International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

A Secure Real-Time Messaging System Using End-to-End Encryption and Hybrid Key Exchange

Aswin A[1], Roashini V[2], Subalakshmi P[3], Kiruthika S[4]
[1,2,3,4]Department of Computer Science (Cyber Security) Sri Krishna College of Technology Coimbatore, India
Emails: *727822tucy010@skct.edu.in[1]* 727822tucy050@skct.edu.in[2], 727822tucy056@skct.edu.in[3], *kiruthika.s@skct.edu.in[4]*

Abstract
VartaRaksha is a live chat application that was created to guarantee confidential and secure communication between the users. Although most of the current chat programs are encrypted, they still tend to use servers in some of their functionality, which may pose a privacy threat. This initiative is aimed at eliminating such a dependency by means of a real End-to-End Encryption (E2EE) solution. When message is sent through this system, it is encrypted in the device of the sender and can be decrypted only by the target receiver. The server is not involved in accessing the actual data being transported, instead it is involved in relaying messages, where information between users in any form stays a secret. The system encrypts messages with AES-256-GCM that does not only secure the confidentiality of the information but also its integrity. The authentication mechanism can be used to detect any changes to the message when transmitting it. In order to achieve a secure connection between the users, they utilize Elliptic Curve Diffie-Hellman (ECDH) to produce a shared secret key and it is not transmitted over the network. Along with existing security measures, the system has been planned in consideration of the future threats. It also has a post-quantum cryptography solution based on Kyber to address any threats posed by quantum computing. This hybrid approach enhances the overall system security and increases the resilience of the system in the long run. VartaRaksha is, thus, a trustworthy, safe, and progressive remedy to the digital communication in the present day.

Keywords: *Secure Messaging, End-to-End Encryption, AES-GCM, ECDH, Hybrid Key Exchange, Real-Time Chat, Data Privacy*

1. Introduction
Communication over the internet has become a normal the internet has been a source of ordinary communication. Individuals chat with their friends, share coursework, talk about work-related issues, and organize work in real-time using messaging applications. The more people use these applications, the more their personal and sensitive information they exchange. Messages do also include personal opinions, confidential records, photographs and in some instances a password or authentication information. Due to this reason, user communication security has been a major concern in the modern digital society since most of the current messaging systems are designed in a centralized format whereby a server handles the users, the messages, and the process of transmitting data between the clients. Such a design simplifies the system to control and scale, although it presents a number of security issues. Attackers find central servers to be very appealing and once their security is compromised, user data can be leaked. The metadata, like communication patterns, can be gathered even in the cases when the content of messages is encrypted, and user privacy is diminished. As indicated in Fig. 1, the traditional messaging systems have challenges like server dependency, risk of exposure to data and no security in future. In order to eliminate such problems, safe communication protocols such as end-to-end encryption are needed. Messages are encrypted on the device of the sender and only decrypted on the receiver of the message in an end-to-end system of encrypted messages. The exchange of keys is however, safe and protection against future threats like quantum computing, is difficult. As shown in Figure 1 Secure Message Architecture with Client-Side Encryption.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

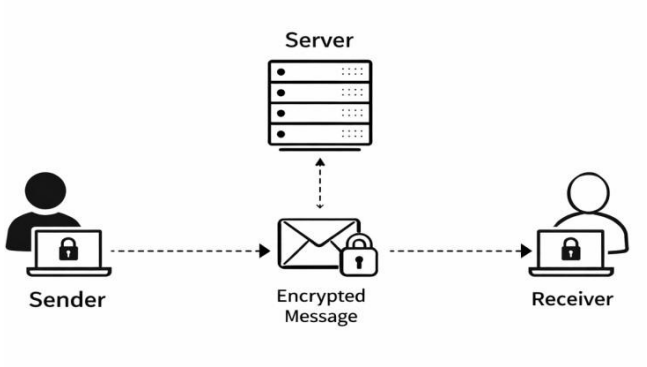

Figure 1 Secure Message Architecture with Client-Side Encryption

This project will solve these issues by introducing VartaRaksha, one of the secure real-time messaging platforms that are concerned with privacy, integrity, and long-term data protection. The system has all cryptographic operations on the client side, which implies that the server cannot have access to sensitive information. Messages get secured with AES-GCM and a hybrid key exchange system, which combines classical and post-quantum techniques is implemented to increase the level of security.

