Article title: Cloud Security Issues in Present Day Context

Authors: Zhimin Guan[1]

Affiliations: Singapore[1]

Orcid ids: 0000-0002-1533-7437[1]

Contact e-mail: sidl2201143508@students.mdis.edu.sg

DOI: 10.14293/S2199-1006.1.SOR-.PP1DI4J.v1

Preprint first posted online: 07 December 2022

Cloud Security Issues in Present Day Context

Guan Zhimin[1] and Dr Rama Bhatia[2]
MDIS / Teesside University, Singapore
Email ID[1]: SIDL2201143508@students.mdis.edu.sg
Email ID[2]: Rama_Bhatia@mdis.edu.sg

Abstract

This research broadly classifies cloud security issues in the present-day context. Over the years, IT experts saw the need of tackling cyber security issues while there is the interaction of software, people, and services through the internet, and what is cyber security? Cloud security is cyber security for safeguarding the cloud environment only. Numerous types of research classify cyber security issues but the list of the issue is still not all-inclusive and hence requires continuous research. This research work throws more light on cloud security issues and is an attempt to make the concept clear not only to serve as a dictionary for IT experts but also to clarify the concept easily to layman who wants to use the cloud for their businesses. The paperwork will make the layman understand the cloud security requirement thereby proving it secure enough and hence encouraging all people to further increase their usage of the cloud for their businesses.

Index Terms

Cloud security, virtualization, privacy, multi-tenancy, CIA triad, cyber security issues in the cloud, virtualization issues, network isolation, repudiation, cyber security issues in the cloud, perspectives, alleviation techniques for various cloud security issues, disruptive technologies, strong encryption tools, SSL, network security, application security, VM security, infrastructure as a code, configuration management, cloud federation related issues, cloud management, cloud billing, pay as you go, top cloud security statistics, Gartner and cloud adoption, existence and cloud adoption, cloud the top priority.

Introduction

Understanding security issues should always be the top priority and a proper taxonomy is a must. The search is further constrained by confining search for computer science followed by Cloud computing and subjects like cyber security and Information security do a world of good in further classification, and the majority of cloud security issues are from Information security and cyber security. However, there is a difference. In general when there is the interaction of software, people and services then there creeps in cyber security issues. The procedures, as well as technologies working for securing the cloud environment from insider and outside cyber security threats, are cloud security. (Tissir et al., 2020) found that the list of security issues in cloud computing is still not clear and the cyber security of cloud computing is more complex than the cyber security of even a large firm on-premise environment apart from individual computers and traditional computer networks not dealing with connectivity through the internet. (Shajan and Rangaswamy, 2021) and many more researchers have put forward cloud security issues but (Tissir et al., 2020) mention that there the security issues when it comes to cloud security are still not clear, The current work is hence a further investigation via the qualitative study of the cloud security issues to sort out the more profound list of cloud security issues in the present-day context. With time some improvements lead to new challenges while solving certain old problems, and all that will be the subject of research in this current research work.

Literature Review

NIST defines cloud computing as the ubiquitous, on-demand self-service broad network access of configurable resources and services via the internet. NIST further classifies cloud computing under three service models IaaS, PaaS, and SaaS, four deployment models public, private, hybrid, and community as well as five essential characteristics

On-demand self-service, measured services, resource pooling, elasticity, and Broad network access (Sharma et al., 2021). Sharma et al. (2021) further mention that SaaS offers software to access via an internet web browser, PaaS offers a developer-level platform for building applications and the IaaS offers infrastructure via APIs through the internet for computing, storage, networking, and memory. And each of these has several security issues. (Tissir et al., 2020) have already mentioned the non-clarity of security issues in a cloud computing environment. The router in a traditional network has different security challenges as compared to the cloud network as the cloud often is accounting for unknown traffic. The traditional network devices can be accessed only through a limited number of devices within the network and connected network. Cloud is connected through the internet and open for all, which leads to more concerning security issues. However, VM servers on the cloud are located within the VPC which can be connected with other VPCs through gateways like AWS transit Gateway and are surrounded by the firewall with a proper policy. Hence, such VMs are secure and in such cases, there is no network issue but there are multi-tenancy issues as the two different VMs can be located on one physical server, and that can lead to violation of boundaries and hence confidentiality and privacy issues (Wu et al., 2010) states that the VMs interconnectivity can pose a security issue if the superuser access to various VMs is configured without much care as one VM can control the other VM and that can create the isolation issue.

Looking at the features of the AWS or Azure network services available for securing the cloud networks it does seem that a knowledgeable person can secure VMs from all issues and hence the cloud with perfection. However, there are cyber security issues related to network security over the cloud as (Thabit et al., 2020) confirm that over the cloud there can be network security issues like DDOS attacks, DOS attacks, Network sniffing attacks, Network spoofing attacks, Phishing attacks, Social engineering attacks, malware attacks, Ransomware attacks, viruses, rogue security software, etc. Hence, there are a bunch of cyber security issues and a list of network security issues based on cloud characteristics, service models, and deployment models. And there are some well-known common cyber security issues related to the network.

