Semiconductor Optoelectronics, *Vol. 41 No. 12 (2022), 1489-1498*
https://bdtgd.cn/

DETERMINING THE TECHNIQUES TO REDUCE SECURITY ATTACKS IN CLOUD COMPUTING

Dibyendu Mahato, Dr. Ajay Jain
Department of Computer Application, Dr. A.P.J. Abdul Kalam University, Indore (M.P.), India

ABSTRACT
Cloud computing is a fast-developing internet technology that provides users with a wide range of useful services. It makes a variety of alluring promises to the public or to giant corporations like Amazon, Google, Microsoft, and IBM etc., in order to help them keep up with the competition in the rapidly expanding cloud computing environment and provide better services to a wide range of customers. Attacks play a critical role in computer networks. In modern times, it also diminishes cloud services. The assaults lower the standard of service provided by both traditional and cloud-based computer networks. An assault that successfully lures in the service's intended customers. Limiting attack vectors and tightening up security are essential steps toward widespread use of cloud computing. Security is a hot topic in academia, and it's important that it's addressed properly to prevent assaults that are disastrous for both service providers and their customers. In this overview, we look at the many techniques that have been developed to combat assaults on cloud computing.
Keywords: Attacks, Prevention, Authentication, Intrusion, Cloud environment

I. INTRODUCTION
Modern Internet-dependent technology is widely used because of the convenience of cloud computing. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for delivering on-demand, convenient, ubiquitous, and reliable network access to a shared pool of configurable computing resources that is both scalable and self-service." It's a cutting-edge IT process that allows for the dynamic sharing of resources over the web, yielding financial gains.

The Pay As You Go (PYAG) concept, in which you only pay for the services you actually use, is a major inspiration for cloud computing. The ability to provide resources on an as-needed basis is one of the biggest advantages of the pay-as-you-go (PAYG) approach. The customer may pick their own operating system, RAM, CPU, LAN, and security settings. When a customer or end-user requests an asset, the provider makes it available. Researchers are interested in cloud computing since it is of considerable benefit to both individual users and businesses. Cloud computing, often known as XaaS, is a model for delivering and consuming on-demand computing resources across a network, with X=[S, P, I]. The ability to pool resources in the cloud increases the reliability of services and shortens their turnaround times. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) all fall under the umbrella of cloud computing, and they help alleviate resource scarcity

worries. The cloud provides access to several programs without requiring the user to download and install anything on their local machine. Developers and designers of apps may create their work without having to shell out cash for a physical server. Furthermore, it provides software emulations of the underlying hardware. Cloud services have the ability to reduce expenses and processing power, but they also pose security risks. Cooperated server might greatly impact both the tenant and the cloud service providers if data breach occurs. Both private and corporate information, such as financial records, customer lists, and customer communications, are at risk of theft. In the present setup, the cloud customer, who may be the service or data owner, places full trust in the cloud service provider to protect their data.

Because user data is kept on a remote server, they risk having it compromised in the event of a data breach. Management of cloud users, multi-tendency support, and application security are just a few of the challenges presented by cloud computing.

Everyone has had some sort of interaction with cloud computing. It provides low- or no-cost software and data storage space delivery as Internet-based services. The vast majority of us regularly make use of cloud services. For communication, we use web-based email systems like Yahoo and Google; for sharing information and keeping in touch with friends, we use social networking sites like Facebook, LinkedIn, MySpace, and Twitter; for watching TV shows and movies, we use on-demand subscription services like Netflix and Hulu; for storing music, videos, photos, and documents online, we use cloud storages like Humyo, ZumoDrive, and Dropbox; and for collaborating with others, we use tools like Google Docs. Businesses have also begun using cloud computing, with the hope that doing so will help them save money and increase their cash flow. For its online forum service, for instance, the social news website reddit uses a rented instance of Amazon Elastic Compute Cloud (EC2). SmugMug's image hosting service is provided by Amazon S3 (Simple Storage Service), which is rented by the company. Mazda USA leases server space from Rackspace to host their promotional ads. HRLocker, a software startup, uses Windows Azure as a rental platform for its human resources management solution.

In the 1960s, only mainframe computers had access to the computing technologies that would eventually become cloud computing. The term "cloud" originated in connection with the representation of the Internet as a "cloud" in early network diagrams. Virtualization, clustering, grid computing, etc. are all components of this technology that work together to provide corporate customers with inexpensive rates and minimize the maintenance costs associated with running an in-house data center.

National Institute of Standards and Technology's (NIST) definition of cloud computing is the most widely accepted one: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Even though many of cloud computing's features are already well-understood, there are still many open security questions that must be answered before the industry can make full use of the cloud's services.

