International Journal of Applied Mathematics

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ANALYZING CYBERSECURITY THREATS: INVESTIGATING HACKING ATTEMPTS TO STRENGTHEN CHAT APPLICATION SECURITY

Shefali Arora[1] and Sherry Verma[2]

[1] Sushant University (Erstwhile Ansal University), School of engineering and technology, Golf Course Road, Sector 55, Gurugram, India

shefaliaroraphd@gmail.com

[2] Sushant University (Erstwhile Ansal University), School of engineering and technology, Golf Course Road, Sector 55, Gurugram, India
sherryverma@sushantuniversity.edu.in

Abstract: Chat apps are an important part of how people communicate these days, but they are still popular targets for assaults like Man-in-the-Middle (MitM), SQL injection, Cross-Site Scripting (XSS), and brute-force tactics. This research examines several security strategies—encryption, compression, and a combination of both—to assess their efficacy in safeguarding chat settings. A mixed-method approach, including attack simulations using tools such as Burp Suite and SQLMap, is used to evaluate vulnerabilities and performance effects. The results show that encryption keeps data private, but compression speeds up the process of sending information. The hybrid technique, on the other hand, is the only one that offers full security with little data loss during simulated assaults. Experimental findings demonstrate substantial improvements in the mitigation of SQL injection, Man-in-the-Middle (MitM), and replay threats using integrated compression and encryption techniques. The study provides a systematic approach for identifying vulnerabilities, assessing performance, and improving security in chat apps. The suggested paradigm improves data integrity and communication privacy by using adaptive encryption, compression, and continuous testing. This hybrid security architecture is a scalable and effective way to protect chat systems from new cyber threats.

Keywords: Hacking attempts, Encryption, chat application, Performance, Cryptographic attacks, Cyber security

1. Introduction

With the increasing reliance on digital communication, chat applications have become a primary means of interaction for individuals and businesses. However, this widespread adoption has also made them a prime target for cyber threats. Hackers exploit vulnerabilities in chat applications using various attack techniques such as man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, phishing, malware injections, and session hijacking. These security breaches can lead to unauthorized access, data theft, privacy violations, and financial losses.

To ensure secure communication, it is crucial to analyze and understand different hacking attempts, their impact, and effective countermeasures. This research aims to investigate various

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

hacking techniques targeting chat applications and propose robust security mechanisms to mitigate these threats. By studying encryption techniques, authentication protocols, and intrusion detection systems, this work will contribute to the enhancement of chat application security.

The study will also explore the role of modern cybersecurity frameworks, artificial intelligence-driven threat detection, and blockchain-based security models in safeguarding chat applications. A comprehensive evaluation of vulnerabilities and security strategies will help developers and organizations build more resilient communication platforms.

2. Literature review

Numerous studies have been conducted on technologies that facilitate online conversation. This section presents research that pertains to compression and security. The possibility of optimizing networks using artificial intelligence to make them more secure, fault-tolerant, and scalable was studied by Uchenna Umoga et al. (2024). Autonomous threat and vulnerability detection and mitigation was their primary emphasis. The Review provides a brief synopsis of the main findings and insights gained from the study, showcasing the game-changing potential of optimization powered by AI to enhance the efficiency and performance of networks. Automation of complex optimization processes, reduction of operational responsibilities, and adaptability to changing network conditions and user needs are all emphasized in the statement as benefits of AI-driven approaches. [1]. To address the challenges and shortcomings of blockchain networks, K. Venkatesan et al. presented hybrid consensus algorithms in their 2024 paper. These algorithms use machine learning (ML) methodologies. When working with distributed systems, consensus procedures may be a real pain in getting everyone on the same page. But modern methods are easier prey for cybercriminals. The need for effective prevention measures has been highlighted in previous study, which has extensively examined the effects of cyber attacks [2]. Considering the moderating effects of team size and tenure, B. A. Kurdi et al. (2023) set out to investigate the factors influencing team social networking and performance in Jordanian SMEs. A survey questionnaire was used to collect data from this particular sector for the investigation. In order to assess the proposed study model, the collected data was then processed using SamartPLS. Results showed that seven traits—team communication, team conflict, team power, team regulation, team collaboration, team engagement, and motivation—had a mostly positive effect. [3]. V. Bhuse et al. (2023) limited their research to social media end-to-end encryption. Integral to the Signal protocol was an open-source method of end-to-end encryption. The algorithms used for cryptography include Curve25519, AES-256, and HMAC-SHA256. At the present time, this protocol is thought to being cryptographically strong, and it offers great protection against hackers. Despite this, a number of social media companies persist in implementing measures that aren't secure enough and are based on questionable principles. Popular social media platforms including Instagram, WhatsApp, Twitter, Facebook, and Snapchat are broken down into their individual cryptographic primitives in this article. [4]. Many popular chat apps have different privacy and security features, which J. Botha et al. (2019) looked studied. This study compares the privacy