Virtualization

(Sabahi, 2011) put forward virtualization level security issues like VM monitoring to check limited CPU cycles and I/O bottleneck which can affect VM performance as well as VM sprawling which results in too many VMs on the same physical server. Sabahi further put forward more virtualization issues like platform-level issues like Cross Site scripting and SQL injection. Moreover, the different VMs need to communicate between them and if this communication channel is not secure then it can lead to security challenges. Similarly, there can be multi-tenancy issues due to VM boundary isolation issues with a VM violating the boundaries of the other VM.

Hence, as the cloud is connected via the internet always except private cloud, there are all cyber security issues chances to exist in cloud computing. And the cloud is much more vulnerable to cyber security issues than the traditional computer system which is not that much subjected to the internet. Like when a user uses cloud services he is more vulnerable to cyber security issues as compared to the situation when he is communicating in a traditional network.

(Thabit et al., 2020) mentions IaaS, PaaS, and SaaS more elaborately, and it's essential for understanding the security threats related to the service delivery model. The best way to sum it up is as below:

Table 1: Security Threats as per Security Model

Delivery Model	Capability	Control over the Service
IaaS	This provides a pool of configurable resources like computing, network, storage, memory, and services on which users can install self-assertive software for various purposes like software development,	The client has control over the Operating system, software, storage, and application as well as storage but they do not have control over the network.

	machine learning, image recognition, web development, content development, or any sort.	
Platform as a Service	This helps clients to have control over the services the developer wants like a Database like DynamoDB, a single page application environment through Appsync, access management service Like Cognito from AWS, and Lambda for serverless, And this is the setup for Angular app development.	The client has control over the application deployed and configurations related to the programmer's environment. They don't have control over the control and board interface.
Software as a Service	Customers utilize the software utility provided by the cloud service provider through the internet browser.	A customer has control over only the application design settings. The confidential cloud infrastructure is hidden from the customer and even the platform level like application development settings. The customer cannot change the application code while using SaaS but they can in the case of PaaS.

(Thabit et al., 2020) further details the deployment models: public, private, community, and hybrid. The details are well known with the community being a cloud service shared by customers with similar interests. The rest of the details and classification are self-understood.

Cloud computing components

(Thabit et al., 2020) further mentions the cloud computing components like network resources, storage, and operating system framework, and under heading it are multi-tenancy, storage, hypervisor, storage, and network. Some more (Thabit et al., 2020) have not mentioned are cloud management services, billing services, memory, and compute is always the component of the cloud. Some more added recently are machine learning services, AI services, analytic services, business intelligence services, Identity and access management services, app development services, DevOps services, etc. And these all are components of cloud computing components. A perfect cloud computing network is made out of the about and not to forget security services.

Cloud Security Issues

(Thabit et al., 2020) as well as agreeing that the trust of the customer lies in the implementation model and the vendor. (Thabit et al., 2020) further mentions security requirements such as confidentiality, authentication, integrity, Authorization, and availability. CIA triad is always the first security requirement.

Some attacks come from internet-based issues like ARP spoofing, DoS, DNS, DDoS, port scanning, and phishing attacks.

(Thabit et al., 2020) have further classified the cloud security issues under the below heading, and it's noteworthy to list it here as it is, as it seems all-inclusive, The issues are life Trust and conviction, Application Issues, Client management issues, Data storage issues, Operating system base issues, network issues, and security policies. It's also noteworthy to further classify each of the above classifications as below:

Trust and Conviction

1. Human factor->Trusted Third party-> Reputation

Security policies

1. Service level agreement-> Antecedent Trust-> Lack of consumer trust

Client Management Issues

1. Authentication issues->Authorization

Client Management Issues

1. Security and Access Management-> Client Experience

Application Issues

1. The user front end-> Framework-> Web application-> Web server and technology, Standard and Protocol, Proxy server
2. User back end->Platform-> Parallel Application

Data Storage Issues

1. Data Warehouse-> Integrity and confidentiality-> Worm and malware

Data Storage Issues

1. Availability-> Metadata-> Data Sanitization and Maintenance, Data separation and location

Network issues

1. Intrusion prevention system-> Intrusion detection system->Firewall

Operating System Base Issues

1. Desktop OS-> Server OS-> Samrt OS
2. Network OS-> Embedded Security Issues-> Virtual Machine isolation, VM monitoring, SNMP server, Programmability

The above is a brief description but from (Thabit et al., 2020) even the detailed table compels to list all of them out here as it is a worthy inference for further investigation and hence included here in future work.

Table 2 Cloud Security Issues (Thabit et al., 2020)

Classification	Topic	Issues of the cloud
Trust And Conviction	1. Trust 2. Trusted third party 3. Governance 4. Lack of customer	1. Termination 2. Information sharing Location of data protection Reliability 3. Trust and privacy
Client Management Issue	1. Data warehouse 2. Anonymity-Availability and Cryptography-Privacy 3. Client-centric 4. Client authentication 5. and Client experience	1. Trust Loss of Control 2. CRM Policy 3. Eavesdropping 4. Identity 5. Authentication 6. Privacy 7. Cookie Poisoning 8. Authentication Attack 9. De Anonymity DOS/DDOS Hidden Identity , 10. Flooding attack 11. Key Management Outages Multiplication 12. Faulty Crypto Algorithm Cloud Disk Drives Die Without Backup
Security	1. SLA	1. SLA

