Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications.

Roll: 1807021 Date: 02/04/2023

My work: I studied the "Introduction" section of the paper in this week. Learnt that some scientists tried various approaches to devise various cryptographic systems for IoT devices. Some of them proposed such methods that would take much more memory and computation power than IoT devices would offer while another group of people published such methods that were either not fully completed or slow in nature. Some of them simulated their results. But authors of this paper believe that actual implementation of cryptosystems would provide more accurate results than simulation and so they used their proposed solution on the Mbed microcontroller NXP LPC1768 and ensured fast encryption speed. In this paper authors tried to utilize the properties of chaotic system. Indeed, chaotic systems have good cryptography features such as unpredictability, nonlinearity, aperiodicity, and high sensitivity to control parameters. In addition, their implementations require fewer resources in terms of processing, storage, and communication footprint compared to conventional approaches. Thus, they are lightweight in software development. These features made chaotic systems attractive for providing strong, lightweight, and efficient cryptography for resource constrained IoT nodes

Plan for future: Need to study more thoroughly about Chaos theory and Cryptosystem. Also need to get comprehensive idea about encryption and decryption in IoT devices. I plan to spend more time on understanding how chaos theory based cryptosystem works and mathematics involved behind the mechanism. Also, I shall try to complete and present the contents of "Background" section of this paper in next week.