International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

COPY RIGHT

ELSEVIER

SSRN

IJIEMR Transactions, online available on 26th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 12

10.48047/IJIEMR/V11/ISSUE 12/85

Title A CRITICAL STUDY ON CONCEPT, TRAITS, & MODELS IN TERMS OF CLOUD COMPUTING

Volume 11, ISSUE 12, Pages: 669-673

Paper Authors **Susanta Kumar satapathy, Dr.Prateek Mishra**

International Journal for Innovative Engineering and Management Research

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

A CRITICAL STUDY ON CONCEPT, TRAITS, & MODELS IN TERMS OF CLOUD COMPUTING

Name- Susanta Kumar satapathy

DESIGNATION- RESEARCH SCHOLAR SUNRISE UNIVERSITY ALWAR

Guide name - Dr.Prateek Mishra

DESIGNATION- Associate professor SUNRISE UNIVERSITY ALWAR

ABSTRACT

When it comes to providing a wide range of services to a large number of people at low cost, cloud computing has emerged as a game-changer. While its use has grown rapidly, so have worries about data breaches, insecure cloud models, and other security flaws This abstract includes research on the fundamentals of cloud computing, including the many cloud models, key security issues, and the difficulties associated with data breaches in the cloud. The research starts out by looking at public, private, hybrid, and multi-cloud deployment options. Decision-makers will benefit from an examination of the relative merits of various cloud computing models with respect to aspects like availability, cost, and data sovereignty. The many benefits of cloud computing and the inherent security risks it offers are both discussed in the abstract. Cloud service providers and consumers alike continue to be very concerned about security. The inquiry looks at commonplace dangers including data leaks, insider assaults, DDoS attacks, and unauthorized access. Additionally, the hazards of using untrusted cloud services and the dangers of sharing data are investigated in the research.

Keywords: - Cloud, Service, Public, Private, Hybrid.

I. INTRODUCTION

DISTINCTIVE CLOUD MODELS

Public clouds, private clouds, hybrid clouds, and even multiple clouds are just some of the deployment types available for cloud computing. Each variant is designed to meet a certain need and comes equipped with its own set of features. Public cloud services are those offered by an external supplier and made available to a wide range of users through an online network. Private clouds, on the other hand, are only used by one company at a time, giving that company more authority and safety. Hybrid cloud blends the scale of the public cloud with the privacy of a private cloud, providing the best of both worlds for businesses. Using various cloud service providers allows businesses more freedom from being tied to one source and more agility in meeting changing demands.

Threats to Critical Infrastructure

Despite the many advantages, businesses must be mindful of the security risks associated with cloud computing. Unauthorized access to private information is a major cause for alarm. When sensitive information is kept and processed on distant servers that are handled by third-party providers, there is a chance that it may get into the hands of criminal actors. Organizations might also be vulnerable to security breaches due to cloud infrastructure vulnerabilities or incorrect setups.

Communication Problems

Concerns about information leaks in the cloud may be broken down into three categories: confidentiality, integrity, and availability. As was previously noted, data breaches may result in the disclosure of sensitive information, which can have serious financial, reputational, and legal repercussions.

II. OVERVIEW

Cloud computing is one of the most impressive technological developments in recent years. While there are many benefits to using Cloud Computing, like scalability, quick flexibility, measurable services, and most importantly the possibility for cost savings to companies, there are also security threats that must be ignored. Organizations are reluctant to accept the otherwise potent environment known as cloud computing due to the security threats arising from the large variety of vulnerabilities inherent in any Cloud computing system. Cloud computing's adaptability, the protection of sensitive information, and the ease of data access and modification are just few of the areas that might be affected by a thorough security and risk assessment. As a result, every cloud-based company operations must prioritize the determination of the most effective solution instructions to bolster security and privacy in the cloud environment.

In this research, we investigate and evaluate the most common threats to cloud infrastructure, including those posed by hackers to your data and your network. Prevalent attacks on cloud networks have been found to include DoS (DDoS, XDoS, HDoS) and Man-in-the-middle attacks. Additionally, the most prevalent and famous data security assaults on the web of cloud networks are Malware injection attacks, which may be broken down into two categories: SQL injection and Cross Site Scripting (XSS) attacks. Our research is narrowly focused on Distributed Denial-of-Service attacks; we want to provide preventive 2 techniques and recommendations for data protection against malware injection assaults. Our third goal is to learn why people are hesitant to utilize Cloud services, and we will base our efforts on this hypothesis.

III. CLOUD COMPUTING

Concept of Cloud Computing

Modern large-scale distributed systems are exceptional in their complexity, interoperability, consistency, and scalability. This is due to the fact that during the last 50 years, researchers in many different domains have produced new theories, models, and methods for doing things like computer architecture, networking, and parallel or distributed computing. Here, we provide an overview of the process that led to the present state of affairs and the major turning points along the way. To be clear, this is not intended to be an all-inclusive list. This section is divided into chronological sections, with summaries of major developments within each segment serving as background.

