NextGen Enterprise Messaging platform for Sensitive Communications using Quantum Technology
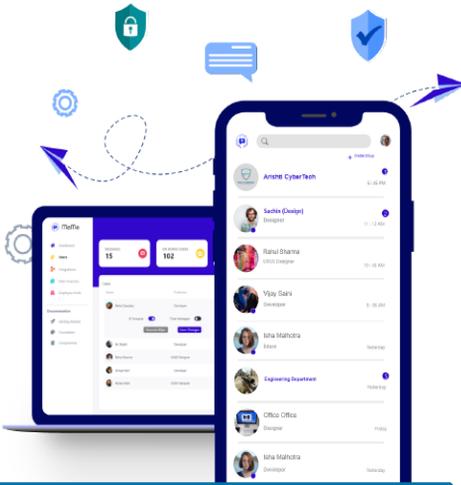
Applications

Arishti has developed a NextGen Enterprise Messaging platform (MessageMe) for sensitive communication using Quantum technology. The platform is the first of its kind which focuses on Consent based messaging focusing on the privacy of data owners. It comes with its own administration dashboard which helps control and monitor the control within the organization. The product solution being developed has a very high potential looking towards the growing cyber-crime in industries and government agencies.

- MoD: Armed Forces
- MEA: Indian Embassies
- Inter & Intra Ministry Communications
- Law Enforcement and Other Security Agencies

- Banking Sector
- Research organizations: ISRO, DRDO
- Health Care Industry
- Insurance Sector

Virtual Platform

Inventor

Mr Kanak Kawadiwale

Arishti CyberTech Private Ltd.
Gopinath Nagar, Kothrud, Pune
Maharashtra, 411038

Categories of this invention

- Computer Science and IT (Artificial Intelligence - Machine Learning)
- Communication & Networking
- Cyber Security

Intellectual Property

Title - **A system and method for information security**

Applicant - **Arishti CyberTech Private Limited**

Indian Patent Filed - **202121015792**

Key Features

- **Quantum Encryption** using Cloud based Quantum Technology
- **Consent Based Messaging** - The sensitive files cannot be reshared without the consent of the data owner.
- Ability/flexibility to **monitor** internal communications with user policy enforcements built using Data Leakage Prevention systems.
- **Message Security features** – to control the confidentiality of the data based on its sensitivity.
- The complete **Data Loss Prevention** (DLP) system makes it highly flexible and controllable to share the sensitive data over the platform.
- **Administration Panel** -- The organization executive members can control and monitor the communications using the admin dashboard.
- **Remote Wipe** -- In case of any loss of device, or employee exit from the organization, the data can be safeguarded with just one click from the admin panel.
- The architecture would be deployed on a **Zero Trust Network Architecture** which proves to be the most secure way for sensitive communication at enterprise level.

Technology

Security in encrypted communication is a top priority because of our highly connected and mobile society's increasing reliance on the internet, and its attendant remote storage and access capabilities. Also, the problem of insecure communications in the enterprises is increasing day by day, which is caused due to use of consumer grade Messaging platforms for business sensitive communications and these platforms are out of centralized control of the organization, and could not restrict the sharing of any sensitive information. The inventors have developed a software application in security & privacy centric which has multiple security features which would help individuals or the organizations to control & manage their data privacy. The platform works on the principle of Consent based messaging; in the sense that the ownership of the data remains with the creator of data. The architecture would be deployed on a zero-trust network architecture which proves to be the most secure way for sensitive communication.

Advantages

- Secure Multimedia Messaging with focus on Security and Privacy
- Administration over internal communications
- Messaging Forensics through Admin Panel
- New age messaging through major focus on users consent over the data
- Increased control over the data
- Easy Integrations within existing enterprise platforms like Zoho, Freshdesk, etc

Potential Value

1 India's Cyber Security market is forecast to grow at a CAGR of 8.05% by FY2027 owing to factors such as adoption of emerging technologies as well as government initiatives for digitalization.

2 Market is segmented into security type, solution type, deployment mode, end use industry and region.

3 Increasing demand for Big Data Analytics and Cloud Services is fueling growth in the cyber security sector to control unauthorized access to sensitive data.

Reach Us