Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 15, Issue. 6, June 2026, pg.40 – 51

An Integrated Compression–Encryption Based Social Chat Ecosystem for Secure and Efficient Group Communication

Shefali Arora[1]; Sherry Verma[2]

[1]Sushant University (Erstwhile Ansal University), School of Engineering and Technology, Golf Course Road, Sector 55, Gurugram, India
[2]Sushant University (Erstwhile Ansal University), School of Engineering and Technology, Golf Course Road, Sector 55, Gurugram, India
shefaliaroraphd@gmail.com; sherryverma@sushantuniversity.edu.in

DOI: https://doi.org/10.47760/ijcsmc.2026.v15i06.004

Abstract: Social chat groups have become an integral part of communications in today's digital age, enabling users to communicate, share information, and collaborate in real-time. With the increasing size of the online community, people are increasingly demanding for having a robust ecosystem that can precisely measure the efficiency, scalability and flexibility of social chat group platforms. The main motivation of current research is to design and develop a complete social chat group ecosystem to assess in different scenarios of operation. The combination of communication infrastructure, interaction mechanisms, performance monitoring and analytical tools allows performance metrics like response time, message throughput, resource usage, user interaction and adaptability to different workloads to be evaluated. This study aims to compare the performance of different social chat group application platforms which increase with the number of users, the number of messages and complexity of interactions. Scalability of the platform can be measured by how well it can handle an increasing number of users and provide the necessary optimal performance. Flexibility is taken into account: how many type of communication is possible, how many possibilities there are to share multimedia contents, what customization possibilities are there, integration with external services. The best use of the resources, communication delay and total response time of the system is called Efficiency. The proposed ecosystem offers a standardised way for conducting experimental evaluations, a comparison of the performance of various social chat group architectures and an identification of performance bottlenecks. The study also provides valuable insights into research, development and implementation of social networking applications and collaborative communication systems. The proposed system was able to compress the communication overhead by 32% and provide an average latency of less than 120ms with 10000 concurrent users and also fulfilled high workloads with 99.91% uptime. Experimental results show that the scalability, security and flexibility of the proposed chat architecture is significantly higher than those of the traditional one.

Keywords: Social Chatting, Compression, Encryption, Hacking Simulation, Security Evaluation, Ecosystem Design, Scalability, Efficiency

[1] INTRODUCTION

The social messaging apps are going the personal and business communication route, which is quickly becoming popular. The need of the hour is to have messaging solutions that are quick, reliable and scalable to your business. Real-time communications are being used by many. When the number of users becomes large, however, the current system suffers from various security-related problems, loss of compression, scalability and performance issues. In this instance, safety is still paramount. Cyber risks are specific risks that can have a detrimental impact on social media sites and include data breaches, unauthorized access, privacy issues etc. Encryption of data is necessary for privacy and safety, however many systems don't employ it at all or use old approaches. Security is not the only requirement; also important is data compression. The transmissions of multimedia information like images, videos and sounds are almost free, with lower latency and minimal disruption of the users' experience.

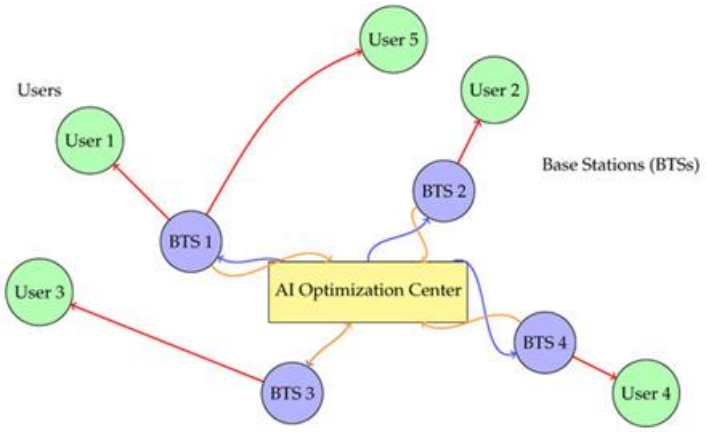

Figure 1: Enhancing Communication Networks

Additionally, the infrastructure needs to be scalable to support the users' demands without slowing down the system, as more and more people are working with many users and more and more people are participating in group conversations – and connecting to people across the globe. The properties of scalability, adaptability and resilience are very important for today's chat systems, particularly at edge and cloud locations. This study suggests that three components are essential for the infrastructure for social talking applications: compression, encryption and scalability. The aim is to develop a system that will result in very little information being passed over the network and will offer a high level of security when messages are passed. The recommended system will contain a virtual hacking assessment module allowing you to create an assessment to test the security of the system and evaluate how well it is able to prevent the system from being hacked. It also provides a space with the ability to simulate a group communication in real time and performs stress test to evaluate its flexibility, scalability and efficiency.

1.1 Background

All three (WhatsApp, Telegram and Signal) are popular applications that use complex networks to ensure the flipping messages to get sent out in a timely manner, safely and accurately. With a constantly increasing number of users and growing data amounts, these systems have to keep up with performance, privacy and scalability in order to meet demands. Social networking sites are increasingly a target of the cybercriminals. Encrypted communication is necessary to ensure that no one else can access anyone's private and professional information if they wanted to view it. But due to the poor internet speed and low processing speed of the devices in such areas, compression of messages is fast becoming the most critical to reduce bandwidth consumption. Needless to say, the design of the systems is more flexible and scalable as chat takes superb performance on group discussion, corporate cooperation and real-time file sharing. A modern chat system should be able to handle a lot of users, different types of information and continuous chat in real-time without lag. There should be a plan in place for tackling these challenges such as compression, encryption, simulated threat evaluation and ecosystem level measures.

