**Enabling secure cloud computation for resource constrained Internet of Medical Things devices**

**Shruthi Ramesh**

Smart healthcare products are ever increasing with a projected market of 348 Billion USD by 2025. It is forecasted that there will be an increased demand and investment for healthcare services that cater monitoring, prevention and diagnoses thereby reducing the expenditures on actual treatment. Such high proliferation rates require healthcare providers to adopt the digital era. However, this adoption and transition can be challenging and expensive. Cloud computing is a promising solution to reduce the cost and providing better security by outsourcing storage and processing of medical data to cloud vendors like Amazon Web services, Microsoft Azure, Google Cloud Healthcare. Data driven cloud services like Analytics and machine learning provided by these vendors can deliver intelligent services that can significantly improve the quality of healthcare.

However, cloud service providers can only provide intelligent insights for un-encrypted data. Thus, there is an inherent conflict between these data driven services and users’ privacy. So, how can healthcare industry benefit from cloud without compromising security and data control? Fully Homomorphic Encryption (FHE) schemes have been proposed in the literature to tackle this issue. However, FHE is too computationally intensive and impractical to be deployed on a small medical device. Alternate approaches proposed so far have inherent limitations making it challenging to practically use them for medical Internet of Things (IoT) ecosystem.

To overcome these issues, the current research work proposes a practical, scalable, secure and ready-to-deploy framework called “*Proxy re-ciphering* as a service” that enables secure cloud computation for medical IoT device generated data.