Policies	2. Human factor 3. Trust, 4. privacy	specifies availability issues Installation and auditing monitoring failure. 2. antecedent trust
Application Issues	1. User front end 2. User back end 3. Platform 4. License 5. Framework 6. Parallel application 7. Forensic value 8. Service availability 9. Web application 10. Reputation	1. Masked Injection Engineering, SQL Injection 2. Proxy Injection Thread Termination 3. Flow Control Access Control Pirated Software 4. Botnet Dos Attack 5. MIM Mutual Authentication 6. IP Spoofing 7. DNS Spoofing 8. ARP Attack 9. XSS Attack 10. Authentication Loop 11. Data Disclosure 12. Data Seizing 13. Phishing, 14. Bating Password Sharing 15. Data Compromising Data Repudiation 16. Isolation Customer Behavior.
Cloud Data Storage Issue	1. Leakage a. Data loss confidentiality - Integrity 2. Malware a. Worm Management 3. Metadata	Data Diddling Attack Malware Botnet Attack Channel Attack Wrongly Session Hijacking Packet Sniffing Phishing Signature Based Implementation Of Destruction Policy Data Leakage, MIM Non Wiped Malware Injection and Side
Operating System Base Issue	1. VM Monitoring 2. Virtual Machine Isolation 3. SNMP Server Programmability Electronic Access Control Embedded Security Server OS Desktop OS 4. Smart OS	1. Cross VM attack Data leakage Untrusted VMM 2. Confidentiality Vendor Patch Configuration Setting Wrapping

	5. Network OS	Attack 3. HTTP Header Configuration Single Point Failure 4. Identity Physical Insecure Setting Remote Code Execution 5. Desktop Virtualization Unpatched Windows Server DoS/ DDoS attack 6. Spoofing 7. Snipping 8. Unpatched Network (Device Memory,) 9. Protocol Implementation In Ipv6 Consumption 10. Or Device Crash Stack Weak Server Side Control
		11. Client Side Injection 12. Broken Cryptography 13. TCP Implementation In Windows Mobile Android Malware Like Trojan, 14. Backdoor
Network	1. Flooding Attack 2. Computer Worm Adware Distributed Denial Of Service (DDoS), 3. Denial Of Service (Dos) 4. Trojan Horse, Spyware Phishing Rootkit, and Internet Protocol 5. Vulnerabilities	1. Network OS 2. Confidentiality and Integrity

Cloud Security Issue further Taxonomy

However, there are some common threats that the cloud is always prone to, and their knowledge is a must for all. (Thabit et al., 2020) has put forward such issues and their study is noteworthy and a must while curating the taxonomy for cloud security issues.

The first one as per (Thabit et al., 2020) is the weak service layer agreement. Issues related to this can be

Data unavailability, lock-in, hidden cost, Nontransparency of the infrastructure, and lack of adequate security measures. The threats are availability, confidentiality, and deferment. And these are the infiltrated attributes. (Thabit et al., 2020) has also mentioned the solution technique which is at the virtualization level, as well as the validation of clients and access controls. However, it does seem that this issue is much more dealing with the cloud service provider experience and optimization, and has less to do with virtualization level and validation of clients and access controls. However, (Thabit et al., 2020) are right in mentioning that this is going to affect IaaS, PaaS, and SaaS all.

(Thabit et al., 2020) further mentions the abusive use of cloud services as an issue and defines it as the unlawful use of cloud services by the client. The infiltrated attributes are Authentication and integrity, and affected services are like IaaS and PaaS. (Thabit et al., 2020) have rightly mentioned the solution as the proper auditing of the network traffic, better credit card monitoring, and a good level of authentication and authorization.

Then we have the denial of service as per (Thabit et al., 2020). In this, an intruder or a foe gets hold of someone else VM and makes some web server out of the reach causing a denial of service. Thabit et al. have rightly mentioned the infiltrated attributes as resource availability and privacy. And affected services are certainly all IaaS, PaaS, and SaaS. As a solution, Thabit et al. have mentioned strengthening the DNS services against DDOS attacks.

Another threat as per (Thabit et al., 2020) is Data breaches. A data breach means delivering, surveying, and utilizing the data for the wrong cause without proper authentication and authorization. The solution is certainly encryption, proper storage, key management, and overall management. And the affected services are all three. (Thabit et al., 2020) has not mentioned any infiltrated attributes.

The next one as per (Thabit et al., 2020) is the advanced persistent threats. This is a digital assault that infiltrates through the framework for setting up the traction in the computing infrastructure of various companies for which the intruder ransacks the information as well as protected innovation. The infiltrated attributes are trust and integrity and the affected service is the SaaS. The solution is intrusion detection.

(Thabit et al., 2020) further mentions TCP/session. In this type of threat, the attacked computer is substituted by another computer and the solutions are concealment as well as integrity and availability. The affected services are like IaaS and the infiltrated attributes are like accountability and weak trust.

(Thabit et al., 2020) further mentions another threat as hijacking. The IP address of the customer Is hijacked and the server keeps on having faith in the sender leading to serious fraud and ultimately a big cyber-attack. The infiltrated are like integrity registration system, and service availability. The solution certainly is the use of a proper firewall with a good firewall policy.