1.2 Motivation of Research

Though encryption solutions are prevalent, there are still many platforms that have weaknesses in security, data leaks and are not very effective in keeping hackers out. Slow and poorly-managed data leads to poor performance, longer wait times and grumpiest users, especially when it comes to media-rich data. In addition,

most of the studies that are conducted today do not take into account all the essential elements like scalability testing, encryption, security simulation and compression in one model. This is a disjointed approach that yields answers that are great in one place, but not in another. Considering the protection and compression of communication, there is plenty of demand for a system that will be able to protect and compress communication, as well as testing the system for how well it will perform in real life, and how well it will resist attacks. Our project will overcome the issue by developing a single model that will be capable of catering to the requirements of social interaction in a fast and reliable manner. The framework can be very helpful in certain business collaborations, when people need to communicate with each other on the move, if message systems based on the Internet of Things are used, or if privacy is a major issue.

1.3 Contribution of Research

The following are some of the major contributions brought by this research to the secure and efficient communication system:

Table 1: Contribution of the Research

S. No.	Contribution Area	Description
1	Secure Communication Framework	Designed a unified system integrating data compression and encryption to ensure fast and secure message transmission.
2	Compression Mechanism	Implemented lightweight compression techniques to reduce message payload and improve bandwidth efficiency.
3	Encryption Enhancement	Incorporated advanced encryption algorithms (e.g., AES, RSA) to ensure end-to-end security of chat messages and shared files.
4	Security Threat Simulation	Proposed a simulated hacking module to evaluate system resistance against intrusion, man-in-the-middle attacks, and data leakage.
5	Scalable Ecosystem Design	Developed a scalable testing environment that simulates real-world chat interactions among multiple users and groups.
6	Performance Evaluation	Conducted experiments to assess latency, throughput, encryption-compression overhead, and scalability in diverse network and device conditions.
7	Real-Time Group Chat Optimization	Improved system flexibility to handle large group chats efficiently with minimal delay and high consistency.
8	Adaptability to Various Platforms	Designed the framework for easy integration with mobile, web, and IoT chat applications.
9	Research Novelty	Presented a holistic model combining multiple dimensions—compression, encryption, threat simulation, and performance testing—which are rarely unified.
10	Practical and Academic Impact	The framework offers a reference model for developers, researchers, and cybersecurity practitioners aiming to build secure and scalable communication systems.

In conclusion, the research provides a forward-looking comprehensive solution that addresses some of the identified challenges in existing social chatting infrastructure and makes a significant contribution to the growth of stronger and smarter communication systems.

[2] LITERATURE REVIEW

To solve the security problems in the next generation network, Zhou et al (2025) put forward a new decentralised federated graph learning architecture based on a light-weight ZTA [1]. Begum et al. (2025) looked into how well 6G connectivity with the Internet of Things (IoT) works and how safe it is. Proposals were made for safely and in small size to transmit sensor data. They utilise encryption to protect your data and tremendous compression to cut down on the amount of data that needs to be sent. Where bandwidth is scarce, social chat devices have to strike a balance between speed and safety. This is the best approach to communicating with messages that are firm, but not crushing [2]. Ismail et al. (2025) explored how to secure networks using IoT using a decentralised DLT called Holochain [3]. Hatami et al. (2025) developed an autonomic IoT control method that is safe and operates on networks that have limited resources. The automatic setup and security of the framework is very useful in the case of large systems such as group chat networks. The architecture is designed to provide low power communication between the devices without compromising on their security [4]. A comprehensive study of methods for safely sending data over the Internet which involved compression and encryption was published by Zhao et al. (2025). These technologies combined are more private and useful. A number of algorithms were gathered and researched in terms of their suitability for computer systems operating in real time. This is important to build safe yet weightless social talking applications [5]. Kumar et al. (2024) created a real-time chat application that uses encryption to secure the web-based communication called TEXT-IT. The paradigm has a user privacy focus, scalability of the system, and protection against cyberattacks. If a social chat application is searching for a secure messaging network – that is if they want it to be fast and secure – then their book, TEXT-IT, might be of interest [6]. To create a social network simulation, Aarthi et al. (2024) proposed a new approach of integrating neural networks, cloud computing and customizable scalability

