Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

31

A Comprehensive Review on Cloud Computing Security

Chinmay Teni*, Aditya Nawale *.

* Department of Computer Science and Applications, Dr Vishwanath Karad MIT World Peace University – Pune

Abstract:

Cloud computing is the model that enables service providers to deliver computing resources over the Internet. Virtualization, pay-as-you-go model, and scalability features of cloud computing make it to be adopted by a diversified set of organizations and individuals. Security, in case, vendor lock-in, data lock-in, load balancing, and resource allocation are major issues associated with cloud computing technology. In this paper, authors have comprehensively studied cloud security issues and analyzed existing solutions to cloud computing security.

***Keywords*:** Cloud computing, security, issues, reliability, scalability,

1. INTRODUCTION

Cloud computing is the model that enables service providers to deliver computing resources over the Internet. Broad network access, rapid elasticity, resource pooling, and on-demand self-service properties of cloud computing make it adopted by an enormous set of users and businesses [1]. Software, platform, and infrastructure are the key services offered through the cloud computing paradigm. Private, public, hybrid, and community are the four types of cloud computing deployment models to build cloud computing infrastructure either on cloud service provider premises or customer premises [4]. Virtualization, the minimum cost requirement of cloud computing allows businesses to grow exponentially. Through disaster recovery, cloud computing providers make it easy for businesses to recover from data loss and system failures. Cloud computing providers typically offer automatic updates for their software and services, ensuring that businesses always have access to the latest technology without having to manually upgrade [3].

Cloud computing faces several challenges and issues. Cloud security issue indicates that cloud providers and users are still vulnerable to cyberattacks and data breaches. Customers must ensure that their data is properly protected by implementing their own security measures and protocols. Cloud computing providers must adhere to various compliance standards, such as HIPAA and GDPR, depending on the type of data they are storing. Customers must ensure that their cloud provider is compliant with the necessary regulations. Cloud computing is heavily reliant on internet connectivity, and any disruptions to the network can cause service outages or data loss [2].

Cloud computing relies on shared resources, this creates problem if other users on the same server are utilizing too many resources. Customers must ensure that their cloud provider has a performance monitoring system in place to prevent these issues. Vendor lock-in issue indicates customers using a specific cloud provider may find it difficult to switch to another provider due to proprietary technologies and formats [2]. Apart from these, there are several cloud computing issues such as selecting proper architecture for designing large-scale and high-performance data center networks [5], resource allocation and load balancing [6], TCP in cast [7], MPTCP in cast [8], data lock-in where data stored at one storage site cannot be moved to another storage site, dynamic resource provisioning [9]. Overall, these challenges and issues must be addressed to ensure that cloud computing remains a reliable and secure solution for businesses. In this paper, we reviewed cloud security issues and analysed a few existing prominent security solutions available for cloud environments.

2. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing is Internet-based technology where computing resources like servers, storage, networking, the software is provided through the Internet. These cloud resources are the target of most security attacks [10]. Attackers employ various security attacks and have unauthorized access to cloud resources.

Security issues in cloud computing can arise due to various reasons such as weak access controls, inadequate data encryption, insider threats where malicious insiders can intentionally or unintentionally cause security breaches, data breaches where cloud service

providers may be targeted by cybercriminals who can steal data, causing serious data breaches [11].

Virtualization security issue: Virtualization has become increasingly popular as a means of improving hardware utilization and reducing costs in IT environments [13]. However, it also introduces new security challenges that must be addressed. With virtualization, there is the possibility of a breach in the hypervisor layer [11]. A compromised hypervisor results in the theft of sensitive data or even complete system compromise. Another security issue with virtualization is the risk of VM escape attacks, where a malicious actor exploits a vulnerability in a virtual machine to break out of it and access the host system or other virtual machines. This can occur due to misconfigurations or unpatched vulnerabilities in the virtual machine's software. In addition, virtualization introduces new challenges for network security, as virtual machines can communicate with each other and with the host system through virtual networks [13]. This can result in increased attack surface and potential for lateral movement by attackers within the network.

Hypervisor vulnerability: One example of a hypervisor vulnerability is a "guest-to-host escape" vulnerability, where an attacker exploits a vulnerability in a virtual machine to break out of it and gain access to the host system [12]. This type of vulnerability can be particularly dangerous if the virtual machine is running untrusted code or is connected to an untrusted network.

