

Welcome Sudarshana Bandyopadhyay

[Sign out](#)

Controller General of Patents, Designs & Trade Marks



सत्यमेव जयते

G.A.R.6
[See Rule 22(1)]
RECEIPT

Docket No 23202

Date/Time 2025/10/13 11:25:14

To
Sudarshana Bandyopadhyay

UserId: SB2802

Flat No. 91, Sector A, Pocket C, Vasant
Kunj, New Delhi - 110070, India

CBR Detail:

Sr. No.	App. Number	Ref. No./Application No.	Amount Paid	C.B.R. No.	Form Name	Remarks
1	202531098341	TEMP/E-1/109786/2025-KOL	4800	12629	FORM 1	ADAPTIVE MULTI-PATH MESSAGING SYSTEM WITH AI-DRIVEN ROUTING AND SELF-SOVEREIGN ENCRYPTION
2	E-12/2041/2025/KOL	202531098341	2500	12629	FORM 9	----
3	E-106/2909/2025/KOL	202531098341	0	-----	FORM28	----

TransactionID	Payment Mode	Challan Identification Number	Amount Paid	Head of A/C No
N-0001769931	Online Bank Transfer	1310250013961	7300.00	1475001020000001

Total Amount : ₹ 7300.00

Amount in Words: Rupees Seven Thousand Three Hundred Only

Received from Sudarshana Bandyopadhyay the sum of ₹ 7300.00 on account of Payment of fee for above mentioned Application/Forms.

* This is a computer generated receipt, hence no signature required.

[Print](#)[Home](#)[About Us](#)[Contact Us](#)

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202531098341 A

(19) INDIA

(22) Date of filing of Application :13/10/2025

(43) Publication Date : 17/10/2025

(54) Title of the invention : ADAPTIVE MULTI-PATH MESSAGING SYSTEM WITH AI-DRIVEN ROUTING AND SELF-SOVEREIGN ENCRYPTION

(51) International classification	:H04L0009400000, H04L0009080000, H04L0009320000, H04W0084180000, H04L0009000000	(71) Name of Applicant : 1)SRJX RESEARCH AND INNOVATION LAB LLP Address of Applicant :Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India Cuttack Orissa India
(31) Priority Document No	:NA	(72) Name of Inventor :
(32) Priority Date	:NA	1)DR DILEEP KUMAR MOHANACHANDRAN
(33) Name of priority country	:NA	2)DR SOUMYA RANJAN JENA
(86) International Application No	:	3)DR NORMALA SUBRAMANIAM GOVINDARAJO
Filing Date	:01/01/1900	
(87) International Publication No	: NA	
(61) Patent of Addition to Application Number	:NA	
Filing Date	:NA	
(62) Divisional to Application Number	:NA	
Filing Date	:NA	

(57) Abstract :

The present invention relates to a secure and intelligent communication system for privacy-preserving digital message transmission integrates artificial intelligence (AI), decentralized networking, and post-quantum cryptography. The system comprises a User Layer for initiating and receiving text, audio, video, or multimedia messages; a User Device hosting an AI Engine, Encryption Layer, and Network Interface modules for on-device processing; a Communication Layer for dynamically selecting optimal paths among Wi-Fi, Mesh, and Cloud interfaces; and a Security and Storage Layer ensuring end-to-end encryption and self-sovereign identity management. The AI Engine optimizes routing, compression, and anomaly detection, while the system supports offline mesh networking and real-time translation. Temporary session keys and data are securely erased post-delivery, ensuring privacy. The system provides reliable, adaptive communication in dynamic network environments without centralized server dependency.

No. of Pages : 23 No. of Claims : 20

<p style="text-align: center;">FORM 2</p> <p style="text-align: center;">THE PATENTS ACT, 1970</p> <p style="text-align: center;">(39 OF 1970)</p> <p style="text-align: center;">AND</p> <p style="text-align: center;">THE PATENTS RULES, 2003</p> <p style="text-align: center;">COMPLETE SPECIFICATION</p> <p style="text-align: center;">(See section 10; rule 13)</p>
<p>1. TITLE OF THE INVENTION</p> <p>ADAPTIVE MULTI-PATH MESSAGING SYSTEM WITH AI-DRIVEN ROUTING AND SELF-SOVEREIGN ENCRYPTION</p>
<p>2. APPLICANT</p> <p>(a) NAME: SRJX RESEARCH AND INNOVATION LAB LLP</p> <p>(b) NATIONALITY: India</p> <p>(c) ADDRESS: Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India</p>
<p>3. PREAMBLE TO THE DESCRIPTION</p> <p>The following specification particularly describes the invention and the manner in which it is to be performed.</p>

FIELD OF THE INVENTION

The present invention relates to the field of digital communication systems, specifically to a secure and intelligent communication framework for privacy-preserving message transmission. The invention further integrates artificial intelligence (AI), decentralized networking and post-quantum cryptographic techniques to enable adaptive, reliable, and secure communication of text, audio, video, or multimedia messages. It pertains to systems employing AI-driven routing, end-to-end encryption, self-sovereign identity management, and hybrid communication models, including Wi-Fi, mesh and cloud interfaces, for optimized performance in dynamic network environments, particularly in scenarios requiring offline connectivity and enhanced data privacy.

BACKGROUND OF THE INVENTION

Existing communication platforms such as WhatsApp, Signal, Telegram, and other similar messaging services have significantly transformed the landscape of digital communication. However, these systems continue to exhibit substantial technical, structural, and security-related limitations. Such drawbacks result in performance inefficiencies, privacy vulnerabilities, and usability constraints which the present invention specifically aims to overcome. The following paragraphs outline the key deficiencies prevalent in the prior art and illustrate the technical distinctions and advantages introduced by the present invention.

1. **Centralised Server Dependency:** Most conventional messaging systems rely heavily upon centralised servers for storage, routing, and authentication functions. This architectural dependency creates single points of failure, thereby exposing such systems to service disruptions, cyberattacks, censorship, and mass surveillance.
2. **Limited Offline Functionality:** Conventional applications such as WhatsApp require uninterrupted internet connectivity for message transmission and reception. Consequently, such systems become

inoperative in low-bandwidth or no-internet environments, restricting accessibility, particularly in rural or disaster-prone regions.

3. **Static Routing and Latency Issues:** Existing systems commonly employ fixed server-based routing paths, resulting in network congestion and latency during periods of high traffic. Moreover, these systems lack dynamic switching capabilities across available networks such as Wi-Fi, mobile data, or Bluetooth.
4. **Dependence on External Certificate Authorities:** Prior art messaging systems typically depend on third-party certificate authorities (CAs) for cryptographic key issuance and management. Such reliance introduces trust and privacy risks, as compromise or misuse of a CA can jeopardise user confidentiality.
5. **Vulnerability to Future Quantum Attacks:** Existing encryption systems primarily utilise RSA or elliptic curve cryptography, both of which are susceptible to potential decryption by quantum computing technologies.
6. **Lack of Adaptive Compression Techniques:** Conventional messaging applications utilise static compression mechanisms that fail to adapt to bandwidth variations, leading to inefficient resource usage and transmission delays for multimedia data.
7. **Limited Multilingual Support:** Existing messaging platforms rely on external translation services or APIs, thereby compromising user privacy and incurring additional latency.
8. **Privacy Concerns and Metadata Leakage:** Although end-to-end encryption protects message content, prior systems such as WhatsApp continue to collect metadata including timestamps, IP addresses, and device identifiers, which can be used for profiling user behaviour.
9. **Absence of User-Controlled Expiry and Visibility Settings:** Current messaging systems provide limited or incomplete message deletion capabilities, wherein deleted content may still remain recoverable from servers or device backups.

