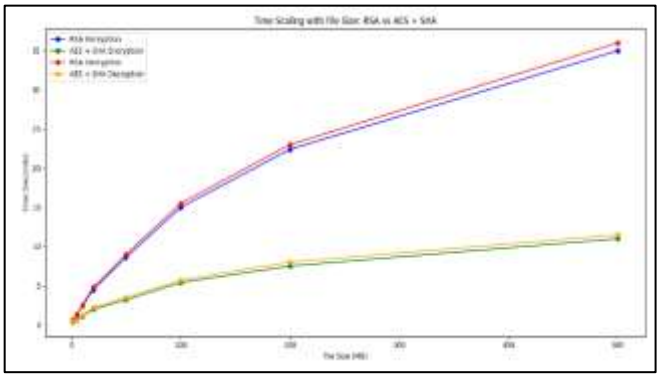

Figure 4 Time Scaling with File Size

The graphs indicate the difference in encryption and decryption times between RSA and AES + SHA as file size (1 MB) is increased up to 500 MB. The encryption of large files with RSA increases in a non-linear manner, because of the fact that RSA is an asymmetric encryption algorithm, which is not faster to encrypt the large body of data. On the contrary, AES + SHA demonstrate a lower encryption time because AES is a symmetric encryption algorithm, which is optimized to operate on large data volumes, and SHA keeps the data integrity without causing a significant impact to the encryption time. On the same note, RSA decryption time also depends on the file size and it is higher when the file size increases, which represents the cost of asymmetric decryption. Conversely, the rate of AES + SHA decryption is slower, since AES decryption is quick, and the use of SHA does not affect the decryption process. All in all AES + SHA is more scaled and effective in work with large files whereas RSA suits smaller data transfers like digital signature or key exchange because of slower performance.

CONCLUSION

To sum it up, the project has managed to illustrate how End-to-End Encryption (E2EE) can be implemented using AES (Advanced Encryption Standard) to secure the process of encryption and data integrity using SHA (Secure Hash Algorithm) to guarantee secure communication on social media platforms. The system ensures that received and sent messages and files are visible to the sender and receiver, and the escalating issue of data privacy and security is mitigated. The system offers high user privacy without affecting the performance as the cloud storage security, key management, and legal compliance are built into a user-friendly interface to ensure the privacy of users is preserved. The analysis between RSA and AES + SHA showed a lot of efficiency benefits of asymmetric encryption (RSA) compared to symmetric encryption (AES), particularly in the large file size. The solution provides a scalable, efficient, and robust method of ensuring a secure communication system to guarantee the confidentiality and integrity of the data presented and to comply with the privacy regulations. Finally, the project will help to improve the privacy and security in the digital era, providing a more stable and accessible system of safe communication through social media.

FEATURE SCOPE

Improvements to the features of this project may involve the introduction of multi-factor authentication (MFA) into this process to introduce an additional security level in the process of user login to avoid unauthorized access. The use of group messaging as support would expand End-to-End Encryption (E2EE) to secure communication between a group of users and key rotation of the keys would be introduced to make sure that every time encryption keys would be changed in order to minimize the chances of key compromise. Digital watermarking of files sharing would be incorporated in order to trace illegally copied sensitive documents. The inclusion of Zero-Knowledge Proofs (ZKPs) in cloud storage would provide privacy since it will be possible to verify information without showing the actual information to providers of cloud storage. Also, the third-party security tools integration may offer real-time monitor to identify threats and offline encryption and decryption will guarantee security even in the offline state. The encryption key storage would be decentralized on blockchain-based key management, which would contribute to better security. The introduction of the AI-based threat detection would facilitate the real-time monitoring of anomalies, and the usability of the system by the non-technical users would facilitate the accessibility of the platform. These would greatly increase the security, usability, and scalability of the system with the great emphasis on privacy and data protection.