Injection attack: An injection attack is a type of security exploit where an attacker injects malicious code or commands into a vulnerable application or system, with the intention of altering its behaviour or accessing sensitive information [12].

Cross-Site Scripting (XSS): In an XSS attack, an attacker injects malicious code into a web page that is then executed by the victim's web browser. There are two primary types of XSS attacks: reflected XSS and stored XSS. Reflected XSS occurs when the malicious code is sent in the request to the web server, which then reflects the code back to the user's browser as part of the web page [13]. This can happen, for example, when the attacker sends a link to the victim that includes the malicious code as a parameter in the URL. Stored XSS, on the other hand, occurs when the malicious code is stored on the server and is served to all users who

view the affected page. This can happen, for example, when the attacker submits a form that includes the malicious code, which is then stored in a database and served to other users who view the affected page [14].

DNS poisoning: In a DNS poisoning attack, the attacker alters the DNS cache of a server or network by sending fake DNS data or DNS queries to the target DNS server [3]. This can be done by exploiting vulnerabilities in DNS software or by using techniques such as DNS spoofing or DNS cache snooping to gain access to the DNS cache [7]. Once the DNS cache has been manipulated, the attacker can redirect users to a fake website that looks identical to the legitimate website [15].

Reliability issues in cloud computing can arise due to various reasons, such as service outages where cloud service providers may experience outages due to technical failures, network issues, or maintenance activities, leading to service disruptions. Data loss if data is not backed up properly, it can be lost in case of hardware failures or other issues [12].

Scalability issues: cloud computing provides organizations with high scalability. However, this scalability can also introduce security challenges. Scalability issues in cloud computing can arise due to various reasons, such as lack of visibility, as the scale of cloud computing grows, it becomes more challenging to maintain visibility into all aspects of the environment, including security controls, configurations, and usage patterns [16]. Complexity indicates as the number of services, users, and applications in the cloud environment grows, it becomes increasingly complex to manage and secure them all. Third-party risks indicate that third-party service providers' security practices must be aligned with the organization's requirements [2]. The attack surface grows due to the number of systems and applications in the cloud environment grows, which increases the risk of successful attacks.

Data management issues are a critical aspect of cloud computing security. Data management issues in cloud computing can arise due to various reasons, such as data privacy where cloud service providers may store data in multiple locations and jurisdictions, which can make it difficult to ensure compliance with privacy laws and regulations. Data portability indicates that organizations store more data in the cloud, they may face challenges when trying to migrate data between cloud providers or back to their own infrastructure [15]. Data

access issue suggests that organizations must ensure that only authorized users have access to sensitive data and that access controls are implemented consistently across all cloud services [14]. Data retention issue arises as the amount of data stored in the cloud grows. Organizations must have clear policies and procedures in place to manage data retention and deletion and ensure compliance with legal and regulatory requirements [12].

3. EXISTING SOLUTIONS TO CLOUD SECURITY

Solutions to cloud security issues: These issues are mitigated through encryption, access controls, monitoring and auditing, and training for employees to identify and mitigate security risks [16].

Solutions to virtualization security issues: To address virtualization security issues, organizations implement a comprehensive security strategy that includes secure virtualization configurations, regular security assessments, and strong access controls [17]. It is also important to maintain up-to-date virtualization software and virtual machines and to monitor virtual network traffic for unusual activity [18].

Solutions to hypervisor vulnerability: To mitigate the risk of hypervisor vulnerabilities, researchers suggested keeping the hypervisor software up to date with security patches and following best practices for secure hypervisor configuration [16]. Additionally, access controls should be implemented to limit access to the hypervisor to authorized users only [14]. Regular security assessments should also be conducted to identify and remediate potential vulnerabilities before they can be exploited by attackers [18].

Solutions to injection attacks: Cloud service providers prevent their cloud resources from injection attacks by verifying inputs Additionally, security controls such as firewalls and IDS can be used to detect and prevent injection attacks [19].