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and security settings, data retention rules, and user-friendliness of the most advanced and seemingly secure messaging apps. Application recommendations and expert advise are given to users to help them choose apps with the best privacy and security features. [5]. Digital data transmission methods that are both secure and efficient were the primary emphasis of B. Carpentieri et al.'s 2018 research. A straightforward, easy-to-understand, and secure method of encoding is what they're seeking. Two procedures, fundamentally incompatible with each other, form the basis of this interaction's arrangement. But to make sure the original file is secure and efficient, you have to do both of those things on it. In this grouping you'll find both encryption and data compression. Digital data compression and encryption was the main focus of this research. Modern compression and encryption methods were put through their paces on a range of digital data types in this article. [6]. According to M. Chase et al. (2019), the focus of their research was on distrustful end-to-end encrypted interactions. Currently, for end-to-end (E2E) systems to be vulnerable to a man-in-the-middle attack, it is necessary for a service provider to have been hacked or pressured into adding their own encryption keys to the allowed users list. Their formalized version of a Privacy-Preserving Verifiable Key Distribution (VKD) system is based on the ideas of CONIKS. With this approach, consumers can see exactly which keys are being handed out to them. In contrast to existing methods, their proposed VKD approach, seamless, provides better privacy and scalability. The novel method we've developed enables us to make huge changes in a matter of seconds. As a result, we can demonstrate empirically that our technique effectively handles delays of one minute or less. [7]. E. N. Ekwonwune et al. (2020) examined SMS encryption in depth, zeroing in on a hybrid cipher algorithm as the means to provide end-to-end security. Prototyping, SSADM, and OOADM are the three methods used in the study. All communications were guaranteed to be secure, private, genuine, and unbreakable by using three separate cryptographic methods: MD5, blowfish, and RSA. The encrypted communications created by the bespoke software are similarly impenetrable via a process of arduous trial and error. Java was used to create the programs that carried out the real duties [8]. K. Giri et al. published a thorough data encryption technique in 2020. Data transferred via a particular network was encrypted to guarantee its security. The best long-distance interpersonal communication companies have been subject to many audits examining their encryption strategies within the last decade. Knowing how End-to-End encryption works and how to put it into practice is crucial. Since new and improved iterations and approaches are always appearing in the innovation domain, the idea of defining the "Best" is useless. Summarizing the benefits of several end-to-end encryption systems, this paper provides a comprehensive overview [9]. The social, legal, and privacy consequences of chatbot use were examined by M. Hasal et al. (2021). The question of whether and how chatbots may exploit such data is investigated in this research. Since many chatbots operate on social or messaging networks, it is essential to understand how these platforms handle user data. The study's overarching goal is to provide light on the issues surrounding chatbot security. There are concerns about how to store and utilize data gathered from chatbot conversations, and this study might start a discussion about those concerns and provide answers [10]. Online social network security and

