UGC APPROVED JOURNAL - 47746

© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed

ISSN : 2454 – 308X | Volume : 03 , Issue : 10 | October – December 2017

Cloud Computing and challenges in the present scenario : A review

Pooja Bansal

Email id poojasinghal273@gmail.com

Abstract

Unlike other computer technologies, cloud computing is a new one. At any given moment, a user may access a cloud computing bundle of resources. New kinds of service delivery might be enabled by cloud computing in the future. Modern technologies and price options have a profound effect on the way businesses are conducted. There is nothing new about cloud computing; it is just a new moniker for an old concept. Consumers may access computer resources in the cloud via the services offered by cloud service providers. Data centres throughout the globe host cloud services. It is possible to access virtual resources through cloud computing. The topic of cloud computing has lately gained traction. Google Engine, Office 365, and Oracle Cloud are all examples of cloud services. Since cloud computing is becoming more popular, so are the risks.

Key words: Cloud, Computing, Modern, Technology, IaaS, SaaS etc.

Introduction

Using cloud computing, computer resources (including networks, servers, storage, applications, and services) may be deployed and delivered quickly with minimum participation from administrators or service providers. Data centres and business applications are being disrupted by the rise of cloud computing. With this new deployment paradigm, traditional preventive measures are being re-examined for their efficacy and efficiency. Classic preventive methods are being assessed. Similar to how multi-user mainframe security is regarded a applied security, cloud security may be seen as an instance of this concept. External administration is encouraged by the nature of cloud computing, whether it is private or public. Companies that provide cloud computing services have a vested interest in improving security. Bug exploitation and recovery, insider threats and management console security are just a few of the issues that need to be addressed when it comes to data segregation, privacy, and security. Cryptography, PKI, numerous cloud providers, consistent APIs, and increased virtual machine support may all help with cloud security. TDT4 and privilege mechanisms were developed by the crypto and IR groups to meet the system's security and usability

requirements. Security and performance should be the primary goals of a new system design. The following are the system's goals:

- Topic recognition and tracking 2004 is used for effective searching. Getting posts from the index and decrypting them takes a long time.
- This approach uses the privilege mechanism to secure cloud servers.

Private Cloud

This is a private cloud operated by the IT department and placed behind the company's firewall. Using a private cloud over a public one offers several benefits, including more control over corporate and customer data, and less security and regulatory worries.

Public Cloud

"In a public cloud, a service provider makes resources like software and storage accessible to the public over the Internet. Pay-per-use public cloud services are available.

Hybrid Cloud

Others are outsourced to a hybrid cloud. The organisation may employ a public cloud service like Amazon S3 to store archived data, but keep operational client data in-house. To take advantage of the scalability and cost-effectiveness of public cloud computing, businesses might adopt a hybrid approach. This concept is also known as hybrid IT. A good hybrid cloud management strategy includes budgeting, change control, and security. From any of these points, a hybrid cloud deployment combining public cloud and private data centre principles is viable. Choosing the ideal starting point will help the organisation accomplish its goals. A hybrid cloud uses both private and public clouds to complete functions inside a single firm. Public clouds are supposed to be cheaper and more scalable than private clouds, while all cloud computing services should be efficient.

Hybrid cloud models can be implemented in a number of ways:

- All cloud service providers work together to create a single offering.
- One cloud provider offers a complete hybrid cloud solution.
- Organizations that possess private cloud infrastructures utilise public cloud services.

Challenges of Cloud Computing

The only thing holding back cloud computing is security. The rapid growth of cloud computing has raised consumer security concerns. Cloud computing offers many benefits, but it also has risks. The threat of unauthorised users or organisations is

increasing. For this reason, cloud computing has developed a new method of distributing data among numerous users who may then access just the files they need at any moment.

- Clients can't see inside the cloud since it's dark.
- Cloud users have little knowledge of or control over cloud operations.
- Even when the cloud service provider is honest, a malicious system administrator may undermine VM integrity and confidentiality.
- Cloud settings still have traditional and novel data confidentiality, integrity, availability, and privacy concerns.

Literature Review

(Bonguet and Bellaiche 2017) studied *A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing* in which ubiquitous, easy, and on-demand access to a common pool of highly adjustable resources is provided (e.g., networks, servers, storage, applications and services). DDoS and DDoS assaults threaten the availability of Cloud services owing to additional vulnerabilities provided by the Cloud's characteristics, such as multi-tenancy and resource sharing. There are many new forms of DoS and DDoS assaults in Cloud Computing, including XML-DoS and HTTP-DoS attacks, which are investigated in this study.

(Lynch 2011) studied *SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0*in which ubiquitous, easy, on-demand network access to a shared pool of programmable computer resources is enabled (e.g., networks, servers, storage, applications, and services). Cloud computing is a revolutionary technology that can improve collaboration, agility, scale, and availability while lowering costs. To offer an on-demand utility-like allocation and consumption model, the cloud model envisions components that may be swiftly managed, provided, installed and decommissioned.

(Sen 2013) studied *Security and Security and Privacy Issues in Cloud Computing* and found that Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand., while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial. However, as the shape of the cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality,

interoperability, security and privacy issues still pose significant challenges. In this chapter, we describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment.

(Swapna et al. 2016) studied *Performance Evaluation of Fuzzy Integrated Firewall Model for Hybrid Cloud based on Packet Utilization* He discovered that Cloud computing is a wonderful tool for distributing information over the Internet. Cloud security has emerged as network managers face data protection and vulnerability issues while exchanging data on cloud systems. On a hybrid cloud, we may configure the network firewall to prevent unauthorised access to our data. However, the firewall is unable to provide multi-layered, secure access to the cloud network. Using efficient packets might create a delay in accessing hybrid clouds.

