Cloud under the microscope: Decoding the signals shaping smarter infrastructure p21

Automation with intent: Rewriting the rules of enterprise security p34

The future unfolds in LED displays p40

November's Best PC games you can't miss p66

₹125

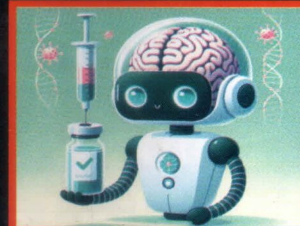
VOL. 38 | ISSUE 11 | November 2025

PCQUEST

www.pcquest.com

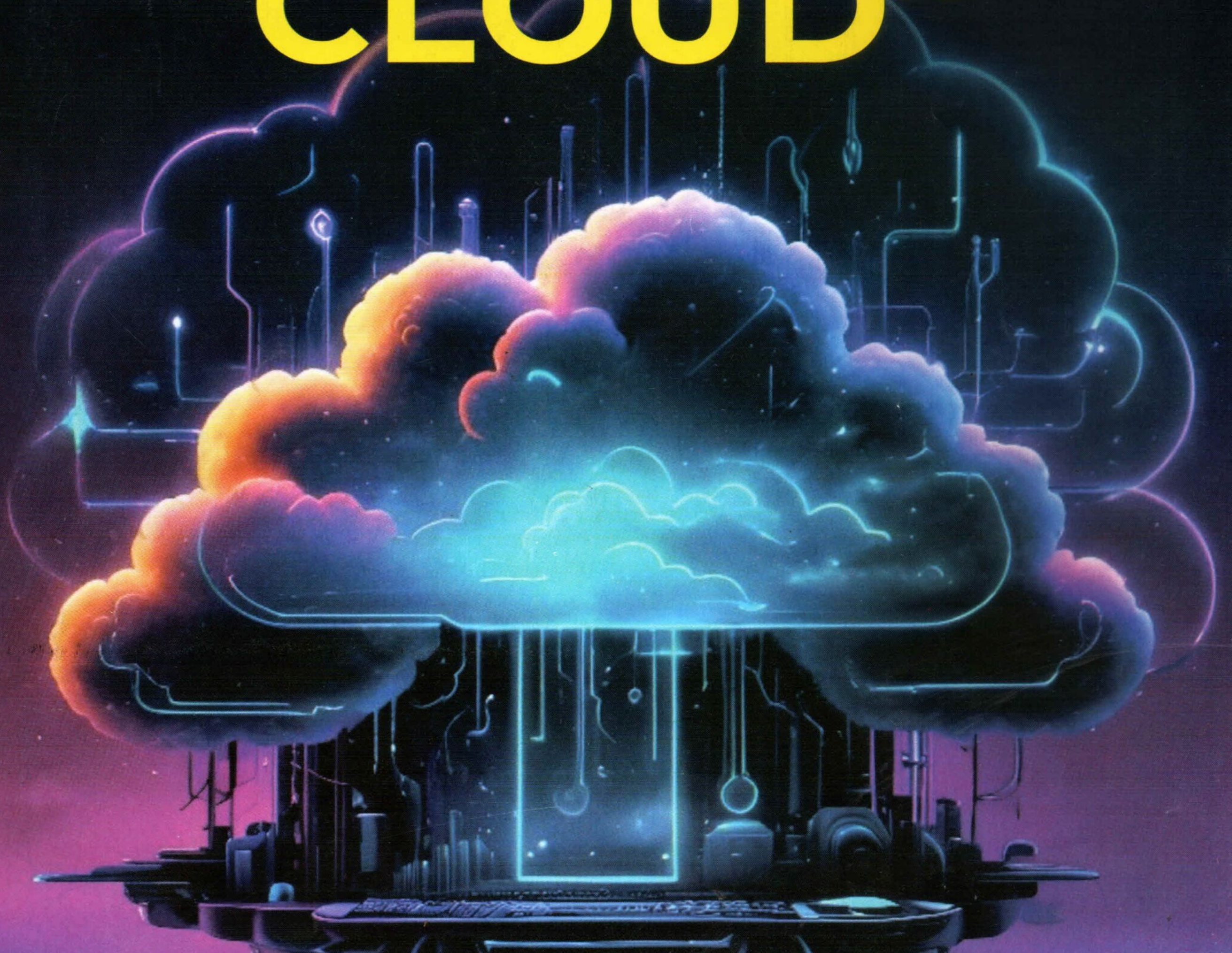
TECH TODAY & TOMORROW

CyberMedia



The AI vaccine:
How preventive care and artificial intelligence can shield India from soaring healthcare costs