It was during the rise of the mainframe computer in the 1950s that the concept of the "Cloud" was first coined. In 1961, John

McCarthy foresaw a future in which computers may operate on a utility paradigm like to that of electricity or water. While the idea of cloud computing has been around since the early 1990s, no one paid much attention to it until recently. The term "cloud computing" was first used by NetCentric in 1977. In a 2001 New York Times article, cloud computing was initially defined by John Markoff.

E-commerce firms like Amazon, Google, and others invested millions updating their server infrastructure after seeing a major spike in web traffic in the late '90s. Due to the non-uniform and time-varying nature of their workload and resource utilization, businesses realized that consolidating the various capacities with the free practice outlines could improve the server efficiency and could become a viable financial archetype to lease the assets to the community. In March of 2006, Amazon introduced its elastic computing cloud capabilities, which made it easier for web developers to use cloud-based services by providing scalable cloud-based processing capacity. In October 2007, Google and IBM promoted cloud computing as a means of reducing the expense of conducting hypothetical research utilizing many remotely located machines.

IV. TRAITS OF CLOUD COMPUTING

In order to get a firm grasp on the common ideas and understandings surrounding the cloud, we can look at the NIST's definition of a cloud-based system as an overarching prototype for providing metered on-demand services, and then extrapolate the following five principal characteristics. Some of the most important details are summarized here.

- **On demand self-service:** Customers may make purchases of property without needing to interact with a live person. It's the gold standard for self-sufficient machines.
- Access to a large network is maintained through the same protocols used on the Internet.
- Multiple tenants may share the same set of hardware, software, networking, and other resources under the multi-tenant model. Due to its use of virtualization technology, it allows for the coexistence of many operating systems on the same hardware. When there is no physical barrier between tenants, security becomes an issue.
- Flexibility: the assets may be given up or released with the minimum amount of effort required. This ensures that our supplies will always be there when we need them. A cloud system's resources can only be truly elastic if they are both scalable and reliable.
- Usage-based billing/reporting/billing (also known as "metered service") occurs when a cloud service provider (CSP) monitors and controls how its cloud clients use their resources, issues reports specific to each service type, and charges consumers accordingly. Therefore, it is crucial to give due consideration to the need for verification and accountability.

- In addition to these unique benefits, Cloud also offers:
- The cloud service provider uses a common pool of resources to serve several customers without requiring any of them to pay anything up advance.
- All it takes to switch ownership is a simple request (supply resources proportionally to the highest load and releases when service demand is low), hence this model has a low operating cost.
- Extreme scalability: both bandwidth and storage may be expanded to previously unheard-of proportions.
- Moderate access: a range of devices with internet connectivity.
- Workplace dangers are reduced because to the infrastructure service provider's superior risk management expertise.

V. CONCLUSION

The scientific and business sectors are starting to pay more attention to Network cloud because of its growing significance. Data access and storage have already begun to undergo a revolution thanks to cloud computing. Some of the most pressing difficulties with cloud computing in networks are security-related. Security concerns needed to be handled in order to promote cloud computing in a variety of apps. Due to hackers' constant attempts to take advantage of security flaws in the cloud architecture, data breaches of cloud services rise every year.

In this study, security is seen as a crucial element that should be monitored between business infrastructure and cloud service providers. It is associated with authorisation and access control. This research focused on the rights, volume of data that the organization stores in the cloud, and safe data storage and retrieval.

Numerous encryption techniques were investigated in this study for data leaks prevention and detection (DLPD), which may provide intrigue security against any number of plotting clients. Due to the fact that prior studies only used one encryption method, there are still several research difficulties and possibilities that call for more research efforts. However, in the suggested approach, the client would utilize an image to save data on the server. To get the secret key needed to apply the AES algorithm to the data streams for encryption, the RSA method is implemented on the picture. Now, storing these encrypted data streams on the server is safe. To improve security and DLPD, it is also advised to store these streams on several cloud servers. Additionally, it will aid in load balancing.

REFERENCES

1. Tianfield, Hua. (2012). Security issues in cloud computing. 1082-1089. 10.1109/ICSMC.2012.6377874.
2. Vistro, Daniel & Rehman, Attique & Mehmood, Sajid & Idrees, Muhammad & Munawar, Adeel. (2020). A LITERATURE REVIEW ON SECURITY ISSUES IN CLOUD COMPUTING: OPPORTUNITIES AND CHALLENGES. Journal of Critical Reviews. 2020. 10.31838/jcr.07.10.282.

3. Salehi, Waleed & Noori, Fakhruddin & Saboori, Raisa. (2019). Cloud Computing Security Challenges and its Potential Solution. Volume-8. 165-175.
4. Khan, Shafat. (2019). Cloud Computing: Issues and risks of Embracing the Cloud in a Business Environment. International Journal of Education and Management Engineering. 9. 44-56. 10.5815/ijeme.2019.04.05.
5. Majadi, Nazia. (2013). Cloud Computing: Security Issues and Challenges. International Journal of Scientific and Engineering Research. 4. 1515-1520.
6. S, Srinivasan & Kothandaraman, Raja. (2014). Security Issues and Challenges in Cloud Computing.