A Comparative Study of BFV and CKKs Schemes to Secure IoT Data Using TenSeal and Pyfhel Homomorphic Encryption Libraries

Yancho B. Wiryen, University of Douala, Cameroon*

Noumsi Woguia Auguste Vigny, University of Douala, Cameroon

Mvogo Ngono Joseph, University of Douala, Cameroon

Fono Louis Aimé, University of Douala, Cameroon

https://orcid.org/0000-0002-7315-0427

ABSTRACT

Internet of things (IoT) devices and applications are on the rise, generating large amounts of sensitive and confidential data that need to be processed securely. Due to resource constraints, the data generated is often stored and processed in the cloud. The drawback of data cloud storage and processing is the fact that it can be hacked, leaked, or sold by cloud companies. Fully homomorphic encryption (FHE) allows computation on encrypted data using basic mathematical operations and has recently been successfully implemented using schemes and libraries with better performance. In this paper, the authors propose a mixture of edge-cloud-based security schemes using FHE to secure IoT data. The authors evaluate the performance of two FHE schemes (BFV and CKKS) based on data: encoding speed, encryption speed, arithmetic operations (addition and multiplication) speed, and decryption decoding speed using two Python libraries (TenSEAL and PyFHEl). The encryption and decryption are done at the edge node using a Raspberry Pi 4, while the processing is done at the cloud node using a laptop.

KEYWORDS

1. INTRODUCTION

In our world today, we have billions of connected devices, sensors, actuators, controllers, and applications that are communicating and interacting to form the Internet of Things (IoT). These IoTs help to improve our health, the quality of life in our homes, save time, and make our workplace more

*Corresponding Author

productive, thereby improving our welfare. By 2030, our world will be revolutionized by the IoT market (Griffiths & Ooi, 2018), and as projected by Gartner, IoT data will arguably become the biggest big data source, possibly overtaking enterprise, media, and entertainment data (Akbar, 2017). Despite the numerous advantages of IoT, they are unable to handle and compute the large amount of data they generate due to resource constraints and because the cost of implementing some computation of massive data on them might outweigh the benefits (Evans & Eyers, 2012). A combination of IoT, machine learning, and cloud computing technology has often been used as a solution to this large amount of data, and even more so due to the prevalence of the COVID-19 pandemic, as everyone is now soliciting for cloud services (Iezzi, 2020).

A security mechanism capable of preserving this data needs to be put in place to ensure that IoT data is not accessed by cloud companies or third parties or does not end up in the wrong hands. This mechanism is difficult to achieve with traditional encryption schemes (Song et al., 2018). For traditional encryption schemes, each time a computation needs to be performed on the encrypted data stored in the cloud, the data is first decrypted. After the decrypted data is processed, it will be re-encrypted and re-uploaded to the cloud. This process often gives the cloud service providers and the model owners' access to the data and is very tedious and time-consuming (Maha et al., 2012). For the users, they want cloud service providers to process the data and extract the valuable information contained while keeping it unknown to other users and third-party services. In other words, there is the desire to manipulate data while ensuring data protection, privacy, and anonymization to ensure that IoT data does not get into the wrong hands..

Homomorphic encryption is capable of handling this challenge and enables computation on encrypted data without decryption. In 2009, there was a remarkable breakthrough when Gentry (Gentry, 2009) successfully demonstrated that fully homomorphic encryption (FHE) was possible, even though it had difficulties in implementation and was time-consuming. FHE refers to a specific class of encryption scheme that allows computing directly (a large number of different types of mathematical operations) on encrypted data without having to decrypt it first. The result of the ciphertext when decrypted is the same as the output of the mathematical operations on the corresponding plaintext.

Several FHE schemes and libraries have been published that allow even those who are not good at cryptography to apply FHE in various domains ranging from data science (Iezzi, 2020), healthcare (Wood et al., 2020), IoT (Song et al., 2018), (Alabdulatif et al., 2019), (Butpheng et al., 2020), (Ramesh & Govindarasu, 2020), and banking (Ren et al., 2021) to enhance data security and privacy. We will evaluate the performance of the two most successful FHE schemes: Brakerski/Fan-Vercauteren (BFV) (Fan & Vercauteren, 2012) and Cheon, Kim, Kim, and Son (CKKS) (Cheon et al., 2017), used in TenSEAL (Benaissa et al., 2021) and PyFHEl (Ibarrondo & Viand, 2021) python base libraries that we have considered in this paper. Their main feature is the use of the residue number system (RNS) for performing operations (Babenko et al., 2020). This is done by determining the execution time of the main functions (encoding, encryption, addition/multiplication operations, decryption, and decoding) in the scheme, thereby determining the most productive scheme.

The majority of the FHE-based IoT data privacy and security models that are currently in use are based on the cloud. There is a need to extend these schemes and models to incorporate edge computing because there is always a possibility for data to be a compromise between the IoT device and the cloud (Ma et al., 2020). Secondly, the overall performance of the BFV and CKKs schemes is affected by certain parameters, which tend to determine and influence the degree of required security, speed and number of mathematical operations done in each scheme (Fawaz et al., 2021). Limited information exists on quantitative comparison as concerns the variation of these parameters according to the various schemes and libraries. This makes different FHE schemes have distinctive advantages (Jiang & Ju, 2022). It is therefore necessary to implement and modify these parameters to determine which schema performs well in a particular scenario.

The remaining sections are structured as follows: Section 2 provides an overview of related works on Fully Homomorphic Encryption (FHE) and introduces two libraries and schemes utilized in this

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/a-comparative-study-of-bfv-and-ckks-schemes-to-secure-iot-data-using-tenseal-and-pyfhel-homomorphic-encryption-libraries/333852

Related Content

Class Distribution Curve Based Discretization With Application to Wearable Sensors and Medical Monitoring
Nicholas Skapuraand Guozhu Dong (2017). *International Journal of Monitoring and Surveillance Technologies Research (pp. 23-37).*
www.irma-international.org/article/class-distribution-curve-based-discretization-with-application-to-wearable-sensors-and-medical-monitoring/204943

Subtle Facial Expression Recognition in Still Images and Videos
Fadi Dornaika, Fadi Dornaika, Bogdan Raducanuand Bogdan Raducanu (2011). *Advances in Face Image Analysis: Techniques and Technologies (pp. 259-278).*
www.irma-international.org/chapter/subtle-facial-expression-recognition-still/43831

An Introduction to Biometrics Image Discrimination (BID)
David Zhang, Xiao-Yuan Jingand Jian Yang (2006). *Biometric Image Discrimination Technologies: Computational Intelligence and its Applications Series (pp. 1-20).*
www.irma-international.org/chapter/introduction-biometrics-image-discrimination-bid/5917

Design and Performance Evaluation of the SCAN Secure Processor
Raghudeep Kannavaraand Nikolaos Bourbakis (2015). *International Journal of Monitoring and Surveillance Technologies Research (pp. 68-91).*
www.irma-international.org/article/design-and-performance-evaluation-of-the-scan-secure-processor/146246

Privacy in Identity and Access Management Systems
Andreas Pashalidisand Chris J. Mitchell (2012). *Digital Identity and Access Management: Technologies and Frameworks (pp. 316-328).*
www.irma-international.org/chapter/privacy-identity-access-management-systems/61542