Visvesvaraya Technological University Belagavi,

Karnataka – 590018

Report on

PLAGIARISM REPORT ON CLOUD COMPUTING

Submitted in partial fulfillment of the requirements for the course

CLOUD COMPUTING AND ITS APPLICATION

(18CS642)

Submitted by

Prithviraj Patil	1JS19CS125
Nandan J S	1JS19CS096
Srinivas S Rathod	1JS19CS173

Under the guidance of

Dr. Bhavani B H

Assistant professor, Dept. of CSE,

JSS Academy of Technical Education, Bengaluru

JSS Academy of Technical Education, Bengaluru – 560060,

Department of Computer Science and Engineering

2021-2022

CONTENTS

Paper 1: Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study

Abstract

The trend of cloud computing is accelerating along with emerging technologies such as utility computing, grid computing, and distributed computing. Cloud computing is showing remarkable potential to provide flexible, cost effective, and powerful resources across the internet, and is a driving force in today's most prominent computing technologies. The cloud offers the means to remotely access and store data while virtual machines access data over a network resource.

Problem

Data security threats can be categorized as external or internal in the cloud environment. Internal threats occur mainly from insider attacks, and external threats from outside attacks as data is accessed by a third party. Attackers can obtain the personal information of a user. The cloud infrastructure should be scalable to ensure availability of data. Six major security issues are listed below :

- Data integrity
- Data privacy and confidentiality
- Location of data
- Availability of data
- Data storage, backup, and recovery ● Data authentication..

Key Idea

However, cloud service providers have not been providing enough secure and reliable services to end users. Blockchain is a technology that is improving cloud computing. This revolutionary technology offers persuasive data integrity properties and is used to tackle security problems. This research presents a detailed analysis of privacy and security challenges in the cloud.

Novelty

Nature of problem	Suggested solutions
● Data confidentiality. ● Web Service Security. ● Uncertainty in service of reliabil ● Unauthorized access to infrastructu components. ● Illegitimate access. ● Eavesdropping and alteration. ● Unauthorized access. and ● Malicious attacks. ● Loss of data integrity confidentiality. ● DDoS ● Data forgery	● Hashing and encryption. ● SSL/TSL for client authentication. ● Authorization and authentication. ● Fragmentation redundancy and scattering techniques. ● Enforcement of access policies. ● Proper integration and confidentiality mechanism. ● Application of one-way hash function. ● Cryptographic techniques. ● Standard cryptographic algorithms. ● Fuzzy logic-based mechanism ● IPS and IDS

Critique

We studied its security and privacy through a case study in a smart campus scenario. We seek to highlight the major security vulnerabilities in cloud computing since it has become the most commonly used method of virtualization in large and modern data centers and cloud infrastructures. The major threats and open security issues are a breach of data, IP spoofing, ARP spoofing, DNS poisoning, injection with SQL, injection with OS, LDAP injection, orchestration of the cloud, and zombies or DDoS. Jain and Jaiswal emphasized cloud security parameters: cloud network, database, operating system, virtualization, resource allocation, transaction management, load balancing, memory management, and concurrency control.

Paper 2: Resolving The Security and Data Concerns in Cloud

Computing by Utilizing Decentralized Cloud Computing Option

Abstract

There are a variety of security concerns around cloud computing infrastructure technology. Some of these include infrastructure security against threats, data privacy, integrity, and infrastructure stability. In modern cloud computing, there are two models that cloud computing infrastructures follow: centralized cloud computing and decentralized cloud computing. Centralized cloud computing is susceptible to outages, data breaches, and other security threats. Decentralized cloud computing is more resilient to outages due to georedundancy technology, and data is better protected by encryption through Reid Solomon erasure coding.

Problem

Regardless of the type of cloud computing infrastructure, users and enterprises alike are heavily concerned with a variety of security concerns, both regarding cybersecurity attacks, data privacy and integrity, and cloud computing infrastructure stability. Since cloud computing resources can be accessed from around the world, data privacy is often the foremost concern of users and enterprises.

Key Idea

There are a variety of security concerns around cloud computing infrastructure technology. Some of these include infrastructure security against threats, data privacy etc. These problems could be tackled by implementing the decentralized models of cloud computing technologies.

Novelty

There are new types of cybersecurity threats emerging every day as new technology develops and evolves. Cloud computing is not immune to traditional cybersecurity threats, and in fact, is more susceptible to certain types of threats.

Phishing: Phishing refers to the practice of sending fraudulent information or messages that appear to be from genuine, trusted sources in an attempt to elicit sensitive information from the target.

Ransomware: Ransomware refers to malicious computer programs or software that prevent the user from using the computer or workstation until a sum of money or another demand is relinquished.

Trojan: In Cybersecurity, Trojan refers to a malicious computer program or software that is packaged to appear as if it is a useful, legitimate piece of software but in the background runs malicious processes meant to record sensitive information and relay it back to the distributor.

Botnet: A botnet refers to a private network of computers that have all been infected with a harmful or malicious piece of software and controlled in unison for unwanted activity such as mass distribution of spam messages.

Distributed Denial of Service: A distributed denial of service attack refers to a malicious attack meant to disturb a network service or resource by flooding the resource with inbound requests to overload its resources and make it unavailable to legitimate requests.

Crypto-mining: Crypto-mining refers to the practice of using computers for the mining of cryptocurrency without the user's knowledge. This results in a monetary gain for the party who deployed the crypto mining malicious software.

Critique

A decentralized cloud computing infrastructure does not provoke the same stability concerns that the centralized cloud computing model does. Decentralized cloud computing infrastructures use geo-redundant resources, which means that if one resource or region goes down, traffic is routed to another region where data and resources are still accessible and available.[3] This is because decentralized cloud computing replicates resources and data across different locations automatically, eliminating outages unless a significant amount of the locations are experiencing outages. Each location is often located in drastically different places than the other locations, such as in entirely different locations rather than just different buildings. This means there is no single point of failure for a decentralized cloud computing infrastructure, giving decentralized cloud computing high stability in comparison to traditional centralized cloud computing infrastructures.