(Thabit et al., 2020) further mentions the Account or service hijacking. This can happen when the intruder gets hold of the login information of the client. This affects IaaS, PaaS, and SaaS, all three. The infiltrated attributes are service availability, integrity, trust, and audibility. (Thabit et al., 2020) mentions the solution as multi-factor authentication, proper knowledge of SLA and security policies, detection of unauthorized activities and stern monitoring, and saving credentials from intruders.

(Thabit et al., 2020) further mentions the data loss as a cloud security issue. By definition, for selling the services to a third party the service provider can fraudulently store the data of a client. The infiltrated attributes are system and privacy protection, availability, and auditing of networks. The affected services are all three IaaS, PaaS and SaaS. The solution is encryption and proper backup. protection of data in transit, proper key management, and regular wipe-up of the persistent media for it being delivered to the pool.

(Thabit et al., 2020) further mentions meltdown as an issue and defines it as the breaking of the detachment between the client’s application and the Operating system framework. The infiltrated attribute is privacy protection, and the solutions are protecting data during transit as well as proper patching at regular intervals. The affected services are SaaS and IaaS.

Then (Thabit et al., 2020) mentions malicious insiders, and the definition of this is the threat from the internal employees of the organization due to their illiteracy or due to their bizarre aspiration. The infiltrated attributes are confidentiality, availability, and deferment. And the affected solutions are all three IaaS, PaaS and SaaS. As a solution, there should be good accuracy between the security and administrative processes, and the HRM should be the section in legal contracts. The flexibility in the chain administration method should be applied.

(Thabit et al., 2020) further mentions online cyber theft is the fraudulent activities of an intruder for financial fraud or sensitive data theft as well as stealing national-level security assets. It affects PaaS and SaaS. The solution is distributed computing administration which reduces cost and makes life easier for clients through various security measures against cybercrime issues.

(Thabit et al., 2020) further mentions privileges elevation as one of the cloud security issues with the definition as when someone tries to break all boundaries and grab higher privileges to get hold of something expensive or top secret. The infiltrated attributes are trust, authorization, confidentiality, and identity. The solution is the use of multi-tier core words for authentication.

Thabit et al. then come up with repudiation. Here the client executes a criminal offense that cannot be tracked. And the solution for this is robust authentication and authorization technique usage.

(Thabit et al., 2020) further mentions insecure API and interfaces, and the infiltrated attributes for this are authentication and authorization, The allude to the API guide as well as the convention which the client use to connect with the cloud. And if the API and interfaces are insecure then they are going to cause the issues. The infiltrated attributes are authentication and authorization. And the solution is good encryption, good authentication, authorization, and good dependency chain administration of the APIs.

(Thabit et al., 2020) further mentions Data manipulation as an issue with infiltrated attributes being integrity, suitability, and availability. The services affected are SaaS. The definition is data insertion, deletion, and modification. The solution is the use of encryption, proper monitoring of log data, and checking for unauthorized access regularly.

(Thabit et al., 2020) further mentions shared technology issues and this covers the multi-tenancy issue which has been covered numerous times previously above.

(Thabit et al., 2020) then put forward the due diligence insufficiency issue which can be the cloud security issue. Here the customer starts making use of the cloud services without proper knowledge of the cloud services. The infiltrated attributes are availability and integrity. The affected service models are all IaaS, PaaS, and SaaS. The infiltrated attributes are integrity and availability. The solution is the implementation of standards for cloud applications and services. Checking log data regularly is also a solution.

Further cloud security issue as per (Thabit et al., 2020) is backed up and that is quite clear to all as issues with backup can create issues, and it's necessary without any doubt. The infiltrated attributes are availability and reliability. The solution is multiple backups.

Some others as per (Thabit et al., 2020) are vendor lock-in, lack of knowledge of risk profiles, and changes in business models. The infiltrated attributes for the three respectively are confidentiality, authorization, and availability for the first, Authorization and authentication for the second, and confidentiality, authorization, and trust for the third. For Lock-in the solution is like the implementation of a firewall, Prevention system, and intrusion detection monitoring. For the unknown risk profile, the solutions are auditing and detecting log files. The solution for changes in business models is like a nursing system of given services, as well as the provisioning of controls. The affected service models in each of the above three cases are all IaaS, PaaS, and SaaS.

Alleviation techniques for various cloud security issues

(Thabit et al., 2020) further mentions the cloud security issues based on the security levels. There are some security levels under which we can find out various cloud security issues. They are:

1. Basic Level
2. Application Level
3. VM level
4. Network level

Various cloud security issues can be classified under these security levels and it's worth discussing and curating the alleviation technique for each of them. Alleviation techniques are the remediation or mitigation techniques with the help of which the cloud security experts get hold of these security issues. Hence, it will be a wise idea to sort down the security attack type, security level, and the alleviation technique. However, it’s also essential to write down a brief description for each of them to clarify what they are as mentioned by (Thabit et al., 2020).

