International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206417

Security Hazards, Attacks and Its Prevention Techniques in Cloud Computing : A Detail Review

Rajeshkumar V. Patel*[1], Dhaval Bhoi[2], Chandrashekhar S. Pawar[3]

*[1]IT Department, Devang Patel Institute of Advance Technology and Research (DEPSTAR), Changa, Gujarat, India
[2]CE Department, Chandubhai S Patel Institute of Technology (CSPIT), Changa, Gujarat, India
[3]CSE Department, Devang Patel Institute of Advance Technology and Research (DEPSTAR), Changa, Gujarat, India

ABSTRACT

Article Info
Volume 6, Issue 4
Page Number: 48-58
Publication Issue :
July-August-2020

Significant technical advances have emerged over the last decade, potentially bringing more simplicity to everyday life activities not only at the level of the organization, but also at the personal level. Recently, it has become apparent that many companies and businesses are moving their workloads to the cloud. Nevertheless, with the rapid growth and appealing products, there are still several concerns surrounding this technology that must be dealt with protection having the biggest obstacle to its acceptance. Safety issues are a continuing field of research that needs to be adequately handled to prevent security breaches and disaster-related attacks for service providers and service users. This survey addresses conceptual architecture of cloud computing, essential criteria of safety for cloud computing, security risks to cloud computing and attacks on security on cloud computing with its mitigation techniques.

Keywords : Cloud Computing, Data Privacy, Security, Confidential Data, Cyber Attacks, Hazards, Prevention Techniques.

Article History
Accepted : 10 July 2020
Published : 15 July 2020

I. INTRODUCTION

Across many fields, Cloud Computing technology was commonly used including communication, real-time applications and file sharing. In recent decades major cloud computing developments have emerged, including substantial development. Thanks to the practicality of its programs, cloud computing has been widely accepted in the private and public sectors, which can potentially bring convenience on many levels.

The National Institute of Standards and Technology defines Cloud Computing (CC) as “A model for enabling ubiquitous, 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” [1]. On other hand, since last few years, Cloud safety incidents have been increased dramatically, possibly because of the phenomenal growth of cloud services [2].

In this survey, Various risks and attacks have also been identified with few guidelines on solutions. However, this review outlines all of the key security threats and protection impacts that occur in the cloud network with clear description of prevention strategies of each. The review structure is as described below: Section II and Section III contains cloud service models and cloud deployment models respectively. Section IV gives a brief overview of main cloud computing security challenges. Section V and Section VI contain an issue statement with its response guidelines including a comprehensive overview of security hazards and malware attacks with their prevention strategies in cloud computing environments respectively.

II. CLOUD SERVICE MODEL

The cloud service models having three types. They are Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service. The below Figure. 1 shows cloud computing architecture and service models.

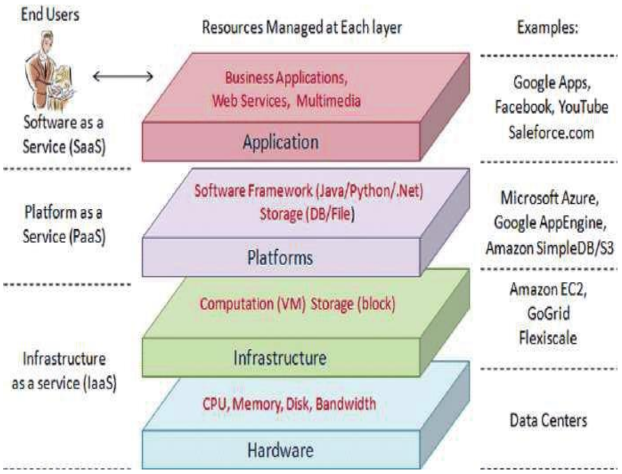

End Users
Resources Managed at Each layer
Examples:
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Software as a Service (SaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Platform as a Service (PaaS)
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

Figure. 1. Cloud Computing Architecture and Service Models

Software as a Service (SaaS)

SaaS is highest layer of the architecture. It offers software frameworks in which end-user apps running on the cloud can be used by the provider. The SaaS software provider has all responsibility to manage the software program, the SaaS provider owns the software and operates it on machines within its data centre, and organisations and individuals do not own it but rent it and purchase subscription-based service from cloud computing vendors. The SaaS enables companies and individuals to quickly reduce dependency on in-house IT segments incorporating distributed computing. Such programs can be used by using client interfaces. A SaaS client does not need to manage, supervise or monitor the infrastructure of core cloud.