Solutions to XSS attacks: To prevent XSS attacks, a secure coding mechanism is recommended by researchers to remove any potentially malicious code [19]. Web applications can also implement measures like Content Security Policy (CSP) or input validation to prevent the injection of malicious code into the application [19]. Additionally, developers can use frameworks and libraries that provide built-in protection against XSS attacks, such as automatic input validation and output encoding [18].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Solutions to DNS poisoning attacks: To protect against DNS poisoning attacks, it is important to implement measures such as securing DNS servers with strong passwords, regularly updating DNS software, and implementing DNSSEC (DNS Security Extensions), which adds digital signatures to DNS responses to verify their authenticity [18]. Additionally, users should be cautious when entering sensitive information on websites and should verify that the website they are visiting is legitimate by checking the URL and looking for security indicators such as a lock icon in the browser address bar [16]. DNS poisoning attacks can be difficult to detect, as they do not involve the theft or compromise of user data, but rather the manipulation of network traffic. Regular monitoring of network traffic and DNS logs can help identify signs of a DNS poisoning attack and allow for quick response and remediation [13].

Solutions to reliability issues: To address reliability issues, cloud service providers must implement redundancy, failover mechanisms, and disaster recovery procedures to ensure service availability and data protection [14]. It's also important for customers to choose reliable service providers, and to have backup and recovery plans in place to mitigate the impact of any potential outages or data loss incidents [20].

Solutions to scalability issues: Scalability issues are mitigated by implementing security measures that are scalable and automated, such as security automation, continuous monitoring, and centralized security management [17]. It's also important to adopt a risk-based approach to security, focusing on the most critical assets and data, and implementing appropriate security controls to protect them. In addition, organizations should choose cloud service providers that offer strong security capabilities, including access controls, encryption, and logging, and that are transparent about their security practices and compliance with industry standards and regulations.

Solutions to data management issues: Implement strong data governance policies and procedures, including data classification, data access controls, data encryption, and data retention and deletion policies [10]. Organizations should also conduct regular data security assessments and audits to ensure compliance with regulations and industry best practices [10]. In addition, organizations should choose cloud service providers that offer strong data management capabilities, including data protection, data backup and recovery, and data

portability, and that are transparent about their data management practices and compliance with relevant regulations [10]. Cloud service providers that have achieved industry certifications and adhere to industry best practices can also provide assurance of their data management capabilities.

4. ANALYSIS AND DISCUSSION:

There are a variety of cloud security issues faced by cloud service providers and cloud users. Researchers have proposed various mechanisms and suggestions to overcome challenges associated with cloud security. Table-1 gives a summary of cloud computing issues and their corresponding solutions proposed by researchers. An access control mechanism is considered a robust solution to cloud security as it prevents security attacks in the first place. Furthermore, access control mechanisms can be implemented at the physical, link, network, transport, and application layer of the TCP/IP protocol suite.

Table-1: Cloud security issues and existing solutions

Cloud security issues	Existing solutions to cloud security issue
Virtualization security issue	Secure virtualization configurations
	Regular security assessments
	Strong access controls
	Keeping virtualization software and virtual machines up to date with security patches
	Monitor virtual network traffic for unusual activity
Hypervisor vulnerability	Keeping the hypervisor software up to date with security patches
	Secure hypervisor configuration
	Access controls to limit access to the hypervisor
	Regular security assessments

Injection attack	Validating user input
	Sanitizing data to prevent the injection of malicious code
	Use of security controls such as firewalls and intrusion detection systems
Cross-Site Scripting (XSS)	Sanitizing user input to remove any potential malicious code
	Content Security Policy (CSP)
	Input validation to prevent the injection of malicious code into the application
	Frameworks and libraries that provide built-in protection against XSS attacks, such as automatic input validation and output encoding
DNS poisoning	Securing DNS servers with strong passwords
	Regularly updating DNS software
	Implementing DNSSEC (DNS Security Extensions)
	Regular monitoring of network traffic
	Maintaining DNS logs
Reliability issues	Keeping redundancy
	Implementing failover mechanisms
	Disaster recovery procedures
	Regular backup and recovery plans
Scalability issues	Continuous monitoring

	Centralized security management
	Access controls, encryption and logging
	Regular security assessments
	Penetration testing
	Security automation
Data management issues	Implementing strong data governance policies
	Conducting regular data security assessments and audits
	Strong data management capabilities

5. CONCLUSION

Cloud computing is Internet based technology. Hence as compared to load balancing, resource allocation, vendor lock-in and incast, security is one of the major challenges for cloud computing technology. Virtualization security, hypervisor vulnerability, injection attack, cross-site scripting, DNS poisoning, data management are some of the important cloud-based security issues. Researchers mitigated these cloud-based security issues by proposing various solutions such as encryption, strong access control, regularly installing security patches, regular security assessment, use of security controls such firewalls and intrusion detection systems, maintaining DNS logs. Out of these, access control mechanism is considered as robust solution to cloud security as it can be implemented at physical, link, network, transport and application layer of TCP/IP protocol suite.

