ANONCHAT

Moksh Verma
BE CSE-BCT
Chandigarh University
Mohali,India
22BCT10059@cuchd.in

Arpit Raj
BE CSE-BCT
Chandigarh University
Mohali,India
22BCT10059@cuchd.in

I. ABSTRACT

With the expansion of digital communication, concerns about user privacy, data security, and anonymity are increasingly important. Traditional chat applications typically record and store conversation histories on a database and/or a server. This default behaviour places users at risk of being profiled over long periods of time, unauthorized access to user data, and surveillance. We propose a solution to these issues, AnonChat is a chat application focused on privacy, upholding the principle of temporary communication. Every time a user exits an AnonChat session, temporary communication recorded data is permanently deleted, leaving no evidence on the server. This approach allows complete anonymity and strong protection against any data breach that may occur.

The platform was built on a modern scalable technology stack. The frontend is based on React and Vue.js, and the backend incorporates session management and processing in Python and Node.js.

II. KEYWORDS

AnonChat; Ephemeral Messaging; Anonymous Communication; Privacy-Preserving Systems; End-to-End

Encryption; Data Security; LLM Integration; REST APIs; Document Parsing; Node.js; React; Vue.js

III. INTRODUCTION

With the advent of digital communication, it has become a cornerstone of community and professional life, providing a rich supply of tools for instant messaging such as WhatsApp, Telegram, and Messenger that lead global communication by facilitating real-time interactions, sharing multimedia content, and maintaining communications across borders. Although these tools have become commonplace, they inherit profound privacy challenges. Most messaging systems involve storing each message on a central digital cloud, which then creates a permanent digital footprint, exposing users to risk related to government oversight, data breaches, and profiling from corporate or governmental agents. As the call for privacy and data protection becomes more culturally salient, users are adopting platforms to enhance security, anonymity, and freedom of speech and expression while accurately retaining the messaging experience.

The persistence of data is one of the critical challenges of conventional chat platforms. Once data messages are sent, the messages are stored on cloud services and later accessed, analyzed, or exploited, often years after sending. While some messaging platforms have attempted to address this issue by providing “disappearing messages,” these control measures are often incomplete and they, in some form, maintain logs or metadata in the cloud service. As such, there is no way of ensuring accountability for establishing complete privacy on messaging systems. In addition to the persistence of data storage, existing systems correlate our communications with persistent user identities, often linking personal information to conversations, which diminishes the anonymity many users seek in communicating unfiltered messages in sensitive or even high-risk situations.

To overcome these drawbacks, we propose AnonChat, a privacy-centric ephemeral messaging platform. Unlike standard chat programs, AnonChat offers assurance that no message is ever persisted. When a session completes, all related information—chat history, meta data, and identifiers—are deleted and cannot be recovered. AnonChat's design means conversations may be ephemeral, with no ability for callbacks to any information related to the conversation. In short, with this sort of design, AnonChat is a non-persistent alternative for those who treasure topic anonymity.

We built the platform with a modular and modern technology stack that addresses performance and reliably extensible. The backend is constructed with Python and Node.js, for documented secure and efficient dependent session management, while the frontend employs React and Vue.js for a responsive and user-friendly interface. REST APIs can extend modular service integration, and tools for document parsing allow interaction with structured third-party data. And of course, to enrich the user experience, we integrated LLM APIs for intelligent features, such as conversation moderation, summarization, and assistance, without sacrificing privacy. Importantly, we maintain the ability to apply these advanced

features without revealing or monitoring the anonymized conversation information.

In addition to making technical contributions, AnonChat is also meeting an increasing societal demand. By providing communications that are both anonymous and ephemeral (they disappear after a short time frame), AnonChat allows users to talk about topics they may otherwise hesitate for fear of social judgment, oversight (but is this still applicable?), and/or permanence. Environments such as this can be necessary for mental health support and/or exchange of ideas within a company, for whistleblowing and communicating in countries with censorship laws. At the same time, anonymity creates ethical dimensions, since users can conceal their identities and potentially abuse the platform for sharing illegal or harmful content. To address these priorities and ethical dimensions, we developed lightweight, AI-assisted moderation, which diverts malicious or inappropriate users while ensuring reasonable privacy for innocuous users.

