© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722662

AI-Enhanced Privacy-Preserving Secure IP-Based Ephermeral Chat with Intelligent Threat Detection and Self-Destructing Data

ACHAL KORDE[1], SNEHAL GHOGALE[2], DIVYANSHU PANBHAK[3], SAUMYA KATEKHAYE[4], KOMAL TIWARI[5], SUSHMA TELRANDHE[6]

[1,2,3,4,] *Students, CSE Department, GNIET, Nagpur, Maharashtra, India,*

[5]*Assistant Professor, CSE Department, GNIET, Nagpur, Maharashtra, India,*

[6]*Associate Professor, CSE Department, GNIET, Nagpur, Maharashtra, India*

Abstract: ***The rising trend in the use of online communication has posed some issues regarding privacy, data retention, unauthorized access, and suspicious activities. Traditional chat programs usually store conversation details and user-related information for a long time which increases the chances of data leakage and privacy violation. This paper suggests an AI Enhanced Privacy Preserving Temporary Chat Web Application that provides secure and temporary communication with least possible data retention. This suggested system utilizes secure session and IP management for controlling temporary connections and monitoring connection activities. An AI-based privacy protection module determines the sensitive information and gives proper warning and protection. There is also a module for suspicious activity and threat detection which monitors user's behavior and finds out any suspicious activity. There is also a self-destructing data mechanism that deletes all temporary chat and session data after a certain period of time. Real time typing indicator is included for enhancing communication without permanent retention of typing activity. The main contribution of this proposed system is the incorporation of AI, privacy protection, threat detection, secure temporary sessions, self-destruction of data and real-time communication in one system.***

Index Terms- artificial intelligence, cybersecurity, privacy protection, self-destructing data, temporary chat

I. INTRODUCTION

With the growing adoption of online communications, there have been an increasing demand for secure and privacy-preserving chat systems. Conventional chat applications store messages, user information, session information, and other metadata that can expose the risks of unauthorized access, data leakage, privacy breaches, and misusage of stored data. Current solutions offer functionality such as encryption, authentication, temporary messages, security monitoring, but these functions are typically implemented separately.

In order to solve this problem, this paper offers a concept of AI-Enhanced Privacy-Preserving Temporary Chat Web Application that allows combining secure temporary communication with AI-based intelligent security methods. This system will employ secure session and IP management technologies to control temporary sessions. AI-based privacy protection technology will detect any sensitive information and will issue relevant warning and/or protection for the user. AI-based suspicious activity and threat detection technology will observe user activities and will identify any suspicious or potentially dangerous activities on user's side. Self-destructing database system will automatically delete all chat and temporary session data upon the expiration of the set period of time, reducing any unnecessary storage of data. Real-time typing indication functionality will be also implemented to enhance user communication experience without unnecessary data storage.

The main innovation of this paper lies in the combination of the above-discussed elements in one privacy-oriented system.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

The AI-Enhanced Privacy-Preserving Secure IPBased Ephemeral Chat System with Intelligent Threat Detection and Self-Destructing Data will be developed

through the course of this research. This idea was generated out of the need to design secure and privacy-preserved online chatting tools wherein users can safely send their private or sensitive information without saving any data from the chat.

In order to check the research feasibility, research articles and systems about secure messaging, temporary/ephemeral communication, privacypreserving technologies, IP-based session management, AI-based privacy protection, suspicious activity detection, cybersecurity, and self-destructing data are explored. Additionally, limitations of existing communication platforms and security measures are reviewed, especially in relation to permanent data storage, privacy breach, metadata leakage, and detection of suspicious activities.

Further, research on AI and cybersecurity will be performed in order to analyze the potential for intelligent identification of abnormal and suspicious communication patterns as well as extra security measures. Automatic data expiration mechanism will also be reviewed for better understanding of secure deletion of chat messages and associated database records.

This research requires learning of some important technical terminology, namely, ephemeral communication, privacy preserving, IP/session security, threat detection, anomaly detection, metadata security, self-destructing data, real-time communication, and AI-based security analysis. Such knowledge will allow building the system combining temporary communication with intelligent privacy and security.

From the above review of the literature, it can be stated that integration of AI-based privacy protection, suspicious activity detection, secure IP/session handling, self-destructing data, and real-time communication into one temporary chat platform offers a valuable ground for research.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

Now it is the time to articulate the research work with ideas gathered in above steps by adopting any of below suitable approaches:

A. Bits and Pieces together

In this approach, information will be gathered from research papers related to secure IP and session management, temporary/ephemeral communication, AI-based privacy protection, suspicious activity/threat detection, self-destructing chat and database data, privacy and metadata security, and real-time communication and typing indicators. These findings are integrated in order to analyze the limitations of current solutions and create a new system design.

Studies included:

1. Secure IP and session management
2. Temporary/ephemeral communication
3. AI-based privacy protection
4. Suspicious activity and threat detection
5. Self-destructing chat and database data
6. Privacy and metadata security
7. Real-time communication and typing indicators

Jump Start

Project guides, researchers, and peers can provide useful guidance and feedback on how to further improve the system architecture, security mechanisms, AI-based threat detection methods, and research methodology altogether.

