

Chapter 86

Security Risks of Biomedical Data Processing in Cloud Computing Environment

Babangida Zubairu
Jaipur National University, India

ABSTRACT

The emergence of new innovations in technology changes the rate of data generated in health-related institutions and the way data should be handled. As such, the amount of data generated is always on the increase, which demands the need of advanced, automated management systems and storage platforms for handling large biomedical data. Cloud computing has emerged as the promising technology for present and future that can handle large amount of data and enhance processing and management of the data remotely. One of the disturbance concerns of the technology is the security of the data. Data in the cloud is subject to security threats, and this has highlighted the need for exploring security measures against the threats. The chapter provides detailed analysis of cloud computing deployment strategies and risks associated with the technology and tips for biomedical data storage and processing through cloud computing services.

INTRODUCTION

Cloud computing environment enables sharing of computing resources and accessing services supported by the technology through the internet; the client of the technology can benefit from tremendous advantages offered by the technology such as boundary less accessibility of remotely stored data. The stored data can be accessed via any computing devices that can support internet connectivity such as PC and smart phone. The merits of this technology can benefit every sector of human endeavors, such as biomedical data handling, one of the challenging issues is the security of the data stored in the cloud environment, the threats can be from the malicious user behavior in the process of data accessing or other form of threat that disturb the functionality of the technology. Due to the sensitivity and concern about biomedical data in the cloud environment, a robust security measures are required for proper

DOI: 10.4018/978-1-5225-8176-5.ch086

storage, delivery and processing of the data. The chapter intends to highlight and digests the security threats that can hinder the processing of biomedical data in the cloud environment and presented the countermeasures against the threats. The chapter also presents details of the merits and demerits of the services supported technologies to the organization and individual that handles data, such as biomedical one and envisaging migrating to the cloud computing. Some vital tips were presented for enhancing the technology deployment, data storage, retrieval and integration for successful delivery of biomedical data processing in the cloud environment.

BACKGROUND

Computers are used in biomedical and health related fields to support data storage, analysis, and integration of biomedical and genetic information. Now a day more advanced technologies are being evolved, the sophistication and advancement of the high throughput technologies will significantly influence more biomedical data generation. This reveals that the ability to measure, store, manage and process precise data on individuals will surpass the capabilities of traditional datacenter of organizations. Enhanced quantitative evaluation and analysis of individual data and qualities become possible due to the advancement in technologies, thereby waiving limits and increases opportunity for advanced studies and evaluation of combined factors that can predict disease and care. As more advanced technologies become available, the demands of handling volumes of increasingly detailed data and analysis may lead to potential increases for drawing erroneous conclusions about the data. This shows the need of an advanced automated system for management, retrieval, and interpretation of biomedical and health related data such as cloud computing technology. Some online database system of nucleic acid exists such as European Molecular Biology Laboratory (EMBL), Gen Bank and DNA databank of Japan, but these databases are not enough to suit the demand of most organizations in biomedical data management. For instance, EMBL is managed by the European Bioinformatics Institute in the UK to support research in molecular biology; GenBank is maintained by the National Center for Biotechnology Information (NCBI) in the US for nucleotide sequences and their protein translations. The DNA Databank is maintained by the National Institutes in Genetics in Japan for the analysis of genetic diseases and genetic fingerprinting for criminology and genetic genealogy (Francesco, Giuliana, & Luigi, 2009). The mentioned online databases may only complement the need of some organizations not all. Therefore, the need for other research institutions and organization handling biomedical data to migrate to cloud technology becomes inevitable; this will provide the avenue for data sharing with other research community around the globe. Securing data is the paramount need of most organizations, peer to peer (P2P) novel technique was presented by (Mohammad, & Adnan, 2018), the approach integrates the P2P with the caching technique and dummies from real queries, this helps in preserving privacy and security of data, Cloudlets technologies were presented by (Panigrahi, Tiwary, Pati, & Das, 2016) as the solution to big data analysis for areas that face low internet connectivity and devices disruptions, the technologies can be useful if employed to manage and process big data in the cloud computing environment. However, watermarking technique was proposed using Odd-Even Method for insertion and extraction of watermark in a bio medical image with large data hiding capacity, security as well as high watermarked quality (Kumar, Nilanjan, Sourav, Achintya, & Sheli, 2014). Similarly, Interpolation and trigonometric techniques were proposed by (Sayan, Prasenjit, Arijit, Debalina, & Nilanjan, 2014) for insertion and extraction of watermark in digital image, this accomplish by embedding secrete bits key into the gray planes of color image.

19 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/security-risks-of-biomedical-data-processing-in-cloud-computing-environment/224655

Related Content

A Study on the Performance and Scalability of Apache Flink Over Hadoop MapReduce

Pankaj Latharand K. G. Srinivasa (2019). *International Journal of Fog Computing* (pp. 61-73).

www.irma-international.org/article/a-study-on-the-performance-and-scalability-of-apache-flink-over-hadoop-mapreduce/219361

Artefact Consistency Management in DevOps Practice: A Survey

Dulani Meedeniya, Iresha Rubasingheand Indika Perera (2020). *Tools and Techniques for Software Development in Large Organizations: Emerging Research and Opportunities* (pp. 98-129).

www.irma-international.org/chapter/artefact-consistency-management-in-devops-practice/247540

Session Hijacking Over Cloud Environment: A Literature Survey

Thangavel M., Pandiselvi K.and Sindhuja R. (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 1984-2013).

www.irma-international.org/chapter/session-hijacking-over-cloud-environment/224667

Monitoring and Detecting Plant Diseases Using Cloud-Based Internet of Things

Taranjeet Singh, Devendra Singhand S. S. Bedi (2021). *Integration and Implementation of the Internet of Things Through Cloud Computing* (pp. 217-235).

www.irma-international.org/chapter/monitoring-and-detecting-plant-diseases-using-cloud-based-internet-of-things/279484

Examining IoT's Applications Using Cloud Services

Saravanan Kand P. Srinivasan (2018). *Examining Cloud Computing Technologies Through the Internet of Things* (pp. 147-163).

www.irma-international.org/chapter/examining-iots-applications-using-cloud-services/191837