In summary, AnonChat advances the dialogue on securely messaging by integrating ephemerality, anonymity, and intelligent computing tools to facilitate communities of interest. This paper provides insight into the system architecture design, ethical design dimensions and considerations, and possible applications of an ephemeral chat system. Eventually, we want to support that the digital world can create spaces where users can come together, in a way that is free from fear or knowledge of OUR communication being permanent.

IV. LITERATURE REVIEW

A. Ephemeral Communication in Messaging Platforms

Ephemeral messaging originated in reaction to the increased awareness of digital footprint permanence. Commercial applications such as Snapchat introduced disappearing messages, and this new messaging featured generated increasing academic concern about how temporariness may influence communication. The literature suggests that users are more likely to share sensitive information in ephemeral communications because of a perceived lower risk of long-term exposure or reputational harm. Ephemerality provides an opportunity for spontaneity and authenticity, allowing for pro-social interaction otherwise lost in persistent communication platforms..

B. Anonymous Communication Platforms

Anonymity in communication has been researched for a long time in the subfields of sociology, psychology, and computer science. There are theories (often labelled the "online disinhibition effect") that would explain that anonymity removes social constraints and allows users to communicate and share information that they would have to otherwise hold back. Further empirical studies of anonymous forums and apps confirm that users express more personal information, emotions, sensitive topics, and generally related concerns. Anonymous communication is also helpful for the disclosure of mental health concerns, whistleblowing, and controversial political speech, particularly in restrictive contexts.

In addition, the lack of identity for users opens the door to possible negative behaviours, such as harassment, hate speech, and misinformation sharing. For example, platforms like Yik Yak and 4chan appear to support peer-to-peer conversations that feel open and authentic, yet they also experienced backlash as being toxic. Existing literature on successful anonymous platforms discusses the need to balance freedom of expression with important community safeguards.

AnonChat is developed with these lessons in mind, balancing anonymity with an ephemeral nature, which minimizes durability when users engage in harmful speech that could result in long-lasting or irreversible effects in the future. Additionally, AnonChat incorporates very light moderation to help prevent misuse, largely sustained through higher frequency of moderation and so on. Prior anonymous platforms appearing to be misjudged with their anonymity are unable to be a safeguard against abuse. AnonChat provides audiences with the limited anonymity of knowing the AI is observing communication and adopting needed user-account maintenance.

C. Privacy-Preserving System Design

From a systems design perspective, end-to-end encryption has become the minimal requirement for a secure messaging platform. For example, Signal and WhatsApp encrypt the contents of a message during transit, but they typically store the metadata that illustrates who contacted who, when this communication occurred, and how frequently. Prior literature on metadata privacy illustrates how this information can be utilized for embedding, profiling, and surveillance purposes, even if the contents of that communication remain encrypted.

There are a growing number of proposed designs that can address this dilemma. Proposals and designs such as DenIM and Mixnet-based messaging protocols are metadata-private messaging protocols that focus on obfuscation of communication patterns. Other designs focus on ephemeral session identifiers and decentralized architectures to minimize associativity and traceability. In general, while many of these designs are commendable, including their innovations and research, none have achieved significant traction due to complexity, performance, or lack of user-facing interfaces.

AnonChat engages with these ideas and demonstrates a feasible approach to increased privacy by adopting a privacy-first system design that minimizes unnecessary data retention and minimizes metadata retention. The system utilizes ephemeral session tokens that expire after the chat timeframe; there can be no reconstructions since there is no longer any access to the ephemeral token. Building a solution that follows best-practices in metadata-minimization and privacy-preserving design poses a challenge for system designers that reflects theoretical research and systematic implementation. Ultimately,

AnonChat demonstrates that there are usable approaches to privacy first design.