10. **Lack of AI-Driven Fault Recovery Mechanisms:** Existing messaging platforms do not include predictive mechanisms to detect or respond to network failures. Consequently, transmission dropouts and delivery interruptions occur frequently.
11. **Security Risks from Cloud Backups:** Traditional messaging systems store user backups on third-party cloud environments, often in unencrypted or semi-encrypted form, rendering them vulnerable to unauthorised access or data breaches.
12. **Lack of Integration with Mesh and IoT Networks:** Prior art systems are limited to internet-based communication and do not support **infrastructure-free or device-to-device networking models** such as mesh or IoT environments.
13. **Limited AI Utilisation:** Existing messaging systems focus primarily on interface design and encryption but lack intelligent self-optimisation, contextual awareness, or adaptive network management.
14. **High Power Consumption:** Conventional applications maintain continuous background synchronisation and central polling mechanisms, resulting in excessive battery drain and inefficient resource consumption.
15. **Lack of Modular and Extensible Architecture:** Most prior systems are closed, monolithic applications that do not permit third-party integration or extension without security compromises.

OBJECTS OF THE INVENTION

The primary object of the present invention is to provide a secure and intelligent communication system for privacy-preserving digital message transmission, integrating artificial intelligence (AI), decentralized networking, and post-quantum cryptography.

One other object of the invention is to enable a user-centric interface for initiating and receiving text, audio, video, or multimedia messages via a User Layer, ensuring intuitive interaction and data confidentiality.

Yet another object of the invention is to provide a decentralized User Device hosting AI-driven routing, encryption, compression, and offline caching for autonomous operation without reliance on centralized servers.

Another object of the invention is to dynamically select optimal communication paths among Wi-Fi, Mesh, and Cloud interfaces using real-time network assessments for reliable transmission in dynamic environments.

One further object of the invention is to ensure end-to-end encryption and self-sovereign identity management using post-quantum cryptographic algorithms, with local key generation and secure data erasure.

Another object of the invention is to support decentralized peer-to-peer communication through a self-organizing Mesh Network Interface for offline connectivity in internet-unavailable scenarios.

Yet another object of the invention is to optimize message transmission through AI-driven adaptive compression, real-time translation, and anomaly detection for enhanced efficiency and security.

One further object of the invention is to provide a hybrid peer-to-peer and cloud-assisted communication model for seamless, fault-tolerant message delivery across heterogeneous networks.

SUMMARY OF THE INVENTION

The present invention provides a secure and intelligent communication system designed for privacy-preserving transmission of text, audio, video, or multimedia messages across diverse network environments. The system comprises four integral components: a User Layer, a User Device, a Communication Layer, and a Security and Storage Layer. The User Layer facilitates user interaction through an intuitive graphical interface, enabling seamless composition and reception of messages. The User Device operates as a decentralized control node, hosting an AI Engine for adaptive routing, compression, and real-time translation, an Encryption Layer for secure data processing, and Network Interface modules for connectivity management. The

Communication Layer dynamically selects optimal transmission paths among Wi-Fi, Mesh, and Cloud interfaces by evaluating real-time network parameters such as latency, bandwidth, and device power status, ensuring reliable delivery even in unstable conditions. The Security and Storage Layer employs post-quantum cryptographic algorithms, including lattice-based and elliptic curve cryptography, for end-to-end encryption, with local key generation and self-sovereign identity management to prevent unauthorized access. The system supports offline communication through a self-organizing Mesh Network Interface, utilizing store-and-forward mechanisms for message relaying in internet-unavailable scenarios. The AI Engine enhances efficiency through adaptive compression, real-time multilingual translation, and anomaly detection to identify and mitigate issues like data corruption or intrusion attempts. Upon message delivery, temporary session keys, routing data, and cached parameters are securely erased, ensuring no residual data remains accessible. This invention provides a self-learning, decentralized communication ecosystem that optimizes performance, maintains stringent privacy standards, and ensures fault-tolerant, secure message transmission without reliance on centralized servers, making it suitable for dynamic and challenging network conditions.

BRIEF DESCRIPTION OF DRAWINGS

Fig 1: Detailed flow chart of the invention

Step 1: Start of Process: The operational sequence begins when a user initiates a communication event, typically by composing a text, audio, video or multimedia message within the application interface. Upon initiation, the system activates its core functional modules, including the AI Engine, Encryption Layer and Network Interface. These modules are initialised to prepare for message handling, routing, and processes.

Step 2: Reception of User Input Message: Once the message is created, the system receives the user input and validates the data format and structure. This step ensures that the message conforms to predefined encoding and transmission standards. Metadata including sender credentials, time stamps,

and message type (text, image or video) is recorded in encrypted form. The validated message is then transferred to the AI-based routing module for further processing.

Step 3: Determination of Available Networks: Next, the system performs an environmental scan to identify all accessible communication channels. These may include Wi-Fi networks, cellular data (4G/5G), Bluetooth mesh networks, or offline peer-to-peer relays. The AI Engine evaluates network performance parameters such as signal strength, available bandwidth, latency and device power status to generate a real-time communication topology. This mapping allows the system to maintain multiple potential routing paths for each message, thereby ensuring operational resilience.

Step 4: Selection of Optimal Communication Path: Based on the available connectivity data, the AI-driven decision engine selects the optimal communication route. The selection process considers dynamic factors such as transmission speed, energy efficiency, error rate, and historical route performance. Reinforcement learning algorithms continuously refine routing accuracy. As a result, each message is transmitted through the most efficient and reliable communication channel available at that moment.

Step 5: Encryption of the Message: Before transmission, the message undergoes encryption within the system's Encryption Layer. The encryption process employs post-quantum cryptographic algorithms to ensure long-term data security. Each message is assigned a unique session key generated locally on the user's device, preventing any reuse of encryption keys. Digital signatures are embedded to authenticate the sender, while integrity hashes verify that the message remains unaltered during transit. This step ensures complete confidentiality and tamper resistance.

Step 6: Transmission of Message via Selected Path: After encryption, the message is transmitted through the selected communication path. If the preferred network becomes unstable during transmission, the AI Engine automatically switches to an alternative route without interrupting the communication flow. This hybrid transmission model, combining cloud-

assisted and peer-to-peer pathways, ensures continuous delivery in adverse or low-connectivity conditions.

Step 7: Verification of Message Delivery: After transmission, the system monitors for a delivery acknowledgment from the recipient.

- If the acknowledgment is received, the system proceeds to the next step.
- If the message remains undelivered, the AI Engine activates adaptive corrective mechanisms such as dynamic re-routing, retransmission, or data recompression.
- This iterative loop continues until the message is successfully delivered or all communication paths are exhausted.

Step 8: Adaptive AI Engine Operations: In parallel with routing and verification, the AI Engine performs auxiliary optimisations:

- **Adaptive Compression:** Reduces message size based on network conditions and message type (text, image, audio, or video).
- **Real-time Translation:** Converts content across languages on-device, ensuring seamless multilingual communication.
- **Anomaly Detection:** Monitors message flow to identify irregularities such as corruption, delay, or intrusion attempts. Upon detecting anomalies or network degradation, the system autonomously triggers route switching, re-encryption, or retransmission procedures to maintain message integrity.

Step 9: Message Decryption: Upon reaching the destination device, the message is decrypted locally using the recipient's private key stored within a self-sovereign identity management system. The decryption process verifies the sender via the embedded digital signature and validates message integrity using the cryptographic hash. Encryption keys are entirely controlled by the user, no third party, including service providers, can access or manipulate the decryption process.

Step 10: Delivery to Recipient Interface: After successful decryption, the reconstructed message is rendered in the recipient's user interface displayed

as text, audio or multimedia output, as applicable. The message is securely archived in encrypted form on the local device for recordkeeping. A confirmation signal (delivery acknowledgment) is generated and sent back to the sender to confirm successful delivery.

Step 11: Termination of Process: The process concludes after confirmed message delivery. All temporary cryptographic session keys, routing data, and cached operational parameters are securely erased from volatile memory. This final step ensures that no residual data remains accessible post-session, maintaining the highest level of security and privacy.

