Google Developer Group
On Campus

TechSprint

Leveraging the power of AI

Team Details :

- **Team name: AstraTech**
- **Team leader name: Pratham Kumar**
- **Problem Statement: Open Innovation**

Google Developer Group
On Campus

Our problem:

- **Most chat applications store user messages on centralized servers, creating privacy and security risks.**
- **User identities are commonly tracked through phone numbers, emails, or persistent user accounts.**
- **Data breaches and surveillance practices threaten the confidentiality of digital communication.**
- **There is a lack of truly anonymous chat platforms with zero data persistence.**
- **Existing platforms require users to trust the server with sensitive data, creating a single point of failure.**

Our solution:

- **Client-side encryption ensures that only intended users can read message content.**
- **No signup is required — no phone number, email, or personal identity.**
- **Zero message storage — data exists only during active chat sessions and is destroyed afterward.**
- **Multiple secure chat modes designed for different communication use cases.**
- **Real-time communication enabled through encrypted WebSocket connections.**
- **With increasing data breaches and stricter privacy laws, privacy-first communication is now a necessity, not a luxury.**

Opportunity & Impact

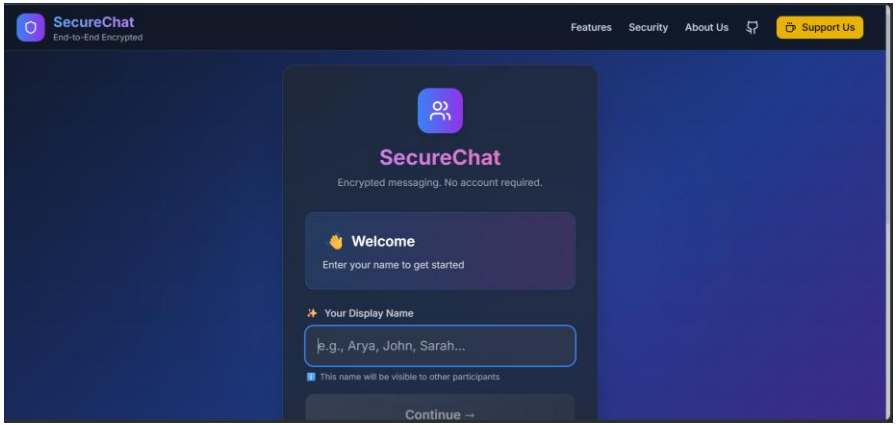
- **Enables secure communication without identity disclosure**
- **Eliminates long-term data breach risks through zero persistence**
- **Reduces dependence on centralized platforms for private messaging**
- **Suitable for privacy-critical use cases (journalism, activism, developers)**
- **Aligns with modern privacy laws and ethical technology principles**

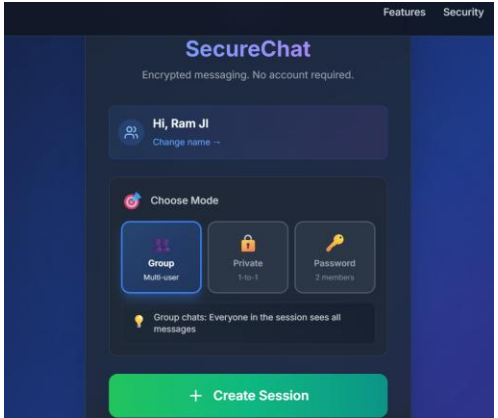
How It Works

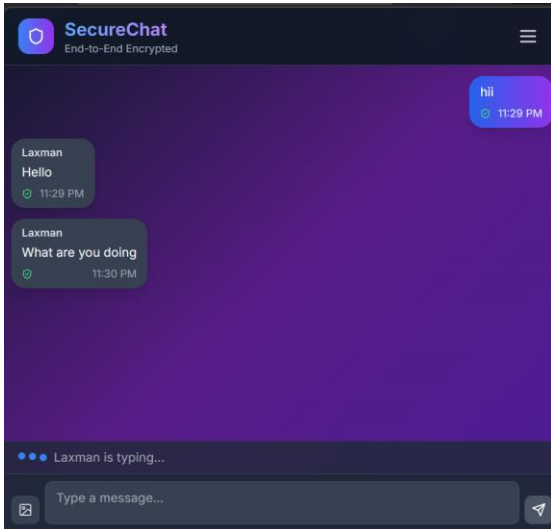
- User creates a secure chat session
- Encryption keys are generated locally in the browser
- Messages are encrypted before leaving the device
- Encrypted data is sent via WebSocket
- Only the recipient can decrypt the message
- Fully functional prototype tested with real-time encrypted sessions

Key Features

- Multiple chat modes: Group, Private, Password-Protected
- End-to-end encrypted real-time messaging
- Anonymous usage (no login, phone, or email)
- Encrypted file sharing (images, documents up to 5MB)
- Screenshot & clipboard protection
- Fully responsive modern user interface
- Built to require zero trust in the server by design





