Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1161–1172
DOI : 10.47974/JDMSC-1971

Security threats and mitigation techniques affecting trust computation in cloud computing

Vinod Saraf *
Vinod Pachghare †
Department of Computer Engineering
COEP Technological University
Pune 411005
Maharashtra
India

Abstract

Cloud Computing is the big evolution in the Information Technology industry. From giant organizations to small retail shops, everyone is moving to the cloud. Till now the Zettabytes of data are already migrated to cloud from private systems, and it is still growing. The actual concern starts when the data is being transferred, stored in some cloud storage, and then accessed. Attackers may attack with various techniques and can steal your data leading to severe security issues. Cloud Service Providers (CSP) must have a robust mechanism to protect their cloud resources from such attacks and ensure the data confidentiality, integrity, and security. If there are any loopholes, it will badly affect the trust computation of that CSP. In this paper we have done a comprehensive study and analysis of the threats in cloud computing which can affect the trust computation of CSPs and discussed the mitigations to those threats.

Subject Classification: *Primary 68Q85 Secondary 68T99.*

Keywords: *Cloud computing, CSP, IaaS, PaaS, SaaS, Malicious, Attacker, Vulnerability.*

The authors wish to acknowledge Information Security Education and Awareness Project, Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, which has made it possible to undertake this research. The authors would also like to thank the anonymous reviewers for their valuable suggestions.

* *E-mail:* `vinod.saraf@outlook.com (Corresponding Author)`
† *E-mail:* `vkp.comp@coeptech.ac.in`

1. Introduction

Cloud computing is a technology which provides on-demand access, through the internet, to computing resources like software applications, physical machines, virtual machines, databases, networking, etc. These computing resources are hosted by a CSP. Cloud users do not have to invest into buying and maintaining computing resources themselves. Cloud Computing is the better, efficient, and cost-effective alternative to the on-premises data center [1]. CSP's also provide various software and platforms as a service for the end user which are prebuilt. The trust and trustworthiness of cloud and CSP has become an important and crucial issue. Cloud trust can be thought of as customer confidence in using the cloud. CSP's need to aim at boosting this confidence by removing technological and psychological hurdles in using the cloud services [2]. The primary barriers in trusting the cloud are lack of transparency, loss of control over sensitive data assets and security assurance. Security assurance can be provided by mitigating all the possible security threats against cloud computing.

2. Trust in Cloud Computing

Trust can be defined as firm belief, honesty, or reliability which one entity expresses on another entity to conduct a transaction or deal within agreed principles and rules. There are two types of trusts in cloud computing viz. Objective trust, Subjective trust [3].

In Objective trust the QoS are being monitored. Such QoS nonfunctional attributes are throughput, response time, reliability, and security. The QoS values are not constant and are subject to change over time. Same service may get different QoS values on same environment in different time [4].

Subjective trust in the cloud is based on the user ratings provided by the users for specific services. The user ratings differ as the perspective of one user may not be same as of another user. It is risky to go with the user ratings for trusting a service as malicious users may be involved in providing or manipulating the user ratings.

To compute the trust and trustworthiness of CSP, objective trust values are more important. Among the various QoS parameters, Security is one of the QoS parameters which affects trust values significantly. Not only for trust computation but in general Security is an essential parameter of cloud computing. To improve security in cloud computing, first we

need to understand the security threats which can occur and then mitigate those security threats by taking appropriate measures. We will discuss the various security threats which can occur and affect trust computation and also provide the ways to mitigate those security threats [3, 4, 5].

3. Security Threats and Risks

Nowadays, most of the organizations have opted for cloud platform basis their business needs. However, by adopting the cloud, it has become inevitable to make sure that the organizations have up to the mark cloud security strategies which can protect them against the top threats to cloud security. Below are the various security threats which are important for trust computation of a cloud or clous service provider.

3.1 Data Loss or Leakage or Breach

One of the features of cloud-based environments is sharing the data stored within the cloud. Data can be shared to other parties via sending the emails or by making the data available on public link. Such environments like email or public links can be accessed directly via Internet. The ease of data sharing in the cloud, which is important and required, can lead to data loss or leakage [6, 7, 8].

Causes of cloud data loss or leakage include:

- Loss of data encryption key
- Inadvertent human errors like storing passwords and sensitive personal data in a plain text file.
- Using old operating system
- Lack of latest security patches
- Malicious attacks
- Using devices without a strict and robust security policy in place
- Data disruption
- Natural disasters

We can prevent data loss or leakage by adopting common sense security practices which includes:

- Use encryption for data.
- Change passwords frequently and use multi-factor authentication.
- Set permissions for accessing data.
- Securing encryption keys

- Continuous monitoring and logging
- Strong disaster recovery strategies
- Follow regulatory compliances.
- Apply the latest security patches.