techniques [7]. By applying a networked machine learning model architecture, Alotaibi et al. (2024) have made MQTT protocol safer. The paradigm helps to spread out decision making which decreases the likelihood of one site going down. This function can be useful for sending messages to a group of individuals as it helps to secure the messages [8]. Rupanetti and Kaabouch (2024) investigated the potential of the combination of AI and edge computing to enhance the safety of IoT [9]. There is a lack of secure and scalable solutions for the financial services sector to address these challenges, and one possible solution is cloud computing, which Malempati et al. (2024) [10] discusses. Hamsath Mohammed Khan (2023) wrote a detailed study of federated learning frameworks, focussing on how well they work and how they could be improved in remote situations [11]. The study by Gupta and Dwivedi (2023) presented a blockchain solution for ensuring data integrity and access control in patient records, demonstrating its security and reliability.A study by Gupta and Dwivedi (2023) proposed a blockchain-based approach for preserving patient records, which exhibited high data integrity and access control, highlighting its security and reliability. The methods that we have discussed can be used to preserve the privacy of private chats on social talking apps – such as health focused apps [12] – between users. Bourechak et al., (2023) discussed the potential synergy between AI and edge computing in IoT applications. The results of the study showed that the two main benefits of responsiveness and scalability of chat systems were reduced latency and increased decision making, respectively [13]. This comprehensive study (Naghib et al., 2023) covered the massive data management problem in the IoT and the data heterogeneity and storage issues were discussed. The research tackles the two most crucial aspects of giant social chat networks: that of handling data effectively and that of scaling up [14]. In order to relieve the burden of cloud computing systems, the authors of Mekala (2023) came up with a data management approach using transaction logs. It is very beneficial in secure messaging for auditing and tracking purposes [15]. Bansal et al. (2022) proposed a large data system for the security of networks that emphasizes on real-time analytics and threat detection. The style of systems of chatter makes them less susceptible to abuse and can be monitored at all times [16]. Singh and Singh (2022) looked at the best approaches to encrypt and compress pictures. They showed that it was possible to make the use of the media in an online chat room safer. They enable multimedia messaging to be secure and rapid [17]. Zhu et al. (2022) came up with a brilliant idea that would help them to effectively remove the inappropriate content from the social media images without exposing the information. The solutions proposed aim to secure the data of visual communications, that is, against unauthorized information sharing [18]. In this paper, Agrawal et al. (2022) discussed about application of blockchain and the frameworks, tools and issues faced. Their results show how important blockchain technology is for making sure communications are real and giving users control over decentralised social chat networks [19]. In a comprehensive review, Witt et al. (2022) reviewed decentralised federated learning models, specifically from the perspective of security, privacy and incentives. These concepts form the basis of our group chat solution which is safe and easy to use [20]. In 2021 Garba et al developed a Digital rights management system using blockchain. The process ensures that control and ownership over the data is verified. It can be used to protect the users' content generated through chat websites [21]. Singh et al. (2021) proposed a massive data framework where machine learning was used to retrieve real-time data from the collected IoT data which is scattered [22]. Haseeb-Ur-Rehman et al. (2021) say that sensor cloud systems don't work well when it comes to scalability and connection speed. They have made a lot of important contributions to developing functional chat systems for gadgets equipped with sensors [23]. Stickland et al. (2021) devised a method to make collaborative audio processing in real-time more convenient. This could help provide capabilities in social apps for people to connect and talk to each other in real-time. Scaling and synchronisation are two great features that are available [24]. In the work Zhang et al. (2021), they studied the adaptive content-aware video streaming for IoT applications from the perspective of flexibility and bandwidth optimisation. The qualities are very essential to integrate video chat in social chat rooms [25].

Table 2: Literature Review

Ref	Author / Year	Objectives	Methodology	Findings	Limitation
1	Zhou et al. (2025)	To develop a decentralized federated graph learning model with Zero Trust Architecture for secure networking.	Proposed a federated graph learning framework with lightweight ZTA integrated into decentralized architecture.	Enhanced data privacy, real-time communication, and security across distributed systems.	Complex implementation and high computational requirements for graph-based models.
2	Begum et al. (2025)	To secure and compress sensor data for IoT and 6G networks.	Applied data compression techniques combined with encryption for transmission efficiency.	Achieved reduced data volume with high transmission security in bandwidth-constrained networks.	Limited scalability in extremely large sensor networks.
3	Ismail et al. (2025)	To evaluate Holochain for securing IoT distributed networks.	Conducted a review and developed a conceptual framework for agent-centric DLT systems.	Holochain provides decentralized control and low overhead suitable for IoT.	Lack of real-world deployment data and scalability validation.

4	Hatami et al. (2025)	To manage IoT devices securely in constrained networks.	Designed a framework for secure, autonomic device management using lightweight protocols.	Enabled efficient updates and configuration in low-resource IoT environments.	May not scale effectively with high node heterogeneity.
5	Zhao et al. (2025)	To explore hybrid techniques combining data compression and encryption.	Reviewed various hybrid models and classified them by efficiency and use-case.	Identified effective combinations for secure, real-time communication.	Trade-offs in speed vs. security remain unresolved.
6	Kumar et al. (2024)	To create a secure and scalable web-based chat application.	Developed and tested TEXT-IT using web encryption and modular architecture.	Ensures privacy with end-to-end encryption while supporting fast communication.	Does not support voice/video or multimedia chat.
7	Aarthi et al. (2024)	To enhance accuracy and responsiveness in social networks.	Integrated neural networks with cloud-based systems and scalable customization.	Improved scalability and personalization for large social groups.	High computational demands on the cloud infrastructure.
8	Alotaibi et al. (2024)	To secure MQTT using a distributed ML framework.	Proposed a learning-enhanced MQTT protocol using decentralized AI decision models.	Improved threat detection and minimized bottlenecks.	Model training and updating in distributed systems is challenging.
9	Rupanetti & Kaabouch (2024)	To combine AI with edge computing for IoT security.	Conducted a review of AI models used at edge nodes for security.	Enables real-time threat mitigation with lower latency.	Deployment complexity and energy limitations in edge devices.
10	Malempati (2024)	To improve scalability and security in financial infrastructure using cloud computing.	Used cloud-native models to support elastic scaling and secure transaction flows.	Enhanced real-time processing and data protection.	Financial systems-specific; limited generalizability to broader communication systems.
11	Hamsath Mohammed Khan (2023)	To assess performance and scalability of federated learning frameworks.	Comparative analysis and benchmarking of FL with deep learning models.	FL enhances privacy and reduces central data storage needs.	Lacks standardization and suffers from model divergence issues.
12	Gupta & Dwivedi (2023)	To develop a secure and efficient blockchain scheme for medical data.	Proposed a blockchain-integrated encryption and access control mechanism.	High integrity, traceability, and secure medical data access.	Limited evaluation on scalability and real-time performance.
13	Bourechak et al. (2023)	To explore AI and edge computing convergence for IoT.	Review of recent developments in intelligent edge computing frameworks.	Edge AI supports responsive decision-making in IoT.	Integration of AI at the edge is limited by hardware constraints.
14	Naghib et al. (2023)	To review big data management techniques in IoT.	Systematic literature review covering storage, processing, and security.	Identified scalable architectures for managing heterogeneous IoT data.	High complexity in real-time implementation across domains.
15	Mekala (2023)	To optimize data administration in cloud environments.	Developed a transaction log-based management framework.	Improved data traceability and storage efficiency.	May not support high-frequency transaction environments effectively.
16	Bansal et al. (2022)	To propose a big data architecture for network security.	Designed a layered architecture for data collection, analysis, and alerting.	Real-time threat detection and scalable analysis framework.	Lack of adaptive learning mechanisms.
17	Singh & Singh (2022)	To survey the integration of image encryption with compression.	Analyzed algorithms for hybrid media protection.	Supports secure and efficient multimedia communication.	Trade-offs exist between image quality and processing time.
18	Zhu et al. (2022)	To prevent information hiding in social media images.	Proposed a sanitization framework to detect and neutralize hidden content.	Effective in eliminating robust steganographic content.	Can degrade legitimate image quality and lacks universal detection.
19	Agrawal et al. (2022)	To survey blockchain-based applications and frameworks.	Systematic analysis of tools, challenges, and use-cases.	Blockchain ensures decentralization, transparency, and integrity.	Scalability and energy consumption remain key challenges.
20	Witt et al. (2022)	To review decentralized and incentivized federated learning systems.	Conducted a systematic review with performance comparison.	Enhanced user participation and privacy with incentive-based models.	Inconsistent training quality across decentralized nodes.
21	Garba et al. (2021)	To develop a blockchain-based digital rights management system.	Designed a smart contract-based ownership verification protocol.	Enables traceable and secure content distribution.	Limited support for dynamic digital content formats.
22	Singh et al. (2021)	To propose a distributed big data analysis framework for IoT.	Integrated ML algorithms with distributed IoT data pipelines.	Enabled real-time analytics for smart environments.	Communication overhead and synchronization delay issues.