Fig 2: The architecture and working principle of the invention

1. User Layer: At the uppermost level of the conceptual block diagram lies the User Layer, which represents the initiator and recipient of all communication processes within the system. This layer corresponds to the human end-user interacting with the application through a graphical user interface (GUI) on a mobile or smart computing device. The user inputs data as text, voice, or multimedia messages, which are processed by embedded AI modules for routing, compression, and encryption. This layer serves as the primary entry point for all communication flows, establishing a user-centric, privacy-first design that ensures intuitive interaction while maintaining data confidentiality and operational transparency.

2. User Device: The User Device, positioned below the User Layer, serves as the primary computational and communication unit. It hosts integrated modules, including the AI Engine, Encryption Layer, local storage, and Network Interface modules. The device acts as a decentralized control node, performing:

- User authentication via cryptographic credentials;
- On-device encryption and decryption;
- AI-drive adaptive routing, compression and translation; and
- Local data storage and offline message caching.

By decentralizing these processes, the User Device minimizes reliance on external servers, enhancing speed, security, and autonomy. All sensitive data remains encrypted on the device, ensuring no unencrypted data is transmitted or exposed externally, thereby guaranteeing confidentiality and user ownership.

3. Communication Layer: The Communication Layer forms the core operational framework, acting as the intelligent routing and transmission control center. It determines the optimal communication pathway based on real-time assessments of network availability, device performance, and environmental parameters. The layer coordinates multiple protocols—Wi-Fi, Mesh, and Cloud—via an AI-driven decision engine, ensuring seamless protocol interoperability, packet synchronization, and end-to-end encryption integrity.

The Communication Layer autonomously switches between network channels to prevent data loss, congestion, or failure, ensuring uninterrupted service. It also performs feedback-based routing and error correction for reliable, high-fidelity message delivery across diverse network environments.

4. Network Interfaces: Beneath the Communication Layer, the block diagram depicts three Network Interfaces—Wi-Fi, Mesh, and Cloud—forming the hybrid adaptive communication framework.

- **Wi-Fi Interface:** Enables high-speed, short-range data transmission under stable network conditions, minimizing latency and optimizing power consumption.
- **Mesh Network Interface:** Supports decentralized, peer-to-peer message relaying without centralized infrastructure. Nearby devices form a self-organizing, self-healing mesh topology, ensuring communication continuity in areas without internet, such as rural, remote, or disaster-affected regions
- **Cloud Interface:** Serves as a supplementary or fallback channel for long-range relay, encrypted synchronization, and cross-device message updates. It operates as an auxiliary node, maintaining full encryption to preserve user privacy.

These interfaces create a resilient, hybrid networking architecture that balances decentralization, redundancy, and scalability for fault-tolerant, adaptive communication in diverse network conditions

5. Data Flow and Interactions: The Data Flow follows a structured, top-down, feedback-enabled progression. Communication originates at the User Layer, proceeds through the User Device for AI-based processing, and is directed to the Communication Layer for transmission via the optimal network channel (Wi-Fi, Mesh, or Cloud). The AI Engine continuously evaluates parameters, including latency, bandwidth, and power efficiency, to select the best route.

After transmission, acknowledgment signals and delivery receipts are returned through the same pathway, forming a closed feedback loop. The AI Engine analyzes this feedback to refine routing and compression decisions, enabling the system to evolve and optimize communication performance over time.

DETAILED DESCRIPTION OF INVENTION

The present invention provides a comprehensive, intelligent communication framework integrating artificial intelligence (AI), decentralized networking, and advanced cryptographic protection within a unified architecture. It enables autonomous, adaptive, and privacy-preserving communication, ensuring high reliability in unstable or adverse network conditions. Unlike conventional messaging systems relying on centralized servers and static routing, this system operates as a self-organizing, self-sovereign ecosystem that dynamically optimizes message transmission, compression, and security in real time.

The system architecture comprises three principal layers: the User Interface Layer, the Intelligence and Routing Layer, and the Security and Storage Layer. The Client Interface Layer provides a simplified and intuitive interface for seamless exchange of text, voice, and multimedia data. It supports accessibility features such as real-time translation, adaptive voice

recognition, and context-aware interface modification based on user preferences. The Intelligence and Routing Layer employs advanced AI algorithms to assess network conditions and automatically select the optimal communication path. It supports multi-path adaptive routing, allowing dynamic switching between Wi-Fi, mobile data, Bluetooth mesh, and peer connections depending on real-time network availability. The Security and Storage Layer ensures complete end-to-end encryption, post-quantum key exchange, and self-sovereign identity management, wherein all cryptographic credentials are generated and stored locally on the user's device to guarantee absolute privacy and ownership.

In one aspect, the invention introduces a resilient network architecture that employs AI-driven adaptive routing to maintain uninterrupted connectivity. The communication framework can intelligently switch between available network interfaces such as Wi-Fi, cellular data, Bluetooth, or mesh relays based on current network performance. The system continuously analyses parameters such as signal strength, bandwidth, latency, and power consumption to determine the most efficient route for message delivery. The AI engine dynamically selects the best path using multi-path routing and predictive analytics to minimise latency, reduce packet loss, and optimise throughput. Unlike prior centralised systems relying on static routing protocols, the present invention establishes a dynamic, self-healing, and energy-efficient network model that enhances reliability and communication speed under diverse conditions.

Another essential aspect of the invention is the incorporation of a self-sovereign cryptographic identity management framework. Conventional messaging systems typically depend on external certificate authorities or service providers for encryption key management, introducing vulnerabilities and dependence on central entities. The present invention overcomes these deficiencies by enabling each user device to independently generate, manage, and store its cryptographic keys locally. This decentralised key ownership ensures that only the end user has access to their credentials, eliminating risks of interception or unauthorised key manipulation. Furthermore, the

invention employs post-quantum cryptographic algorithms, including lattice-based and elliptic curve cryptography, to safeguard communications against potential quantum decryption threats, thereby providing a future-proof security model.

The invention further embodies a hybrid peer-to-peer and cloud-assisted communication model seamlessly integrating decentralised resilience with cloud scalability. Under standard operation, messages are transmitted through secure P2P encrypted socket channels. When internet connectivity becomes weak or unavailable, the system automatically forms ad hoc mesh networks that enable nearby devices to relay messages through store-and-forward mechanisms until the recipient device is reached. In situations where both P2P and mesh communication are infeasible, the system utilises synchronisation via cloud relay nodes to guarantee message delivery. This tri-layered redundancy ensures continuous communication availability even in remote, rural, or disaster-prone environments.

The invention employs AI-based adaptive compression and intelligent encoding mechanisms to ensure efficient transmission and resource optimisation. The system automatically identifies message types—such as text, images, audio, or video and applies context-specific compression strategies. By dynamically adjusting encoding parameters in response to bandwidth variations and latency conditions, the invention achieves substantial data efficiency without compromising quality. This adaptive compression framework conserves bandwidth, enhances message delivery speed, and reduces overall data usage, thereby outperforming conventional static compression systems.

The invention also provides an AI-enhanced multilingual communication interface to improve usability, accessibility, and inclusivity. This interface integrates real-time translation, speech-to-text conversion, and contextual summarisation, allowing users speaking different languages to communicate seamlessly. These operations are performed locally on the device without transmitting sensitive data to external servers, thereby ensuring privacy and responsiveness. The interface further adapts to user behaviour and

accessibility preferences, offering predictive typing, contextual shortcuts, and adaptive visual layouts to enhance user experience across diverse linguistic and accessibility needs.

A further distinctive aspect of the invention lies in its zero-knowledge backup and data sovereignty mechanism. All user data, including messages, media, and encryption keys, remain encrypted end-to-end throughout transmission, storage, and backup processes. Only the user retains control over the decryption credentials, ensuring that neither service providers nor third parties can access any stored or archived content. Even during synchronisation or recovery operations, encryption integrity is maintained, upholding compliance with global privacy standards such as the General Data Protection Regulation (GDPR). The system also supports configurable data retention, message expiry intervals, and selective visibility settings, enabling granular user control over data lifecycle management.