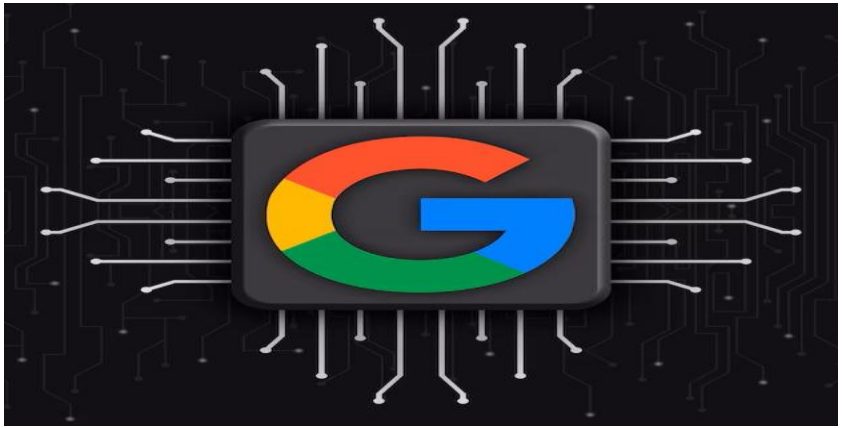


Google Developer Group
On Campus

Google Technologies Used in the Solution

Web Crypto API – Client-side encryption in the browser

HTTPS (TLS) – Secure communication channel



Planned / Experimental:
- Google Gemini AI – smart replies & moderation
- Google Cloud Translation API – demo/mock only

Firebase Realtime Database – Session metadata & user presence
(No message storage)

Architecture diagram of the proposed solution

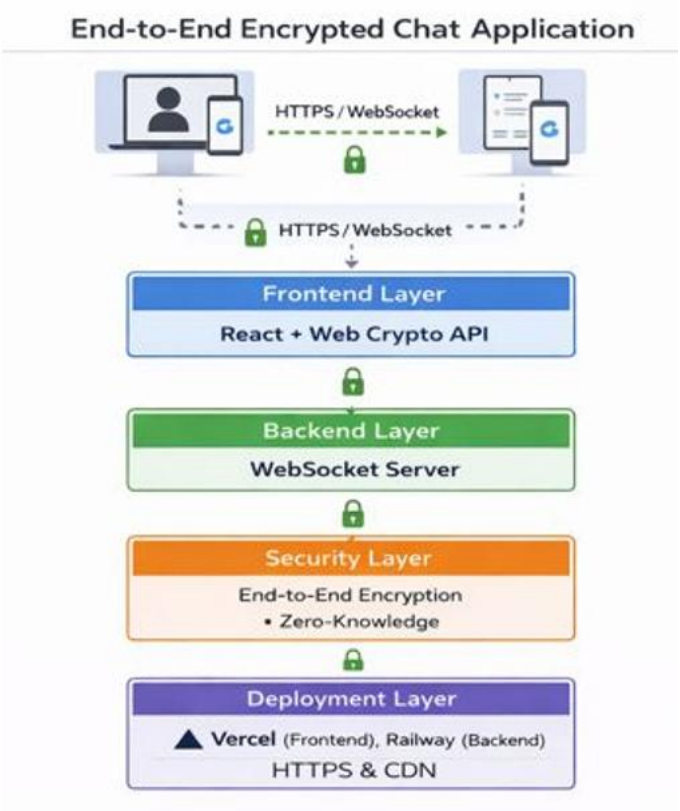
User Device (Browser / Mobile)
Session creation, UI, client-side encryption

Frontend Layer (React + Web Crypto API)
Encrypts and decrypts messages locally

Backend Layer (WebSocket Server)
Encrypted message relay, in-memory sessions only

Security Layer
End-to-End Encryption, Zero-Knowledge design

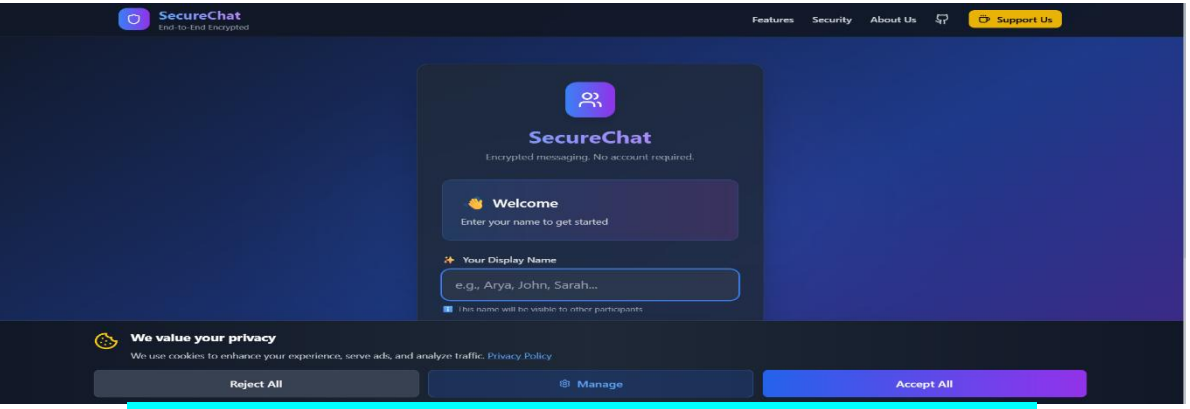
Deployment Layer
Vercel (Frontend), Railway (Backend), HTTPS & CDN