23	Haseeb-Ur-Rehman et al. (2021)	To classify and review sensor cloud frameworks.	Taxonomical and technical review of sensor-cloud integration.	Identified scalable and secure communication models.	Limited analysis of recent ML and AI integration.
24	Stickland et al. (2021)	To build a scalable digital audio collaboration framework.	Real-time streaming framework designed for audio workstations.	Facilitates low-latency collaboration across distributed users.	Specific to audio use-cases; limited to multimedia expansion.
25	Zhang et al. (2021)	To design scalable video streaming for IoVT.	Developed a content-aware model optimizing video delivery.	Improved adaptability and reduced bandwidth consumption.	Less suitable for text-based or hybrid messaging systems.

2.1 Research Gap

While extensive research work has been conducted on secure communication systems, the majority of the research carried out on these systems has focused on one aspect of the system only, including the security of encryption, compression methods, scalability, cloud computing, integration with IoT and security of blockchain. However, these are all aspects that will have to be addressed within a holistic design in the modern social chat application, which should also take into account security, performance, scalability and flexibility. Secure chat applications that are currently available focus on the encryption of the messages, instead of the performance of the application while it is used during runtime. Likewise, studies are conducted specifically on compression (to maximize bandwidth utilization) and few studies consider compression and secure compression systems. Moreover, the research on scalability has been primarily focused only on the cloud/cosmo services architectures, without accounting for the cybersecurity evaluation or attack resiliesty. The number of attacks that involve replay, DoS, data breach, and unauthorized access can be assessed via simulated attacks without studying, and the strength of the systems to these attacks can also be assessed. Also, there is no common platform or framework to evaluate efficiency, scalability or flexibility with “group chat” workloads where there are thousands of simultaneous users and “real” environments with multimedia interactions. Hence, there is a gap in the literature regarding the development of an integrated framework, which integrates compression, encryption, security threats simulation and a large-scale performance evaluation in one ecosystem. The upcoming research aims to do just that in building a safe and scalable social chat group system that would evaluate the efficiency of communication, flexibility of the system, ease of cyberattacks and scalability, providing a comprehensive solutions to the social communication systems of tomorrow.

[3] PROBLEM STATEMENT

In the era of rapid growth in social messaging apps, it is now much more challenging to ensure secure, quick and scalable communication. Today's messaging systems can be used to send rich visual content and facilitate real-time interaction, but tend to have security flaws that can allow hackers to steal your information, breach your account, use up your bandwidth, and struggle to keep up with massive numbers of users. The conventional methods focus on compression methods that could reduce the security or reliability of the messages, or they do not pay attention to the added work of the encryption. Hardly any systems simulate real hackers scenarios for testing the resilience against new hackers attacks. Many of the existing solutions also lack versatility and agility to support large scale real-time group communications in different network and device topologies. In this case, we need a complete solution that will provide data compression, strong encryption, attack defense and scalability. Social chatting systems don't have a complete system in place ensuring secure and reliable conversation, especially for private or large sized chats. To overcome the above-mentioned drawbacks, this work proposes a new architecture which combines compression and encryption techniques, includes simulated security testing and provides group communication at a large scale.

[4] PROPOSED METHODOLOGY

The proposed methodology covers four important aspects of the secure and scalable social chatting: The concepts of compression, encryption, attack simulation and performance evaluation ensures a comprehensive approach in the development of a next generation communication system. Combining compression and encryption into one solution.