II. ADVANTAGES OF CLOUD COMPUTING

- **Lower IT costs Infrastructure**

The move to cloud computing has the potential to reduce the ongoing and maintenance costs

of IT systems. By leveraging the resources of a cloud computing service provider, as opposed to investing in costly in-house systems and equipment, businesses may save money. Due to factors such as the elimination of the need to pay the salaries of specialized personnel, the reduction or elimination of the need to purchase additional hardware and software, and the elimination or reduction of the time and effort required to implement these changes, cloud computing has the potential to reduce operational expenses.

- **Timeliness**

Fast scalability means that a company may increase or decrease its processing and storage demands as needed. Cloud computing eliminates the need for users to buy and install costly upgrades on their own computers. Using the cloud saves time, allowing us to focus on running the company.

- **Durability in Business**

Protecting information and infrastructure is a crucial aspect of making a business sustainable. If you save your data in the cloud, you can rest certain that it is backed up and contained in a secure and safe spot in the event of a natural disaster, power outage, or other emergency. Regaining access to data as quickly as possible allows businesses to resume normal operations, avoiding losses in both time and money.

- **Effective collaboration**

When businesses work together in the cloud, they are able to communicate and share information in ways that go beyond what has traditionally been possible. If your team is working on a project in many places, you may provide everyone involved access to the same data via the cloud. Users of cloud computing choose for a graphical depiction that makes it simple to send their work to an advisor.

III. SECURITY ISSUES

Today, security in cloud computing environments is a top priority. There has to be further debate and clarification of the identified security problems and attacks.

- **Embedded Security Issues**

The relatively unexplored realm of embedded systems built on cutting-edge tech. Improvements in productivity tools made possible by embedded systems are largely responsible for the field's recent breakthroughs. Because of how they're different, they encounter a number of difficulties. The primary driver of the embedded security problems is virtualization. The SNMP (simple network management protocol) Server, Electronic Access Control, Virtual Machine Monitoring, and Isolation of Virtual Machines are all examples.

- **Application Issues**

When it comes to cloud security, application software is a major weak spot. Parallel programs, front- and back-end frameworks, and other sorts of frameworks are common in modern software. A software program might also have many millions of lines of code. In addition to this, there is great variety in the programming languages and authors available for software development. Multiple vulnerabilities result from these causes. Concerns about cloud security can arise from a variety of application-specific factors, including platform choice, user front end design, user back end, license, framework, service availability, and the parallel structure of applications.

- **Trust Issues**

The level of trust may be gauged by looking at how satisfied a client or user is with their

experience. Trust is also related to data persistence, stakeholder engagement, access to computational algorithms, and virtualization. There are several stages involved in determining trust, each of which is influenced by different variables. The next-generation security transparency ideas provided by TCP seek to protect the privacy and security of whatever information the service provider collects. Human error, forensic values, reputation, governance, trusted third parties (TTPs), and a lack of customer faith are all sources of distrust. It is possible to draw three essential conclusions about the trustworthiness of cloud service provisioning. These include the system's operating performance, the quality of service provided, and the security and privacy of data stored in the cloud.

- **Web Application Issues**

Similar vulnerabilities exist with the security of internet services, such as port scanning, IP spoofing, social engineering injection holes, and many others. Virtualization and Web 2.0, two technologies impacted by cloud computing, also bring their own security problems. Threats to this sort of system are also highlighted. By exploiting these vulnerabilities, an attacker can take over slave systems and carry out nefarious actions. Web server, technology, proxy server, protocol, and standard all come into play here.

- **Client Management Issues**

One of the primary concerns in protecting the privacy of cloud computing is the efficient management of customers in accordance with the secure consumption of resources. Protecting the president at home is a lot like protecting the president on the road. In a similar vein, cloud storage vs. a user's own private system. Problems in managing clients arise when dealing with their identities, privacy, and authentication.

- **Metadata Issues**

Metadata is full with private and secret data, which is why security experts treat it with such caution. Risks to an organization might arise from the accidental disclosure of private information stored in metadata. An intruder might glean implementation and accounting metadata, which contains sensitive security information, to compromise the system. In a metadata spoofing attack, the attacker can change the wording used to describe the service. Protection of data location, separation, maintenance, and sanitization are all examples of metadata concerns.

- **Data Storage Issues**

Data storage is one of the most important aspects of cloud computing. The complexity of distributed computing, data security, and data storage is a major factor in the fast expansion of Internet-connected devices and a wide variety of online applications. Location of data warehouses, data leakage and loss, sanitization, unreliable data, anonymity, availability, integrity management, cryptography, metadata location protection and maintenance, and the use of outdated encryption methods are all potential security risks associated with cloud storage.

- **Operating System Issues**

The security of cloud computing environments is complicated by the wide variety of server types, networks, OSes, and VMs used. IOS, BSD, Windows, and Linux are all targets of numerous security threats. Operating system exploits, such the stack overflow attack and GNU Bash, led to critical vulnerabilities since they allowed remote code execution. OS vulnerabilities with high risk and significant danger include the GNU Bash Common

Vulnerability and stack buffer overflow concerns.