REFERENCE

[1] Kapil, Divya, Parshant Tyagi, Sonu Kumar, and Vinay Prasad Tamta. "Cloud computing: Overview and research issues." In *2017 International Conference on Green Informatics (ICGI)*, pp. 71-76. IEEE, 2017.

[2] Pal, Gajender, Kuldeep Kumar Barala, and Manish Kumar. "A review paper on cloud computing." *International Journal for Research in theApplied Science and Engineering Technology* 2 (2014): 401-403.

[3] Al-Ahmad, Ahmad Salah, and Hasan Kahtan. "Cloud computing review: features and issues." In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pp. 1-5. IEEE, 2018.

[4] Ilango Sriram, Ali Khajeh-Hosseini, "Research Agenda in Cloud Technologies", "*arxiv.org/pdf/1001.3259*"

[5] Suryavanshi, M. M. "Comparative analysis of switch-based data center network architectures." *J Multidiscip Eng Sci Technol (JMEST)* 4, no. 9 (2017): 2458-9403.

[6] Yaser Ghanam, Jennifer Ferreira, Frank Maurer; Emerging Issues & Challenges in Cloud Computing— A Hybrid Approach

[7] Suryavanshi, Mahendra, and Jyoti Yadav. "Mitigating TCP incast in data center networks using enhanced application layer technique." *International Journal of Information Technology* 14, no. 5 (2022): 2523-2531.

[8] Suryavanshi, Mahendra, Ajay Kumar, and Jyoti Yadav. "Balanced Multipath Transport Protocol for Mitigating MPTCP Incast in Data Center Networks." *International Journal of Next-Generation Computing* 12, no. 3 (2021).

[9] A Vouk, Mladen. "Cloud computing–issues, research and implementations." *Journal of computing and information technology* 16, no. 4 (2008): 235-246.

[10] Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. *Cloud computing: Principles and paradigms*. John Wiley & Sons, 2010.

[11] Branco Jr, Teófilo, Filipe de Sá-Soares, and Alfonso Lopez Rivero. "Key issues for the successful adoption of cloud computing." *Procedia computer science* 121 (2017): 115-122.

[12] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[13] Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." *Journal of Network and Computer Applications* 79 (2017): 88-115.

[14] Popović, Krešimir, and Željko Hocenski. "Cloud computing security issues and challenges." In *The 33rd international convention mipro*, pp. 344-349. IEEE, 2010.

[15] Sridhar, S. D. S. S., and S. Smys. "A survey on cloud security issues and challenges with possible measures." In *International conference on inventive research in engineering and technology*, vol. 4. 2016.

[16] Ruan, Keyun, and Joe Carthy. "Cloud forensic maturity model." In *Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012, Lafayette, IN, USA, October 25-26, 2012, Revised Selected Papers 4*, pp. 22-41. Springer Berlin Heidelberg, 2013.

[17] Tiwari, Pradeep Kumar, and Bharat Mishra. "Cloud computing security issues, challenges and solution." *International journal of emerging technology and advanced engineering* 2, no. 8 (2012): 306-310.

[18] Sharma, Maneesha, Himani Bansal, and Amit Kumar Sharma. "Cloud computing: Different approach & security challenge." *International Journal of Soft Computing and Engineering (IJSCE)* 2, no. 1 (2012): 421-424.

[19] Jain, Prince, and Arti Jaiswal. "Security Issues and their solution in cloud computing." *International Journal of Computing & Business Research* (2012): 2229-6166.

[20] Verma, Amandeep, and Sakshi Kaushal. "Cloud computing security issues and challenges: a survey." In *Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV 1*, pp. 445-454. Springer Berlin Heidelberg, 2011.