3.2 *Service or Account Hijacking*

Service or Account Hijacking is another potential threat in the cloud computing environment. [4] As cloud computing provides the facility for accessing the data via remote platforms or over the internet, there is a great potential for service or account hijacking where the security mechanisms are weak [6, 7, 9, 10]. In account hijacking the attacker gains access to the user's account and carries out malicious or unauthorized activities through impersonation. [6]

Service or account hijacking can be carried out by techniques like:

- Phishing attacks
- Brute force password attacks
- Cross Site Scripting (XSS) attacks
- Manipulation of insecure applications
- Server-side request forgery (SSRF) attacks
- Cookie Poisoning
- Credential-stealing malware
- Spyware

We can prevent service or account hijacking by adopting below preventive measures

- Enabling Multi-Factor Authentication
- Implementing the least privilege or zero trust principles
- Opt for DLP (Data Loss Prevention) solutions.
- Segregate Duties
- Monitoring the activities for detecting unauthorized access

3.3 *Malicious Insider*

A malicious insider may be a current employee or an ex-employee of the organization who is having access to the cloud infrastructure and who steals the sensitive data without the organization's permission [6]. Such malicious insiders can infect the code also which may lead to security breach. Security breaches can result in various losses like financial, resource and data loss. It can even result into technical failure [1]. The

insiders can become malicious insiders due to many reasons like revenge, ego, ideology, coercion, espionage, for financial gains [2]. It is hard to identify such malicious insiders, but strong practices can reduce the risk of damage [2]. The indicators of such malicious activities by an insider can be activities at unusual times, the type of activity, the volume of the traffic.

We can prevent Malicious Insider threats by applying some strong policies like:

- Use multi-factor authentication.
- Monitoring and controlling outbound emails and files.
- Controlling removable storages
- User and behavior analytics
- Strong access control policies
- Logging and monitoring the activities.
- Protect critical assets.

3.4 *Insecure Interfaces or Application Programming Interfaces (API's)*

Software Interfaces or Application Programming Interfaces (APIs) are provided by cloud service providers with basic security features and controls [7]. Such API's can provide access to a customer's system or sensitive data. Such API's can be accessed by some third party or hackers, and they can provide harm to the customer's system or data. API threats occur because of API dependencies, weak authentication and authorization, limited monitoring, and logging capabilities. This can result in severe threats like unauthorized access, data breaches, identity theft [6, 7, 8, 10].

Below are the techniques through which we can prevent unsecured API's.

- Strong authentication and authorization systems in place
- Encrypted transmission of data
- Recognize and control API dependencies.
- Enabling strong monitoring and logging capabilities
- Keep the system updated with the latest security patches.
- Use rate limiting and throttling.
- Implement API authentication.

3.5 *Abuse of Cloud Services*

Abuse of cloud services refers to making use of cloud resources by attackers to target the users and cloud service providers themselves. It can

also be defined as illegal, harmful, or fraudulent behavior of cloud customers with cloud service providers. Due to the cloud service provider's shaky enrollment system, anyone having a valid credit card can enroll and access the cloud system [1]. Once they get access, attackers try to spam other systems by sending malicious code and can attack their system [8]. Attackers can also carry out DDoS attacks, dynamic attacks, control the CAPTCHA, circumvent access control, and leak information [2, 11, 12].

Abuse of cloud services can be prevented by:

- Implementing strict enrollment and registration policies
- Introspect the customer cloud network traffic.
- Use of network-based Intrusion Detection Systems
- Monitor the public backlists and block their access to the network.
- Use firewalls to inspect the incoming and outgoing traffic.
- Reduce collaboration with unknown cloud providers.

3.6 *Insufficient Due Diligence*

Due diligence with respect to cloud computing refers to understanding the complete information about the nature of cloud, cloud benefits, cloud functionalities, cloud internal security provisions, security configurations, security patches, security logs and auditing. Many times, the cloud benefits are focused, and security concerns are overlooked, which leaves customers with unknown risks and threats [7]. Such threats need to be assessed by illustrating the main issues and challenges of cloud computing, understanding the nature of cloud operations, and building the skills to deal with cloud structure [10, 13, 14, 15].

Customers need to do the proper due diligence to overcome the threats associated with

- Build the expertise to deal with the complex cloud structure and its associated operations.
- Customers need to thoroughly understand the complete information about the cloud system and not only its benefits.
- Comply with the industry standards to build the cloud systems and applications, applicable to cloud providers and customers.
- Cloud providers should circulate regular updates about the changes in its structure or operations.