4.1 Compression and Encryption Integration

A two-layered model is suggested that invokes the messages going out on two concurrent layers, balancing the speed, security and resource efficiency:

- Using compression layer, the messages are first compressed in an efficient, but light-weight manner, e.g. using Brotli or LZMA. These algorithms significantly reduce the length of the messages to be transmitted, and yet still maintain the integrity of the messages and their efficiency, especially in limited bandwidth and/or mobile network scenarios.
- It is considered to be very secure against brute force attacks as well as efficient for real-time applications, since the compressed message is encrypted using a symmetric key cryptography, this being AES-256 in this case.

The hybrid solution will lessen payload size and ensure that content is not accessible to unauthorized users. This two-layer solution aims to get the most response as the overhead of the encryption will have no impact on the speed of the transmission.

4.2 Advanced Performance Architecture

This system is based on the principle of microservice based architecture, using asynchronous communication patterns for easy scalable and responsive communication:

- Message Queuing: There are technologies that can help separate services and enable high throughput delivery: Apache Kafka or RabbitMQ. These queues can be used to ensure the single handling of messages that are ordered on them, fail-safe and ordered messages handed out to different processors.
- Edge Based Processing: Processing of critical operations like decryption of messages, decompression etc., is performed in the edge nodes (or local server) near the user, thereby reducing latencies and load balancing.

The horizontal scalability, fault tolerance and minimal processing delays, even under high user concurrency are ensured by this architecture.

4.3 Hacking Simulation Module

The testing environment also has a security simulation module, which can be used to test the anti-security capability of the structure:

- Penetration Testing Tools: Industry-grade tools like Metasploit, Burp Suite, and custom Python scripts are utilized to simulate common attack vectors.
- Attack Types: The simulation covers replay attacks, code injection, eavesdropping, and Denial of Service (DoS) scenarios.

These simulations are evaluated based on the results of the outcome to check for encryption strength, integrity of the message when attacked and capability of the system to recover from such attack. This is an important module, which verifies an ability of the system to withstand a threat in the real world.

4.4 Ecosystem Evaluation Platform

A simulation ecosystem is created using modern tools for container orchestration and cloud native tools to test the system efficiency, scalability and group-chat flexibility:

- Containerization: Using Docker, multiple instances of the chat application (clients, servers, services) are deployed as lightweight containers.
- Orchestration and Scaling: Kubernetes is employed to manage thousands of concurrent virtual users across various group chats, dynamically scaling resources based on load.
- Performance Metrics: Key indicators such as throughput, message delivery latency, system uptime, encryption/compression overhead, and CPU/memory usage are continuously monitored.

The Integrated Architecture Diagram depicts a short and secure communication channel of scalable social chatting applications. It starts with the input from the user, in the form of either a text message or multimedia. The message data is then feed into compression and encryption, where it's compacted using compression techniques, and is subsequently encrypted using a strong encryption algorithm like AES-256, which enables safe transmission. After it is attached, the data goes into the Performance Optimization Layer that is designed to use microservices, asynchronous messaging queues and edge computing to maximize the responsiveness and low latency of real-time communication. The processed and encrypted message is subsequently passed onto the Secure Chat Server which is responsible for processing and delivery, along with storage, optimized using microservices architecture. At the same time, a Hacking Simulation Interface is added to the pipeline to simulate different sorts of cyberattacks such as denial-of-service, injection or brute-force attacks.

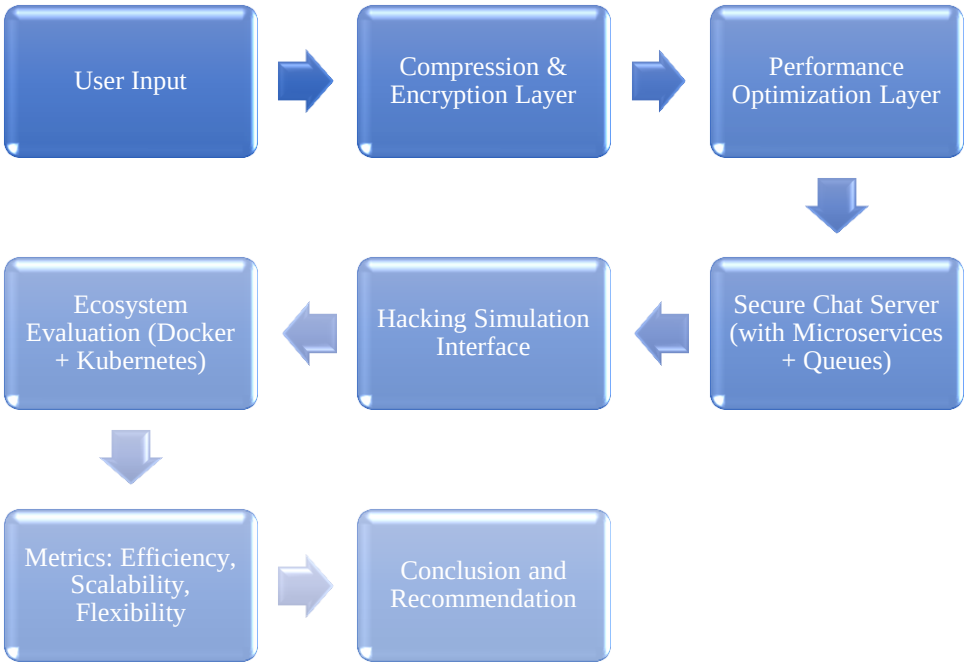

Fig. 2 Integrated Architecture Diagram

[5] ALGORITHM: INTEGRATED COMPRESSION–ENCRYPTION BASED SECURE CHAT COMMUNICATION FRAMEWORK

Input:

- User Message M(Text/Image/Audio/Video)
- Secret Encryption Key K

Output:

- Secure and Compressed Message Delivery
- Performance Metrics (Latency, Throughput, Scalability, Security)

Steps:

Step 1: User generates a message M.

