Conferences >2024 International Conference...

Homomorphic Encryption for Genomics Data Storage on a Federated Cloud: A Mini Review

Publisher: IEEE

Philip Ewejobi; Kennedy Okokpujie; Emmanuel Adetiba; Babatunde Alao

Abstract

Document Sections

-

Show Full Outline
Authors
Figures
References
Keywords
Metrics

Abstract:
This paper provides an analysis and review of the fundamental aspects of securing genomics data on a federated cloud. It highlights the concept of cloud computing and the security issues associated with it. Furthermore, the concept of genomics, ethical and privacy concerns relating to genomics data, and existing attacks on genomics data. Various cryptographic approaches to data breach the importance of employing homomorphic encryption schemes to safeguard genomics data. It discusses security issues in cloud computing, the concept of federation in cloud computing, the genomics concept and cryptographic approaches for protecting genomics data.

Published in: 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)

Date of Conference: 02-04 April 2024

Date Added to IEEE *Xplore*: 15 August 2024
ISBN Information:

DOI: 10.1109/SEB4SDG60871.2024.10630232
Publisher: IEEE

Conference Location: Omu-Aran, Nigeria
Funding Agency:

I. Introduction

In the contemporary landscape, the proliferation of cloud-related activities has surged, leading to a substantial expansion in sensitive information. This surge is fuelled by the rapid growth of interconnected devices, laboratory equipment, genomics data, and cloud computing, catalysing advancements in bioinformatics and the economy. However, this intertwined growth also amplifies cybersecurity and information security challenges [1]. Cloud security issues have surfaced due to the presence of unauthorized users, often referred to as intruders, engaging in malicious activities. These intruders primarily seek to access confidential data [2]. The most daunting challenge in cloud data security is the realization that attackers often outpace organizations, exploiting security vulnerabilities overlooked by company employees. Moreover, the swift evolution of new technologies, particularly cloud and mobile, presents additional hurdles. Attackers adeptly adapt to and exploit these technologies, necessitating cybersecurity experts to remain vigilant and anticipate their tactics. Many security measures concentrate on detecting malware and preventing breaches, leading to a reactive approach rather than proactive measures against current and future threats [3].

Sign in to Continue Reading
Authors
Figures
References
Keywords
Metrics

More Like This

A Unique Textbook for Teaching Courses in Bioinformatics [review of Discovering Genomics, Proteomics, and Bioinformatics, 2nd ed. (Cummings, B.; 2006)]

Computing in Science & Engineering

Published: 2008

Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing

IEEE Access

Published: 2024