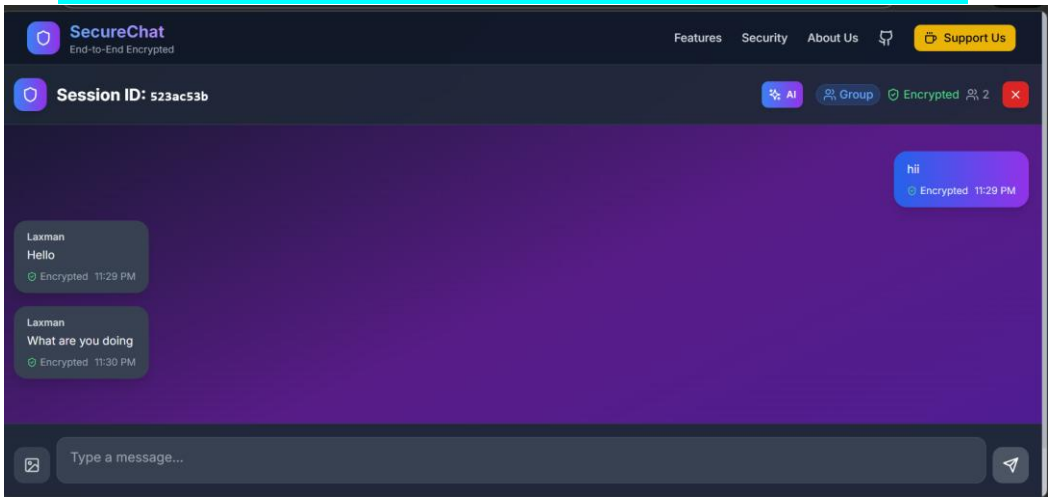
Google Developer Group
On Campus

Snapshots of the MVP

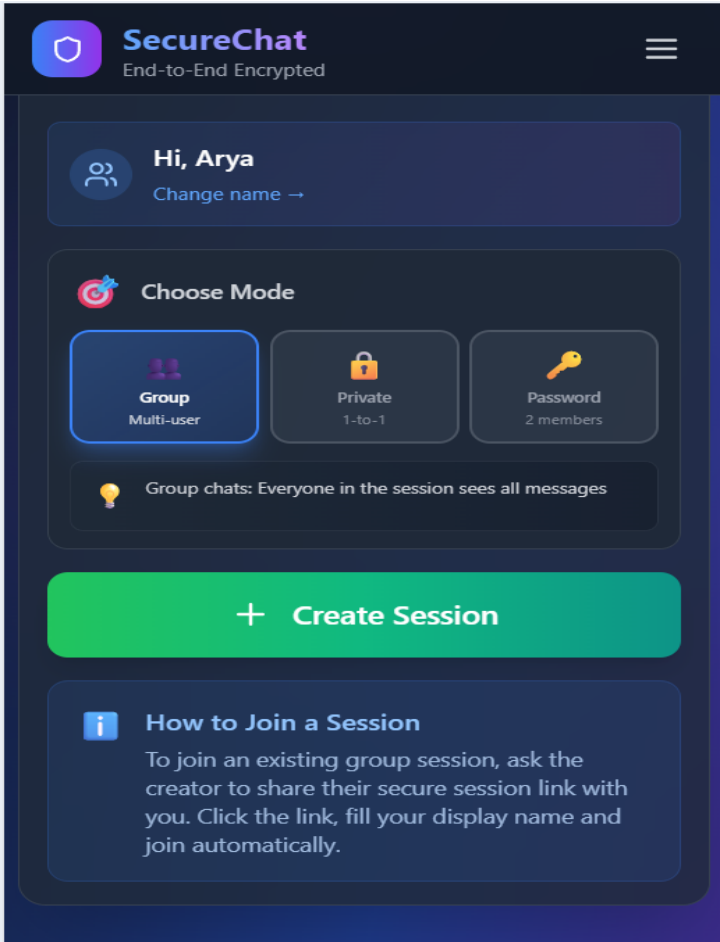
Main Window



Chat window with screenshot block feature



Chat-Box Creation Window



Why End2End Chat Is Different

- No user accounts, phone numbers, or email required
- No server-side message storage (zero persistence)
- Client-side encryption by default (server cannot read data)
- Temporary session-based chat links
- Zero-knowledge architecture by design
- Privacy-first approach from the ground up

Future Enhancements

- Full integration of Google Cloud Translation API
- Independent cryptographic security audits
- Metadata minimization and privacy hardening
- Optional self-hosted backend support
- Progressive Web App (PWA) support

Project Links:

1. GitHub Repository : https://github.com/Arya182-ui/End2end-Chat
2. Demo Video : https://www.youtube.com/watch?v=Hcb_m-iWIIU
3. MVP Link : https://chatend2end.vercel.app/

Google Developer Group
On Campus

TechSprint

Leveraging the power of AI

If you can’t read our users’ messages, neither can attackers.