The invention additionally extends secure communication to offline environments through its integrated mesh and store-and-forward communication capabilities. When conventional internet connectivity is unavailable, nearby devices automatically form local mesh networks utilising short-range communication protocols such as Bluetooth or Wi-Fi Direct. Messages are relayed through intermediary devices, ensuring that communication continuity is preserved. This functionality is particularly advantageous for emergency response, defence operations, rural communication, and disaster management scenarios where infrastructure is limited or compromised.

The modular and scalable architecture of the invention enables seamless integration with Internet of Things (IoT) networks, enterprise platforms, and third-party applications through secure and standardised application programming interfaces (APIs). This modular framework facilitates the addition of new features, such as AI assistants, identity verification modules, or secure file transfer systems, without altering the core security and communication architecture. The design ensures that future technological

upgrades can be accommodated while maintaining system integrity, interoperability, and compliance.

The invention also incorporates an AI-powered threat detection and anomaly monitoring subsystem. The embedded AI continuously analyses traffic patterns, communication flows, and device behaviour to identify potential threats such as replay attacks, spoofing, or unauthorised message tampering. Upon detection, the system autonomously isolates compromised nodes, regenerates encryption keys, or reroutes communication paths to sustain operational continuity and maintain overall network integrity. This proactive threat management approach enhances trust and ensures persistent security within the communication ecosystem.

Energy efficiency and intelligent resource management are additional features of the invention. The AI subsystem monitors device conditions such as battery levels, CPU utilisation, and network activity, and optimally schedules background processes to conserve energy. By reducing redundant synchronisation and minimising idle resource consumption, the invention significantly extends device battery life compared to conventional always-on messaging applications. This optimised energy management contributes to both user convenience and sustainability in large-scale deployments.

The novelty of the present invention resides in its holistic integration of artificial intelligence, decentralised communication, adaptive routing, and post-quantum cryptographic security within a unified and self-learning communication system. Unlike conventional systems that rely on centralised architectures, external trust authorities, or static routing, the invention establishes an autonomous, privacy-first framework in which devices function as intelligent cooperative nodes. These nodes collaboratively form hybrid communication channels and dynamically adapt to changing network conditions without dependence on central servers or intermediaries.

By merging decentralisation, AI-driven optimisation, and cryptographic sovereignty, the invention redefines the paradigm of mobile communication. It introduces a self-evolving ecosystem capable of continuously learning from

operational data to enhance routing accuracy, compression efficiency, and system security. The invention thereby ensures that communication remains private, reliable, and efficient, marking a significant advancement in the field of intelligent, secure, and adaptive digital communication systems.

We claim:

1. A secure and intelligent communication system for privacy-preserving digital message transmission, comprising:
 - a) a User Layer configured to enable a user to initiate and receive communication events via a graphical user interface on a computing device, supporting text, audio, video, or multimedia messages;
 - b) a User Device configured as a decentralized control node hosting an AI Engine, an Encryption Layer, a local storage unit, and Network Interface modules, wherein the User Device performs on-device encryption, decryption, adaptive routing, compression, and offline message caching;
 - c) a Communication Layer configured to dynamically select an optimal communication path from a plurality of network interfaces including Wi-Fi, Mesh, and Cloud, based on real-time assessment of network parameters such as latency, bandwidth, and device power status; and
 - d) a Security and Storage Layer configured to employ post-quantum cryptographic algorithms, self-sovereign identity management, and local key generation to ensure end-to-end encryption, sender authentication, and message integrity,wherein the system operates as a self-organizing, self-learning communication ecosystem that autonomously optimizes message transmission, compression, and security in real-time without reliance on centralized servers.
2. The communication system as claimed in claim 1, wherein the AI Engine is configured to evaluate network performance parameters including signal strength, bandwidth, latency, and device power status to generate a real-time communication topology, enabling maintenance of multiple potential routing paths for operational resilience in dynamic network environments.
3. The communication system as claimed in claim 1, wherein the Communication Layer employs reinforcement learning algorithms to continuously refine routing accuracy based on historical route performance, transmission speed, energy efficiency, and error rate.

4. The communication system as claimed in claim 1, wherein the Encryption Layer generates a unique session key locally on the User Device for each message, preventing key reuse, and embeds digital signatures and integrity hashes to authenticate the sender and verify message integrity during transit.
5. The communication system as claimed in claim 1, wherein the Network Interface modules include:
 - a) a Wi-Fi Interface configured for high-speed, short-range data transmission under stable network conditions;
 - b) a Mesh Network Interface configured to form a self-organizing, self-healing mesh topology for decentralized peer-to-peer message relaying in the absence of internet connectivity; and
 - c) a Cloud Interface configured as a supplementary channel for long-range relay, encrypted synchronization, and cross-device message updates while maintaining full encryption.
6. The communication system as claimed in claim 1, wherein the AI Engine performs adaptive operations comprising: a) adaptive compression to reduce message size based on network conditions and message type; b) real-time translation for on-device multilingual communication; and c) anomaly detection to identify irregularities such as message corruption, delays, or intrusion attempts, triggering autonomous rerouting, re-encryption, or retransmission.
7. The communication system as claimed in claim 1, wherein the User Device is configured to decrypt received messages locally using a recipient's private key stored within a self-sovereign identity management system, ensuring no third party, including service providers, can access the decryption process.
8. The communication system as claimed in claim 1, wherein the system supports a hybrid peer-to-peer and cloud-assisted communication model, utilizing store-and-forward mechanisms in mesh networks for offline communication in remote or disaster-affected regions.
9. The communication system as claimed in claim 1, wherein the Security and Storage Layer implements a zero-knowledge backup and data

sovereignty mechanism, ensuring all user data, including messages and encryption keys, remains encrypted during transmission, storage, and backup, with decryption credentials controlled solely by the user.

10. The communication system as claimed in claim 1, further comprising an AI-powered threat detection and anomaly monitoring subsystem configured to analyze traffic patterns and device behavior, autonomously isolating compromised nodes, regenerating encryption keys, or rerouting communication paths to maintain network integrity.
11. The communication system as claimed in claim 1, wherein the AI Engine optimizes energy efficiency by monitoring device conditions such as battery levels and CPU utilization, scheduling background processes to minimize redundant synchronization and idle resource consumption.
12. The communication system as claimed in claim 1, wherein the User Layer includes an AI-enhanced multilingual communication interface supporting real-time translation, speech-to-text conversion, and contextual summarization, performed locally on the User Device to ensure privacy and responsiveness.
13. The communication system as claimed in claim 1, wherein the system architecture is modular and scalable, enabling integration with Internet of Things (IoT) networks, enterprise platforms, and third-party applications through secure application programming interfaces (APIs) without compromising core security or communication functionality.
14. The communication system as claimed in claim 1, wherein the AI Engine is configured to perform adaptive compression by dynamically reducing message size based on network conditions and message type, including text, image, audio, or video, to optimize bandwidth usage and transmission speed.
15. The communication system as claimed in claim 1, wherein the Security and Storage Layer employs lattice-based or elliptic curve cryptographic algorithms to provide post-quantum protection, ensuring long-term security against quantum decryption threats.
16. The communication system as claimed in claim 5, wherein the Mesh Network Interface enables devices within proximity to form a self-

organizing mesh topology, relaying messages through store-and-forward mechanisms to ensure communication continuity in the absence of internet connectivity.