B.Use of Simulation software

Using the proposed web application, experimental testing with different scenarios, including suspicious activity, unauthorized access attempts, expiration of sessions, automatic data deletion, and real-time messaging, will provide interesting results for analysis in the research paper.

IV. GET PEER REVIEWED

Once the research paper is completed it, must be critically reviewed by the project guides, faculty members, cyber security and AI experts and other researchers. The main goal of conducting a peer review is to ascertain that the research is technically sound,

relevant, novel, and well-presented. The reviewers can make certain suggestions which might not come out of the researches themselves.

In the review process, the reviewers should study the literature survey, problem statement, methodology, architecture, privacy protection using AI, secure IP and session management, suspicious activity and threat detection, self-destructing database, and realtime communication system. In addition, they should analyze the testing methodology and results so that the reviewer is able to ascertain the extent to which the proposed system will improve privacy and security compared to other systems.

In particular, the reviewers need to focus on the risk of privacy issues, unauthorized access, IP and metadata protection, false detection of suspicious activities and proper deletion of temporary chat data. The reviewers can also recommend some changes in AI model, security approach, performance evaluation and design of the whole system.

All the comments and suggestions obtained during the review process need to be studied thoroughly. Thereafter, necessary changes need to be made in the research paper and system. This will be followed by a second round of review to ensure that all the problems highlighted in the first review are addressed. Lastly, the revised paper needs to be reviewed once again for its technical accuracy, proper referencing and experimental results.

V. IMPROVEMENT AS PER REVIEWER COMMENTS

Once the reviewer commentary has been received, all of them must be thoroughly analyzed and comprehended before implementing changes in the research paper. The comments associated with the proposed system, the methodology, AI-based privacy protection, threat detection, secure IP/session management, self-destructing data, and experimental results must be addressed properly.

Necessary changes should be done where there are any technical errors identified, missing information, poor explanation, security issues, or lack of proper experimental evaluation. Wherever a comment is not clearly stated, the necessary clarification should be obtained from the reviewer or the subject matter expert before making any changes.

The improvements in the proposed project can be done in terms of improving the AI-based suspicious activity detection, IP and metadata privacy, selfdestructing database, testing scenarios, performance, and security evaluation. Comments must be taken as an opportunity to improve the quality and reliability of research instead of failure.

After making all necessary modifications, the research paper should once again be reviewed for accuracy, consistency, originality, references, methodology, and presentation. The improved research paper should finally be submitted to the journal/conference for further review.

VI. CONCLUSION

The proposed AI Enhanced Privacy Preserving Temporary Chat Web Application has several features which make the application a safe and temporary mode of communication. These include secure IP and session management, AI based privacy protection, suspicious activity and threat detection, self-destructing data and real time communication.

The main benefit of the system is the ability to remove the chat and temporary session data after certain period. In addition, the use of AI based techniques increases the level of privacy protection and allows detecting the suspicious activities. The system is designed in order to provide a user-friendly environment with real-time communication using instant messages and typing indicators.

Nevertheless, there can be some limitations of the system such as the accuracy of AI based detection, correct functioning of the network connection and false warning when detecting the suspicious activity. Further development of the system can consist of increasing the accuracy of AI based detection and improvement of privacy protection and threat analysis techniques.

It is possible to consider the application as a good tool for temporary and privacy related communication,

sharing of confidential data, short term collaborative discussion, etc.

ACKNOWLEDGMENT

We gratefully acknowledge the help rendered by our project guide and professors for their valuable advice and support provided to us during the course of this project. We are also thankful to our college for all the resources provided to us. Finally, we sincerely thank all those who have helped us in the design of our proposed system.

REFERENCES

[1] V. Vaishnav, “Secure Chat Application with Privacy and Anonymity,” Center for Development of Telematics, New Delhi, Dec. 2024.

[2] N. Zala, J. Fiaidhi, and V. Agrawal, “ChatterBox – A Real Time Chat Application,” TechRxiv, 2022, doi: 10.36227/techrxiv.21699692.v1.

[3] K. Mohit, P. Akash, G. Kaushik, Y. Pavan, and Dr. P. Pulicherla, “Secure Chat Application,” International Journal of Creative Research Thoughts (IJCRT), vol. 12, no. 11, 2024.

[4] Dr. S. Sathya et al., “Real-Time Chat Application with Web Socket for Network Efficiency,” International Journal of Scientific Research in Science and Technology (IJSRST), vol. 12, no. 4, pp. 830–835, July–Aug. 2025.

[5] R. Gayathri and C. Kalieswari, "Real Time Chat Application," International Journal of Engineering and Advanced Technology (IJEAT), 2020.

[6] A. Bhat and S. Shinde, "Network-Aware Chat Systems for Enterprises," 2023.

[7] K. Kim and J. Park, "Latency Optimization Techniques in Web-Based Chat Applications," 2023