J Forensic Res 2015, 6:5
http://dx.doi.org/10.4172/2157-7145.C1.018

OMICS International
conferenceseries.com

4th International Conference on
Forensic Research & Technology
September 28-30, 2015 Atlanta, USA

Computational forensics techniques in the era of big data: Cloud security and privacy

Gebeyehu Belay Gebremeskel[1], **Derbe Roba Dagne**[2] and **Yi Chai**[1]
[1]Chongqing University College of Automation, China
[2]Chongqing Mexin Property Management Co. Ltd, China

Purpose: Managing big data security and privacy as distributed computing environments and cloud-based infrastructures are high-tech technology and challenging. It demands advancing and scientific or digital investigating methodology via augmenting forensic science and techniques. The issues are how to secure and safe users and cloud providers in the cloud ecosystem. How to use computational forensics techniques for cloud big data and its performance analysis? What improvement is needed for live analysis techniques for the better of big data applications? How to improve large-scale data analysis techniques using computational forensics? These issues are impossible to address using traditional security mechanisms which are tailored to securing small-scale static data. Conventional approaches are inadequate the use of large-scale cloud infrastructures with a diversity of software platforms, spread across large networks of computers, also increases the attack surface of the entire system. Therefore, the aim of this paper is to investigate these and other related issues to improve big data applications, security and privacy matters in the cloud systems.

Method: The method is augmenting computational forensics techniques in the field of big data to demystifying cloud security and privacy challenges. It is the technique of analyzing large-scale and federated data of certain features and quantizes the likelihood that a well-known source has created it using various forensic techniques.

Results: The approach is discussed the existing big data security and privacy challenges. In this research, we introduced a novel and generic methodology of computational forensics engineering and present a set of techniques that can adopt and scale up to various related issues. We are also proposing a dynamic analytic approach for feature and statistical data collection, extraction, entity clustering and validation. We also discussed in details how big data within the cloud protection and paradigm applications.

Scope & Limitation: The research focused on big data technology towards cloud security and privacy using forensic techniques. The details about cloud computing architecture, applications and challenges did not include in this work.

Originality: Proponents of the big data cloud ecosystem tout its vastness, flexibility and scalability as advantages for the implementation of cloud services. However, from security and privacy point of view, this can be a veritable security and privacy challenge which demands dynamic and paradigm computational forensics techniques. It is vitally essential to gather and analyze any fraud detections in terms of time, location and various computing techniques. The benefit of forensics for big data cloud security is a fundamental to establish and map computational and storage structures, which support the scope and realm of risk management. The computational forensic technique is capable and adaptable to cope with security and privacy challenges by trying to identify the tool used to generate a particular big data cloud safety. The developed computational forensics technique tool identifies one from a pool of synthesis tools that has been used to generate a particular optimized design.

Gebeyehu@cqu.edu.cn
chaiyi@cqu.edu.cn
derbe.r@yahoo.com