(Mallika 2017) studied *A Secured Decentralized Cloud Firewall to achieve Resources Provisioning Cost Optimization and QOS* and found that Cloud computing is becoming popular as the next infrastructure of computing platform in the IT industry. The large volume hardware and software resources pooling and delivered on demand, cloud computing provides rapid elasticity. In this service-oriented architecture, cloud services are broadly offered in three forms: Infrastructure- as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-aService (SaaS). Cloud computing also brings down both capital and operational expenditure for cloud customers by outsourcing their data and business.

(Ullrich et al. 2016) studied *The role and security of firewalls in cyber-physical cloud computing* and discovered that Clouds, as well as cyber-physical systems, are here to stay. In light of these shifting paradigms, it is critical to rethink security. Clouds eliminate zonal networks and redirect internal traffic to the Internet. Because many physical pieces were initially designed to be stand-alone, cyber-physical systems are vulnerable to cyber assaults. With cyber-physical cloud computing comes a new level of security. Firewalls are an essential component of network security and are supplied by many cloud providers, however their effectiveness is questioned. We compare five major cloud providers' firewall offerings for cyber-physical system integration. So we examine their

default settings, configuration options, documentation, and filtering behaviour. We created an extendible firewall monitoring tool that lets clients look into their provider's filtering activity for risk management or security purposes.

(Yan et al. 2011) studied *The Research and Design of Cloud Computing Security Framework* and found that discovered Cloud computing has grown rapidly in recent years. Despite the fact that security issues have hampered the growth and popularity of cloud computing, their relevance and urgency cannot be disregarded. A cloud computing security paradigm that successfully solves these difficulties is proposed in this study. It is noted that only by addressing the security issues can cloud computing continue to grow in popularity and applicability.

(Yeasmin et al. 2018) studied *Performance evaluation of multi-cloud compared to the single-cloud under varying firewall conditions* The primary goal of this article is to compare multi-cloud network performance versus single cloud network performance under various firewall settings. This project's simulation tool is Riverbed Modeler, and it's a series of projects. There are four projects: single cloud with single server, single cloud with multiple servers, and multiple clouds with multiple servers. In the first project, there are two possible outcomes: no cloud firewall protection, or a firewall that admits all essential traffic. The second, third, and fourth projects simulated no cloud security, true firewall security, and a firewall solution that discards web traffic.

Security of Digital Data in Cloud using Encryption mechanism

Cloud data has been encrypted on many instances. Alternatively, cryptography is the study of secure communication methods that only the sender and recipient can read. The origin of the English word kryptos is the Greek word kryptos. They have everything they need to decipher and understand intercepted data. The suggested research compares polynomial encryption to RSA and AES.

Conclusion

Cloud computing is now defined and discussed in many ways throughout the ICT sector. Cloud computing is defined as having a server corporation that can host services for people linked via network. Computing, communication, and networking advancements have shifted technology in this direction. Cloud computing requires fast and dependable connection. Cloud computing is undeniably one of today's most appealing technological sectors, owing to its low cost and high flexibility. Cloud computing worries are stifling

momentum and jeopardising the concept of cloud computing as a new IT procurement paradigm. Despite the hyped financial and technological benefits of cloud computing, many prospective customers have yet to sign up, and those who do mostly utilise it for less sensitive data". Contrary to the initial promise of cloud computing, when cloud implementation is irrelevant, lack of control equals transparency.

References

1. Bonguet, Adrien, and Martine Bellaiche. 2017. A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. *Future Internet* 9(3). doi: 10.3390/fi9030043.
2. Lynch, Liam. 2011. Security Guidance for Critical Areas of Focus in Cloud. *Csa* 0–176.
3. Mallika, T. M. 2017. A Secured Decentralized Cloud Firewall to Achieve Resources Provisioning Cost Optimization and QOS. 5(20):1–6.
4. Sen, Jaydip. 2013. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology Infrastructures* (iv):1–45. doi: 10.4018/978-1-4666-4514-1.ch001.
5. Swapna, Asma Islam, Ziaur Rahman, Md Habibur Rahman, and Md Akramuzzaman. 2016. Performance Evaluation of Fuzzy Integrated Firewall Model for Hybrid Cloud Based on Packet Utilization. *2016 1st IEEE International Conference on Computer Communication and the Internet, ICCCI 2016* 253–56. doi: 10.1109/CCI.2016.7778919.
6. Ullrich, Johanna, Jordan Cropper, Peter Frühwirt, and Edgar Weippl. 2016. The Role and Security of Firewalls in Cyber-Physical Cloud Computing. *Eurasip Journal on Information Security* 2016(1). doi: 10.1186/s13635-016-0042-3.
7. Yan, Xiaowei, Xiaosong Zhang, Ting Chen, Hongtian Zhao, and Xiaoshan Li. 2011. The Research and Design of Cloud Computing Security Framework. *Lecture Notes in Electrical Engineering* 121 LNEE(January 2014):757–63. doi: 10.1007/978-3-642-25541-0_95.
8. Yeasmin, Mahbuba, Nahida Akter, Mohammed Humayun Kabir, and Javed Hossain. 2018. Performance Evaluation of Multi-Cloud Compared to the Single-Cloud under Varying Firewall Conditions. *Cogent Engineering* 5(1):1–13. doi: 10.1080/23311916.2018.1471974.