Table 3: Security Issues related to Security level

Security Assaults	**Definition**	**Security Level**	**Mitigation technique**
Data Structure-related Assaults	The intruder takes advantage of the system attributes and finds loopholes in the information structure via system management.	Application Level, VM level	There should be a good authentication setup in place. Content filtering is a must. There should be continuous monitoring of the vulnerabilities and configuration changes. There should be continuous monitoring of the changes and malicious activities.
Inclusion of Malicious codes	In each of the codes, there can be malignant code that can sabotage the application and make it vulnerable to cyber-attacks.	VM level	This provides the required clarity to administrative and security processes.
SQL Injection	The intruder infuses the malicious code for inquiry into the program code and injects the malware to alter the database.	Application level Basic level	The user input must be sterilized. Eschow with the help of the dynamic SQL code into the program code. Make use of proxy-based architecture for dynamically disclosing as well as extracting the input by the end user.
Plashing Assault	The attacker makes use of cloud services for phishing attacks. He gets hold of the webserver to divert the client to some fraud connection.	Basic level	Know about phishing over the cloud.
Cross-Site Scripting assault.	The attacker inserts the malignant	Basic Level Applicati	Make use of the web application

	code to divert the client site to the attacker's site for gaining important and secret information that has monetary or strategic value.	on Level	vulnerability discovery technology. Make use of the collaboration browser. Make use of technology to stop data leakage. Use of Secured Socket layer. Ensure regular filtering of content. Make use of anti-malware software. Reduce the dependency on the browser.
Authentication Exploitation	Here the attacker gets hold of the administrative and management interfaces and excess client profiles, as well as inappropriate verification and approval, which can help the attacker for making wrong use of the indirect access weakness.	Application Level	Make use of the intrusion detection system Proper and reliable authentication and authorization.

DNS attacks	Here the attacker makes evil use of the Domain name server vulnerabilities.	Network level	Making use of the DNS security what we know as DNSSEC.
Dos Attack	Here the attacker makes the services of some high-profile company websites inaccessible. Various types are like ICMP flooding, HTTP flooding, UDP flooding, SYN flooding, NTP application, Ping of Death, etc.	Application level	Making use of the IDS system Proper authentication and authorization
DDOS attack	Distributed Denial of Service attack is a kind of Dos attack where there are multiple online devices which we know as the BotNet connected to the website which makes the website look vulnerable by directing a large volume of traffic to the	Application level	Making use of the IDS Making use of proper authentication and authorization.

	website.		
Man in the middle attacks	At any point between the connections, the attacker tries to infuse the malicious packet to gain important secret shared data.	Application level	Making use of the SSL Making use of hard-to-beat encryption tools like Wsniff, Airjack, etc.
Probabilistic technique	Here the attacker refers to likelihood-based assault.	Network Level VM level	Making use of strong encryption tools and making use of SSL,
IP which is reused	The IP address delegated to the one user is assigned to a new client when the first client leaves the connection.	Network level	Proper use of authentication and authorization Proper use of Intrusion detection system.
Zombie Assaults	In this, the affected VM is over-flooded via methods for sending demands from various VMs in the network. A Malicious code on a VM can turn it into a zombie.	Network level VM level	Proper use of the authentication and authorization as well as IDS/IPS system.
Sniffer Attacks	The network interface card of the client is embedded with the malicious code and the streaming bundles are sniffed for stealing secret information, and is important to understand that the network traffic is controlled by the attacker during a sniffing attack,	Network level	Making use of the Round trip time for sniffing detection. Making use of technology like ARP for sniffing detection.
Wrapping Attacks	The attacker injects a fake element into the message. The valid signature covers the unmodified message and the application logic processes the fake one.	Application level	Make use of SSL and good signature methods.
Cookie Poisoning	Here the cookie content is altered to gain access to some web services or unauthorized applications.	Application level	Use of better encryption technique Regular brushing of the cookie content, For developing sessions with the help of different authentication processes. Through whirling of web

			browser security policies.
Protocol Manipulation	Here the attacker subverts the communication protocol for coming up with a cyber-attack.	Network Level VM level	Make use of IDS Proper authentication and authorization,
Resource depletion	In this type of attack the resources are made to deplete faster and as they finish the access to the node by devouring it is stopped much like the DOS attack.	Application level VM level	Making use of IDS and IMS for proper authentication and authorization
Captcha Breaking	Captcha images can be broken within 15 minutes these days through machine learning and computer vision.	Application level	Making use of background perturbative. By raising the string strength. Through avoidance of the vertical segmentation attacks Varying font size Opting for letter overlap
Spoofing attacks	In this someone attempts to prove that he is someone else to gain confidence. And then he leads to a cyber-attack after gaining a certain strategic location.	VM level Network level	Detecting unauthorized activities Multi-factor authentication Preclude sharing of information between client and services.
Google hacking attacks	Here client makes use of the Google search engine to find the loopholes in the design.	Application level	Making use of the standard security technology to discover vulnerabilities associated with the web. Proper authentication and authorization. Implementing policies related to the backups like continuous data protection CDP.
Hypervisor assaults		VM level	Making use of proper hypervisor security monitoring tool. Making use of proper VM isolation techniques.
Path Traversal Attacks	The goal is to access files and directories which are outside the web-root folder.	Application level	Making use of SSL Making use of standard techniques for signature.

