

Project Title: Construction of Scalable and Robust Signcryption Scheme for IoT devices

1. Project Description:

This document defines the project delivered by **Dr. Jayaprakash Kar** from The LNM Institute of Information Technology, Jaipur, Rajasthan-India thereafter referred to as "LNMIIT-Jaipur" to Data Security Council of India thereafter referred to as "DSCI". This document is governed by, incorporated into, and made part of the terms and conditions of the proposal shared by LNMIIT-Jaipur.

The aim of this project is to design a novel Signcryption scheme for IoT Systems. The IoT devices should ensure security and privacy of data specially during the transmission. We propose using signcryption where both the signing and encryption perform in one single logical step so that the cost of signcryption would be less than the combined cost of signing and the cost of encryption. This cryptographic primitive is more compatible to be implemented on constrained devices, like the IoT devices.

These devices follow a 4-layer architecture –

- Application Layer: This acts as an interface between user and IoT device through which even the user can view their medical data.
- Sensor Layer: This layer collects data of patients using various sensors (core IoT device layer).
- Middleware: This layer is for data privacy and secrecy and acts as a filter for the sensor layer. This will be the layer where the signcryption protocol will be implemented.
- Network Layer: This layer is responsible for sending the data to appropriate paths using various technologies such as wired connection, Wi-Fi, and Bluetooth.

In order to preserve the privacy of the stored data and achieve other security goals such as integrity, non-repudiation and authentication in the communication system, Signcryption would be implemented in the middleware layer.

The complete project is divided into four phases:

Phase 1 - Study of the hardware architecture of IoT devices.

Phase 2 - Construction of novel signcryption scheme.

Phase-3 - Validation of proposed scheme by using the formal method.

Phase 3 - Prototype Implementation on the device.

Phase 4 - Security Analysis and evaluation of computational cost.

Salient Information:

- IoTs are used to remotely monitor patients.
- Providing a secure environment for the transmission of sensitive medical data.
- Ensuring privacy of patients and doctors is maintained.
- Secure IoTs will help in popularising the devices resulting in better healthcare



- especially in rural areas.
- Significant reduction of computation costs and increase in battery life.

2. Project Investigator:

Dr. Jayaprakash Kar

3. Project Outcome:

Signcryption provides more secure way of communication in IoMT Devices. In case of IMD Devices, which are implanted in the body through surgery, they need to have a long lasting battery for continuous operation. Hence, low computation cost directly increases the battery life of the device. It ensures privacy of the patient's data, integrity, non-repudiation, confidentiality.

4. Project Investment:

DSCI will invest the sum of **INR Five Lakh Five thousand (5,05,000) + Applicable Taxes** for the execution of this project.

The fund will be utilized for equipment purchase, travel, manpower and consultancy. It may also involve industry collaboration, interactions, and support to prototype deployment in the industry environment.

5. Institutional commitment, if any:

LNMIIT-Jaipur will provide the grant of INR 261 for the execution of this project.

6. Project duration & timeline:

- 6 months from the issue of the order

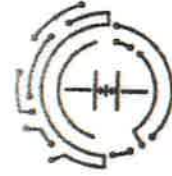
7. Intellectual Property Rights (IPR):

The inventor will have and retain the absolute intellectual property rights (IPR) over any content, technology and source code etc. developed by LNMIIT Jaipur during this period of project & DSCI has the right to use the technology invented at a very low or no cost.

8. Start-up Share, if any :

The start-up will use technology outcomes from projects on which LNMIIT has IP rights. Therefore, royalty/ revenue expected from the start-up will be worked out at the time of the start-up launch. Moreover, it will depend on whether the start-up will be by an LNMIIT faculty or an outsider agency; accordingly, revenue sharing will be worked out.


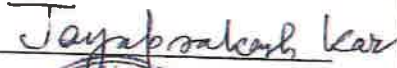
Commercial outcomes will also be protected as per LNMIIT IP policy.



This Agreement shall be binding upon the parties, their heirs, successors, assigns, and personal representatives. This Agreement constitutes the entire understanding of the parties. Its terms can be modified only by written signed by both parties. Any dispute arising out of this agreement will be resolved by negotiation between the parties.

I hereby agree to and approve this proposal.

The parties hereto have caused this Agreement to be executed by their duly Authorized Representatives.

<p>Data Security Council of India (DSCI), Noida</p> <p>Name: Mr. Vinayak Godse</p> <p>Title: CEO</p> <p>Date:</p> <p>Signature: </p>	<p>The LNM Institute of Information Technology, Jaipur, Rajasthan-India</p> <p>Name: Dr. Jayaprakash Kar</p> <p>Title: Associate Professor, Dept. of CSE</p> <p>Date: 30/01/2023</p> <p>Signature: </p>
--	---

