IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203151 |

Addressing Cloud Computing security issues: A Survey

Monika Kumari[1] , Prof. Rahul Pawar[2]

Student of MCA, Department of Computer Science & IT, JAIN (Deemed-to-be University) Bangalore, India[1]

Assistant Professor, Department of Computer Science & IT, JAIN (Deemed-to-be University) Bangalore, India[2]

ABSTRACT: The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fueled concerns on a critical issue for the success of information systems, communication, and information security. From a security perspective, a few unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result, the aim of this paper is twofold; firstly, to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained. Cloud computing is an emerging technology paradigm that migrates current technological and computing concepts into utility-like solutions like electricity and water systems. Clouds bring out a wide range of benefits including configurable computing resources, economic savings, and service flexibility. However, security and privacy concerns are shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the security community. Addressing these challenges requires, in addition to the ability to cultivate and tune the security measures developed for traditional computing systems, proposing new security policies, models, and protocols to address the unique cloud security challenges. In this work, we provide a comprehensive study of cloud computing security and privacy concerns. We identify cloud vulnerabilities, classify known security threats and attacks, and present the state-of-the-art practices to control the vulnerabilities, neutralize the threats, and calibrate the attacks. Additionally, we investigate and identify the limitations of the current solutions and provide insights of the future security perspectives. Finally, we provide a cloud security framework in which we present the various lines of defence and identify the dependency levels among them. We identify 28 cloud security threats which we classify into five categories. We also present nine general cloud attacks along with various attack incidents, and provide effectiveness analysis of the proposed countermeasures.

KEYWORDS: Vulnerability Management, Data Security, Access Control & Identity Management.

I. INTRODUCTION

The meteoric rise of cloud computing has revolutionized how we access and utilize computing resources. Its on-demand scalability, cost-effectiveness, and flexibility offer a plethora of benefits for businesses and individuals alike. However, this paradigm shift comes with a significant caveat: security.

In this paper, survey of cloud computing security issues. We delve into the inherent vulnerabilities that arise from the very nature of cloud environments, such as multi-tenancy and shared infrastructure. By shedding light on these security challenges, we aim to equip readers with a deeper understanding of the potential threats lurking within the cloud. This survey goes beyond mere problem identification. We explore the existing body of research to uncover the various approaches and methodologies proposed to address these security concerns. We will critically analyze the effectiveness of these solutions, highlighting their strengths and limitations. Ultimately, this paper seeks to pave the way for further research by identifying gaps in current knowledge and charting a course for robust cloud security practices.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203151 |

Security threats and vulnerabilities specific to cloud computing environments the impact of cloud deployment models (public, private, hybrid) on security risks Existing security solutions and mitigation strategies Unresolved challenges and opportunities for future research Define key cloud security concepts like confidentiality, integrity, availability (CIA triad). Explain different cloud deployment models (public, private, hybrid) and their security implications. Discuss the shared responsibility model in cloud security. Cloud Security Issues: Conduct a thorough review of existing literature on cloud security issues. Categorize issues based on different viewpoints (data security, access control, network security, etc.). Discuss prominent threats and attack vectors like data breaches, malware injection, insider threats, etc. Addressing Cloud Security Issues: Review on security solutions and best practices for cloud environments. Explore security measures offered by cloud providers (encryption, access controls, etc.). Discuss client-side security practices like data encryption, user authentication, and activity monitoring. Analyze emerging security solutions like homomorphic encryption, multi-factor authentication, and blockchain for cloud security. Comparison and Evaluation: Compare and evaluate different security solutions based on their effectiveness, complexity, and cost. Discuss the trade-offs between security and performance, scalability, and cost. Future Research Directions: Identify emerging trends and challenges in cloud security. Discuss potential research areas for improving cloud security, such as intrusion detection, secure multi-tenancy, and privacy-preserving cloud computing.

Considerations Conduct a comprehensive literature review using academic databases and reputable sources. Include relevant statistics, figures, and case studies to support your arguments. Discuss limitations of existing solutions and identify areas for improvement. Maintain a neutral and objective tone throughout the paper. Proofread and edit your paper carefully before submission.

II. DESIGN OF CLOUD COMPUTING

The design of cloud is centred around idea to pooling computing resources and making them available over the network to multiple clients. The cloud infrastructure is composed of virtualized computing bandwidth, and is connected to clients through the underlying network. Virtualization: Cloud computing is built on virtualization technology, which enables the creation of virtual machines that can run multiple operating systems and applications. This pool and allocate resources as needed, without the need for dedicated physical hardware for each user. And manage their own computing resources. This provides users with increased control and reduces the burden on IT staff.

- Automation: Cloud computing is designed with automation in mind, with processes such as resource provisioning, configuration,
- and management automated using software tools and scripts.
- Security: Security is a key aspect of cloud computing, and the cloud infrastructure must be designed and implemented with security in mind.
- This includes the use of encryption, access controls, and backup and recovery processes to protect sensitive data.

These design elements provide the foundation for a scalable, flexible, and secure cloud computing infrastructure. The design must be carefully planned and implemented to ensure that it meets the needs of users and provides the benefits of cloud.