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

privacy were thoroughly examined and evaluated by A. K. Jain et al. (2021). Luckily, we also included information on assaults on Open Social Network web apps and provided statistics to back up our claims. On top of that, they have covered a wide range of security precautions for OSNs. In order to strengthen the trustworthiness of social media platforms, the study concludes by discussing open questions, future obstacles, and applicable security legislation. [11]. J. Kim et al. (2019) just published their findings on a state-of-the-art key-value store that achieves better performance by combining compression and encryption. The results of this investigation were presented. After implementing the proposed techniques on a distributed integrated Key-Value Store (KVS), the researchers weigh the pros and cons of including these features at various points along the dataflow path. By comparing Grand Tave' at the Swiss National Supercomputing Centre to Cori at the National Energy Research Scientific Computing Centre, we can see how drastically different their effective bandwidth, latency, and additional computational cost are. [12]. Systems that provide secure encryption and compression were shown by H. Korane et al. (2021) in their research. In order to make ETC systems more secure, this method was developed. After comparing the suggested approach to the present encryption methodology, it becomes clear that the former allows for more blocks with lower sizes. No matter how many color channels an original picture contains, the proposed encryption method still uses grayscale images to decrease the color information. The security against jigsaw puzzle solvers and brute-force attacks has been greatly improved by these enhancements. Furthermore, color sub-sampling may be used to expedite the compression process, even if the encrypted photographs do not include any color information. By using state-of-the-art compression algorithms and uploading and downloading encrypted photographs from social networking sites, we were able to get practical data that prove the efficacy of the proposed solution for ETC systems. in [13]. Cryptographic chat room security was the focus of Kuliya et al.'s (2020) research. Chat apps are popular among smartphone owners and internet users alike. On a daily basis, an astounding hundred million people with mobile phones utilize messaging apps. Since these chat programs provide free communication and the most of them do not need any setup costs, they were very attractive to prospective users. Most of these messaging applications fail to adequately protect their users' private information, despite the fact that they provide a lot of features and services. The vast majority of these messaging apps do not provide enough security for their customers, according to an EFF study [14]. Social data compression methods developed for very sparse datasets were thoroughly examined by C. K. Leung et al. (2020). The goal of this study is to find new connections between massive social network datasets that are relatively empty. Due to the bitmap compression of the social entities in the data, useful information could be extracted and interesting new insights could be explored, even if the data was not very dense. An evaluation scenario for very sparse and very large social network datasets demonstrated the efficacy of our compression approach [15].

3. Problem Statement

Finding a happy medium between speed and security is a major problem for traditional chat apps. Problems with performance result from dealing with massive amounts of data in real-time, such as text, multimedia files, and audio or video communications. Latency may be

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

introduced by compression methods owing to the computational cost necessary for data compression and decompression, even while compression techniques improve transmission speed and reduce bandwidth utilization. Chat apps also have a heavy security burden since they must safeguard users' personal information from hackers. Although strong encryption helps protect data, it can also slow down applications since it requires computing resources. Compatibility testing across many systems and devices is another source of complexity, as is the need to standardize compression and encryption protocols. Encryption techniques that are either out of date or not applied correctly may still lead to security risks, and securely storing encryption keys is both important and difficult. The problem is made much more complicated by the fact that resources are limited, especially on mobile devices, making it necessary to create efficient algorithms that do not use up too much processing power or battery life. Continuous innovation and diligent management are necessary to preserve the dependability and safety of traditional chat apps in the face of these combined performance and security issues.

4. Proposed work

The research methodology for evaluating security measures against various attacks in a chat application involves multiple stages, beginning with an assessment of the increasing vulnerabilities in chat applications due to cyber threats such as Man-in-the-Middle (MitM), Cross-Site Scripting (XSS), and SQL injection attacks. The study aims to evaluate the effectiveness of security measures, particularly data compression and encryption, in mitigating these risks. A literature review is conducted to analyze existing security challenges and mechanisms employed in chat applications. The research adopts a mixed-methods approach that integrates attack simulations and qualitative assessments, focusing on specific threats like MitM, XSS, and SQL injection. Security measures are then implemented, detailing data compression for efficiency and encryption for secure transmission and storage. Simulation and testing involve designing attack scenarios using tools such as Burp Suite and SQLMap, followed by data collection and analysis to assess the resilience of implemented security mechanisms. A thorough evaluation is carried out through quantitative analysis of attack success rates and qualitative insights into security effectiveness. Additionally, the process flow of work involves setting up a secure testing environment with monitoring tools, simulating various network, application-level, and cryptographic attacks, and analyzing system responses. Attack simulations, including MitM, replay attacks, SQL injection, and XSS, are executed, and performance metrics are measured. Findings are used to patch vulnerabilities, enhance encryption and compression security, and integrate continuous security testing into the development cycle. This structured approach ensures a comprehensive evaluation of security measures, proactively identifying and mitigating potential vulnerabilities in the chat application.