The services provided by SaaS providers must be safe by different techniques such as WS (Web Service) security, XML encryption and different other techniques used for data security. E.g. Facebook, Youtube, etc.

Platform as a Service (PaaS)

PaaS is the second layer of the architecture. It gives user tools where they can deploy, build or develop applications on the cloud infrastructure, by the user. The user cannot manage or monitor the basic cloud infrastructure like servers, network, storage or operating systems but has monitor over the applications deployed and the application execution process. This layer's services have team collaborations, testing, development, deployment, hosting, application design database integration, web service integration, security, storage, scalability, state management and versioning.

It is a framework, where a user without the infrastructure or computer resources underlying control is able to create and upload their own application. PaaS supplier deliver a specified mixture of application servers like MySQL, Apache, Linux, etc. For example Google App Engine, Microsoft Azure, Amazon Simple DB/S3 etc.

Infrastructure as a Service (IaaS)

IaaS is the lowest layer of the architecture. The IaaS technologies are adopted from the layer of hardware and infrastructure. The user has the processes managing ability, supervise storage, network and other major computing resources that are useful for handling arbitrary programming, and that can integrate operating systems and applications. The cloud service provider (CSP) is liable for operating and maintaining the underlying cloud infrastructure while the user is responsible for virtual machine management.

IaaS is based on virtualization technology which has virtualized resource layer (virtual storage, virtual machines, virtual networks) and virtualization layer (hypervisors) [3]. Example includes GoGrid, Amazon EC2, Flexiscale, etc.

The Layer of Hardware is responsible for handling cloud physical infrastructure usually located in data centres. This can have problems such as hardware setup, fault tolerance, traffic control, power and resource cooling [4].

III. CLOUD DEPLOYMENT MODELS

Cloud deployment models indicate how the cloud services made available to users. Depending on ownership, size, user and access of the cloud, the cloud deployments has distinguished in the four different type. They are: Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud. Figure. 2 shows the cloud deployment models.

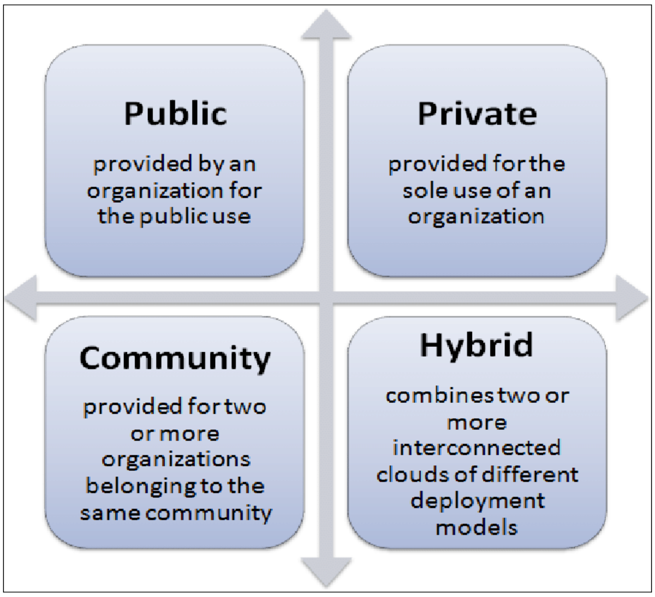

Public
provided by an organization for the public use
Private
provided for the sole use of an organization
Community
provided for two or more organizations belonging to the same community
Hybrid
combines two or more interconnected clouds of different deployment models

Figure. 2. Cloud Deployment Models

Public Cloud

In this type of cloud deployment model, the hardware and software is provided by an organization for the public use. Depending on the demand the services are dynamically given to the user on pay-per-user method. As it is shared to the public, it might be prone to malicious attacks and hence it’s not secure. It gives different types of advantages to the users like independence of location, scalability, no infrastructure requirement, versatility, etc.