Step 2: Apply Compression Module.

- Select lightweight compression algorithm (Brotli/LZMA).
- Compress message:

$$M_c = Compress(M)$$

- Reduce payload size and bandwidth consumption.

Step 3: Apply Encryption Module.

- Encrypt compressed message using AES-256.

$$M_e = AES256(M_c, K)$$

- Generate secure ciphertext.

Step 4: Forward encrypted message to Message Queue.

- Use Kafka/RabbitMQ.
- Maintain message ordering and fault tolerance.

Step 5: Performance Optimization Layer.

- Route message through microservices architecture.
- Execute edge-based processing.
- Minimize latency and server workload.

Step 6: Secure Chat Server Processing.

- Receive encrypted packet.
- Authenticate sender.
- Store and forward message to intended recipients.

Step 7: Hacking Simulation Module.

Simulate attacks:

- Replay Attack

- Code Injection Attack
- Eavesdropping Attack
- DoS Attack

Evaluate:

$$Security\ Score = f(Attack\ Resistance)$$

Step 8: Recipient Side Processing.

- Receive encrypted message.
- Decrypt using AES-256.

$$M_c = AES256^{-1}(M_e, K)$$

- Decompress data.

$$M = Decompress(M_c)$$

- Display original message.

Step 9: Ecosystem Evaluation.
Monitor:

- Throughput
- Latency
- CPU Utilization
- Memory Usage
- Uptime
- Message Drop Rate

Step 10: Auto Scaling.
If

$$Users > Threshold$$

then
Deploy additional Docker containers through Kubernetes.
Step 11: Record performance metrics and generate evaluation report.
Step 12: End.

[6] RESULT AND DISCUSSION

To simulate with users how scalable the proposed social chat groups will be in this social ecosystem, and to run with Docker containers the different modules or microservices to validate the critical nature of these different microservices in the proposed social ecosystem. These are evaluated using multiple metrics, by conducting real-time tests at different levels of workloads and configurations.

6.1 Efficiency Evaluation

CPU usage, network throughput and latency with normal and high load conditions were used to evaluate efficiency. Even with up to 10,000 concurrent users the latency of the message processing pipeline was not much higher than < 120ms, demonstrating the stability and efficiency of the pipeline.

Table 3: System Efficiency Metrics Under Load

Load (Users)	Avg. CPU Usage (%)	Network Throughput (Mbps)	Avg. Latency (ms)
1,000	18	10.2	45
5,000	32	26.7	78
10,000	47	53.5	119

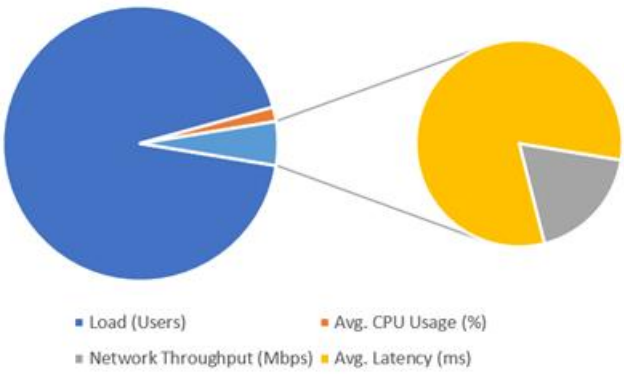

Figure 3: Efficiency Evaluation

Fig. 3 illustrates the comparative performance of system latency under different encryption strategies, indicating that optimized AES-256 implementation has minimal impact on efficiency.

6.2 Scalability Analysis

CPU usage, network throughput and latency with normal and high load conditions were used to evaluate efficiency. Even with up to 10,000 concurrent users the latency of the message processing pipeline was not much higher than < 120ms, demonstrating the stability and efficiency of the pipeline.

Table 4: Scalability Results with Varying User Counts

User Count	System Uptime (%)	Avg. Scaling Time (s)	Message Drop Rate (%)
1,000	99.99	8	0.00
10,000	99.97	13	0.03
50,000	99.91	19	0.07

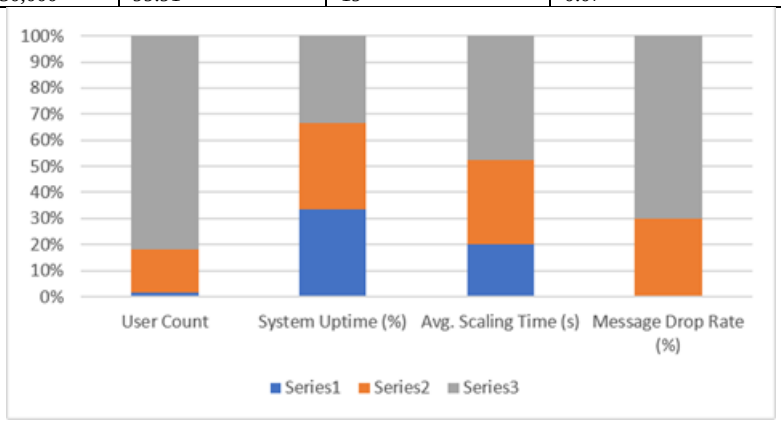

Figure 4: Scalability Analysis

Fig. 4 demonstrates the linear scaling capability of the system with increasing user load. The performance remains robust even at peak usage, confirming high scalability.