Here’s an algorithm outlining the workflow for evaluating security measures against various attacks in a chat application:

Algorithm: Security Evaluation of a Chat Application

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Input: Chat application with data compression and encryption implemented
Output: Identified vulnerabilities and enhanced security mechanisms

Step 1: Environment Setup

1. Deploy the chat application with implemented security measures.

2. Configure a testing framework using tools like Metasploit, Burp Suite, and SQLMap.

3. Set up monitoring tools (Wireshark, Splunk) to capture logs and analyze security events.

Step 2: Identify Attack Vectors

4. Define attack types:

- **Network Attacks:** MitM, replay attacks
- **Application-Level Attacks:** SQL injection, XSS
- **Cryptographic Attacks:** Brute force, compression-based exploits

Step 3: Execute Simulated Attacks

5. **MitM Attack Simulation:**
a. Intercept encrypted data using Burp Suite.
b. Attempt to decrypt or manipulate messages.
c. Log encryption effectiveness and system response.

6. **Replay Attack Simulation:**
a. Capture encrypted messages using Wireshark.
b. Resend recorded messages to the chat server.
c. Observe if the system detects duplicate transmissions.

7. **SQL Injection Simulation:**
a. Inject SQL payloads through chatbot input fields.
b. Monitor database response for vulnerabilities.

8. **XSS Attack Simulation:**
a. Insert malicious scripts into chat fields.
b. Observe if scripts execute in unintended contexts.

9. **Brute Force & Compression Attacks:**
a. Capture encrypted data packets.
b. Attempt brute-force decryption using Hashcat.
c. Test if compression mechanisms expose sensitive data.

Step 4: Analyze and Report Findings

10. Review logs and security tool outputs.

11. Identify weaknesses in encryption, data compression, or input validation.

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

12. Measure performance impact under simulated attacks.

Step 5: Implement Security Enhancements

13. Patch vulnerabilities identified in testing.
14. Strengthen encryption by updating algorithms or key lengths.
15. Improve input validation and sanitization mechanisms.

Step 6: Continuous Testing & Monitoring

16. Integrate automated security testing into CI/CD pipelines.
17. Perform periodic security audits and simulations.
18. Monitor real-time security threats and refine defenses.

End of Algorithm

5. Simulation work

The effectiveness of different security approaches—uncompressed/non-encrypted, compressed/non-encrypted, uncompressed/encrypted, and hybrid (compressed and encrypted)—is evaluated to understand their resilience against various cyber threats within a chat application. The study simulates multiple attack scenarios, including Man-in-the-Middle (MitM), brute force, replay attacks, SQL injection, and Cross-Site Scripting (XSS), to assess how each security approach mitigates risks. In the case of uncompressed and non-encrypted data, the application is highly vulnerable, as attackers can intercept, manipulate, and exploit communication through MitM, brute force, replay, and XSS attacks. When data is compressed but not encrypted, bandwidth efficiency improves, yet it remains susceptible to interception and manipulation, leaving authentication mechanisms and user data exposed. Conversely, uncompressed but encrypted data offers strong protection against MitM, brute force, and replay attacks by securing data transmission, though vulnerabilities in application code may still allow XSS attacks. The most robust approach is the hybrid method, where data is both compressed and encrypted, ensuring confidentiality and integrity while significantly reducing exposure to cyber threats. This combined approach not only enhances security by mitigating interception and manipulation risks but also optimizes data transmission efficiency, making it the most effective solution for securing chat applications against modern cyber threats.