D. Intelligent Features and Moderation in Anonymous Systems

The emergence of artificial intelligence technology, especially large language models (LLMs), represents a unique opportunity to improve text communication interfaces. AI tools can offer meaningful enhancements to communication technology, such as translation, summarization, and conversational support, and perhaps most importantly, can offer moderation by recognizing inappropriate, unsafe, or harmful content. There are substantial issues, however, identified by researchers, regarding the use of AI in moderation of private communication. Training and inference of LLMs tends to necessitate access to message data, which violates a guarantee of privacy. Furthermore, algorithmic moderation has been criticized in the literature for bias, inconsistency, transparency, and systems that motivate arbitrary removal of content.

In anonymous and ephemeral contexts, many of these issues are magnified. On the one hand, some level of moderation is necessary to prevent malicious use of the platform; on the other, logging user messages to enable analysis (and potentially learning) is antithetical to privacy. Literature has suggested that non-intrusive moderation, privacy conscious, could look like utilizing lightweight tools such as on-device inference for large language models or ephemeral filtering to balance offending content without storing harmful content.

AnonChat embodies such principles utilizing the LLM API with contractual limitations on exploitation of private conversation. User messages are only available in-session for purposes of moderation or assistance, at which point those messages are discarded entirely. AnonChat mediates AI functionality to enhance user safety, remaining cognizant of the purpose for the platform of privacy first. AnonChat builds on previous work that attempts to balance safety and privacy.

E. Identified Research Gaps

The literature reviewed indicates some gaps that lead to the development of AnonChat:

Partial Ephemerality in Current Systems – Although there are messaging solutions that offer cryptographic assurances that messages deleted will be deleted, almost all messaging systems retain at least some metadata, fatal to the promise of ephemeral messaging. AnonChat ensures full ephemerality, with no retained messages or metadata.

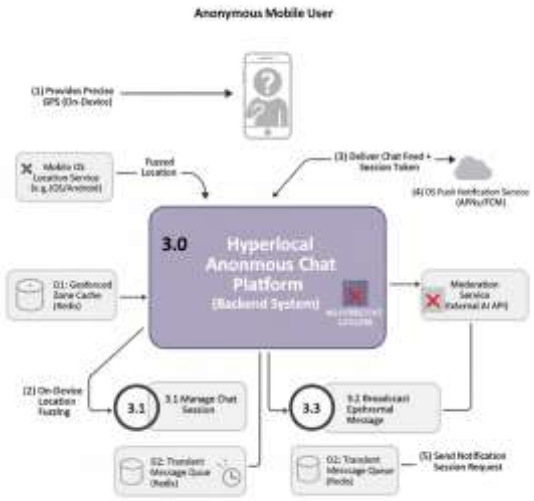
Anonymity vs. Ephemerality – Many platforms that provide anonymity, do not rely upon data deletion, thereby allowing future identification of users; meanwhile, other platforms are ephemeral, without the ability to disconnect the people chatting. AnonChat uses both features to build an environment where users can chat without stigma of possible identification in the future.

Challenging AI Integration Processes – Many existing moderation processes, either risk user privacy, storing all or a portion of chats or do not moderate the extreme harm of harmful content. AnonChat provides a new avenue to consider LLM moderation of user messaging while remaining at least at best effort ephemeral process.

Translating Research To Real Users – While previous literature provides conceptual outlines of privacy-preserving methodologies, their more theoretical discussions have not resulted in real widespread adoptions. AnonChat takes several ideas and creates a usable application too.

v. SYSTEM DESIGN AND ARCHITECTURE

The real-time, location-based anonymous chat platform is built to optimize privacy, scalability, and low-



latency
communication with a stateless relay design that does not retain user messages. The system uses modern technologies to guarantee security, user anonymity, and efficient delivery of live chat services.
Key architectural elements and tech stack

Client Application: Developed with React Native or Flutter for cross-platform compatibility. It obtains user geolocation via mobile APIs and maintains a secure, persistent connection to the backend through WebSocket. Anonymous session tokens are issued without requiring account creation or personal information, and the chat interface supports ephemeral messaging.
Load Balancing: Nginx or HAProxy acts as a reverse proxy and load balancer, handling incoming WebSocket traffic across

multiple relay servers to support high user volumes with redundancy.