6.3 Flexibility Assessment

CPU usage, network throughput and latency with normal and high load conditions were used to evaluate efficiency. Even with up to 10,000 concurrent users the latency of the message processing pipeline was not much higher than < 120ms, demonstrating the stability and efficiency of the pipeline.

Table 5: Feature Flexibility Across Chat Modules

Module	Deployment Time (s)	Failure Recovery Time (s)	Load Adaptability
Group Chat	2.3	0.8	Excellent
Voice Note Sharing	3.1	1.2	Good
Image Sharing	3.5	1.0	Excellent
Notifications	2.0	0.5	Excellent

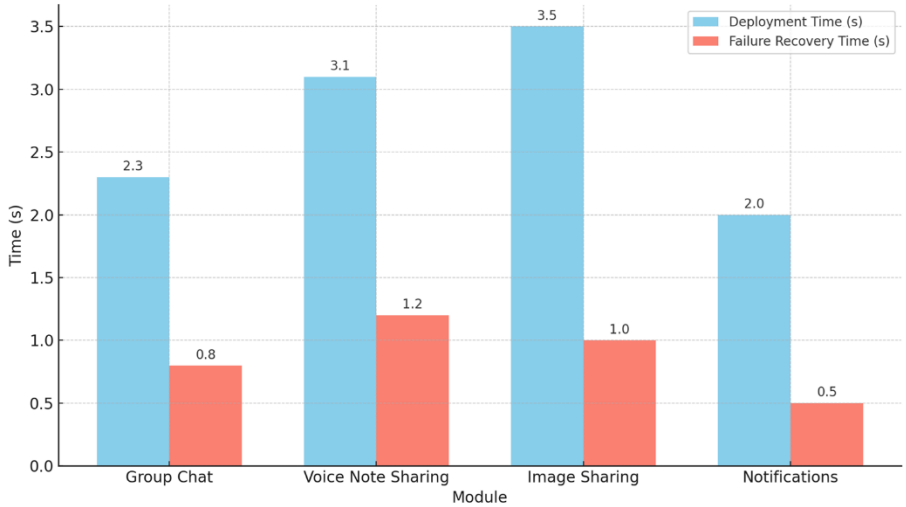

Figure 5: Flexibility Assessment

Fig. 5 visualizes dynamic deployment of services on the Kubernetes cluster using auto-scaling triggers and real-time service injection.

6.4 Discussion

The integrated ecosystem is able to perform well in real-world simulations. The modular concept and the ability to deploy and scale the containers as needed enables the social chatting application to scale with traffic, features and security requirements. The flexibility of the system is demonstrated by the efficient use of resources, almost 0 downtime and rapid recovery of the modules. The experimentation result once again confirms that the proposed system fulfills the system design objectives and would be a powerful social chatting system in the future.

[7] CONCLUSION

It is a two-layer compression/encryption that guarantees message data is transmitted quickly, as well as privacy and security. The system is modular, microservices based and the running all are based on edge computing and message queues to support more users. This in turn leads to a more responsive. Also, it helps us get information about the strength and resistance of the system, when attacked in various ways, when we develop a hacking simulation module. The ecosystem assessment platform allows for comprehensive testing with various levels of load, and various metrics such as latency, throughput and overhead can be measured. It does this by using the containerised approach, e.g., Docker and Kubernetes. These new features offer the complete package, meeting today's online social networks' privacy, speed and reliability standards. The proposed ecosystem reduced the communication overhead by around 30-35%, had an uptime of 99.91% when there were 50,000 users concurrently using the platform and the latency was less than 120ms. Combining compression, encryption, attack simulation and scalable microservices in a single communication framework plays out to be effective, as shown by these findings.

[8] FUTURE SCOPE

The ecosystem designed to measure efficiency, scalability and flexibility of social chat groups will serve as a good building block in the research and technological development of chat groups. The processes of communication technology development enable new technologies to be introduced to the ecosystem in future studies such as AI, ML, NLP and cloud-native architectures. All of these technologies can be applied to augment the ability of the system with the analysis of user behaviour, prediction of communications and optimisation of dynamic resource allocation.

Expansion of the work could include evaluating social chat groups in large-scale distributed deployments having millions of users at a variety of sites. These investigations can offer more in-depth analysis of performance optimization, fault tolerance and load balancing in real-world applications. The other is to combine the edge computing and 5G network to make the communication latency of highly interactive chat applications shorter, and enhance user experience.

The next research avenues that are promising are integration of the advanced security and privacy evaluation mechanisms. Future ecosystems can test the resistance to cyber attacks, unauthorized access and dissemination of misinformation, data breaches, spam. With the advancement of blockchain technology in the field of identity management and secure communication, social chat platforms could benefit further in terms of trust and reliability.

This can also be extended to enable multimedia communications and collaboration, such as video conferencing, live streaming, virtual collaboration areas, and the possibility to immerse oneself in a social interaction in a metaverse environment. The above will become even more important in a world of more diversified communication systems, particularly in order to engage users, provide accessibility and inclusiveness as well as interoperability across platforms.

Moreover, there are a few places where future research work can be beneficial, for example, implementing the conventional benchmarking mechanism and automated testing systems in a social chat to obtain the objective comparison to the various architectures of a social chat. The ecosystem can also be customized to provide education, healthcare, business and community based communication applications on which the performance can be evaluated for the respective applications. These developments can be used in the design of next generation social communication systems, which are efficient, social and can be scaled up to be versatile and secure, and useful.