3.7 *Shared Technology Vulnerabilities*

Cloud infrastructure and services are designed to be shared among various cloud customers [10]. This is also called multi-tenancy, where the same infrastructure has been shared across various tenants through segregation or separation [13]. If appropriate security measures are not taken in a multi-tenant environment, it may cause several problems. Malicious attackers can take advantage of such vulnerabilities and access the cloud resources as authentic users and can install malicious code to get the user's data [10]. Databases, Storage Systems, Services, CPU can be shared across multiple tenants. IaaS works on shared infrastructure delivering their services in a highly scalable way [7, 12]. Sometimes, for multi-tenant deployments, the cloud computing components (GPUs, CPU, Caches, etc.) are not structured or architected to provide the strong isolation. Virtualization hypervisors can help to address a few of the issues occurring due to shared technology vulnerabilities. However, virtualization hypervisors also have known vulnerabilities that can influence the underlying systems [8].

The below mechanisms can protect the threats associated with shared technology vulnerabilities:

- Incorporate MFA
- Deploy the host-based intrusion detection system (HIDS), as it monitors the system activities and detects network-based attacks.
- Deploy network-based intrusion detection system (NIDS), as it monitors network elements like firewalls, routers, key servers, files, databases, and alarms if found any vulnerability.
- Use access control lists.
- Use strong compartmentalization or separation between the cloud infrastructure to isolate users.
- Use encryption to protect sensitive data.
- Vulnerability scanning and configuration audits must be done regularly.
- SLAs mentioned for security patch application and vulnerabilities remediation may also reduce the risk associated with Shared Technology Vulnerabilities.

3.8 *Identity Theft*

Identity theft means stealing someone's identity who is a legitimate user and pretending to be that legitimate user to access the data or application. This leads to compromisation of data confidentiality and integrity. This identity theft is committed in many ways like gathering transactional information of another person to do transactions. There are several types of identity theft like Personal identity theft, medical records related identity theft, social identity theft, financial identity theft. Identity theft can happen by following various techniques like Pretext calling, Mail theft, Phishing, Card Verification Value (CVV) code requests etc. [2, 12, 14, 16].

Identity theft can be prevented by following security measures.

- Use strong passwords.
- Do not share your PIN or CVV
- Incorporate multi-factor authentication.
- Implement strong authorization techniques.
- Don't install random software downloaded from the internet.
- Sensitive information should not be posted on social media.
- While committing any transaction online ensure the website's authenticity
- Change your PIN and password regularly.
- Never share personal information to anyone

3.9 *Inadequate Authentication & Authorization Controls*

This threat occurs when the authentication and authorization management system is weak or not efficient. This is also termed as Identity and Access Management (IAM) system. Attackers can steal your identity using various malicious techniques and can use it illegally, which can cause destruction. Weak IAM systems can lead to the exposure of administrative management interfaces through which the attackers can exploit the vulnerabilities. After stealing the identity, the attacker can pose himself as an authentic user and try to modify data, snoop on data in transit, disclose the data, participate in nation-state sponsored intrusion, damage the brand, carry out financial impact, hamper productivity or compromise the entire system [7, 10, 11, 17].

Inadequate Authentication and Authorization threats can be overcome by following below measures.

- Deploy strong authentication and authorization mechanisms.
- Use multi-factor authentication.
- Periodically change the passwords and cryptographic keys
- Implement a strong alerting mechanism to alert the users in case their account is breached by an unauthorized user.
- Immediately revoke the access of users who left the organization.

3.10 *Spectre and Meltdown*

Speculative execution was designed into chips to boost the processing speed of computers and also makes computers multitask more efficiently. Spectre is a vulnerability which allows the program to read the data from arbitrary locations in the allocated memory. Meltdown is a kind of vulnerability which allows a process to read all the memory locations in a given system. Spectre breaks down the layer of isolation between different applications whereas the fundamental layer of isolation between applications and the operating system is broken down by Meltdown. These hardware vulnerabilities are a malicious program to exploit Meltdown and Spectre vulnerabilities and can get all the information stored in the memory of other running programs on the same system. The secrets might include passwords stored in a password manager, browser or in cookies. It also includes personal make it easy for the programs to steal data which is currently being processed on the computer. An intruder can use photos, emails, instant messages, and even business-critical documents. It is also possible to steal the data of another customer hosted in a cloud environment. It has been found in the testing that some Intel and AMD processors with out-of-order execution implementation are also prone to Meltdown threats [13, 18].