Table 1 Comparison of Different attack Simulations in different circumstances

	Normal chat (case 1)	**Compressed chat (case 2)**	**Encrypted chat (case 3)**	**Hybrid approach (case 4)**
SQL Injection	36	33	30	21
Brute force	68	68	59	57
Replay Attack	66	63	54	46

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cross Script attack	90	82	77	69
MitM Attack	65	63	54	50

Considering Table 1 the following chart has been plotted to visualize the result of simulation. It has been observed that there is a minimum impact of data loss in the case of a hybrid approach.

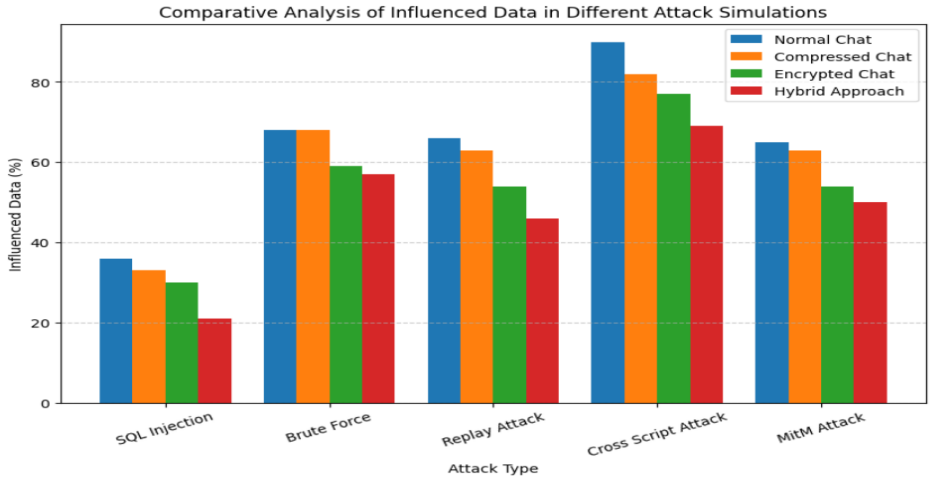

Fig 2 Comparative analysis of Influenced data in case of different hacking attacks

The bar chart visually represents the percentage of influenced data across different attack scenarios (SQL Injection, Brute Force, Replay Attack, Cross-Site Scripting, and MitM) for four security approaches:

- **Normal Chat (Case 1)**: The highest data vulnerability, with the most significant impact from all attack types due to the absence of encryption and compression.
- **Compressed Chat (Case 2)**: A slight improvement in mitigating attacks compared to normal chat, but still highly vulnerable as compression alone does not provide security.
- **Encrypted Chat (Case 3)**: A notable reduction in attack impact, especially in MitM, brute force, and replay attacks, showing the effectiveness of encryption. However, some threats, such as XSS, still pose a risk.
- **Hybrid Approach (Case 4)**: The lowest percentage of influenced data across all attack types, confirming that combining encryption and compression provides the best protection against cyber threats.

6. Conclusion

The analysis demonstrates that the hybrid approach (compressed and encrypted data) provides the most robust defense against various attacks, significantly reducing data exposure.

Received: August 11 2025

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Encryption alone is effective in protecting data integrity and confidentiality, but when combined with compression, it enhances security while optimizing bandwidth usage. This result highlights that chat applications should adopt a hybrid security model to ensure maximum protection against cyber threats like MitM, brute force, and replay attacks while minimizing data loss.

7. Future Scope

Data compression and encryption chat applications have a huge potential for growth and innovation in a number of important domains. Better algorithms will become available for these systems in the future, allowing for even more rapid and efficient encryption and compression without sacrificing security. With the advent of quantum computing and AI, encryption techniques may undergo a radical shift, providing hitherto unseen levels of protection against ever-evolving cyber threats. Machine learning may also improve data compression methods, which improves the efficiency of real-time communication by adapting compression settings in real-time to different data kinds and network circumstances. Increased need for sophisticated compression and encryption methods is a direct result of the growing importance of safe and effective communication protocols for the networked devices that make up the Internet of Things (IoT). Trustless communication is vital for applications in healthcare, banking, and other fields, and safe and efficient chat systems will play a major role in enabling this in the area of decentralized apps (dApps) and blockchain technology. Further, data privacy regulations will be changing over time, so there will need to be constant innovation in encryption standards to keep up with the changes and keep user data safe. As these technologies develop further, they will allow for safe, instantaneous communication across a variety of platforms and devices, including mobile, desktop, and wearables, greatly improving the user experience. As a result of this continuous development, data compression and encryption will play an increasingly important role, making chat programs vital in both personal and professional settings.