Engineering the Self-Optimizing "CLOUD"



Adaptive orchestration, AI control loops, and real-time telemetry at cloud scale

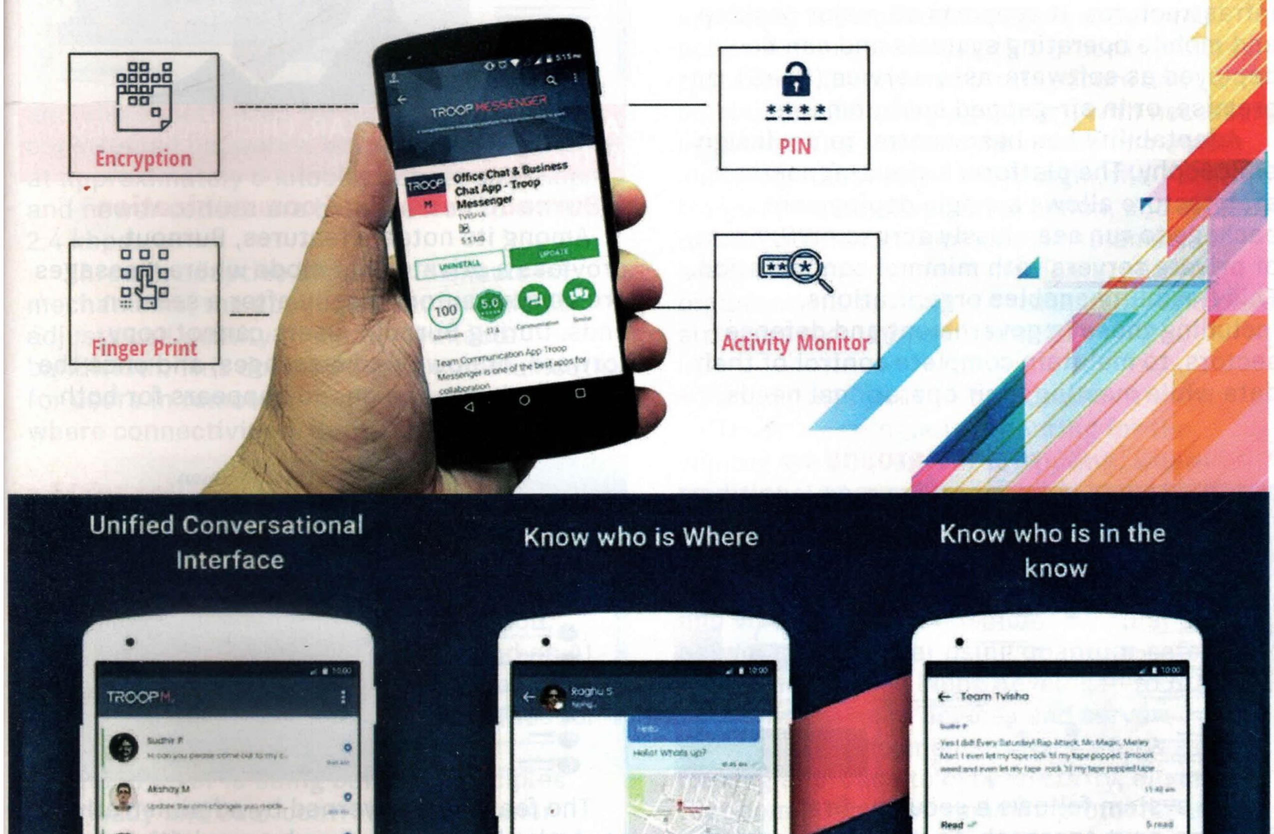
Scan QR and pay

Special Subscription offer on page 64

76 pages including cover

Inside Troop Messenger
AI, security, and the future of collaboration

Harsh Sharma
harshs@cybermedia.co.in



From secure whispers in air-gapped rooms to AI that respects your privacy, this is the story of a platform reshaping how the world collaborates—quietly powerful, obsessively private, and future-proofed for a quantum tomorrow