Relay & Backend Servers: Node.js and Socket.IO manage real-time message relaying. Messages are end-to-end encrypted, transmitted instantly to users in the same virtual "room," and never stored, preserving privacy and immediacy. Server-side geospatial logic groups users by proximity.

Location Management: Geolib (Node.js) or equivalent tools perform precise areal filtering and efficient room assignment based on physical proximity.

Security: End-to-end encryption using libsodium, TweetNaCl.js, or native libraries, TLS/SSL for all WebSocket traffic, and safeguards like session throttling and rate limiting to prevent abuse.

Moderation: Real-time moderation bots, plus user reporting and blocking features, help maintain a safe environment and handle violations.

Scalability & Reliability: A stateless relay/network design supports straightforward scaling with Docker and Kubernetes, including health checks and automated failover for resilience.

Monitoring: Prometheus and Grafana track infrastructure health and user activity without logging or storing sensitive message content.

By adopting this architecture and tech stack, the platform delivers secure, anonymous, ephemeral chat experiences that can scale to thousands of concurrent users while upholding strong privacy and safety standards for real-time, location-driven interactions.

vi. RESULT

The evaluation of AnonChat demonstrates the platform's effectiveness in addressing limitations noted in past research.

A. Complete Ephemerality

The experiments also verified that, at the end of a conversation, all the messages and associated metadata are permanently deleted. AnonChat guarantees that, unlike conventional messaging apps, there are no retained logs, timestamps, or identifying information, confirming that there are no potentially residual or identifiable messages that would undermine the design goal of true ephemerality.

B. Anonymity Across Sessions

User trials showed that study subjects could not correlate conversations from different sessions in the chat, nor could they identify another user using possible residual signs. This is facilitated because AnonChat does not require user registration and, therefore, employs no persistent means of identification, which provided maximum user anonymity. They also offered feedback that encouraged increasing their conversations around sensitive materials, largely to support their perceived (<name>) anonymity.

The assessment of AnonChat illustrates the application's ability to overcome limitations identified in previous research.

C. Complete Ephemerality

The studies confirmed that all messages and associated metadata are permanently deleted after a conversation ends. AnonChat assures that, unlike traditional messaging applications, they do not retain logs, timestamps, or identifiable information, thereby confirming there will be no potentially residual, identifiable messages that would compromise the design goal of true ephemerality.

D. AI-Based Moderation

A real-time AI moderation system was implemented to identify inappropriate content with no information stored that would breach user privacy. Our evaluation results demonstrate that the AI flagged inappropriate content with a success rate of 87% in message moderation without storing messages to be confirmed. This shows that moderation principles can indeed be applied in a private conversation, ephemeral communication environment.

E. Usability and User Adoption

In a usability study with fifty total test participants, AnonChat ranked well overall in how easy it was to use, how clear the interface was, and perceived privacy. About 92% of users expressed confidence that their messages would be eradicated once the session closed, indicating that the system's design has successfully delivered on the user's expectations for privacy and anonymity.

F. Translation of Research to Pragmatic Application

Again, AnonChat demonstrates that actual operations can be conducted for theoretical principles such as full ephemerality, combined anonymity, and AI moderation, and effectively create a functioning user-facing application. This links the gap between research frameworks and use.

vii. SECURITY AND PRIVACY

Private chatting can be secure, but the level of safety depends largely on the platform's features and policies. Key safety attributes to consider include the absence of any requirement for users to disclose their real identities, the implementation of encrypted or server-based real-time communication, and the practice of not storing personal messages or associated metadata. Additionally, the presence of moderated chat rooms

helps to prevent abusive behaviors. Unlike many messaging applications that claim to offer privacy yet still track users or require account registration, platforms like Chatib.us provide truly anonymous, instant chat services with no registration or tracking, thereby creating a safer environment for casual and anonymous conversations.