2. Background Theory

The primary use of secure messaging systems is to secure private communication on the internet. The chat applications today are used by people in a variety of ways including exchanging personal messages, education, work in the office and even in sensitive information. Since messages are sent over public networks, there is never the certainty that they will not be picked by attackers or altered. In order to prevent it, encryption is employed. With encryption the content of the actual message is concealed so that even in an event whereby a person intercepts the data, it is not legible. The encryption algorithm that is used most widely is the Advanced Encryption Standard (AES) primarily due to the fact that it is fast and reliable [2]. In the cases of AES being employed coupled with the Galois/Counter Mode (GCM), it does not only encrypt the message it also ensures that the message has not been modified during transmission [3]. This assists in the identification of tampering. Although AES is suitable in safeguarding data, the secret key should be shared among both the sender and receiver. It is insecure to send this key through the internet. Key exchange techniques are employed to address this problem. The Diffie Hellman method enables two users to come up with a shared secret but they do not transmit the secret [1]. The improved version is called Elliptic Curve Diffie Hellman (ECDH), with smaller key sizes that allow it to be used in the modern applications [19]. This implies that in case one of the keys is compromised in the future, the messages that were transferred earlier are secure [21]. In the recent times, the effect of quantum computing on cryptography has been extensively talked about. The next generation quantum computers can become such that they can break some of the current cryptographic algorithms that are secure [11]. It is due to this that it is possible that traditional cryptography methods are not adequate in the long term. Post-quantum cryptography attempts to resolve this issue by proposing the new cryptographic algorithms that are expected to be resistant to quantum attacks [12]. The combination of classical key exchange techniques with post-quantum methods is usually deemed to be a reasonable strategy, as it would enhance the security, yet does not impact the performance as significantly [14]. End-to-end encryption is another concept of secure communication. In this model, the encryption is performed in the device of the user and can no longer be decrypted to any other device. The server is unaware of the encryption keys and is unable to decode the messages [6]. This decreases the degree of trust in the server. The content of the message is not compromised even in case the server can be attacked or compromised. This method applies to many modern messaging applications in order to enhance the privacy of the user [22]. Messaging in real time demands rapid and uninterrupted communication. WebSocket protocol also has the concept of persistent connections, and this feature enables the delivery of messages and reception in real-time [17]. This renders it appropriate to chat systems. Both low latency and security can be attained when sending encrypted data using WebSockets.

It is also necessary to maintain message integrity. Attackers might attempt to alter messages or re-transmit past messages in order to defraud users. Secure encryption algorithms like AES-GCM can be

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

used to avoid such problems by ensuring that all messages are authentic [7]. The background theory is a combination of encryption algorithms, secure key exchange, post-quantum security concepts, end-to-end encryption and real-time communication technologies in the event of failure in the verification. It is these concepts that we will use to build the VartaRaksha secure messaging system.