- **Distributed Computing Issues**

Cluster is a type of distributed computing that uses a group of interconnected computers, virtual machines, or servers to perform a single task and be treated as if they were a single entity. Increasing the number of nodes in a single cluster creates a number of problems for the system administrator, and this gives rise to new security concerns for virtual, physical, hierarchical, and multi-cluster configurations.

- **Service Level Agreement (SLA) Issues**

Customer service goals and expectations may be measured through the use of service level agreements (SLAs). Security in the context of service level agreements (SLA) is a topic of discussion. Errors in operating system installation and the accidental disabling of security events auditing by the administrator during crucial vendor monitoring are two examples of security vulnerabilities related to service level management.

IV. KEY SECURITY REQUIREMENTS IN CLOUD COMPUTING

Concerns about cloud computing's main security criteria for an efficient and safe technological solution are defined by the International Standards Organization (ISO). Here are some explanations of these:

- Confidentiality involves preserving user information and restricting access to it to authorized parties.
- Data integrity refers to the degree to which it is protected from unauthorized access or tampering during storage or transmission, and to which only authorized users have access.
- Authentication refers to the process of verifying a user's identification before to granting them access to a restricted resource, such as a database.
- Availability refers to the state of being available at all times, at any location, to receive the information or services sought by a user.
- Authorization ensures that only the individuals who are legally permitted to see a document have done so.

V. SECURITY ATTACKS AND THEIR PREVENTION TECHNIQUES IN CLOUD COMPUTING

This section details the many assaults that might be launched against cloud computing, along with the corresponding preventative solutions. Table 1 below displays these assaults in terms of safety attack, impacted cloud services, and mitigation techniques.

Table 1: Security attacks with their prevention techniques in cloud computing

Security Attack	Affected Cloud Services	Prevention Techniques
DOS Attack	IaaS, PaaS and Saas	• Using authorization and fast authentication.

		• Use a filter technique. • Use methods focused on signature. • Usage of device for intrusion detection or intrusion prevention.
SQL Injection	SaaS	• Do not use SQL generate by dynamic technique in the code. • Sanitize user feedback by proper filtering technique. • Use of the proxy-based architecture for automatically identifying and extracting user data.
Authentication Attacks		• Use of strong passwords and a better mechanism for authentication. • Applying Secure Assertion Markup Language, Service Provisioning Markup Language and Extensible Access Control Markup Language standards to secure federated identities. • Channel encryption of communication to protect the authentication tokens.

Phishing Attacks	IaaS, PaaS and Saas	• Using secure links to the web. • Identification of spam e-mails. • Ignoring short URLs. • Avoiding to click when someone is forcing you to click.
Port Scanning Attacks	IaaS, PaaS and Saas	• Using a set of functionalities independent of time. • Using neural networks and packet counts. • Using firewalls. • Evolving TCP/IP packets. • Capturing packets.
MITM Attacks	IaaS, PaaS and Saas	• Requiring proper architecture for Secure Socket Layer. • Using an Algorithm for encryption and decryption. • Use a Monitoring Method for Intrusion.
Back Door Channel Attack	IaaS	• Strong isolation and authentication mechanisms required
Metadata Spoofing Attack	PaaS and SaaS	• The service's functionality and other details should be kept encrypted to access the file which requires

		a strong authentication technique
User to Root Attack	SaaS	• Using better authentication technique and strong password.
VM Rollback Attack	IaaS	• Using suspend and resume.
VM Escape Attack	IaaS	• Monitoring of activities of the hypervisors. • VM Isolation Needed. • Use a safe Hypervisor. • Configuring relationship with the host/ quest.

Denial of Service (DoS) Attack

Using a variety of techniques, the suspect attempts to disrupt service by launching a denial-of-service assault on the legitimate user. It is possible for an attacker to exhaust a victim's resources by sending a barrage of internet request packets to them. The transmission of these data packets uses up valuable network capacity and tax the server's processing power. As a result, the functionality and accessibility of cloud services might be compromised by this type of assault. Distributed denial-of-service (DDoS) assaults are an evolved form of DoS attacks in which the attacker uses a swarm of compromised servers across a network to inflict crippling effects on a single target. DDoS attacks are much more sophisticated and challenging to detect than DoS attacks.

SQL Injection

The attacker in this attack modifies the regular SQL code in order to get access to the database and steal private information about the users. The primary goal is to get sensitive user information, such as login credentials, from the target web application. If an attacker is able to breach this system, they may get unauthorized access to sensitive data, conduct activities from a distance, or even alter the structure of a database.