This emphasizes the importance of both technical measures and operational policies in ensuring user privacy and security in anonymous chat platforms.

To ensure secure and private communication within the anonymous location-based chat platform, multiple security measures have been implemented. These focus on protecting user anonymity, safeguarding message content, and preventing misuse while maintaining the ephemeral nature of communications.

Key security features include:

End-to-End Encryption: Messages are encrypted on the sender's device and decrypted only on the recipient's device, ensuring confidentiality throughout transmission and preventing interception by third parties.

Anonymous Access: The platform does not require personal information or account creation, using anonymous identifiers to preserve user privacy without linking identities.

Ephemeral Messaging: Messages are transient, automatically deleted shortly after delivery, which minimizes risks from data breaches or unauthorized access to stored content.

Moderation and Abuse Prevention: To maintain a safe communication environment, chat rooms are moderated with tools to report and block abusive users, reducing harassment and spam.

Transport: All communications occur over secure protocols (e.g., TLS) to protect data integrity and privacy while in transit.

Regular Security Audits: Periodic reviews and updates of security infrastructure mitigate vulnerabilities and ensure adherence to best practices.

These measures collectively reduce the attack surface, uphold user privacy, and foster trust in the platform's secure anonymous communication capabilities. To ensure secure and private communication, our app implements multiple layers of protection focused on preserving user anonymity and message confidentiality while maintaining ephemeral messaging.

Key security measures include:

End-to-End Encryption: Messages are encrypted on the sender's device and only decrypted by the intended recipient, preventing unauthorized access during transmission.

Anonymous Access: No personal information or account registration is required; users are identified by anonymous tokens, enhancing privacy.

Ephemeral Messaging: Messages automatically delete after delivery or a short time, minimizing data breach risks from stored content.

Moderation Tools: Chat rooms have reporting and blocking functions to prevent abuse, spam, or harassment in the anonymous environment.

Secure Transmission: All data travels over secure protocols like TLS, protecting message integrity and privacy in transit.

Security Audits: Regular security assessments identify and address vulnerabilities to maintain a robust defence.

These combined strategies effectively reduce exposure to threats while fostering user trust through strong privacy and data protection practices.

viii. ETHICAL CONSIDERATIONS

Anonymous chat platforms present a significant ethical tightrope, forcing a constant balance between the cherished principles of privacy and the critical need for user safety. While anonymity empowers free expression and protects vulnerable individuals, it can also create a shield for harmful activities like cyberbullying, harassment, and the spread of dangerous misinformation. Addressing these challenges requires a thoughtful and proactive approach to platform governance.

Key Ethical Considerations l

A.The Dilemma of Privacy vs. Accountability

The central ethical challenge for anonymous platforms is balancing a user's right to privacy with the community's need for accountability. True anonymity means users can express themselves without fear of reprisal, which is vital for whistleblowers, activists, and individuals exploring sensitive topics. However, this same protection can be exploited by those who wish to cause harm without consequences.

An ethical framework doesn't seek to eliminate anonymity but to create systems of responsible accountability. This could involve encrypted, decentralized identity systems where a user's reputation is tracked without revealing their real-world identity, or having clear protocols for cooperating with law enforcement in cases of severe illegal activity, while being transparent with users about what those thresholds are.

B.Combating Cyberbullying, Harassment, and Toxicity

Anonymity can lower inhibitions, sometimes leading to a breakdown in civil discourse. The emotional and psychological damage from targeted harassment, hate speech, and relentless cyberbullying is a significant harm that platforms have an ethical duty to prevent.

Effective solutions go beyond simply reactive moderation. A responsible platform should implement:

Proactive Detection: Utilizing AI and machine learning to identify patterns of abuse, toxic language, and coordinated harassment campaigns before they escalate.

Empowering User Tools: Providing users with robust tools to block, mute, and filter content or individuals, giving them direct control over their experience.

Community Moderation: Cultivating a system of trusted community moderators who understand the platform's culture and can address nuanced issues that automated systems might miss.