17. The communication system as claimed in claim 1, wherein the Communication Layer is configured to autonomously switch between Wi-Fi, Mesh, and Cloud interfaces in response to network instability, maintaining uninterrupted message transmission through feedback-based routing and error correction.
18. The communication system as claimed in claim 1, wherein the User Layer supports real-time translation performed locally on the User Device, converting message content across languages to facilitate seamless multilingual communication without transmitting sensitive data to external servers.
19. The communication system as claimed in claim 1, wherein the AI Engine monitors message flow for anomalies, including corruption, delays, or intrusion attempts, and triggers corrective actions such as dynamic rerouting, re-encryption, or retransmission to maintain message integrity.
20. The communication system as claimed in claim 1, wherein the system securely erases temporary cryptographic session keys, routing data, and cached operational parameters from volatile memory upon confirmed message delivery, ensuring no residual data remains accessible post-session.

Dated this 12th day of October 2025



Sudarshana Bandyopadhyay

Regn. No.: IN/PA 2802

Agent for the applicant

Phn No. 9748818235

Email: bandyopadhyay.sudarshana@gmail.com

ABSTRACT

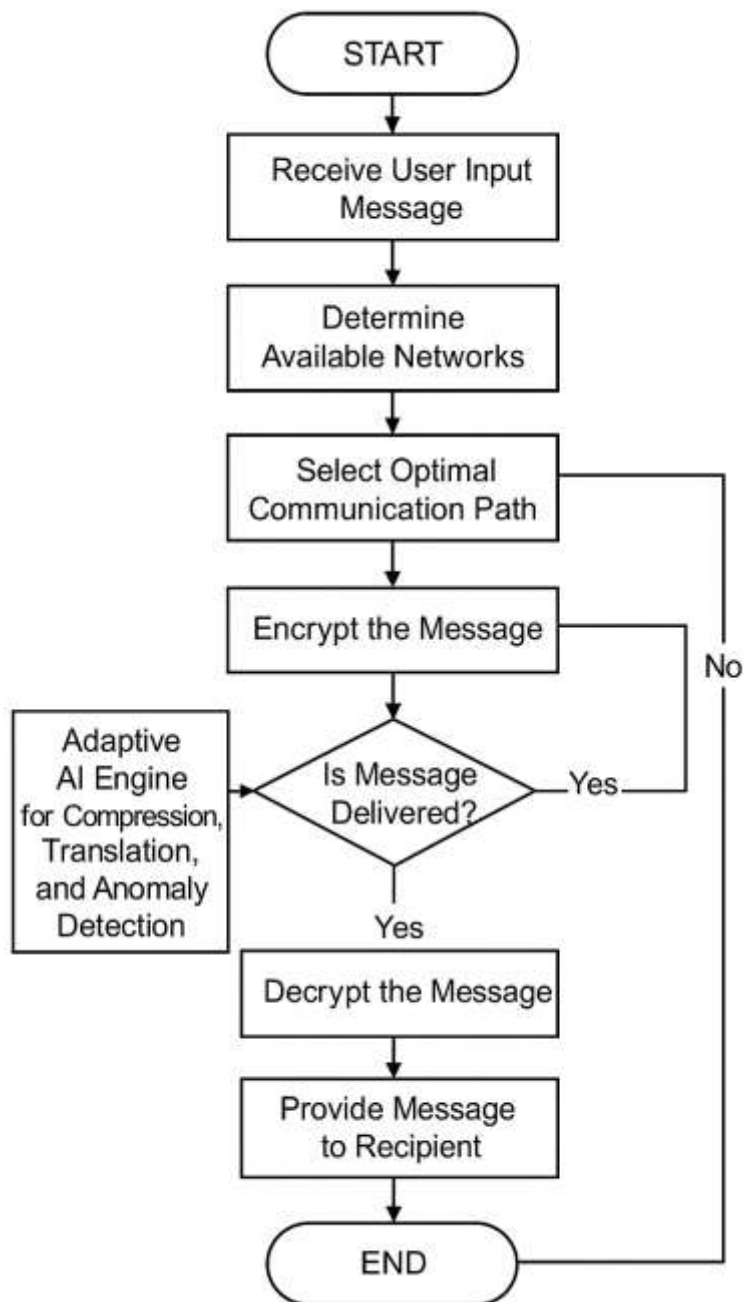
**ADAPTIVE MULTI-PATH MESSAGING SYSTEM WITH AI-DRIVEN
ROUTING AND SELF-SOVEREIGN ENCRYPTION**

The present invention relates to a secure and intelligent communication system for privacy-preserving digital message transmission integrates artificial intelligence (AI), decentralized networking, and post-quantum cryptography. The system comprises a User Layer for initiating and receiving text, audio, video, or multimedia messages; a User Device hosting an AI Engine, Encryption Layer, and Network Interface modules for on-device processing; a Communication Layer for dynamically selecting optimal paths among Wi-Fi, Mesh, and Cloud interfaces; and a Security and Storage Layer ensuring end-to-end encryption and self-sovereign identity management. The AI Engine optimizes routing, compression, and anomaly detection, while the system supports offline mesh networking and real-time translation. Temporary session keys and data are securely erased post-delivery, ensuring privacy. The system provides reliable, adaptive communication in dynamic network environments without centralized server dependency.

Fig 2

Appl No. -

Sheet 1 of 2



Detailed Flowchart

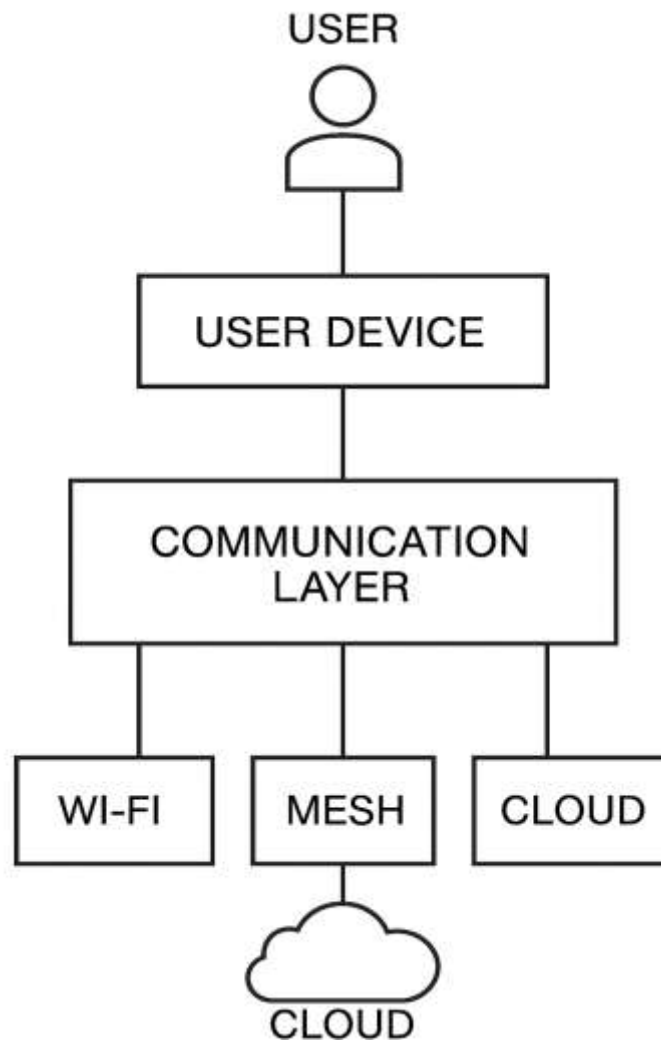
Figure 1

Sudarshana

Sudarshana Bandyopadhyay
Regn No.: IN/PA 2802
Agent for the Applicants

Appl No. -

Sheet 2 of 2



Conceptual Block Diagram

Figure 2

Sudarshana

Sudarshana Bandyopadhyay
Regn No.: IN/PA 2802
Agent for the Applicants

FORM 5
THE PATENTS ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003

Declaration as to Inventorship
[See section 10(6) and rule 13(6)]

1. NAME OF APPLICANT: SRJX RESEARCH AND INNOVATION LAB LLP,

hereby declare that the true and first inventor(s) of the invention disclosed in the complete specification filed in pursuance of our application numbered _____ dated 12 October 2025 are:

2. INVENTORS:

- I.** Name: **DR DILEEP KUMAR MOHANACHANDRAN**
b) Nationality: An Indian National
c) Address: International Research Fellow, SEGi University, 47810 Petaling Jaya, Selangor Darul Ehsan, Malaysia
- II.** a) Name: **DR SOUMYA RANJAN JENA**
b) Nationality: An Indian National
c) Address: Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India
- III.** a) Name: **DR NORMALA SUBRAMANIAM GOVINDARAJO**
b) Nationality: Indian
c) Address: E 305, Vaishnavi Ratnam Apartment, Jalahalli Cross, Bangalore, Karnataka-560057, India

Dated this 12th day of October 2025



Name of the signatory:

Signature Not Verified

Digitally Signed.
Name: Sudarshana
Bandyopadhyay
Date: 12-Oct-2025 14:05:17
Reason: Patent Filing

Dated this 12th day of October 2025

Sudarshana Bandyopadhyay

Regn No.: IN/PA 2802

Agent for the Applicants

Email: bandyopadhyay.sudarshana@gmail.com

Phn No: 9748818235

To,
The Controller of Patents,
The Patent Office
At Kolkata

UDYAM REGISTRATION CERTIFICATE

UDYAM REGISTRATION NUMBER

UDYAM-OD-07-0095836

NAME OF ENTERPRISE

SRJX RESEARCH AND INNOVATION LAB LLP

TYPE OF ENTERPRISE *

SNo.	Classification Year	Enterprise Type	Classification Date
1	2025-26	Micro	16/08/2025

MAJOR ACTIVITY

SERVICES

SOCIAL CATEGORY OF
ENTREPRENEUR

GENERAL

NAME OF UNIT(S)

S.No.	Name of Unit(s)
1	SRJX RESEARCH AND INNOVATION LAB LLP

OFFICAL ADDRESS OF ENTERPRISE

Flat/Door/Block No.	PLOT NO-3E/474	Name of Premises/ Building	SECTOR-9
Village/Town	CDA CUTTACK	Block	NA
Road/Street/Lane	Avinab Bidanasi	City	Cuttack Sadar
State	ODISHA	District	CUTTACK , Pin 753014
Mobile	9090255155	Email:	soumyajena1989@gmail.com

DATE OF INCORPORATION /
REGISTRATION OF ENTERPRISE

05/05/2025

DATE OF COMMENCEMENT OF
PRODUCTION/BUSINESS

05/05/2025

NATIONAL INDUSTRY
CLASSIFICATION CODE(S)

SNo.	NIC 2 Digit	NIC 4 Digit	NIC 5 Digit	Activity
1	72 - Scientific research and development	7210 - Research and experimental development on natural sciences and engineering	72100 - Research and experimental development on natural sciences and engineering	Services

DATE OF UDYAM REGISTRATION

16/08/2025

* In case of graduation (upward/reverse) of status of an enterprise, the benefit of the Government Schemes will be availed as per the provisions of Notification No. S.O. 2119(E) dated 26.06.2020 issued by the M/o MSME.

Disclaimer: This is computer generated statement, no signature required. Printed from <https://udyamregistration.gov.in> & Date of Printing: 12-Oct-2025 14:35:47
Reason: Patent Filing

Signature Not Verified

Digitally Signed.
Name: Sudarshana
Bandyopadhyay
Date: 12-Oct-2025 14:35:47
Reason: Patent Filing

For any assistance, you may contact:

1. District Industries Centre: CUTTACK (ODISHA)

2. MSME-DFO: CUTTACK (ODISHA)

Visit : www.msme.gov.in ; www.dcmsme.gov.in ; www.minmsme.gov.in



Follow us @minmsme & @msme



@msme



Udyam Registration Number : UDYAM-OD-07-0095836

Type of Enterprise	MICRO	Major Activity	Services
Type of Organisation	Limited Liability Partnership	Name of Enterprise	SRJX RESEARCH AND INNOVATION LAB LLP
Owner Name	SRJX RESEARCH AND INNOVATION LAB LLP	PAN	AFPPFS4480L
Do you have GSTIN	No	Mobile No.	9090255155
Email Id	soumyajena1989@gmail.com	Social Category	General
Gender	Male	Specially Abled(DIVYANG)	No
Date of Incorporation	05/05/2025	Date of Commencement of Production/Business	05/05/2025

Bank Details

Bank Name	IFS Code	Bank Account Number
Punjab national bank	PUNB0787800	7878002100002490

Employment Details

Male	Female	Other	Total
3	2	0	5

Investment in Plant and Machinery OR Equipment (in Rs.)

S.No.	Financial Year	Enterprise Type	Written Down Value (WDV)	Exclusion of cost of Pollution Control, Research & Development and Industrial Safety Devices	Net Investment in Plant and Machinery OR Equipment[(A)-(B)]	Total Turnover (A)	Export Turnover (B)	Net Turnover [(A)-(B)]	Is ITR Filled?	ITR Type
1	2023-24	Micro	0.00	0.00	0.00	0.00	0.00	0.00	No	NA

Unit(s) Details

SN	Unit Name	Flat	Building	Village/Town	Block	Road	City	Pin	State	District
1	SRJX RESEARCH AND INNOVATION LAB LLP	PLOT NO-3E/474	SECTOR-9	CDA CUTTACK	NA	Avinab Bidanasi	Cuttack Sadar	753014	ODISHA	CUTTACK

Official address of Enterprise

Flat/Door/Block No.	PLOT NO-3E/474	Name of Premises/ Building	SECTOR-9
Village/Town	CDA CUTTACK	Block	NA
Road/Street/Lane	Avinab Bidanasi	City	Cuttack Sadar
State	ODISHA	District	CUTTACK , Pin : 753014
Mobile	9090255155	Email:	soumyajena1989@gmail.com
Latitude	20.5021859203546	Longitude:	85.88860428847029

National Industry Classification Code(S)

SNo.	Nic 2 Digit	Nic 4 Digit	Nic 5 Digit	Activity
1	72 - Scientific research and development	7210 - Research and experimental development on natural sciences and engineering	72100 - Research and experimental development on natural sciences and engineering	Services

Are you interested to get registered on Government e-Market (GeM) Portal	No
Are you interested to get registered on TReDS Portals(one or more)	No
Are you interested to get registered on National Career Service(NCS) Portal	No
Are you interested to get registered on NSIC B2B Portal	No
Are you interested in availing Free .IN Domain and a business email ID	N/A
Are you interested in getting registered on Skill India Digital Portal	No
District Industries Centre	CUTTACK (ODISHA)
MSME-DFO	CUTTACK (ODISHA)
Date of Udyam Registration	16/08/2025
Date of Printing	16/08/2025

IEC Details	
IEC Number	
IEC Status	Inactive
IEC Registration Date	
IEC Modification Date	

"FORM 1 THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003 APPLICATION FOR GRANT OF PATENT (See section 7, 54 and 135 and sub-rule (1) of rule 20)				(FOR OFFICE USE ONLY)	
				Application No.	
				Filing date:	
				Amount of Fee paid:	
				CBR No:	
				Signature:	
1. APPLICANT'S REFERENCE / IDENTIFICATION NO. (AS ALLOTTED BY OFFICE)					
2. TYPE OF APPLICATION [Please tick (✓) at the appropriate category]					
Ordinary (✓)		Convention ()		PCT-NP ()	
Divisional ()	Patent of Addition ()	Divisional ()	Patent of Addition ()	Divisional ()	Patent of Addition ()
3A. APPLICANT(S)					
Name in Full		Nationality	Country of Residence	Address of the Applicant	
SRJX RESEARCH AND INNOVATION LAB LLP		Indian	India	SRJX RESEARCH AND INNOVATION LAB LLP, Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack- 753014, Odisha, India	
3B. CATEGORY OF APPLICANT [Please tick (✓) at the appropriate category]					
Natural Person ()		Other than Natural Person			
		Small Entity (✓)	Startup ()	Others ()	
4. INVENTOR(S) [Please tick (✓) at the appropriate category]					
Are all the inventor(s) same as the applicant(s) named above?		Yes ()		No (✓)	