Private Cloud

In this type of cloud deployment model, the infrastructure operates on a private network and is operated only by a single organization, and the external network has no access to it. It is provided for the sole use of an organisation. It is highly secure, as a single company manages, runs, and processes the private cloud services. The organization shall bear the maintenance and operating expenses.

Community Cloud

In this model, the cloud structure built to be used within a single community by multiple organizations with shared interests. It is provided for two or more organizations belonging to the same community. In the group of cloud, everybody has free access to data and applications. The shared resources may be handled in this type of cloud, either by members of the community involved or by other service provider.

Hybrid Cloud

The hybrid cloud is a combination of two or more interconnected clouds of different deployment models to share the data and software irrespective of location and ownership. Hybrid cloud model offers high level of scalability, versatility and many data delivery options.

IV. Security Challenges in Cloud Computing

Cloud essentially provides its customers tools on the basis of its service's subscription. While it has some benefits over conventional computing, it needs to face some challenges. This section discusses some of the key challenges:

Privacy

Cloud service providers save their private information in the cloud which is stored around the world on certain physical devices. All the data is transmitted via the internet only. It isn't guaranteed that malicious users can't hack the data.

Integrity

It means ensuring that data is not changed or updated while it is being processed or moved, and that only permitted users have permission to update, edit, copy or remove the information.

Authentication

It means ensuring the user's identity prior to give access of data, and this can be accomplished by using some security in user's profiles.

Reliability

Data of the consumers are stored in the server of third parties. They are not aware about the location where their data is saved. They don't know about what protective measures they offer to protect their private information [5].

Bandwidth

If resource demands to store very large amount of data in the cloud, it will require high bandwidth.

Availability

When at a time, the very large amounts of resources are being served, the cloud becomes incapable of meeting all the requirements of the consumer.

Authorization

This means ensuring that the person who request to have specific information should have the right to access it [6].

Security Hazards And Solutions

A hazard is a possible danger that could be target a weakness to break protection, and hence can be harmful to a system or an organization. The most dangerous threats and their possible solutions are suggested in this section. Table.1 shows security threats with its solution techniques and cloud services that they can damage in cloud computing.

Data Loss

Data loss may be done with good or poor intention in different ways. Data can be lost due to modifications, deletions etc. Organizations should take data backup to prevent these risks. To ensure reliability, accessibility and extensibility cloud computing providers should cover the loss of the data [7] [8].

Data Breaches

This threat involves the transmission of important and confidential data to the individual or organization not allowed to do so. Data breach or data leakage may occur for several reasons, but the main reason may be incorrect authentication or authorization system, control of audit, unreliable use of encryption keys. The possible way to reduce this is by encrypting the data, but when the encryption key is lost it can also lead to data loss [9] [10]

Insecure Interface and APIs

Cloud Application Programming Interfaces (APIs) are the specifications and protocols that can be used by cloud users to connect to the cloud and access cloud resources. These interfaces provide their customers with all services of provisioning, management, and monitoring. Because the cloud security depends on these APIs, they must have proper access controls, secure certification standards and mechanisms for observing activities to avoid hazards such as passwords or token which can use multiple time, anonymous access, limited observation and inappropriate authorization [11].

Malicious Insiders

The malicious attack from insiders is one of the main risks and it is triggered by the cloud organization's trusted individuals who can access sensitive information from the company. Such individuals may participate in unprivileged acts that cause damage to the properties of the organization. The loss may be financial loss, loss of resource, loss of security or technological failure. This type of threat can obtain encryption keys, passwords and data easily [12] [13].

Account, Service and Traffic Hijacking

Account or service hijacking may occur if login credentials are obtained by an attacker. The intruder can manipulate data by using it, repay false information and can also launch multiple attacks. Nowadays, this vulnerability is broadly spread and crucial; many unauthorized users are getting credentials of account from different cloud consumers. [14].

Abuse and Nefarious Use of Cloud Computing

These types of facilities may be defined as immoral and illegal acts on the part of customers to exploit the services. Lax registration procedures, provisioning, loWcost infrastructure, high-resource have enabled hackers, spammers and other attackers anonymity for fulfilling their goal to do attack in the network.