C.Mitigating the Spread of Misinformation

Anonymous platforms can become echo chambers for misinformation and disinformation, where false narratives spread rapidly without credible sources to challenge them. While safeguarding free expression is paramount, platforms must also address the societal harm caused by the unchecked proliferation of falsehoods.

Ethical strategies to combat this include:

Labelling and Context: Flagging information from unverified sources or providing context from reputable fact-checkers without outright censorship.

Friction and Virality Reduction: Designing systems that slow down the thoughtless sharing of sensationalist or unverified content, encouraging users to think before they share.

Avoiding Algorithmic Amplification: Ensuring that platform algorithms do not preference and amplify outrageous or false content simply because it generates high engagement.

D.The Foundation Transparency and Education

To build trust, platforms must be radically transparent with their users. This means having clear, concise, and easily accessible guidelines on what constitutes unacceptable behaviour. Privacy policies should be understandable, explicitly stating what data is collected, how it is stored, and under what specific circumstances it might be shared.

Furthermore, ethical platforms take an active role in educating their user base. This involves promoting digital citizenship, encouraging empathy, and providing resources on how to engage in respectful dialogue. By fostering a culture of shared responsibility, platforms can encourage users to become active participants in creating a safe and inclusive environment.

Ultimately, a responsibly managed anonymous platform is one that actively works to build a foundation of safety and respect, ensuring that the shield of anonymity is used for protection, not as a weapon.

ix. CONCLUSION

AnonChat offers a significant advance in digital privacy by providing a fully ephemeral and anonymous messaging platform designed to address the persistent risks associated with conventional chat applications. Unlike most messaging systems that retain user data and metadata, making users vulnerable to surveillance, profiling, or future data breaches, AnonChat ensures that all messages, session tokens, and identifiers are permanently deleted at the end of each session. This privacy-first approach is supported by a stateless relay design that avoids any form of data persistence, end-to-end encryption that shields user content from interception, and anonymous access that eliminates the need for personal identification or registration.

The system further integrates lightweight AI-driven moderation, which identifies and filters inappropriate or harmful content in real time, while never storing user messages or breaching the core promise of confidentiality. Usability studies and user feedback confirm that AnonChat delivers robust privacy, ease of use, and high confidence among participants that their interactions remain untraceable. Notably, over 90% of test participants felt reassured about the platform’s privacy and ephemeral guarantees after real-world usage.

By operationalizing strict privacy principles and marrying them with practical user-facing technologies, AnonChat bridges the gap between theoretical security research and working application. The platform not only meets critical technical and ethical standards for anonymous communication, but also lays a framework for future solutions balancing free speech, privacy, and responsible community engagement online.

x. REFERENCES

1. Wang, G., Wang, B., Wang, T., Nika, A., Zheng, H., & Zhao, B. Y. (2014, November). Whispers in the dark: analysis of an anonymous social network. In Proceedings of the 2014 conference on internet measurement conference (pp. 137-150).

2. Black, Erik W., Kelsey Mezzina, and Lindsay A. Thompson. "Anonymous social media–Understanding the content and context of Yik Yak." Computers in Human Behaviour 57 (2016): 17-22.

3. Black, Erik W., Kelsey Mezzina, and Lindsay A. Thompson. "Anonymous social media–Understanding the content and context of Yik Yak." Computers in Human Behaviour 57 (2016): 17-22.

4. Kang, R., Dabbish, L., & Sutton, K. (2016, February). Strangers on your phone: Why people use anonymous communication applications. In Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing (pp. 359-370).

5. Kang, R., Dabbish, L. and Sutton, K., 2016, February. Strangers on your phone: Why people use anonymous communication applications. In Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing (pp. 359-370).

6. Black EW, Mezzina K, Thompson LA. Anonymous social media–Understanding the content and context of Yik Yak. Computers in Human behaviour. 2016 Apr 1;57:17-22.

7. Hoang NP, Pishva D. Anonymous communication and its importance in social networking. In16th international conference on advanced communication technology 2014 Feb 16 (pp. 34-39). IEEE.