3. Literature Survey

The primary use of secure messaging systems is to secure private communication on the internet. The chat applications today are used by people in a variety of ways including exchanging personal messages, education, work in the office and even in sensitive information. Since messages are sent over public networks, there is never the certainty that they will not be picked by attackers or altered. In order to prevent it, encryption is employed. With encryption the content of the actual message is concealed so that even in an event whereby a person intercepts the data, it is not legible. The encryption algorithm that is used most widely is the Advanced Encryption Standard (AES) primarily due to the fact that it is fast and reliable [2]. In the cases of AES being employed coupled with the Galois/Counter Mode (GCM), it does not only encrypt the message it also ensures that the message has not been modified during transmission [3]. This assists in the identification of tampering. Although AES is suitable in safeguarding data, the secret key should be shared among both the sender and receiver. It is insecure to send this key through the internet. Key exchange techniques are employed to address this problem. The Diffie Hellman method enables two users to come up with a shared secret but they do not transmit the secret [1]. The improved version is called Elliptic Curve Diffie Hellman (ECDH), with smaller key sizes that allow it to be used in the modern applications [19]. This implies that in case one of the keys is compromised in the future, the messages that were transferred earlier are secure [21]. In the recent times, the effect of quantum computing on cryptography has been extensively talked about. The next generation quantum computers can become such that they can break some of the current cryptographic algorithms that are secure [11]. It is due to this that it is possible that traditional cryptography methods are not adequate in the long term. Post-quantum cryptography attempts to resolve this issue by proposing the new cryptographic algorithms that are expected to be resistant to quantum attacks [12]. The combination of classical key exchange techniques with post-quantum methods is usually deemed to be a reasonable strategy, as it would enhance the security, yet does not impact the performance as significantly [14]. End-to-end encryption is another concept of secure communication. In this model, the encryption is performed in the device of the user and can no longer be decrypted to any other device. The server is unaware of the encryption keys and is unable to decode the messages [6]. This decreases the degree of trust in the server. The content of the message is not compromised even in case the server can be attacked or compromised. This method applies to many modern messaging applications in order to enhance the privacy of the user [22].Messaging in real time demands rapid and uninterrupted communication. WebSocket protocol also has the concept of persistent connections, and this feature enables the delivery of messages and reception in real-time [17]. This renders it appropriate to chat systems. Both low latency and security can be attained when sending encrypted data using WebSockets. It is also necessary to maintain message integrity. Attackers might attempt to alter messages or re-transmit past messages in order to defraud users. Secure encryption algorithms like AES-GCM can be used to avoid such problems by ensuring that all messages are authentic [7]. The background theory is a combination of encryption algorithms, secure key exchange, post-quantum security concepts, end-to-end encryption and real-time communication technologies in the event of failure in the verification. It is these concepts that we will use to build the Varta Raksha secure messaging system.

4. Methodology

The specified system provides a safe real-time communication system, VartaRaksha, to deliver confidential communication with the assistance of End-to-End Encryption (E2EE). The design will ensure the basic entity like the server is not certain to access authentic message contents. Not only does the system include a subset consisting of AES-GCM encryption, but the exchange of keys is also provided

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

by ECDH and an initial post-quantum security solution is Kyber to provide both future and present security.

4.1.System Model and Security Assumptions

The system is based on client server architecture where the server will be used only in the transmission of the messages. It is assumed that the attackers can either make attempts to intercept the network traffic, or modify messages in the process of their transmission. It could also occur that unauthorized users could get encrypted data that exists in the database. However, the users do not distribute the personal keys and they only create and store them in their machines. Because of this, one cannot get encrypted data and be unable to decrypt it without the correct key. This will reduce the credibility of the server and will increase security in general.

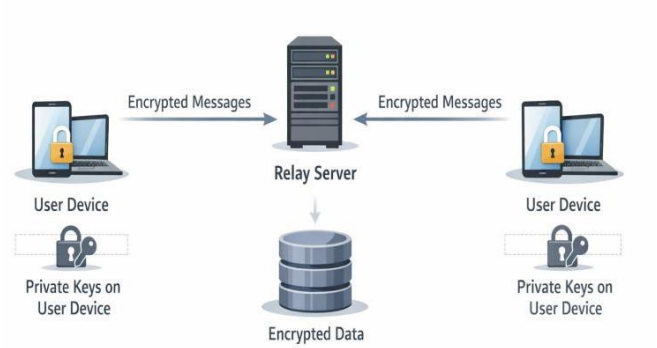

Figure 2 End-to-End Encryption of Safe Client-Server Data Transfer

The diagram shows the way two users may communicate over a relay server. The messages are encrypted and the encryption and decryption of the message is done solely at the receiver end. The server does not intercept in the process of data decryption and does not have access to the content within the messages.