If “No”, furnish the details of the inventor(s)			
Name in Full	Nationality	Country of Residence	Address of the Inventor
DR DILEEP KUMAR MOHANACHANDRAN	Indian	Malayasia	International Research Fellow, SEGi University, 47810 Petaling Jaya, Selangor Darul Ehsan, Malaysia
DR SOUMYA RANJAN JENA	Indian	India	Plot No - 3E/474, Sector-9, CDA, Post-Markat Nagar, Cuttack-753014, Odisha, India
DR NORMALA SUBRAMANIAM GOVINDARAJO	Indian	Indian	E 305, Vaishnavi Ratnam Apartment, Jalahalli Cross, Bangalore, Karnataka-560057, India
5. TITLE OF THE INVENTION			
ADAPTIVE MULTI-PATH MESSAGING SYSTEM WITH AI-DRIVEN ROUTING AND SELF-SOVEREIGN ENCRYPTION			
6. AUTHORISED REGISTERED PATENT AGENT(S)	IN/PA No.	2802	
	Name	Sudarshana Bandyopadhyay	
	Mobile No.	9748818235	
7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA	Name	SUDARSHANA BANDYOPADHYAY	
	Postal Address	Ground Floor, S-456, LGF, Greater Kailash – II, New Delhi – 110048, India	
	Telephone No.	NA	
	Mobile No.	97488 18235	
	Fax No.	NA	
	E-mail ID	bandyopadhyay.sudarshana@gmail.com	
8. IN CASE OF APPLICATION CLAIMING PRIORITY OF APPLICATION FILED IN CONVENTION COUNTRY, PARTICULARS OF CONVENTION APPLICATION			

Country	Application Number	Filing date	Name of the applicant	Title of the invention	IPC (as classified in the convention country)
N.A.					
9. IN CASE OF PCT NATIONAL PHASE APPLICATION, PARTICULARS OF INTERNATIONAL APPLICATION FILED UNDER PATENT CO-OPERATION TREATY (PCT)					
International application number			International filing date		
10. IN CASE OF DIVISIONAL APPLICATION FILED UNDER SECTION 16, PARTICULARS OF ORIGINAL (FIRST) APPLICATION					
Original (first) application No.			Date of filing of original (first) application		
N.A.					
11. IN CASE OF PATENT OF ADDITION FILED UNDER SECTION 54, PARTICULARS OF MAIN					
Main application/patent No.			Date of filing of main application		
N.A.			N.A.		
12. DECLARATIONS					
<p>(i) Declaration by the inventor(s)</p> <p>(In case the applicant is an assignee: the inventor(s) may sign herein below or the applicant may upload the assignment or enclose the assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period).</p> <p>We, the above-named inventor(s) is/are the true & first inventor(s) for this Invention and declare that the applicant(s) herein is/are my/our assignee or legal representative.</p> <p>(a) Date:</p> <p>(b) Signature:</p> <p>(c) Name: Dr Dileep Kumar Mohanachandran</p> <p>(a) Date</p> <p>(b) Signature(s):</p> <p>(c) Name: Dr Soumya Ranjan Jena</p> <p>(a) Date:</p> <p>(b) Signature:</p> <p>(c) Name: Dr Normala Subramaniam Govindarajo</p>					

(ii) Declaration by the applicant(s) in the convention country

(In case the applicant in India is different than the applicant in the convention country: the applicant in the convention country may sign herein below or applicant in India may upload the assignment from the applicant in the convention country or enclose the said assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period)

I/We, the applicant(s) in the convention country declare that the applicant(s) herein is/are my/our assignee or legal representative. – **N.A.**

- (a) Date
- (b) Signature(s)
- (c) Name(s) of the signatory

(iii) Declaration by the applicant

We the applicant hereby declare that: -

- ☒ We are in possession of the above-mentioned invention.
- ☒ The complete specification relating to the invention is filed with this application.
- ☐ The invention as disclosed in the specification uses the biological material from India and the necessary permission from the competent authority shall be submitted by me/us before the grant of patent to me/us.
- ☒ There is no lawful ground of objection(s) to the grant of the Patent to us.
- ☐ We are the true & first inventor(s).
- ☒ We are the assignee or legal representative of true & first inventor(s).
- ☐ The application or each of the applications, particulars of which are given in Paragraph-8, was the first application in convention country in respect of my invention(s).
- ☐ We claim the priority from the above mentioned application(s) filed in convention country/countries and state that no application for protection in respect of the invention had been made in a convention country before that date by us or by any person from which I derive the title.
- ☐ Our application in India is based on international application under Patent Cooperation Treaty (PCT) as mentioned in Paragraph-9.
- ☐ The application is divided out of my /our application particulars of which is given in Paragraph-10 and pray that this application may be treated as deemed to have been filed on DD/MM/YYYY under section 16 of the Act.
- ☐ The said invention is an improvement in or modification of the invention particulars of which are given in Paragraph-11.

13. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION

(a) Form 2

<i>Item</i>	<i>Details</i>	<i>Fee</i>	<i>Remarks</i>
Complete/ provisional specification	No. of pages: 16	1600	Including Form 2, description,
No. of Claim(s)	No. of Claims = 20 No. of Pages = 4	-	Claim pages
Abstract	1		Abstract page
No. of Drawing(s)	No. of drawings = 2 and No. of pages = 2		Drawing sheets

In case of a complete specification, if the applicant desires to adopt the drawings filed with his provisional specification as the drawings or part of the drawings for the complete specification under rule 13(4), the number of such pages filed with the provisional specification are required to be mentioned here.

- b. Form 3: Statement and Undertaking
- c. Form 5: Declaration as to inventorship
- d. Power of Attorney
- e. Form 28
- f. Form 9

Total fee ₹ 7300/- is being paid online through electronic portal

We hereby declare that to the best of our knowledge, information and belief the fact and matters stated herein are correct and we request that a patent may be granted to us for the said invention.

Dated this 12th day of October 2025.

Signature:



Name: Sudarshana Bandyopadhyay

(Regn No: IN/PA 2802)

Agent for the Applicant

Phn no.: 97488 18235

email: bandyopadhyay.sudarshana@gmail.com

To,
The Controller of Patents
The Patent Office,
at Kolkata


FORM 28
THE PATENTS ACT,
1970 (39 of 1970)

AND

THE PATENTS
RULES, 2003

TO BE SUBMITTED BY A SMALL ENTITY /STARTUP/EDUCATIONAL
INSTITUTION

[See rules 2 (fa), 2(fb), 2(ca) and 7]

1	Name, address and nationality.	We, SRJX RESEARCH AND INNOVATION LAB LLP, of the address Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India, applicant in respect of the patent application no. _____ dated 12 October 2025 hereby declare that we are a micro entity in accordance with rule 2(fa) and submit the following document as a proof :
2	Documents to be submitted	
	i. For claiming the status of a micro entity:	
	A. For an Indian applicant: Evidence of registration under the Micro, Small and Medium Enterprises Act, 2006 (27 of 2006).	
3	To be signed by the applicant(s) / patentee (s) / authorised registered patent agent.	The information provided herein is correct to the best of my/our knowledge and belief. Dated this 12 th day of October 2025
4	Name of the natural person who has signed.	 Signature:

Signature Not Verified

Digitally Signed.
Name: Sudarshana
Bandyopadhyay
Date: 12-Oct-2025 14:35:47
Reason: Patent Filing

	<p>Designation and official seal, if any, of the person who has signed.</p>	<p>Sudarshana Bandyopadhyay Regn. No.: IN/PA 2802 Agent for the applicant Phn No. 9748818235 Email: bandyopadhyay.sudarshana@gmail.com</p> <p>To The Controller of Patents, The Patent Office, At Kolkata</p>
--	---	---

FORM 9
THE PATENTS ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003
REQUEST FOR PUBLICATION
[See Section 11A(2); Rule 24A]

We, SRJX RESEARCH AND INNOVATION LAB LLP, of the address Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India, hereby request for an early publication of our Patent Application No. _____ filed on 12 October 2025 under Section 11A(2) of the Act.