TABLE I. SECURITY HAZARDS WITH THEIR PREVENTION TECHNIQUES IN CLOUD COMPUTING

Security Hazards	Affected Cloud Services	Prevention Techniques
Data Loss	IaaS, PaaS and SaaS	• Frequent backup • Use appropriate encryption techniques. • By protecting the transit data. • Strengthen key generation, storage and management implementation. • Legitimately defining strengthening and repair methods for suppliers
Data breaches	IaaS, PaaS, and SaaS	• By securing information on-transit • Use appropriate encryption techniques. • To protect data, both architecture and runtime should be analyzed. • Effective implementation of key generation, management and storage; • Legally identifying service provider for cleaning persistent media prior to discharge into the pool. • Lawfully specifying strategies for retention and replacement • By making good use of Application Programming Interfaces (API).
Insecure Interface and APIs	IaaS, PaaS, and SaaS	• High mechanisms for access and authentication verification. • Encrypted Data Transmission.

		• Cloud Provider Interface Analytics. • Adequate understanding of API-associated dependency chain.
Malicious Insiders	IaaS, PaaS and SaaS	• Render handling human resources (HRM) part of a formal agreement. • Strict implementation of protocol for supply chain management. • Giving security and administrative process proper clarity
Account, Service and Traffic Hijacking	IaaS, PaaS and SaaS	• Having knowledge of Service Level Agreement (SLA) and safety norms. • Methods of multifactor authentication are used. • Strict surveillance to detect unauthorized activities. • Impedes exchange of credentials between customers and services.
Abuse and Nefarious Use of Cloud Computing	IaaS and PaaS	• Using strong authentication and authorization. • Audits network traffic properly. • Enhanced oversight of credit card fraud.
Insufficient Due Diligence	IaaS, PaaS and SaaS	• Implementing applications and service according to the standards of industry in the cloud. • Provide details of data, applicable logs and infrastructure.
Shared Technology Issues	IaaS	• Use of mechanisms for stronger control of access and identity verification. • Observing threats and implementation. • Tracking condition for unwanted modifications / processes. • Use of Service Level Agreement SLA to patch and to remediate hazards.
Identity Theft	IaaS, PaaS and SaaS	• Strong credential, identity and access control mechanisms.
Different Service Delivery / Receiving Model	IaaS	• Services provided under control and supervised
Unknown Risk Profile	IaaS, PaaS and SaaS	• Disseminating details of possible data, and architecture. • Monitoring data breach alerting system.
Lock-In	IaaS, PaaS and SaaS	• Observing by the use of Instruction Detection System (IDS) and firewall implementation.

Insufficient Due Diligence

Insufficient due diligence can occur when organizations that use services provided by service providers do not have adequate information of cloud models and their workings, and do not understand which model fit with the risks they entail.

Shared Technology Issues

These issues happen in a multi-level environment where services are being offered on request through distributed. network between various authorized clients to the same virtual machine. In a multi-level environment the hypervisor can permit a suspicious user to have user data. The sharing principle could impact the cloud infrastructure overall allowing a user to have data of another user. Several methods for avoiding this problem are strong authentication and access control

Identity Theft

It is a kind of misdirecting in which attacker impersonates a legitimate user's identity, associated resources, credits, and other benefits of service. This hazard can happen due to the poor method of recovering passwords, phishing attacks, keyloggers etc. The security model integrates efficient multi-level verification techniques, efficient way of recovering password.

Different Service Delivery / Receiving Model

For transmitting or receiving of the service the dedicated methods has been used in business as well as cloud computing model. Hence, cloud computing is competent of changing the way services are delivered. All services and applications are assigned by the provider to a remote site, the company needs to look at all the risks related to the command loss over the cloud. Cloud information passes from every place apply various techniques of the security. That’s the key hazard arising at the time of use. A good encryption at source and destination, common protocol of security, etc. are required to eliminate these risks.

Unknown Risk Profile

This hazard can happen concurrently to the major benefits like saving time by owning and maintaining infrastructure. However, users are not anticipated to carry out patching, auditing, etc., resulting in an unknown risk profile that may enable critical hazards [15] [16].