Reference

[1] Uchenna Joseph Umoga et al., “Exploring the potential of AI-driven optimization in enhancing network performance and efficiency,” Magna Scientia Advanced Research and Reviews, vol. 10, no. 1. GSC Online Press, pp. 368–378, Feb. 28, 2024. doi: 10.30574/msarr.2024.10.1.0028.

[2] K. Venkatesan and S. B. Rahayu, “Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques,” Scientific Reports, vol. 14, no. 1. Springer Science and Business Media LLC, Jan. 11, 2024. doi: 10.1038/s41598-024-51578-7.

[3] B. A. Kurdi et al., “Factors affecting team social networking and performance: The moderation effect of team size and tenure,” Journal of Open Innovation: Technology,

Volume 38 No. 9s , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Market, and Complexity, vol. 9, no. 2. Elsevier BV, p. 100047, Jun. 2023. doi: 10.1016/j.joitmc.2023.100047.

[4] V. Bhuse, "Review of End-to-End Encryption for Social Media," Int. Conf. Cyber Warf. Secure., vol. 18, no. 1, pp. 35–37, 2023, doi: 10.34190/iccws.18.1.1017.

[5] J. Botha, C. Van 't Wout, and L. Leenen, "A comparison of chat applications in terms of security and privacy," Eur. Conf. Inf. Warf. Secure. ECCWS, vol. 2019-July, pp. 55–62, 2019.

[6] B. Carpentieri, "Efficient compression and encryption for digital data transmission," Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/9591768.

[7] M. Chase, E. Ghosh, A. Deshpande, and H. Malvai, "Seemless: Secure end-to-end encrypted messaging with less trust," Proc. ACM Conf. Comput. Commun. Secur., pp. 1639–1656, 2019, doi: 10.1145/3319535.3363202.

[8] E. N. Ekwonwune and V. C. Enyinnaya, "Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm," J. Softw. Eng. Appl., vol. 13, no. 03, pp. 25–40, 2020, doi: 10.4236/jsea.2020.133003.

[9] K. Giri, N. Saxena, Y. Srivastava, and P. Saxena, "End-to-End Encryption Techniques," Int. Res. J. Eng. Technol., no. June, pp. 1089–1093, 2020, [Online]. Available: www.irjet.net

[10] M. Hasal, J. Nowaková, K. Ahmed Saghair, H. Abdulla, V. Snášel, and L. Ogiela, "Chatbots: Security, privacy, data protection, and social aspects," Concurr. Comput. Pract. Exp., vol. 33, no. 19, pp. 1–13, 2021, doi: 10.1002/cpe.6426.

[11] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex Intell. Syst., vol. 7, no. 5, pp. 2157–2177, 2021, doi: 10.1007/s40747-021-00409-7.

[12] J. Kim and J. S. Vetter, "Implementing efficient data compression and encryption in a persistent key-value store for HPC," Int. J. High Perform. Comput. Appl., vol. 33, no. 6, pp. 1098–1112, 2019, doi: 10.1177/1094342019847264.

[13] H. Korane, A. P. Singh, C. P. Mirdul, and S. Thokale, "Secure Encryption then Compression Systems using Encryption Algorithms," Int. J. Adv. Res. Sci. Commun. Technol., vol. 6, no. 1, pp. 513–517, 2021, doi: 10.48175/ijarsct-1428.

[14] M. Kuliya and H. Abubakar, "Secured Chatting System Using Cryptography," vol. 8, no. 9, pp. 23–36, 2020.

[15] C. K. Leung, Y. Zhang, and F. Jiang, "Compression for Very Sparse Big Social Data," Proc. 2020 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2020, pp. 659–666, 2020, doi: 10.1109/ASONAM49781.2020.9381370.

Received: August 11 2025