indium
Make Technology Work

# App & Infrastructure Development in Technology & Cybersecurity

Digital Services

## Success Story

www.indiumsoftware.com

## Client

The client is a data security solutions company developing a highly innovative, polymorphic encryption technology designed to enable an iron-clad layer of protection to be added to existing solutions. It plans to introduce an innovative and revolutionary new type of encryption technology with five international patents and four US patents.

## Overview

This project entails developing an email-chat hybrid mobile app that enables a robustly encrypted and secure communication channel for the client's enterprise customers.

## Background

Given the end-to-end encryption, only the intended recipient of a message logged-in on the app can decrypt the message. It is not possible to decrypt the messages/emails at any stage outside the application (including by the client itself) making it totally secure. If a message is sent to an external email (to a user who is not registered in the app), the recipient would receive an email on his regular email ID notifying him that the sender has sent him an encrypted message and that he would have to register on the app to decrypt it.

Additionally, the app's UX (frontend and backend) is intelligently designed so that the communication experience mimics the formality of email but also the conversational nature of a chat. The integration between email and chat should be fluid and intuitive to enable a user to seamlessly switch between them. For example, an email being sent with reference to a chat message should be able to be sent with the specific message & chat history attached in a well-integrated.

Preferred technologies & tools: The client wanted the application to run in an Ejabberd server for secure encryption. The backend was to be developed using NodeJS and the frontend using React Native for both Android and iOS. Encryption was to be done using AES 256 algorithms.

## Solution

Indium Software successfully proposed the architecture presented in fig 1 and proceeded to deliver the project through the following high-level approach:

- The full UI, including all the latest functionalities and features in email and messaging apps, were developed using React Native (Android & iOS).
- Node JS was used for the backend development and to route a message from front end to back end.
- Json Web Token Authentication- Once a user registers he is issued a token which is stored in the database and in the devices local storage. In app opening, the tokens are automatically matched and login in automated.

## Business

App Development & Cybersecurity

## Domain

Technology, Cybersecurity

## Tools

NodeJS, Ejabberd, MySQL, React Native

## Key Highlights

- 30% reduction in deployment time
- An innovative newproduct that reenvisions peer to peer communication by combining the best features of both email and chat
- Highly secure, scalable and robust communication channel

- AES 256 encryption and decryption were coded into the app's front end. Following encryption, the front end will send the messages to the NodeJS server. The Node JS server will validate the message and send it to the Ejabberd server. The server will send the message the receiver's mobile device where it will be decrypted.
- Indium structured a robust and highly scalable architecture to address the data storage and processing needs of the client's business.
  - A MySQL database was set up and deployed on AWS. User registration, usage data and certain messages were stored in the MySQL database.
  - An Ejabberd server on AWS was also set-up, integrated and deployed for storage of all messages and hosting of all non-local components. This server, as seen in the flow diagram, served as the central distribution layer of all message transfers. Several security enhancements, integrations and proprietary technologies were also incorporated.
- Receiver verification flow was coded in NodeJS. This began with searching the MySQL database for an address match.
  - If the user already has the app, messages are connected directly to the Ejabberd server using SMTP for storage and then the message ae delivered from the server to the receiver for decryption.
  - If the user is not recognized, the encrypted message is stored in the MySQL database and a message notification and an app invite are sent to the recipient's regular email address. Following the receiver registering on the app, the message will be moved from the MySQL database to the Ejabberd server and then sent for decryption.

## Business Impact

Indium Software was able to deliver the following benefits to the client:

- **Time to deployment** was reduced by 30% due to a rapid deployment plan that increased the number of developers working concurrently offshore.
- **Major cost savings** were realised due to lower offshore rates, the use of only open source and free tools/technologies.
- **A highly scalable and robust** framework was delivered to enable rapid onboarding and expansion.
- **A highly secure** communication channel was opened through encryption.
- An exciting new communication mode- **a hybrid of email and chat**- was conceptualised in a highly intuitive & visually appealing UI and deployed.

Fig 1: System Architecture

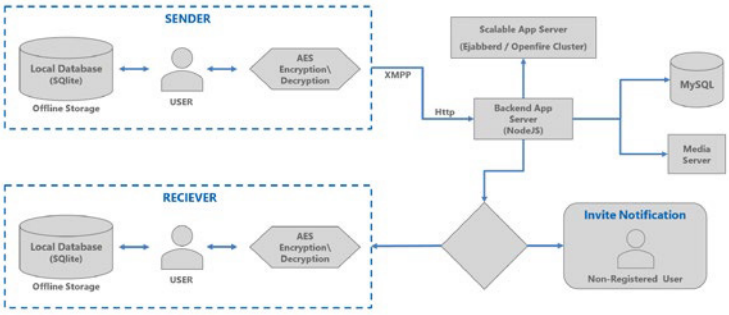
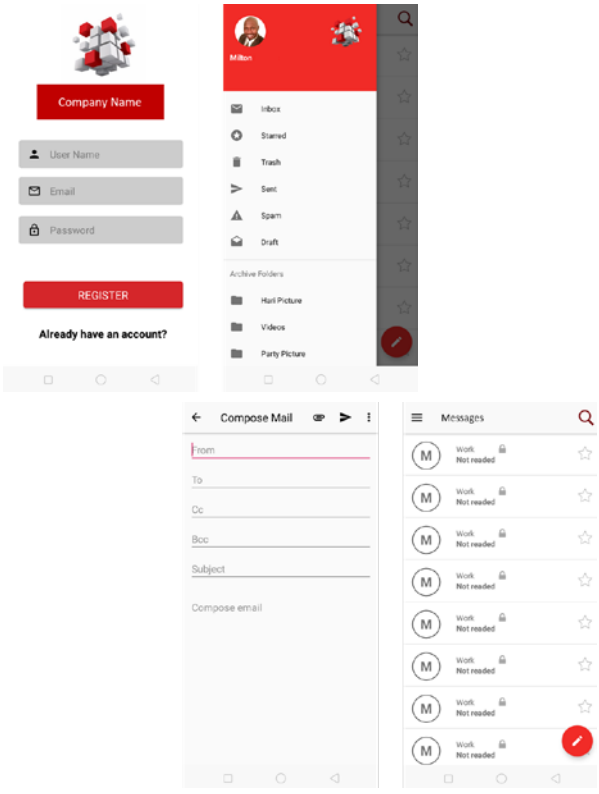



Fig 2: Sample Screens



**INDIA**

Chennai | Bengaluru | Mumbai
Toll-free: 1800-123-1191

**USA**

Cupertino | Princeton
Toll-free: 1 888 207 5969

**UK**

London

**SINGAPORE**

+65 9630 7959



General Inquiries
info@indiumsoftware.com

Sales Inquiries
sales@indiumsoftware.com