Further classification of Cloud Security Issues

To sum it up, and all angles for a Cloud, there are security issues that come under the below headings as per (Saurabh et al., 2016):

1. Embedded Security issues
    a. VM monitoring
    b. VM induction
    c. Electronic access control system
    d. SNMP server
    e. Programmability
2. Trust and conviction
    a. Human factor
    b. Forensic factor
    c. Governance
    d. Reputation
    e. No consumer trust
    f. Trusted third party
3. Application issues
    a. Front end
    b. Back end
    c. Application
    d. Framework
    e. Service availability
    f. Parallel applications
    g. License
    h. Web applications
    i. Proxy server
    j. Web server
    k. Protocol as well as standard
4. Client management issues
    a. Client experience
    b. Client-based privacy issue
    c. Client authentication issue
    d. Service level management
5. Cluster computing
    a. Physical cluster
    b. Multi cluster
    c. Virtual Cluster
    d. Creation of data-intensive apps
6. Cloud data storage
    a. Anonymization
    b. Availability
    c. Data loss and leakage
    d. Cryptography
    e. Confidentiality and Integrity
    f. Unreliable data
    g. Data warehouse
    h. Metadata
        i. Maintenance
        ii. Data Sanitization
        iii. Data Separation
        iv. Data Protection
7. Operating system issues
    a. Desktop OS
    b. Server OS
    c. Network OS
    d. Smartphone OS
        i. iPhone OS
        ii. Android OS

However, there is a lot of similarity between (Saurabh et al., 2016) and (Thabit et al., 2020), and both Saurabh et al. and Thabit et al. are finally up with the same sorts of vulnerabilities.

Cloud Security Concepts

However, it's also important to understand what the cloud security concepts are and they are as below:

- Software security
- Network security
- Infrastructure security
- Storage Security

And there can be a fifth security issue which is the virtualization security not mentioned by (Saurabh et al., 2016).

So the fifth cloud security concept is the

- Virtualization security

(Saurabh et al., 2016) has in their research described each of these and it looks worthy to have a little bit of explanation for each of these.

Software Security

This requires building the cloud environment so that the security of the environment is critical which the software security problem is. The implementation bug, design flaws, flaws in error handling, and buffer overflow are some of the prime concerns (Saurabh et al., 2016).

Infrastructure security:

It's should be an account as only then virtual as well as physical infrastructure will be trustable. Infrastructure must be secured and business requirements are the top priority when selecting infrastructure. To be more accurate virtualization security is discussed under infrastructure security only and the main issues have been discussed already and hence skipped here.

Storage Security

The end users store the data on the cloud and don't have control over it. The correctness of the user data over the cloud through the utilization of appropriate technologies is the top priority. (Saurabh et al., 2016) has mentioned one method like utilization of homomorphic tokens with erasure-coded data distributed verification. More concerns are data sanitization, data remanence, data availability snooping, cryptography, data leakage, and malware.

Network security:

Internet is the backbone of cloud computing and network security as per (Saurabh et al., 2016) is essential to save from both internal and external assaults. The security problems of the virtual and physical networks are a prime concern.

And (Saurabh et al., 2016) have mentioned the cloud computing components as network, virtualization, storage, hypervisor, and multi-tenancy which are already discussed.

(Sharma et al., 2021) put forward the scanners such as Nessus, IBM QRadar, Nmap, Acunetix, and QRadar are good enough to catch the vulnerabilities in the cloud system. And for penetration testing, Sharma et al. have mentioned Kali Linux as the best option, and cyber security certainly confirms that these tools are awesome but the Vulnerability analyst must have knowledge about the vulnerability, and only then they will have the best value for the reputed seat. Also, they need to investigate various parameters related to the vulnerabilities like CVSS score, and the number of ports open as they need to rank the vulnerabilities based on severity and CVSS tally.

And thus, we have a detailed list of cloud security issues and hence the cloud security vulnerability list. Further cyber security steps need to be taken for further investigation, and final remediation or mitigation of the issues as required.

Methodology

The topic of this research paper requires a qualitative study as it is listing the cloud security issues in the present-day context that turns out to be vulnerabilities to be exploited by intruders for their non-judicially correct benefits. Also, the authors have preferred to gain insights from the past 2-3 years' research papers found on Google scholar via sites like reputed IEEE and springer via their institution access. The authors have used the best keywords for selecting the best and latest research papers. And once, the top cloud security issues from the present-day context have been sorted out, only then they have gone to the older research papers, merely to collect the histories of the security issues. It's well said the old is gold and the authors have seen through the past as well hence. The concepts of systematic review like PRISMA have been used partially to sort out the research papers which are most subjects oriented but equal concentration has been laid on each of the research papers to ensure the best 360-degree research to come up with the best list.

And mostly it is the textual research that has been conducted for understanding the research papers, and there has been no use of AI for the research for gaining any insights. All inferences are purely manual research results.

Moreover, the authors have focused on past research papers, however, some textbooks have also been consulted, and all authors have been properly cited to ensure they get the due respect for their work. The paper is purely academic work. Sources like Survey Monkey and Linked In were under the author's radar but they have managed to close the requirements without any other expert's point of view. However, the authors do encourage the research scholars to use these as they help in the best level of research. There is no practical involved but the research work will inspire and open the gate for practicality for all the readers as per the authors.