Authentication Attack

Because of the weak username and password mechanism, authentication assaults will happen in cloud settings. As a result, cloud authentication is especially vulnerable to assaults like dictionary attacks and brute-force attacks. Attackers in this scenario aim to compromise the user's chosen method of authentication in order to gain access to the system.

User To Root Attack

By locking out a legitimate user and changing their password, a hacker can get complete control of the system in a user to root assault. An overflow is used to assault a static buffer by writing too much information into it.

Phishing Attacks

An attempt to link manipulation phishing attack. By tricking a user into visiting a fake version of a legitimate website, the attacker can then access the victim's private information and take control of their account. Through the detection of pop-ups and spam emails, anti-spam software can put an end to phishing attacks.

Port Scanning Attack

The goal of a port scanning attack is to get precise information about the processes executing the program and the working environment by using open ports services like IP and MAC address that refer to the connection. After the port scanning process is complete, the hacker uses this information to his advantage by launching a direct attack.

Man-In-The-Middle (MITM) Attack

The attacker gains access to sensitive information shared between users by strategically inserting bogus information into the cloud environment. However, the attack can happen in a continuous communication if the medium is not secure enough.

Back Door Channel Attack

The suspect's resources may be monitored remotely thanks to an attack on the backdoor channel. Yet another way that attackers keep tabs on victim services is by listening in on back-door channels. It might compromise the security and privacy of sensitive information.

Metadata Spoofing Attack

For a metadata spoofing attack to be successful, the hacker must get access to the Web Services Description Language (WSDL) file that describes the service and all of its features and information. If the hacker in the WSDL file can disrupt the code that calls the service, they will achieve their goal.

VM Rollback Attack

Tenant users in a cloud infrastructure can quickly and easily access VMs. As a result, they pose the greatest threat to the whole virtualized infrastructure. In a VM rollback attack, the attacker takes advantage of a previously captured image of the virtual machine and secretly re-executes it. Although the guest OS restricts the number of failed login attempts, a hacker can obtain the VM's credentials through a brute-force attack. In addition, the attacker can modify user rights by utilizing the rollback permission control module.

VM Escape Attack

Guest OS destruction, memory control of the hypervisor, and functionality injection are all targets of this type of attack. The attacker must have direct communication with the hypervisor in order to bypass the isolation layer.

VI. CONCLUSION

Nowadays, more and more people are turning to cloud computing. Since cloud storage allows users to access their files from any internet-connected device, it has become increasingly popular for people to keep their data in the cloud. Yet, concerns about data security are increasingly presenting difficulties for service providers. Both the cloud service provider and the client should verify that the cloud they are using is safe from external threats and that no

unauthorized third parties may access the data stored there. Security in the cloud is an active area of study, but researchers and safety engineers have not yet been able to provide long-term solutions to the rapidly expanding set of challenges in this space because of how quickly the underlying technology is evolving. Research summarizes several security threats, preventative measures, and intrusion threats.

REFERENCES: -

1. P. Ravi Kumar. P. Herbert Raj, P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing", 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India.
2. Priyanka Chauhan, Rajendra Singh, "Security Attacks on Cloud Computing with Possible Solution", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, Issue 1, January 2016.
3. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
4. Singh, Saurabh, Young-Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." Journal of Network and Computer Applications 75 (2016): 200-222.
5. M. A. Khan, ―A survey of security issues for cloud computing, J. Netw. Comput. Appl., vol. 71, pp. 11– 29, 2016.
6. Mathkunti, Nivedita M. "Cloud Computing: Security Issues." International Journal of Computer and Communication Engineering 3, no. 4 (2014): 259.
7. Dr. V. Venkatesa Kumar, M. Nithya, "Improving Security issues and Security Attacks in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10 October 2014.
8. Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. "A survey on security issues and solutions at different layers of Cloud computing." The journal of supercomputing 63, no. 2 (2013): 561-592.
9. Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." International journal of engineering research and applications 3, no. 4 (2013): 1922-1926.
10. K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, An analysis of security issues for cloud computing, J. Internet Serv. Appl., vol. 4, no. 1, p. 5, 2013.
11. V. S. K. Maddineni and S. Ragi, Security Techniques for protecting data in Cloud Computing. 2012.
12. R. Bhadauria and S. Sanyal, Survey on security issues in cloud computing and associated mitigation techniques, arXiv Prepr. arXiv1204.0764, 2012.
13. Lamba, Harjit Singh, and Gurdev Singh. "Cloud Computing Future Framework for e-management of NGO's." arXiv preprint arXiv:1107.3217 (2011).
14. H. Wu, Y. Ding, C. Winer, and L. Yao, Network security for virtual machine in cloud computing, in Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, 2010, pp. 18–21.
15. S. Gajek, M. Jensen, L. Liao, and J. Schwenk, "Analysis of Signature Wrapping Attacks and Countermeasures," IEEE International Conference on Web Services, pp. 575–582, Miami, Florida, July 2009.