Privacy has become the new priority in workplace communication. While most teams rely on cloud-based tools for speed and convenience, many organizations are now seeking stronger control over how their data moves.

In a conversation with ***Akshay Mangrulkar, Chief Technology Officer, Troop Messenger***, we explored how this Indian-built workplace communication platform is focusing on the balance between usability, security, and governance.

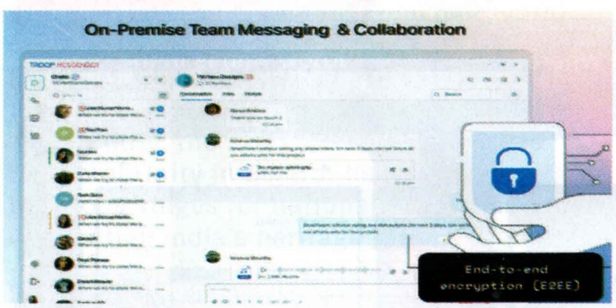
The platform supports secure collaboration across multiple environments and is now aligning its roadmap with artificial intelligence (AI) and advanced encryption technologies.

Designed for flexibility

Troop Messenger began in 2017 as an enterprise communication tool built to function across both public and private infrastructures. It supports all major desktop and mobile operating systems and can be deployed as software-as-a-service (SaaS), on-premise, or in air-gapped environments.

Adaptability has been central to its design philosophy. The platform's cloud-agnostic architecture allows a single deployment package to run seamlessly across AWS, Azure, or private servers with minimal configuration. This flexibility enables organizations, including those in government and defense sectors, to maintain complete control of their data while meeting their operational needs.

Security built from the ground up



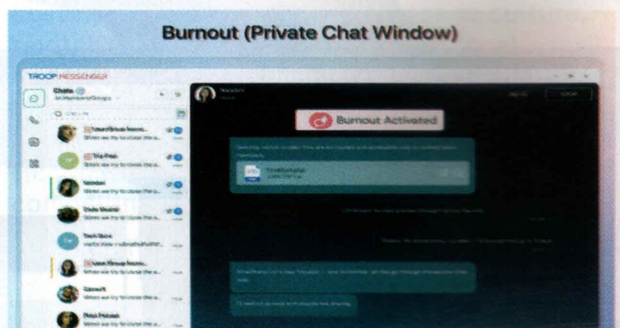
The system follows a security-first, features-next approach. Encryption operates at the device level, with every user generating a key pair when accessing the application for the first time. Only the public key is transmitted to the server, while the private key remains stored locally on the user's device. Even with multiple device logins, the QR-based key exchange process ensures that the private key is never exposed to Troop's infrastructure.

This model eliminates any possibility of backdoor access or third-party data exposure. For clients handling classified or regulated information, the platform allows customizable encryption key management to meet specific compliance requirements.

AKSHAY MANGRULKAR, Chief Technology Officer, Troop Messenger

Burnout: controlled communication

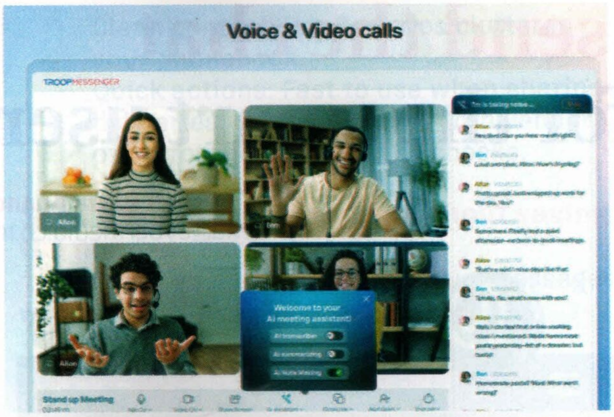
Among its notable features, Burnout provides a private chat mode where messages are deleted automatically after a session ends. During Burnout, users cannot copy, forward, or download messages, and once the session closes, the chat disappears for both participants.



