INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

A Lightweight Security Framework for the Internet of Things: Home Automation.

Project PSPD by

Mr. Sulakkya Peiris **(w1790616/20191293)**

Supervised by

Mr. Sithira Hewaarachchi

Submitted in partial fulfilment of the requirements for MSc in cyber security and forensics at the University of Westminster.

August 2023

Abstract

The escalating adoption of Internet of Things (IoT) devices has necessitated robust data encryption methods to safeguard sensitive information. An essential component of encryption is generating white noise to provide a reliable source of randomness. However, the challenge lies in developing lightweight white noise generation techniques suitable for resource constrained IoT devices, where computational efficiency and energy consumption are critical concerns.

White noise serves as a fundamental building block for cryptographic algorithms, including key generation, initialization vectors, and one-time pads. However, the challenge lies in developing lightweight white noise generation techniques suitable for resource constrained IoT devices, where computational efficiency and energy consumption are critical concerns. Traditional cryptographic methods may be computationally heavy and impractical for the limited processing power and memory of IoT devices. Moreover, energy-efficient white noise generation is imperative to extend the battery life of battery-powered IoT devices, enhancing their overall operational lifespan and reducing maintenance costs. To address this, we leverage pseudorandom number generators (PRNGs), aiming to strike a balance between cryptographic strength and resource utilization.

Finally, we will evaluate the effectiveness of the proposed IoT security framework. Ultimately, our research aims to contribute to the advancement of secure IoT applications, safeguarding sensitive data in the interconnected world of tomorrow.

Keywords: Internet of things, IoT security, White noise generators, cryptographic algorithms

Subject Descriptors: Security and privacy → Software and application security →Software security engineering