Lock-In

This state addresses to the limitation of transmitting data through various clouds. This hazard happens when companies adopting the service of cloud with the lack of knowledge about which cloud environment matches them efficiently to prevent lock-in.

Attacks and Prevention Techniques in Cloud Computing

This section specifies the possible attacks with its prevention technologies on cloud computing security that can be adjustted to deal with those attacks. The following Table. II shows these attacks in terms of safety attack, cloud services that have been affected and their mitigation techniques.

Denial of Service (DoS) Attack

The suspector tries to disable the service in a DoS attack that is assigned to the authorized user by several techniques. An attacker may flood plenty of internet request packets to the victim to eliminate all of the resources. These data packets take up the network bandwidth and consume the resources of the server. This form of attack can thus impact the cloud's actual actions and cloud services availability.

The DoS attacks have several types, such as Distributed DoS (DDoS) attacks, that are expanded out of DoS attacks and include an attacker using multiple network hosts to exploit the victim with more debilitating effects [17],[18].Compared with a DoS attack, a DDoS attack is very complex and difficult to identify.

SQL Injection

In this attack, the attacker inserts nefarious code into the standard SQL code for unauthorized access to the database to gain user sensitive data. The main motive of it is to capture information from user such as usernames and passwords from the Web Application. By successful attack of it the attackers may get illegal access to the information and can perform the operations remotely, and may change the data in the standard database design [19],[20].

