

Research Article

Somewhat Homomorphic Encryption: Ring Learning with Error Algorithm for Faster Encryption of IoT Sensor Signal-Based Edge Devices

V. Subramaniaswamy,¹ V. Jagadeeswari,¹ V. Indragandhi,² Rutvij H. Jhaveri,³
V. Vijayakumar,⁴ Ketan Kotecha,⁵ and Logesh Ravi⁶

¹School of Computing, SASTRA Deemed University, Thanjavur, India

²School of Electrical Engineering, Vellore Institute of Technology, Vellore, India

³School of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat, India

⁴School of Computer Science and Engineering, University of New South Wales, Sydney, Australia

⁵Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune, India

⁶Department of Computer Science and Engineering,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

Correspondence should be addressed to Rutvij H. Jhaveri; rutvij.jhaveri@sot.pdpu.ac.in

DW[HW # (6 VWV TVd\$ " \$ #- DW[eW # " < gSk \$ " \$ \$ - 3 UWWfW #) < gSk \$ " \$ \$ - BgT [eZW \$ & 8WdgSk \$ " \$ \$

Academic Editor: Mamoun Alazab

Copyright © 2022 V. Subramaniaswamy et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, Homomorphic Encryption (HE) has shown the possibility of securely running a computation arbitrarily without performing the data decryption. Many authors have shown Somewhat Homomorphic Encryption (SHE) or Fully Homomorphic Encryption (FHE) schemes implemented practically on both the addition and multiplication operations for SHE. The recent methods for implementing the FHE methods completely depend on arbitrarily reducing the time taken to perform the encrypted multiplication operation to increase the computation power required by SHE methods. This paper aims to accelerate the encryption primitives in an integer-based SHE based on the duration between each data transmission from the sensor and data packaging method. If the number of sensors increases exponentially in an edge device environment, the signals have to be encrypted faster in a packed mode in the edge environment and transferred to the cloud without a loss in data. The presented SHE method reduces the time taken for encryption based on the input number from the sensor and invariably increases the performance of the edge device. This advantage also helps the deploying healthcare application obtain end-to-end privacy in transmitting sensitive patient data.

1. Introduction

The ecosystem required for the Internet of Things (IoT) is growing exponentially because of the large-scale availability of low-cost sensors, actuators, microprocessors, and high-speed Internet infrastructure. These devices can be integrated seamlessly for gathering data from the required environment, depending on the application. The collected data have to be processed and monitored continuously for effective implementation. The healthcare industry is one of the largest revenue-generating sectors in India with a market

share of 133 billion USD by 2022 [1]. The continuous monitoring of hospitalized patients and a timely prediction of complications that arise from disease leads to early recovery and reduces patient hospital stay. Apart from increased revenue, the reduced hospital stay of the patient will translate into less strain in the current healthcare infrastructure as well as saving the patient lives through the early detection of diseases.

With the established Internet framework, multiple sensor devices integrated with individual patients transmit their vital information through the network in the Edge

