Chapter 21
A Forensic Way to Find Solutions for Security Challenges in Cloudserver Through MapReduce Technique

D. Usha

Dr. M. G. R Educational and Research Institute, India

Reshma Raman

Dr. M. G. R Educational and Research Institute, India

ABSTRACT

Cloud computing is a large and distributed platform repository of user information. But it also extensively serves the security threats in the research aspect. This chapter attempts to find the solution to the security challenges through the MapReduce technique in a forensic way. Four security challenges are included in this chapter: losing the user information during the mapping process for different reasons such as the shutdown of the server, which causes parallel or unrelated services to get interrupted; the velocity of attack, which enables security threats to amplify and spread quickly in the cloud; injecting malicious code; and finally information deletion. MapReduce and dynamic decomposition-based distributed algorithm with the help of Hadoop and JavaBeans in the live forensic method is used to find solution to the problem. MapReduce is a software framework and live forensics is the method attempting to discover, control, and eliminate threats in a live system environment. This chapter uses Hadoop's cloud simulation techniques that can give a live result.

INTRODUCTION

An essential idea behind cloud computing is the placement of the service, and lots of the main points like the hardware or software package on that it's running, area unit for the most part inappropriate to the user. These 'time-sharing' services were for the most part overhauled by the increase of the computer

that created owning a laptop rather cheaper than successively by the increase of company information centers wherever firms would store huge amounts of knowledge. MapReduce has emerged because of the preferred computing framework for giant processing because of its easy model and parallel execution. MapReduce and Hadoop concepts are implemented by top companies like Yahoo, Google and Facebook for tremendous applications which include machine learning, bioinformatics and cyber security. Security is the term which safeguards all the information from malicious activities. The intruders or hackers were used as the backdoor or loopholes or vulnerabilities. During this paper ascertain the answer for a few security challenges that area unit within the cloud server that will be with the assistance of the newer technology massive information and MapReduce. Mainly in this paper discuss the challenges that are in a cloud environment and others also. Losing the information during the mapping process such as shut down the computer, the velocity of attacking, infecting malicious code, and finally information deletion. The rest of the paper is organized as follows. In section II, literature review, Section III, we review the existing model and its disadvantages also. Section IV explains the security issues in cloud and Section V presents a proposed system and methodology. The experiment results are discussed and finally, Section VI concludes the paper.

LITERATURE SURVEY

Some methods have been proposed in literature for handling security issues in organizations implementing cloud computing. (Yu,W., Xu,G., Chen,Z., & Moulema,P.,2013) discussed security issues, requirements and challenges that cloud service providers (CSP) need to address in cloud engineering: Security issues describe the problems encountered during implementation of cloud computing(CC). Security standards provide some security templates, which are mandatory for cloud service providers. The Open Visualization Format (OVF) is a standard for creating new business models that help the company to sell a product on premises, on demand, or in a hybrid deployment model. Security management models are designed based on the security standards and best practices.

(Wang,J., Crawl,D., Altintas,I., Tzoumas,K., & Markl,V.,2013) addressed countermeasures (anti-viruses, intrusion detection systems) developed to mitigate well-known security threats. The focus is mainly on anomaly-based approaches which are mostly suited for modern protection tools and not for intrusion detectors. The pattern-based changes (example: from thin client connected to the main frame or powerful workstations connecting to thin clients) are observed, which cause some simultaneous changes in work environment and new problems to security of CC.

(Mackey,G et al.,2008) mentioned CC's features like reduced total cost of ownership, scalability and competitive differentiation. They claim CC also minimizes complexity and provides faster and easier acquisition of services to customers. Virtualization is the technique used to deal with quality of service (QOS). Usage of CC is considered to be unsafe in an organization. For dealing with this type of situation, they investigated a few major security issues with CC and also existing countermeasures to those security challenges. Advantages for implementing CC from a different point of view are also discussed. They also stated that some standards are required in CC for security.

(Rosen,J et al.,2013) dealt with the security risks faced in the CC. They provided empirical evidence on security risks and issues encountered during deployment of service delivery models in an organization. The service models are placed in cloud and the empirical validation was made in order to justify

7 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/a-forensic-way-to-find-solutions-for-security-challenges-in-cloudserver-through-mapreduce-technique/301836

Related Content

Digital Mastery: The Skills Needed for Effective Virtual Leadership
Shelly R. Roy (2012). *International Journal of e-Collaboration (pp. 56-66).*
www.irma-international.org/article/digital-mastery-skills-needed-effective/68166

The Interaction Between Technologies, Techniques, and People in Higher Education Through Participatory Learning
Vijaya Lakshmi Daraand Saradha M. (2022). *Handbook of Research on Technologies and Systems for E-Collaboration During Global Crises (pp. 339-356).*
www.irma-international.org/chapter/the-interaction-between-technologies-techniques-and-people-in-higher-education-through-participatory-learning/301837

Using Social Networking Analysis to Facilitate Knowledge Sharing in the British Council
Bonnie Wai-yi Cheuk (2009). *E-Collaboration: Concepts, Methodologies, Tools, and Applications (pp. 833-841).*
www.irma-international.org/chapter/using-social-networking-analysis-facilitate/8833

Evolving Gender Communication Issues in E-Collaboration
Cathy L.Z. DuBois (2008). *Encyclopedia of E-Collaboration (pp. 259-264).*
www.irma-international.org/chapter/evolving-gender-communication-issues-collaboration/12435

Standardization in User Modeling and Learning Objects Retrieval: Recent Contributions
Sotirios Botsiosand Dimitrios Georgiou (2010). *Monitoring and Assessment in Online Collaborative Environments: Emergent Computational Technologies for E-Learning Support (pp. 22-40).*
www.irma-international.org/chapter/standardization-user-modeling-learning-objects/36841