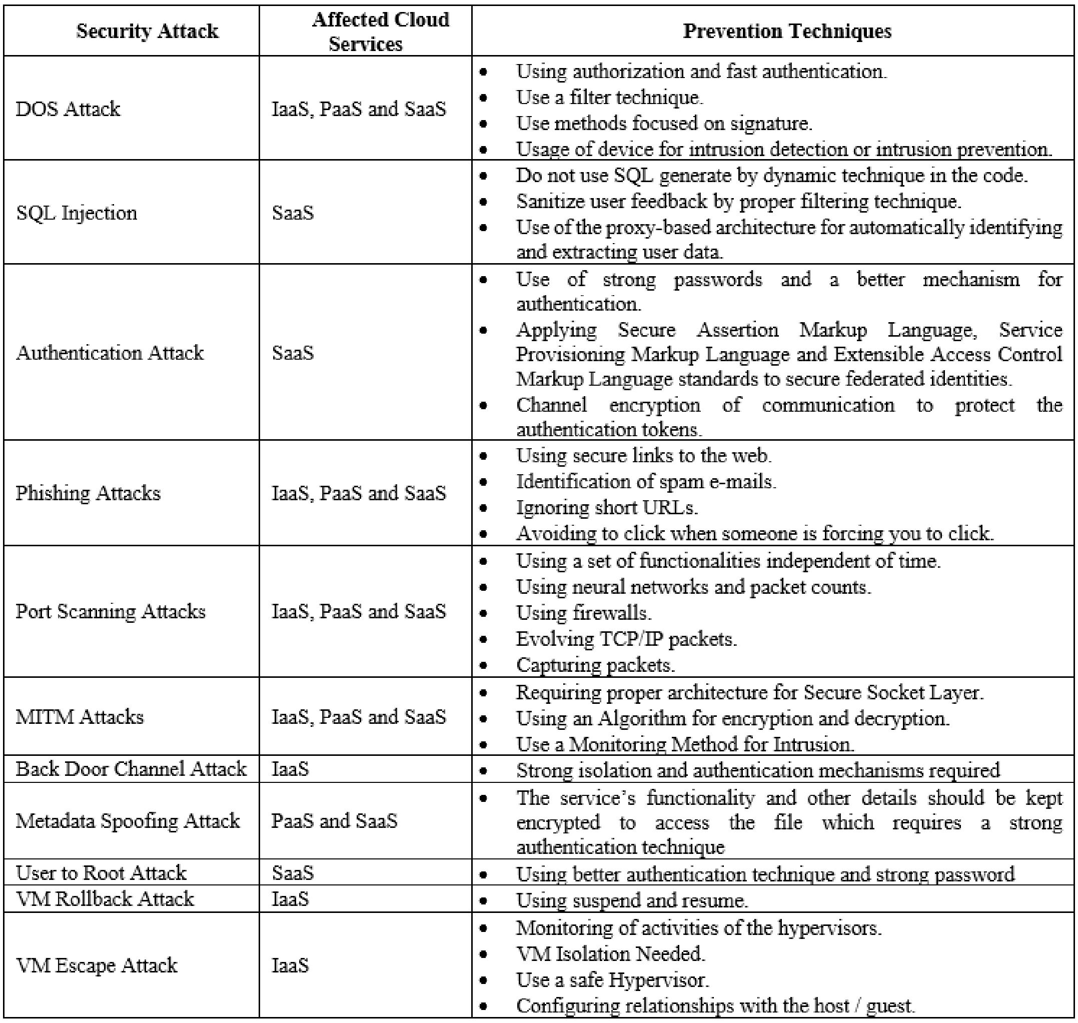
Authentication Attack

In cloud environments, authentication attacks will occur because of the poor username and password process that users often use. Consequently, cloud authentication attacks like dictionary attacks and brute-force attacks are the very susceptible [21]. In this attack, the attackers target the way of authentication used by the user for system's authentication [18],[22].

User To Root Attack

In user to root attack, the hacker gets unlimited control to the whole system by freezing an authorized user's account and password. This attack is carried out by overflowing data which sends excessive data to a static buffer.

TABLE II. 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 Attack	SaaS	• 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 relationships with the host / guest.

Phishing Attacks

Phishing attack for manipulating a web link is performed. In this attack the attacker redirects an authenticate person to a duplicate web page and gains control of sensitive data by hacking the user's account. Anti-spam software can be used to eliminate phishing attacks by finding outs the pop-ups or spam emails.

Port Scanning Attack

In port scanning attack, the attacker uses open ports services such as IP and MAC address that refers to the link to acquire accurate data of the processes running the application and working environment. The hacker then exploits this knowledge and takes advantages of weakness to direct attack as it is performed after the port process has been scanned [23],[24].

Man-In-The-Middle (MITM) Attack

This attack happens when the attacker is positioned in a cloud environment to insert false information in order to access the confidential information exchanged between two users. Nevertheless, if the medium of contact between two parties is secure less, the attack may occur in a continuous communication [25].

Back Door Channel Attack

The attack on the backdoor channel allows attackers have access to a remote computer program that monitors suspect's resources. Attackers, however, also use rear door channels to monitor victim services. It may infringe data privacy and data confidentiality.

Metadata Spoofing Attack

In metadata spoofing attack, the hacker wishes to have access of the file of Web Services Description Language (WSDL), which contains the functionality and details of the service, to do modification on the file. This can be achieved, if the hacker in the WSDL file succeeds in interrupting the service invocation code [26].

VM Rollback Attack

In the cloud environment, the tenant users have easy access to virtual machines (VMs). Therefore, they are the most dangerous area of the virtualized system. The attacker benefits from an old screenshot of a VM in a VM rollback attack and plays it without the user's knowledge. By a brute-force attack, the hacker can have the credentials for the VM though, the guest operating system has a limitation on the false attempts. Additionally, rollback, a permission control module, allows the attacker to change user permissions [27].

VM Escape Attack

In this attack, the hackers try to destroy the guest operating systems or have the control over the memory for controlling the hypervisor or insert the functionalities [22]. To break the isolation layer the attacker communicate directly with the hypervisor.

V. CONCLUSION

Nowadays, the Cloud Computing is one of the very emerging technology that provides enticing and remarkable quantifiable services allowing companies to exploit their levels of productivity and benefit while reducing expenses. Meanwhile, it has the capability to become a leading technology with virtual, secure and financially feasible solution available. It requires much more security due to its complex and dynamic nature. Much research is under way carried out on security of cloud to address its problems but owing to the very fast development of researchers of this technology and safety engineers were not in a position to provide sustainable options along the lines of the problems faced in this area rapidly increasing. Research sums up many of the threats to security and the prevention strategies and intrusion threats. It also classifies them as cloud services affect. The application of the proposed preventive measures are however limited. Future research work will begin to incorporate one of the proposed mitigation strategies and the probability of the risks.

