National Institute of Technology Rourkela

Departmental Seminar

Seminar Title	: SecFit: Secured Hardware Prototype for IoT-based Healthcare Applications.
Speaker	: Prof Manish Okade.
Supervisor	: Prof. Manish Okade
Venue	: EC-138 Electronics and Communication Engineering Department
Date and Time	: 12 Mar 2025 (05.30PM)
Abstract	: In this paper, a prototype is developed for securing healthcare gadgets involved in handling sensitive medical data. The plain vanilla Fitbit architecture is chosen as a use case, and hardware security modules are developed for it with the motivation of securing the Fitbit architecture. The purpose of securing a Fitbit architecture is to address the rising concern about its vulnerabilities to side-channel attacks. The hardware security modules developed for the plain vanilla Fitbit architecture include an encryption layer and an obfuscation layer, and the proposed architecture is referred to as secured Fitbit (SecFit). The encryption layer consists of optimized non-linear substitution boxes (S-box) and linear permutation layers (Player) taken from the lightweight Midori symmetric cipher, the preferred cipher for IoT applications. The proposed architecture adopts obfuscation countermeasures, making it resilient to side-channel attacks. The additional hardware inculcated gives an area overhead of 1.61%. However, the energy and power consumption of SecFit are reduced by 50% and 17.24%. The SecFit architecture exhibits high throughput compared to the plain vanilla Fitbit architecture without security features. The proposed architecture can be plugged into other application architectures demanding security, making the design generic.