Chapter 5
Cloud Security Architecture Based on Fully Homomorphic Encryption

Vaishali Ravindra Thakare
https://orcid.org/0000-0002-5148-5672
Vellore Institute of Technology, India

K. John Singh
Vellore Institute of Technology, India

ABSTRACT

Cloud computing is a new environment in computer-oriented services. The high costs of network platforms, development in client requirements, data volumes and weight on response time pushed companies to migrate to cloud computing, providing on-demand web facilitated IT services. Cloud storage empowers users to remotely store their information and delight in the on-demand high quality cloud applications without the affliction of local hardware management and programming administration. In order to solve the problem of data security in cloud computing system, by introducing fully homomorphism encryption algorithm in the cloud computing data security, another sort of information security solution to the insecurity of the cloud computing is proposed, and the scenarios of this application is hereafter constructed. This new security arrangement is completely fit for the processing and retrieval of the encrypted data, successfully prompting the wide relevant prospect, the security of data transmission, and the stockpiling of the cloud computing.

DOI: 10.4018/978-1-7998-0194-8.ch005

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Enterprises are the quick approaching new advanced time in which we store our information and perform our extravagant computation remotely. With the use of cloud there are numerous points of interest in expenses and usefulness, but the issue with the cloud is secret data may not be secure (Bhushan & Reddy, 2016; Bhushan & Pradeep, 2016). Today, enterprises are looking towards cloud computing environment to expand their on-premise infrastructure, but most cannot afford the cost of the danger of trading off the security of their applications and information. Recent advances in Fully homomorphic encryption (FHE) allows us to perform arbitrarily complex dynamically picked computations on encrypted data, despite not having the secret decryption key. Processing encrypted data homomorphically requires greater number of computations than processing the data unencrypted.

Scientifically talked is a homomorphic cryptosystem, a cryptosystem whose encryption function is a homomorphism and thus preserves group operation performed on cipher texts. The two group operations are the arithmetic addition and multiplication (Bhushan & Reddy, 2018, 2016). A homomorphic encryption scheme is said to be additive if the followings holds:

$$E(x+y) = E(x)+ E(y)$$

What's more it is said to be multiplicative if

$$E(x, y) = E(x) * E(y)$$

Where E characterizes an encryption function.

The cryptosystem that support either of the two operations are said to be partially homomorphic encryption system, and the once that supports both the additions and multiplications of cipher texts is called as fully homomorphic encryption (FHE).

Cloud Computing and Fully Homomorphic Encryption

The progression of FHE has empowered the cloud service providers a better approach to ensure confidentiality and privacy of user data. a solution to the old open issue of developing a fully homomorphic encryption scheme. This idea, formerly called a privacy homomorphism, was presented by Rivest, Adelman and Dertouzous (Rivest, Adleman & Dertouzos, 1978; Poluru et al., 2019) shortly after the invention of RSA by Rivest, Shamir and Adleman.

To provide the better security we are going to extend the security solution for cloud computing with the help of fully homomorphic encryption cryptosystem.

5 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/chapter/cloud-security-architecture-based-on-fully-homomorphic-encryption/236442

Related Content

A Case Study of the Health Cloud
Roma Chauhan (2014). *Cloud Computing Applications for Quality Health Care Delivery (pp. 272-283).*
www.irma-international.org/chapter/a-case-study-of-the-health-cloud/110439

Elastic Application Container System: Elastic Web Applications Provisioning
Sijin He, Li Guoand Yike Guo (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications (pp. 920-942).*
www.irma-international.org/chapter/elastic-application-container-system/119890

From Cloud Computing to Fog Computing: Platforms for the Internet of Things (IoT)
Sanjay P. Ahujaand Niharika Deval (2018). *International Journal of Fog Computing (pp. 1-14).*
www.irma-international.org/article/from-cloud-computing-to-fog-computing/198409

Application of Artificial Intelligence in Cybersecurity
Geetika Munjal, Biswarup Pauland Manoj Kumar (2024). *Improving Security, Privacy, and Trust in Cloud Computing (pp. 127-146).*
www.irma-international.org/chapter/application-of-artificial-intelligence-in-cybersecurity/338352

Development of Community Based Intelligent Modules Using IoT to Make Cities Smarter
Jagadish S. Kallimani, Chekuri Sailusha, Pankaj Latharand Srinivasa K.G. (2019). *International Journal of Fog Computing (pp. 1-12).*
www.irma-international.org/article/development-of-community-based-intelligent-modules-using-iot-to-make-cities-smarter/228127