Research Findings/Analysis

(Saurabh et al., 2016; Thabit et al., 2020) have mentioned all the threats in the cloud and are all-inclusive. However, various others (Sharma et al., 2021; Shajan et al., 2021; Rosian et al., 2021; Wu et al., 2011) have also put forward the cloud security issues, and a briefing of all in a nutshell with the required elaboration has been stitched together in the Literature review. Further textual analysis of the content collected confirms that the showdown in the literature review is the all-inclusive list of the cloud security issue that as a virtual analyst one needs to keep in mind while investigating the cloud for vulnerabilities.

The issues mentioned in the Literature review are further extended with issues like elasticity engines, Vendor-Lock-in, multi-tenancy, data management, and SLA management which are always on the forehead of cloud security experts. As per (Sridhar and Smys, 2016) the cloud consumer perspective concerns the adoption of cloud models. Also, there is an issue of Loss of control as it's the third party that hosts the IT hardware and software.

Perspective:

VM issues are already being mentioned in detail in the Literature and that is all-inclusive. However, perspective requires mentioning like:

1. Architecture based issues
2. Cloud Stakeholders' relevant issues,
3. Service delivery model-related issues,
4. as well as cloud characteristics-based issues

Both the cloud provider and the cloud consumer need to understand their part in the shared security responsibilities. (Almorsy et al., 2016) have thrown light on the above for cloud providers and vendors. Various security standards like Cloud security alliance, ISO IEC 27001, and Open virtualization format play a major role in explaining cloud security. The IaaS, PaaS, and SaaS-related issues have already been mentioned in the Literature review.

Also when it comes to cloud security policy there is a lack of transparency and also SLAs are high-level documentation lacking smaller issues that are essential to be included.

Also, further in VM security malware and viruses do affect it. Also, there can be DNS server-related issue which is already covered.

VM boundary issue already covered is still an issue and results in an attack on the CIA triad.

The hypervisor-related issue is already covered. Containers are more scalable but they also pose boundary isolation issues.

To be more precise, we can further classify the issues as:

1. PaaS security issues
2. SaaS security issues
3. IaaS security issues
4. Cloud Management Layer Security Issues:
5. Cloud Access Methods security issues:
   Cloud provides resources through the internet, and it's possible to access these resources through the HTTP requests-response when it comes to web applications, or the RPC, REST, or SOAP when we talk of the API-PaaS and CML-APIs. In the case of the VM, the access is through the VPN and FTP which ensures a remote connection. The security controls need to target the issues related to these protocols for the best level of cloud security.
6. Key Management
   As per (Almorsy et al., 2016) Key management is another concern when it comes to data security. The public key needs to be securely generated and shared across the users. Remember, we now have the PKI but this was a big issue in the past, and with improper key management the cloud security is certainly challenged by intruders. Even PaaS API requires Key exchange and improper key exchange methods can lead to big cloud security issues without any doubt.
7. Security Management
   Security Management should act as a plugin for the CML. The security concerns in the security management policies must be addressed through the implementation of required security controls.
8. Secure Software Development Lifecycle
   Through the implementation of DAST and SAST web applications are analyzed for vulnerabilities. However, security engineering has taught a lot of lessons, and now secure code for tackling all coding issues like DDOS, and SQL injection is possible, and the code can be written such these kinds of security issues can be avoided and that helps in planning secure software development lifecycle.
9. Security Performance tradeoff optimization
   (Almorsy et al., 2016) then mentions that the SLA mentions the criteria for performance, reliability, and security. However, too much security necessitates too voluminous security controls, and this can destroy performance. Hence, there should be a tradeoff between performance and security

created on the current and expected threat level and seeing other tradeoffs. Unquestionably, the augmented security concerns affect the performance as that necessitates so many possessions like security tools, and that destroys the performance.

10. Federation of security among multi-cloud When the application makes use of more than one cloud service provider, if there is a federation of such CSPs then it will be possible to apply and implement the security across the clouds what we know as the multi-cloud. Such federation is very essential.

Some Useful Statistics results collected:

Cloud Adoption Surprises:

a. Lack of visibility 49%
b. Not secure: 22%
c. Not enough control: 42%
d. High cost 43%

Biggest Security concerns:

a. 62% Misconfiguration of cloud platforms and incorrect setup
b. 51% Exfiltration of sensitive data
c. 52% Insecure Interfaces/APIs
d. 37% of foreign state-sponsored security attacks

Key cloud security priority

a. Preventing Cloud Misconfiguration 20%
b. Reaching regulatory compliance at 19%
c. Security major cloud apps already in use 16%
d. Defending against malware 15%
e. Cloud security training 11%
f. Securing Mobile devices 8%
g. Discovering unsanctioned cloud apps in use 5%
h. Securing Bring your own device 5%

Improving security controls

a. Encryption of data at rest 54%
b. Automating compliance 46%
c. Setting and enforcing security policies across clouds: 46%
d. APIs for reporting, auditing, and alerting on security events: 42%
e. Isolation/protection of virtual machines 41%
f. Creating data boundaries 41%
g. Leveraging data leakage prevention tools: 41%

Multi-cloud security challenges

a. Having the right skills to deploy and manage a complete solution across all cloud environments 61%
b. Ensuring data protection and privacy for each environment 53%
c. Understanding how different solutions fit together 51%
d. Loss of visibility and control 47%
e. Understanding service integration options44%
f. Keeping up with the rate of change37%
g. Selecting the right set of services36%
h. Managing the costs of different solution36%

Single Cloud Security Platform

a. 78%of professionals consider the use of a single cloud security platform with a single dashboard to be very to extremely helpful.