Dated this 12th day of October 2025



Sudarshana Bandyopadhyay
Regn No.: IN/PA 2802
Agent for the Applicants
Email: bandyopadhyay.sudarshana@gmail.com
Phn No: 9748818235

Signature Not Verified

Digitally Signed.
Name: Sudarshana
Bandyopadhyay
Date: 12-Oct-2025 14:17:46
Reason: Patent Filing



सत्यमेव जयते

INDIA NON JUDICIAL

Government of National Capital Territory of Delhi

₹100

e-Stamp

Certificate No. : IN-DL35961746213944X
 Certificate Issued Date : 16-Aug-2025 11:10 AM
 Account Reference : IMPACC (IV)/ dl962703/ DELHI/ DL-ESD
 Unique Doc. Reference : SUBIN-DL96270305293890128756X
 Purchased by : SRJX RESEARCH AND INNOVATION LAB LLP
 Description of Document : Article 48(c) Power of attorney - GPA
 Property Description : Not Applicable
 Consideration Price (Rs.) : 0
 (Zero)
 First Party : SRJX RESEARCH AND INNOVATION LAB LLP
 Second Party : ZAINAB SYED AND ASSOCIATES
 Stamp Duty Paid By : SRJX RESEARCH AND INNOVATION LAB LLP
 Stamp Duty Amount(Rs.) : 100
 (One Hundred only)

₹100₹100₹100₹100



Please write or type below this line

IN-DL35961746213944X



Statutory Alert:

1. The authenticity of this Stamp certificate should be verified at 'www.shcllestamp.com' or using e-Stamp Mobile App of Stock Holding. Any discrepancy in the details on this Certificate and as available on the website / Mobile App renders it invalid.
2. The onus of checking the legitimacy is on the users of the certificate.
3. In case of any discrepancy please inform the Competent Authority.

Signature Not Verified

Digitally Signed
 Name: Sudarshana
 Bandyopadhyay
 Date: 12-Oct-2025 12:05:17
 Reason: Patent Pending

SRJX RESEARCH AND INNOVATION LAB LLP SRJX RESEARCH AND INNOVATION LAB LLP SRJX RESEARCH AND INNOVATION LAB LLP SRJX RESEARCH AND INNOVATION LAB LLP

FORM-26
The Patents Act, 1970
(39 of 1970)
FORM FOR AUTHORIZATION OF A PATENT AGENT/OR ANY PERSON IN A
MATTER OR PROCEEDING UNDER THE ACT
[See Sections 127 and 132; Rule 135]

I, **SRJX RESEARCH AND INNOVATION LAB LLP**, Indian, of the address **SRJX RESEARCH AND INNOVATION LAB LLP, Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India**, hereby authorize **Zainab Syed & Associates** having address **3E, Nawab Bhagwanpora, Lal Bazar, Srinagar, Jammu & Kashmir, 190023, India** (**Mobile No.: +91 9748818235, Email: bandyopadhyay.sudarshana@gmail.com**) through **Ms. Sudarshana Bandyopadhyay (IN/PA 2802)** and **Ms. Meenu Sharma (IN/PA-2856)**, registered Indian Patent Agents, to act on our behalf and to further appoint attorney(s)/agent(s) in connection with the filing and prosecution of our patent applications for grant of Letters Patent, filing of request for examination, filing request for amendment, recordal of change of name and address, ownership, change of address of service in India, renewal of patent, recordal of assignments, filing and defending oppositions and infringement actions, restoration of patents, registration of documents and such other actions and all proceedings under the Patents Act, 1970 and the Patent Rules, 2003 and all such proceedings before the Patent Office or the Government of India or any Court in India and all acts and things as the said attorney may deem necessary or expedient in connection therewith or incidental thereto.

We further request that all notices, requisitions and communication relating thereto may be sent to such person/s at the corresponding address mentioned below:

Ground Floor, S-456, LGF, Greater Kailash – II, New Delhi – 110048, India,

(Contact No.: +91 9748818235; Email: bandyopadhyay.sudarshana@gmail.com)

We, hereby, revoke all previous authorizations, if any, in respect of the proceedings.



We, hereby, assent to the action already taken by the said person/s in the above matter.

Dated this 14th day of August, 2025

SRJX RESEARCH AND INNOVATION LAB LLP

Through:

Signature: *Soumya Ranjan Jena*

Name: Dr. Soumya Ranjan Jena

Company
Seal:

SRJX Research and Innovation Lab LLP
LLPIN: ACO-1435

To,
The Controller of Patents,
The Patent Office,
Kolkata



ATTESTED

Notary Public Delhi

16 AUG 2025

FORM 9
THE PATENTS ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003
REQUEST FOR PUBLICATION
[See Section 11A(2); Rule 24A]

We, SRJX RESEARCH AND INNOVATION LAB LLP, of the address Plot No - 3E/474, Sector-9, CDA, Post- Markat Nagar, Cuttack-753014, Odisha, India, hereby request for an early publication of our Patent Application No. _____ filed on 12 October 2025 under Section 11A(2) of the Act.

Dated this 12th day of October 2025



Sudarshana Bandyopadhyay
Regn No.: IN/PA 2802
Agent for the Applicants
Email: bandyopadhyay.sudarshana@gmail.com
Phn No: 9748818235


Signature Not Verified

Digitally Signed.
Name: Sudarshana
Bandyopadhyay
Date: 12-Oct-2025 14:04:35
Reason: Patent Filing

FORM 3 THE PATENTS ACT, 1970 (39 of 1970) and THE PATENTS RULES, 2003 STATEMENT AND UNDERTAKING UNDER SECTION 8 (See section 8; Rule 12)					
1. Name of the applicant(s).			We, SRJX RESEARCH AND INNOVATION LAB LLP, Plot No - 3E/474, Sector-9, CDA, Post-Markat Nagar, Cuttack-753014, Odisha, India hereby declare:		
2. Name, address and nationality of the joint applicant.			(i) that we have not made any application for the same/substantially the same invention outside India Or (ii) that we who have made this application No date 12 th October 2025 alone/ jointly with, made for the same/ substantially same invention, application(s) for patent in the other countries, the particulars of which are given below:		
Name of the country	Date of application	Application No.	Status of the application	Date of publication	Date of grant
N.A.					
3. Name and address of the assignee			(iii) that the rights in the application(s) have been assigned to SRJX RESEARCH AND INNOVATION LAB LLP, Plot No - 3E/474, Sector-9, CDA, Post-Markat Nagar, Cuttack-753014, Odisha, India		

Signature Not Verified

Digitally Signed.
 Name: Sudarshana Bandyopadhyay
 Date: 12-Oct-2025 14:05:17
 Reason: Patent Filing

	<p>that we undertake that upto the date of grant of the patent by the Controller, we would keep him informed in writing the details regarding corresponding applications for patents filed outside India within six months from the date of filing of such application.</p> <p>Dated this 12th day of October 2025</p>
4. To be signed by the applicant or his authorized registered patent agent.	 <p>Signature.</p>
5. Name of the natural person who has signed.	<p>Sudarshana Bandyopadhyay Regn. No.: IN/PA 2802 Agent for the applicant Phn No. 9748818235 Email: bandyopadhyay.sudarshana@gmail.com</p>
	<p>To The Controller of Patents, The Patent Office, at Kolkata</p>
Note.- Strike out whichever is not applicable;	