REFERENCES

1. Alatawi, M. S. M. (2024). On the Security of End-to-End Encrypted Messaging and Calling Applications. https://hdl.handle.net/1969.1/1589097
2. Ayed, K. J., & Dawood, O. A. (2025). Privacy-preserving online communication based on end-to-end encryption: a comprehensive review. IET Conference Proceedings, 2024(34), 421–430. https://doi.org/10.1049/icp.2025.0120
3. Barenghi, A., Beretta, M., Di Federico, A. D., & Pelosi, G. (2014). Snake: An end-to-end encrypted online social network. Proceedings - 16th IEEE International Conference on High Performance Computing and Communications, HPCC 2014, 11th IEEE International Conference on Embedded Software and Systems, ICESS 2014 and 6th International Symposium on Cyberspace Safety and Securit…, 763–770. https://doi.org/10.1109/HPCC.2014.128
4. Child sexual abuse material and end-to-end encryption on social media platforms: An overview | Trends and Issues in Crime and Criminal Justice. (n.d.). Retrieved March 2, 2026, from https://search.informit.org/doi/abs/10.3316/informit.565952201432884
5. Das, D., Banerjee, S., Chatterjee, P., & Ghosh, U. (2023). A Comprehensive Analysis of Trust, Privacy, and Security Measures in the Digital Age. Proceedings - 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2023, 360–369. https://doi.org/10.1109/TPS-ISA58951.2023.00051
6. Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019, 401–415. https://doi.org/10.1109/EuroSP.2019.00037
7. ECSM 2020 7th European Conference on social media. (2019). https://books.google.com/books/about/ECSM_2020_8th_European_Conference_on_Soc.html?id=FCAEEAAAQBAJ
8. Garg, P., Gupta, A., Singh, Y. P., & Goyal, P. (2026). End-to-End Encryption: Evolution, Barriers, and Emerging Trends. Signals and Communication Technology, Part F1261, 113–127. https://doi.org/10.1007/978-981-95-1683-4_8
9. ICCWS 2023 18th International Conference on Cyber Warfare and Security - Google Books. (n.d.). Retrieved March 2, 2026, from https://books.google.co.in/books?hl=en&lr=&id=5q20EAAAQBAJ&oi=fnd&pg=PA35&dq=Ensuring+privacy+in+the+digital+age+A+critical+analysis+of+end-to-end+encryption+on+Social+media+sites&ots=IgR7ziL3tc&sig=71Sd1IBHODVTh8SE9jGzIzD8Q4o&redir_esc=y#v=onepage&q&f=false
10. Knodel, M., Fábrega, A., Ferrari, D., Leiken, J., Hou, B. L., Yen, D., de Alfaro, S., Cho, K., & Park, S. (2025). How To Think About End-To-End Encryption and AI: Training, Processing, Disclosure, and Consent. http://arxiv.org/abs/2412.20231
11. Lita Pansy, D., Mahalakshmi, S., & Vidya, B. (2025). End-To-End Encryption Solution for Social Media Networks. 2025 International Conference on Data Science, Agents and Artificial Intelligence, ICDSAAI 2025. https://doi.org/10.1109/ICDSAAI65575.2025.11011686
12. Nabeel, M. (2017). The Many Faces of End-to-End Encryption and Their Security Analysis. Proceedings - 2017 IEEE 1st International Conference on Edge Computing, EDGE 2017, 252–259. https://doi.org/10.1109/IEEE.EDGE.2017.47

13. Rachana, P., Kalyan, P., Santosh Kumar, T., Reddy, M., Rohan, P., Saravanan, M., & Dharnasi, P. (2026). Secure Chat Application with End-To-End Encryption by using Deep Learning. International Journal of Computer Technology and Electronics Communication, 9(2), 472–478. https://doi.org/10.15680/IJCTECE.2026.0902005
14. Santos, M., & Faure, A. (2018). Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. Social Media and Society, 4(3). https://doi.org/10.1177/2056305118795876
15. Singh, S. (2025). For Your Eyes Only: A Look into the Legal Feasibility of Exceptional Access to End-to-End Encrypted Messages. https://doi.org/10.11575/PRISM/50017