Spectre and Meldown threats can be prevented by taking below measures:

- Apply security patches.
- Regularly update the BIOS and Operating System

4. Discussion and Conclusion

Cloud computing is the next future for industries. It is useful in getting the infrastructure ready within minutes, storing, and sharing the

data, building, and running the business applications etc. To this all it is need of time to have scalable and world class computing infrastructure at a reasonable price. Along with the large benefits of cloud computing, it is also vulnerable to many security challenges. This comprehensive study analyzes cloud computing threats thoroughly, describes their characteristics and also states the ways to mitigate these threats. Security is an essential and prime factor while computing the trust or trustworthiness of cloud. The appropriate security measures, controls and mitigations need to be studied, planned, and deployed before using the cloud infrastructure or services. Our study will help cloud beginners to know about security threats, ways to overcome them and how important these security threat mitigations are while computing the trust for a cloud.

References

[1] Suman Sansanwal, Nitin Jain, "Security Attacks in Cloud Computing: A Systematic Review", Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, pp. 501-508, (2021).

[2] Tabrizchi, H., Kuchaki Rafsanjani, M., "A survey on security challenges in cloud computing: issues, threats, and solutions", *The Journal of Supercomputing, Springer Nature* 76, pp. 9493–9532 (2020).

[3] Pooja Pol, V K Pachghare, "Quality of Service Estimation Enabled with Trust-Based Resource Allocation in Collaborative Cloud Using Improved Grey Wolf Optimize", The British Computer Society, *The Computer Journal,* Volume 65, Issue 12, Pages 3209–3222, (2022).

[4] Gupta, Shaurya, Ramesh Chandra Poonia, Vijander Singh, and Linesh Raja. "Tier application in multi-cloud databases to improve security and service availability." In Handbook of research on cloud computing and Big Data applications in IoT, pp. 82-93. IGI Global, (2019).

[5] Pooja Pol, V K Pachghare, "Impact of I-GWO Towards Trust Based Resource Allocation in Collaborative Cloud", Volume 13, Issue 1, *International Journal of Next-Generation Computing*, (2022).

[6] Umer Ahmed Butt, Rashid Amin, Muhammad Mehmood, Hamza Aldabbas, Mafawez T. Alharb, Nasser Albaqami, "Cloud Security

Threats and Solutions: A Survey", *Wireless Personal Communications,* Volume 128, pp. 387-413, (2023).

[7] Poonia, Ramesh C., and Linesh Raja. "On-demand routing protocols for vehicular cloud computing." In Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing, pp. 96-122. IGI Global, (2021).

[8] Ruchi Bhatnagar, "Proposal Of Security Schemes For Protecting Services In Cloud Computing" *International Journal of Engineering Research & Technology* (IJERT), Vol. 1, Issue 3, May (2012).

[9] Deepti Singh Kshatriya, Manju Vishakh Nair, "Cloud Computing: Threats and Security", *International Journal of Engineering Research & Technology* (IJERT), Volume 3, Issue 20, (2015).

[10] Najib A. Kofahi, Areej Rasmi Al-Rabadi, "Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey", *Advances in Networks.* Vol. 6, No. 1, pp. 1-13, (2018).

[11] Annette Shajan, Shanta Rangaswamy, "Survey of Security Threats and Countermeasures in Cloud Computing", *United International Journal for Research & Technology*, Volume 02, (2021).

[12] Aditi Patel, Nisarg Shah, Dipak Ramoliya, Amit Nayak, "A detailed review of Cloud Security: Issues, Threats & Attacks", Fourth International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 758-764, (2020).

[13] Fursan Thabita, Prof.Sharaf Alhomdyc, Abdulrazzaq H. A. Al-Ahdalc, Prof. Dr. Sudhir Jagtap, "Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques", *Journal of Information and Computational Science,* Volume 10 Issue 12 – (2020).

[14] Giuseppe D'Alconzo, Alessio Meneghetti, Paolo Piasenti, "Security Issues of CFS-like digital signature algorithms", *Journal of Discrete Mathematical Sciences and Cryptography,* Volume 27, Issue 1, Pp 175-187, (2024).

[15] Tanya Garg, Ruchi Goyal, Dinesh Goyal, "A study of e-learning security system and its impact on educators", *Journal of Discrete Math-*

ematical Sciences and Cryptography, Volume 26, Issue 5, Pp 1489-1498, (2023).

[16] Amara Naseer, Awais Ali, "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 244-251, (2017).

[17] Aishani Dagar, Karan Singh, Tayyab Khan, "Comprehensive analysis of continuous authentication for mobile devices", *Journal of Discrete Mathematical Sciences and Cryptography,* Volume 26, Issue 7, Pp 2007-2024, (2023).

[18] Vaibhav Jha, "Boosting Security for Cloud Storage", *International Journal for Research in Applied Science & Engineering Technology* (IJRASET), Volume 8, (2020).