4.2.Hybrid Key Exchange and Key Generation

Two keys, ECDH key pair and Kyber key pair are produced locally by the users. The user machine is left with the private key and the public keys are distributed through the server.

The common key is calculated in the two ways:

$$K = HKDF(S_{ecdh} || S_{kyber}) \quad (1)$$

It is this key that is used to encrypt messages. The hybrid strategy will ensure that in the event that either of the approaches proves to be ineffective in future, the other approach will be safe.

4.3.AES-GCM Message Encryption

Encryption of messages using AES-GCM is done after key-generation. A different IV is given to each message.

$$C = AES\_GCM(K, M, IV) \quad (2)$$

The encrypted output will be referred to as the CCC and the message will be referred to as MMM in this case. There is also production of an authentication tag as well as the ciphertext to ensure integrity.

4.4.Real-Time Communication and Message Flow

This platform is founded on the Socket.IO. These are the login process, transfer of keys, encryption, message transfer and decryption. A sender side encrypts the message and transmits it on the server. The server has no idea whatsoever what is being encrypted in it, and is only sending it across. The receiver gets the shared key by which the message is decrypted.

4.5.Data Storage and Security

The database contains encrypted messages of all the messages. The ciphertext, IV and authentication tag are the values stored.

$$(C, IV, Tag) \quad (3)$$

It can only be decrypted by the appropriate key:

$$M = AES\_GCM^{-1}(K, C, IV) \quad (4)$$

This is to ensure that even after it was accessed, the data remains safe in the database.

4.6.System Implementation and Testing

The message integrity is verified by use of authentication tag. The failure of verification occurs in case the message is modified. The replay attacks can be prevented by making sure that each message has unique IVs. This will ensure that the encrypted message of the same message will not have the same encrypted message.

4.7.System Implementation and Testing

It is grounded on the React (frontend), node.js (backend), socket.io (real-time communication), and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

MongoDB (database). They do testing by message transmission, encryption and decryption as well as integrity.

$$K = HKDF\ (S_{ecdh} || S_{kyber}) \qquad (5)$$

Should a message be modified, it cannot be decrypted and this means that the system knows of intrusion. As shown in Table 1 Performance Comparison

Table 1 Performance Comparison

Feature	Description
Encryption	AES-256-GCM
Key Exchange	ECDH + Kyber
Communication	Socket.IO
Storage	Encrypted MongoDB
Security	End-to-End Encryption

4.8.Performance Evaluation

The functionality of the proposed system is checked in terms of the successful provision of secure and fair communication. The system ensures that all messages are coded and only at the recipient side, they are decoded. The privacy of the user is guaranteed because the server cannot read plaintext messages. AES-GCM will enable the process of identifying any type of interference in the information that was authenticated. Furthermore, every message is encrypted by means of a special Initialization Vector (IV) and, therefore, not possible to repeat messages. All these will make the system more secure and reliable in carrying out real time communication.

4.9.Security Analysis

The proposed system is very secure since it ensures a feeling of confidentiality, integrity, and forward secrecy. Encryption AES-GCM would ensure confidentiality since the content of the message would not be retrieved by third parties. This guarantees integrity through the authentication tags that detect any alteration in the information when passing through it. Secure key exchange systems guarantee forward secrecy wherein the keys of the session are generated dynamically and they are never reused. The keys used in cryptography are never stored on the server therefore there is a low probability of leakage of data through breaching of the server.

4.10. Advantages

The proposed system has a number of advantages over the common messaging systems. It is also a strong end to end encryption and this implies that the content of the message cannot be accessed by any other party other than the users of the message. The mechanism of hybrid key exchange is applied to enhance the degree of security as it is a mixture of the classical and post-quantum techniques. The system also removes the ability to access sensitive information on a server side and hence a low-risk of privacy. Its design is also meant to accommodate future security requirements like application of quantum-resistant techniques, therefore, appropriate in the secure long-distance communication.