The feature is governed by administrative controls that determine who can initiate Burnout sessions and whether deleted messages are retained for compliance metadata or permanently removed. It addresses the growing need for data governance by giving organizations control over the information lifecycle without undermining accountability.

Reliable communication at any bandwidth

Troop Messenger's real-time communication framework is engineered for reliability, even in low-bandwidth environments. The platform uses Socket.io for instant messaging and WebRTC for voice



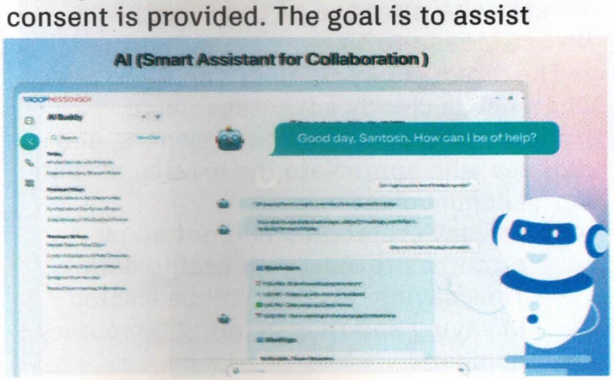
and video, optimized for performance in constrained networks. Voice calls can operate at approximately 6 kilobits per second (kbps), and newer codecs are being tested to work at 2.4 kbps.

Through adaptive bitrate and simulcast mechanisms, the application automatically adjusts call quality to match available bandwidth. This ensures stable communication for users in remote or high-security locations where connectivity is limited.

AI for collaboration, not control

The next stage of Troop Messenger's evolution centers on integrating AI into everyday workflows. Planned AI-enabled features include meeting summarization, transcription, contextual insights, and an AI Buddy that can manage schedules, generate reminders, and summarize chat histories for users joining conversations later.

The AI layer is being built on principles of privacy and user control. No customer data is used to train external models, nor is it shared with third-party servers. Any AI functions that analyze usage patterns operate locally on the user's device and only after consent is provided. The goal is to assist



users intelligently without compromising data confidentiality.

Air-gapped updates and compliance

For organizations operating within isolated or classified networks, Troop Messenger provides updates through a Self-Service Portal (SSP). Administrators can download deployment packages on a system with internet access, transfer them to the closed network, and apply the updates using an automated script. Although manual, this process ensures that isolated systems remain secure and compliant while staying current with necessary upgrades. The platform maintains immutable audit logs that record every login, file transaction, administrative action, and system event. Each record includes timestamps, IP addresses, and relevant metadata, allowing organizations to maintain traceability and meet stringent regulatory standards.

Preparing for the post-quantum era

Troop Messenger is preparing for the coming era of quantum computing, where traditional encryption methods like AES-256 may no longer be sufficient. The platform is adopting post-quantum encryption algorithms such as Kyber to strengthen both messaging and voice security. A dedicated virtual private network (VPN) layer using quantum-safe encryption is also being developed to protect all traffic between devices and servers.

These enhancements reflect a forward-looking approach to cybersecurity, ensuring that communication remains protected even against emerging computational threats.

A balanced approach to collaboration

Troop Messenger's framework represents a broader shift in enterprise communication, where collaboration and control must coexist. By embedding data sovereignty, flexible deployment, and privacy-aware AI into its core architecture, the platform demonstrates how technology can enable speed without sacrificing trust.

Security continues to serve as the foundation on which every feature is built. Everything else, including AI and automation, is designed to extend that principle into the next generation of enterprise communication. ■