Executive Summary

<<Dipanwita Roy Chowdhury>>
<<Professor, Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur>>

1. **Title of the Project:** Design and Implementation of Secure Implantable Medical Devices (IMDs)

2. **Date of Start of the Project**: 01.10.2022

3. **Aims and Objectives**: IMDs (Implantable Medical Devices) are man-made devices surgically placed inside the human body that replace, support, and enhance biological structures. There has been a growing trend in electrophysiology toward remote monitoring of IMDs like, implantable cardioverter defibrillators (ICD), cardiac resynchronization therapy (CRT) devices, pacemakers, and implantable cardiac monitors. This allows the patient to send his data to the doctor from home without going to the hospital. While this is beneficial to both the patient and the doctor, the wireless connectivity can be exploited to compromise the security of IMDs. The aim of this research work is to study and analyze the probable IMD attacks and to develop lightweight cryptographic protocols for memory and power aware IMDs so that the IMD itself can detect any adversarial attempts/attacks on it. The final aim is to design and implement a prototype for secure IMD(s).

4. **Significant achievements** (not more than 500 words to include List of patents, publications, prototype, deployment etc): Based on the research work that has been carried out till date, the following two conference papers (one presented and communicated).

   - Anisha Mitra, Dipanwita Roy Chowdhury," Unmasking the Dominant Threat of Data Manipulation Attack on Implantable Cardioverter Defibrillators", In proceedings of

The 20th Annual International Conference on Privacy, Security and Trust (PST2023), Copenhagen, Denmark, 21-23 August 2023 [Presented].

- Anisha Mitra, Dipanwita Roy Chowdhury," Guarding the Beats by Defending Resource Depletion Attacks on Implantable Cardioverter Defibrillator", 10th International Conference On Mathematics and Computing (ICMC), 2024 [Communicated]

5. **Concluding remarks**:

During the current phase of the project, we explored the primary functionalities of ICDs based on market-available ICD manuals and existing literature. Our in-detailed study identified two of the most dangerous attacks on the ICD environment, data manipulation attack and resource depletion attack. We recognize a genuine need to simulate these attack scenarios based on currently available ICD models in the market. Thus, we intend to verify the realistic relevance of proposed attack scenarios in correct medical settings by using a particular ICD device and necessary equipment in our next phase of work.