5. Results And Discussion

The VartaRaksha system proposed was tested against its capability of offering safe and effective communication. The system has been able to establish encryption and decryption of all messages sent to the receiver and only decryption of the message was done at the receiver side. The server could not read any plaintext data as in the traditional messaging systems, thus enhancing the privacy of the users. The AES-GCM encryption mechanism had a high level of protection against unauthorized access. It was seen that encrypted message could not be decrypted with any alteration in the message, which proved the integrity of the message. The encryption of each message with a distinct Initialization Vector (IV) also meant that similar messages would not encrypt to the same message, making it impossible to do a replay attack. The hybrid ECDH-Kyber key exchange protocol demonstrated good results in terms of the production of secure session keys. The technique offered more security since it would offer resistance against future cryptographic attacks such as quantum-based attacks.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

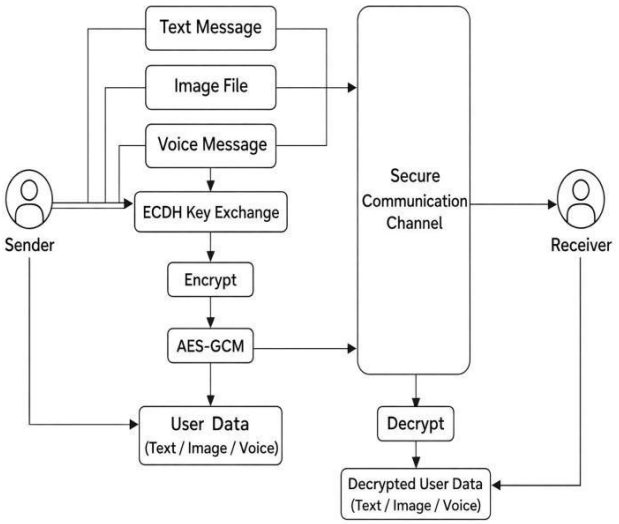

Figure 3 Secure Message Architecture with Client –Side Encryption

The figure represents the message encrypted transmission and validation. It demonstrates the encryption of messages at the senders end, the transmission of messages via the server and the decryption of messages at the receiver end as well as checking the integrity of messages. The system exhibited real-time communication that was efficient by use of Socket.IO. The gap between sending and receiving a message was less and it was therefore fit to be used in practical use. In spite of encryption and exchange of keys, the system was able to establish steady and continuous interaction among users.

6. Security and Data storage Analysis

Data protection was verified on the database. It was noted that the presence of all the stored messages was in an encrypted format, and also there were IV and authentication tags. The data was not readable yet without the respective decryption key even in those cases when database access was simulated. This ascertains that the system does not allow any data to leak even when there is a database attack.

7. Analysis: Attack and Security Analysis:

The system was put to test concerning attacks that are popular like interception and tampering of messages. Attackers could merely read encrypted data in case of interception. Attempts at tampering were also identified, and the authentication mechanism discarded the message. The system is based on a zero-trust model where sensitive information is not trusted to any party, including the server. All cryptographic operations are done on the client side, decreasing the extent of attack and enhancing security.

Conclusion

The proposed system is VartaRaksha, which is a secure real-time messaging solution through End-to-End Encryption. The system guarantees the confidentiality of messages, integrity of messages, and future security with the help of AES-GCM and hybrid key exchange (ECDH + Kyber). Encryption and decryption processes are all done on the client side ensuring the server does not gain access to sensitive information. The system also takes care of message-tampering and replaying attacks. In general, VartaRaksha is a stable and safe communication platform that can be used in the contemporary application.