VI. REFERENCES

[1]. Jansen, W. A., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing.

[2]. Chowdhury, R. R. (2014). Security in cloud computing. International Journal of Computer Applications, 96(15).

[3]. Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition.

[4]. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), 7-18.

[5]. A. Asma, M. A. Chaurasia and H. Mokhtar, Cloud Computing Security Issues, International Journal of Application or Innovation in Engineering & Management, 1(2) (2012) 141 - 147.

[6]. Ughade, K. A., & Chopde, N. R. (2015). Survey on Security Threats and Security Algorithms in Cloud Computing. International Journal of Science and Research, 4(4), 2196-2200.

[7]. Kajal, N., & Ikram, N. (2015, May). Security threats in cloud computing. In International Conference on Computing, Communication & Automation (pp. 691-694). IEEE..

[8]. Catteddu, D. (2009, December). Cloud Computing: benefits, risks and recommendations for information security. In Iberic Web Application Security Conference (pp. 17-17). Springer, Berlin, Heidelberg.

[9]. Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In 2011 World Congress on Information and Communication Technologies (pp. 217-222). IEEE.

[10]. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. The journal of supercomputing, 63(2), 561-592.

[11]. “CSA: The Notorious Nine Cloud Computing Top Threats," Cloud Security Alliance, 2013.

[12]. Claycomb, W. R., & Nicoll, A. (2012, July). Insider threats to cloud computing: Directions for new research challenges. In 2012 IEEE 36th Annual Computer Software and Applications Conference (pp. 387-394). IEEE.

[13]. Panah, A., Panah, A., Panah, O., & Fallahpour, S. (2012). Challenges of security issues in cloud computing layers. Rep. Opin, 4(10), 25-29.

[14]. Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

[15]. "CSA: Top Threats to Cloud Computing," Cloud Security Alliance, 2010.

[16]. Shah, H., Rajani, I. K., & Ramoliya, D. (2019). RENDERING THE GPGPU ACTIVITIES FOR ACCELERATION OF DYNAMIC THREAD PROGRAMMING IN HIGH PERFORMANCE COMPUTING.

[17]. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30-48.

[18]. S. T.K and D. B, “Security Attack Issues and Mitigation Techniques in Cloud Computing Environments,” Int. J. UbiComp, vol. 7, no. 1, pp. 1–11, Jan. 2016.

[19]. Wu, T. Y., Chen, C. M., Sun, X., Liu, S., & Lin, J. C. W. (2017). A countermeasure to SQL injection attack for cloud environment. Wireless Personal Communications, 96(4), 5279-5293.

[20]. Deshpande, P., Sharma, S. C., Peddoju, S. K., & Abraham, A. (2018). Security and service assurance issues in Cloud environment. International Journal of System Assurance Engineering and Management, 9(1), 194-207.

[21]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[22]. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[23]. Deshpande, P., Sharma, S. C., Peddoju, S. K., & Abraham, A. (2018). Security and service assurance issues in Cloud environment. International Journal of System Assurance Engineering and Management, 9(1), 194-207.

[24]. Akbarabadi, A., Zamani, M., Farahmandian, S., Zadeh, J. M., & Mirhosseini, S. M. (2013). An overview on methods to detect port scanning attacks in cloud computing. environment, 1, 22-25.

[25]. Singh, A., & Shrivastava, D. M. (2012). Overview of attacks on cloud computing. International Journal of Engineering and Innovative Technology (IJEIT), 1(4).

[26]. Anitha, R., Pradeepan, P., Yogesh, P., & Mukherjee, S. (2013, August). Data storage security in cloud using metadata. In 2nd International Conference on Machine Learning and Computer Science (IMLCS'2013), Kuala Lumpur (Malaysia) (pp. 26-30).

[27]. Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U. (2017). Intrusion detection techniques in cloud environment: A survey. Journal of Network and Computer Applications, 77, 18-47.

Cite this article as :

Rajeshkumar V. Patel, Dhaval Bhoi, Chandrashekhar S. Pawar, "Security Hazards, Attacks and Its Prevention Techniques in Cloud Computing : A Detail Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 48-58, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206417
Journal URL : http://ijsrcseit.com/CSEIT206417