Several types of design in cloud computing;

- Design:

This type of design focuses on the underlying cloud computing infrastructure, such as servers, storage, and network components. It includes the selection of hardware and software components, the placement of components in the data canter, and the design of the network infrastructure.

- Service Design:

This type of design focuses on the services provided by the cloud, such as compute, storage, and networking services. It includes the selection of service offerings, the design of service-level agreements (SLAs), and the creation of service catalogues.

- Application Design

This type of design focuses on the applications and services that run on the cloud, including both custom and third-party applications. It includes the selection of applications, the design of application architectures, and the creation of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203151 |

application deployment and management processes.

- Data Design:

This type of design focuses on the data stored in the cloud, including both structured and unstructured data. It includes the selection of data storage technologies, the design of data management processes, and the creation of data backup and recovery strategies.

- Security Design:

This type of design focuses on the security of the cloud computing infrastructure and the data stored in the cloud. It includes the selection of security technologies, the design of security policies and procedures, and the implementation of security controls such as encryption, access controls, and network security.

- Compliance Design:

This type of design focuses on ensuring that the cloud computing infrastructure and the data stored in the cloud meet regulatory requirements, such as HIPAA, PCI-DSS, and GDPR. It includes the design of compliance processes and the implementation of controls to ensure compliance with regulations.

III. CLOUD SECURITY AND DEPENDENCIES

This chapter discusses the security state of cloud environments thoroughly by describing its security issues. Each section of this chapter represents a category of cloud computing environment. Moreover, each section is further divided to some topics that group security issues common in some property. The Access Control category is a user-oriented category and includes identification, authentication, and authorization issues. The Cloud Infrastructure category includes security issues within SaaS, PaaS and IaaS and is particularly related with virtualization environment.

Fig 1.1

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203151 |

Fig 1.2

IV. THE CHALLENGES OF CLOUD COMPUTING

Cloud computing has revolutionized the way organizations consume and manage computing resources, but it is not without its challenges. Some of the most common challenges include:

- **Security:**

One of the main concerns with cloud computing is security. There have been instances of data breaches and security incidents in the cloud, leading organizations to be cautious about storing sensitive information in the cloud. To address this challenge, organizations need to implement strong security measures and regularly monitor their cloud infrastructure for vulnerabilities

- **Compliance:**

Many organizations are subject to regulations that require them to maintain certain levels of security and control over their data. Cloud computing can make it difficult for organizations to comply with these regulations, as they may not

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203151 |

have complete control over their data and infrastructure. Organizations need to work with their cloud service providers to ensure that they are compliant with relevant regulations.

- **Interoperability:**

Different cloud service providers offer different services and technologies, making it difficult for organizations to seamlessly move their data and applications between different cloud environments. This can lead to vendor lock-in and limit organizations' ability to take advantage of new cloud services

- **Data Privacy:**

With the increasing amount of personal and sensitive information being stored in the cloud, privacy has become a major concern. Organizations need to ensure that their cloud service providers have strong privacy policies in place and that they are transparent about how they handle customer data.

- **Performance:**

The performance of cloud computing systems can be affected by several factors, such as network latency and congestion, the availability of resources, and the configuration of the cloud infrastructure. Organizations need to carefully evaluate their performance requirements and work with their cloud service providers to ensure that their applications perform as expected.

V. CONCLUSION

This review examined the current landscape of security challenges in cloud computing. By outlining the vulnerabilities inherent to cloud systems, from data breaches to access control, the importance of robust security measures. Fortunately, various solutions exist, including encryption techniques, identity and access management protocols, and collaboration between cloud providers and users. By acknowledging these security concerns and implementing appropriate safeguards, organizations can leverage the full potential of cloud computing with greater confidence.

ACKNOWLEDGMENTS

work would not have been possible without the insightful research of previous have identified and explored cloud computing security issues.

REFERENCES

1. K. Stanoevska-Slabeva, T. Wozniak, Grid and Cloud Computing-A Business Perspective on Technology and Applications, Springer-Verlag, Berlin, Heidelberg (2010)
2.National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
3.E. Naone, Technology overview, conjuring clouds, MIT Technology Review, July–August, 2009.
4.Merrill Lynch, The cloud wars: $100+ billion at stake, Merrill Lynch, 2008.
5.D. Harris, why ‘grid’ does not sell, 2008.
6.G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, Theory in Practice, O’Reilly Media (2009)
7.B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009)
8.D. Artz, Y. Gil, A survey of trust in computer science and the semantic web, Journal of Web Semantics: Science, Services and Agents on the World Wide Web (2007)
9.DoD Computer Security Center, Trusted computer system evaluation criteria, DoD 5200.28-STD, 1985.
10.A. Nagarajan, V. Varadharajan, Dynamic trust enhanced security model for trusted platform based Future Generation Computer Systems (2010),
11.International Telecommunication Union, X-509 | ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks, ITU, X-Series, 2001.
12. Lekkas, Establishing and managing trust within the public key infrastructure, Computer Communications, 26 (16) (2003)

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details