Reference

[1]. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976
[2]. NIST, "Advanced Encryption Standard (AES)," FIPS Publication, vol. 197, no. 1, pp. 1–51, 2001.
[3]. M. Dworkin, "Recommendation for block cipher modes of operation: GCM," NIST Special Publication, vol. 800-38D, no. 1, pp. 1–37, 2007
[4]. V. S. Miller, "Use of elliptic curves in cryptography," Lecture Notes in Computer Science, vol. 218, no. 1, pp. 417–426, 1986.
[5]. N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.
[6]. D. J. Bernstein, J. Buchmann and E. Dahmen, "Post-quantum cryptography," Springer Series, vol. 1, no. 1, pp. 1–245, 2009.
[7]. CRYSTALS-Kyber Team, "Kyber algorithm specifications," NIST PQC Documentation, vol. 1, no. 1,pp. 1–50, 2021.
[8]. T. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF protocols," RFC 8439, vol. 1, no. 1, pp. 1–45, 2018.
[9]. K. Cohn-Gordon et al., "A formal security analysis of the Signal protocol," IEEE European Symposium on Security and Privacy, vol. 1, no. 1, pp. 451–466, 2017

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5193 - 5199
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0679

[10]. M. Green and M. Smith, "The cryptopals crypto challenges," Cryptography Reports, vol. 1, no. 1, pp. 1–30,2016.
[11]. J. Katz and Y. Lindell, "Introduction to modern cryptography," CRC Press, vol. 2, no. 1, pp. 1–600, 2014.
[12]. B.Schneier,"Applied cryptography," Wiley Publications, vol. 1, no. 1, pp. 1–784, 1996.
[13]. A. Menezesetal. "Handbook ofapplied cryptography," CRC Press, vol. 1, no. 1, pp. 1–780, 1996.
[14]. D. Boneh and V. Shoup, "A graduate course in applied cryptography," Cryptography Notes, vol. 1, no. 1, pp. 1– 800, 2020.
[15]. R. Anderson, "Security engineering," Wiley, vol. 2, no. 1, pp. 1–1000, 2008.
[16]. OWASP Foundation, "OWASP Top 10 Web Security Risks," Security Report, vol. 1, no. 1, pp. 1–20, 2021. [17] MongoDB Inc., "MongoDB Atlas documentation," Database Documentation, vol. 1, no. 1, pp. 1–100, 2023.
[17]. Socket.IO, "Real-time communication framework," Technical Documentation, vol. 1, no. 1, pp. 1–50, 2023.
[18]. Meta Platforms Inc., "React.js documentation," Web Development Docs, vol. 1, no. 1, pp. 1–200, 2023
[19]. OpenJS Foundation ,"Node.js documentation,"Backend Development Docs, vol. 1, no. 1, pp. 1–200, 2023
[20]. J. F. Kurose and K. W. Ross, "Computer networking," Pearson, vol. 7, no. 1, pp. 1–850, 2017.
[21]. A. Perrig et al., "Security in wireless sensor networks," Communications of the ACM, vol. 47, no. 6, pp. 53–57, 2004.
[22]. S. Goldwasser and M. Bellare, "Lecture notes on cryptography," MIT Publications, vol. 1, no. 1, pp. 1–300,2008.
[23]. Y. Gu and X. Wang, "Dynamic modeling of cyberphysical attacks using Petri Nets," International Journal of Critical Infrastructure Protection, vol. 30, no. 1, pp. 100369, 2020.
[24]. J. Daemen and V. Rijmen, "AES proposal: Rijndael," NIST Submission, vol. 1, no. 1, pp. 1–50, 1999.
[25]. D. Eastlake, "Secure hash algorithm (SHA-2)," RFC 4634, vol. 1, no. 1, pp. 1–30, 2006.
[26]. NIST, "Post-quantum cryptography standardization,"NIST Report, vol. 1, no. 1, pp. 1–40, 2022.
[27]. Signal Foundation, "Signal protocol documentation," Security Documentation, vol. 1, no. 1, pp. 1–60, 2021.
[28]. Telegram Messenger LLP, "Telegram security model," Technical Whitepaper, vol. 1, no. 1, pp. 1–40, 2022.
[29]. WhatsApp Inc., "WhatsApp encryption overview," Security Whitepaper, vol. 1, no. 1, pp. 1–30, 2023.
[30]. Cloudinary Inc., "Cloudinary media management documentation," Cloud Documentation, vol. 1, no. 1, pp. 1–50,2023.