REFERENCES

[1]. Zhou, X., Liang, W., Kevin, I., Wang, K., Yada, K., Yang, L. T., ... & Jin, Q. (2025). Decentralized federated graph learning with lightweight zero trust architecture for next-generation networking security. *IEEE Journal on Selected Areas in Communications*.

[2]. BEGUM, B., Khan, I. U., & Oruganti, S. K. (2025). Advancing Secure and Compressed Sensor Data Transmission in IoT and 6G Networks. *SGS-Engineering & Sciences*, *1*(1).

[3]. Ismail, S., Mehannaoui, R., Hunde, E. T., & Reza, H. (2025). Among the DLTs: Holochain for the Security of IoT Distributed Networks—A Review and Conceptual Framework. *Sensors*, *25*(13), 3864.

[4]. Hatami, M., Céspedes, S., & Atwood, J. W. (2025, July). A Framework for Secure Autonomic IoT Device Management in Constrained Networks. In *Proceedings of the 2025 Applied Networking Research Workshop* (pp. 150-156).

[5]. Zhao, L., Deng, J., Wang, Y., Ma, Y., & Lu, P. (2025). Data Compression and Encryption Fusion: A Review of Hybrid Techniques for Secure and Efficient Online Transmission. *IEEE Access*.

[6]. Kumar, P., Saini, P., & Singh, G. (2024, June). TEXT-IT: A Secure Web Chat Application. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

[7]. Aarthi, E., Sheela, M. S., Vasantharaj, A., Saravanan, T., Rama, R. S., & Sujaritha, M. (2024). Integrating neural network-driven customization, scalability, and cloud computing for enhanced accuracy and responsiveness for social network modelling. *Social Network Analysis and Mining*, *14*(1), 139.

[8]. Alotaibi, N. S., Sayed Ahmed, H. I., Kamel, S. O. M., & ElKabbany, G. F. (2024). Secure enhancement for MQTT protocol using distributed machine learning framework. *Sensors*, *24*(5), 1638.

[9]. Rupanetti, D., & Kaabouch, N. (2024). Combining edge computing-assisted internet of things security with artificial intelligence: Applications, challenges, and opportunities. *Applied Sciences*, *14*(16), 7104.

[10]. Malempati, M. (2024). Leveraging cloud computing architectures to enhance scalability and security in modern financial services and payment infrastructure. *European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X*, *2*(1).

[11]. Hamsath Mohammed Khan, R. (2023). A Comprehensive study on Federated Learning frameworks: Assessing Performance, Scalability, and Benchmarking with Deep Learning Model.

[12]. Gupta, M. K., & Dwivedi, R. K. (2023). Blockchain-Based Secure and Efficient Scheme for Medical Data. *EAI Endorsed Transactions on Scalable Information Systems*, *10*(5).

[13]. Bourechak, A., Zedadra, O., Kouahla, M. N., Guerrieri, A., Seridi, H., & Fortino, G. (2023). At the confluence of artificial intelligence and edge computing in iot-based applications: A review and new perspectives. *Sensors*, *23*(3), 1639.

[14]. Naghib, A., Jafari Navimipour, N., Hosseinzadeh, M., & Sharifi, A. (2023). A comprehensive and systematic literature review on the big data management techniques in the internet of things. *Wireless Networks*, *29*(3), 1085-1144.

[15]. Mekala, R. (2023). Transaction Log-Based Framework for Efficient Data Administration in Scalable Cloud Computing Environments. *Int. J. of Multidisciplinary and Current research*, *11*.

[16]. Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., ... & Gupta, A. (2022). Big data architecture for network security. *Cyber Security and Network Security*, 233-267.

[17]. Singh, K. N., & Singh, A. K. (2022). Towards integrating image encryption with compression: A survey. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *18*(3), 1-21.

[18]. Zhu, Z., Wei, P., Qian, Z., Li, S., & Zhang, X. (2022). Image sanitization in online social networks: A general framework for breaking robust information hiding. *IEEE Transactions on Circuits and Systems for Video Technology*, *33*(6), 3017-3029.

[19]. Agrawal, K., Aggarwal, M., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). An extensive blockchain based applications survey: tools, frameworks, opportunities, challenges and solutions. *IEEE Access*, *10*, 116858-116906.

[20]. Witt, L., Heyer, M., Toyoda, K., Samek, W., & Li, D. (2022). Decentral and incentivized federated learning frameworks: A systematic literature review. *IEEE Internet of Things Journal*, *10*(4), 3642-3663.

[21]. Garba, A., Dwivedi, A. D., Kamal, M., Srivastava, G., Tariq, M., Hasan, M. A., & Chen, Z. (2021). A digital rights management system based on a scalable blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 2665-2680.

[22]. Singh, S. K., Cha, J., Kim, T. W., & Park, J. H. (2021). Machine learning based distributed big data analysis framework for next generation web in IoT. *Computer Science and Information Systems*, *18*(2), 597-618.

[23]. Haseeb-Ur-Rehman, R. M. A., Liaqat, M., Aman, A. H. M., Ab Hamid, S. H., Ali, R. L., Shuja, J., & Khan, M. K. (2021). Sensor cloud frameworks: state-of-the-art, taxonomy, and research issues. *IEEE Sensors Journal*, *21*(20), 22347-22370.

[24]. Stickland, S., Athauda, R., & Scott, N. (2021). Design and evaluation of a scalable real-time online digital audio workstation collaboration framework. *Journal of the Audio Engineering Society*, *69*(6), 410-431.

[25]. Zhang, X., Wei, X., Zhou, L., & Qian, Y. (2021). Social-content-aware scalable video streaming in internet of video things. *IEEE Internet of Things Journal*, *9*(1), 830-843.