Configuration Management
Configuration management can be a cumbersome task and a never-ending saga. However, this research throws light on tools that are available these days like Chef, Puppet, Ansible, SolarWinds, etc. And their usage can make the configuration management task much easier. However, these also throw light on how many types of configuration management we have, and what we need to configure in the software industry (SCM tools in 2022, 2022).
Infrastructure as a Code has solved the issues related to configuration management considerably.

Domains in cloud Security by Cloud Security Alliance:

Apart from the above studies, it’s always a good thing to have a look at the documentation of a cloud security alliance for cloud security. There are 14 domains in CSA documentation for the cloud security issues:
Domain 1: Issues related to the cloud architecture
Domain 2: Enterprise a Risk management and governance
Domain 3: Legal issues: Contracts and E-Discovery
Domain 4: Compliance and Audit Management

Domain 5: Information management and Data Security
Domain 6: Interoperability and Portability
Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
Domain 8: Data Center Operations
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Encryption and Key management
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Virtualization
Domain 14: Security as a Service
For cloud security, it’s essential to look into the above issues as a whole. And that briefs the cloud security issue as a whole (Citadel Information Group, no date).

Conclusion

With time Cloud computing is becoming more important and companies cannot ensure their existence without applying for cloud computing. Cloud computing saves time and reduces the cost considerably but the security issues discussed herein are a major concern and stop especially small organizations from opting for the cloud. However, there is no other choice. And cloud security is a shared responsibility. The vulnerabilities in this paper clarify the issues a consumer can face while using the cloud and it also lets the providers know where they need to work. The paper hence is an attempt to sort out all cloud security issues. And with this list majority of the cloud security issues are indexed and even their mitigation techniques. The providers are always researching the vulnerabilities in their system, and hence this paper must be read by cloud consumers or clients before they opt for the cloud for their businesses. This will get them ready to tackle all the issues that they have to deal with when they opt for the cloud.

Recommendations

The work on the Multi-tenancy issue is certainly the foremost requirement, and data security, network security, and application security needs more elaboration ensuring business continuity and disaster recovery in the worst condition should be the top priority for the cloud providers. Cloud consumers should, however, keep themselves updated with all the cloud security issues or their security shell, And they must ensure adherence to the standards set by the top organizations like NIST and also follow the instructions provided by the cloud service provider to ensure the fulfillment of their part in security. However, a transparent SLA should also be the responsibility of the cloud service provider as without it the cloud consumer or clients are never going to be fully satisfied and they always will be up with issues as they will not know completely and clearly what role they need to play to ensure the best level of cloud security. Also, the container issue should be among the top priority of the cloud service provider.

Also, it’s a confirmed fact that no company will now be able to stand in the market without the cloud, and it's also true that cloud security is a shared responsibility. Hence, both the cloud service provider and the cloud consumer or the clients should understand their role and they need to act as such to ensure the best level of cloud security as it also confirmed that even a single security breach can be lethal and end of roads for small companies as they will not be able to manage the such level of monitory loss as an average cost of one cyber security breach is in million dollars. This paper is an attempt to sort out the vulnerabilities and cyber security concepts that are very elaborate now. The authors feel that however, the first step starts with understanding vulnerabilities, and only then a cyber-security team can be up with risk and vulnerability management. And for a better future, all of these issues should be the prime concern for tackling cyber security issues.

Also, technology is increasing its dominance in society and after covid 19, cloud computing technology which is a disruptive technology has become even more important. All the citizens of the world must make sure that they get themselves ready to make the best use of the technology as with the best technology they can tackle cybersecurity issues much better.

References:

[1]. 11 best software configuration management tools (SCM tools in 2022) (2022) Software Testing Help. Available at: https://www.softwaretestinghelp.com/top-5-software-configuration-

management-tools/ (Accessed: November 17, 2022).

[2]. Ahmed, A. and Zakariae, T., 2018. IaaS cloud model security issues on the behalf of the cloud provider and user security behaviors. Procedia computer science, 134, pp.328-333.

[3]. Ahmed, M., Chowdhury, A.S.M.R., Ahmed, M. and Rafee, M.M.H., 2012. An advanced survey on cloud computing and state-of-the-art research issues. IJCSI International Journal of Computer Science Issues, 9(1), pp.1694-0814.

[4]. Almorsy, M., Grundy, J. and Müller, I., 2016. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[5]. Almorsy, M., Grundy, J. and Müller, I., 2016. An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[6]. Antonenko, D. (2021). Cloud computing security issues and challenges - Businesstechweekly.com. [online] Businesstechweekly. Available at: https://www.businesstechweekly.com/cybersecurity/data-security/cloud-computing-security-issues-and-challenges/.

[7]. Battina, D.S., 2020. DevOps, A New Approach To Cloud Development & Testing. International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, pp.2349-5162.

[8]. Citadel Information Group (no date). Available at: https://citadel-information.com/wp-content/uploads/2012/08/security-guide-cloud-security-alliance-csaguide.v3.0.pdf (Accessed: November 21, 2022).

[9]. Cloud Security Report. (2022). [online] Available at: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-cloud-security.pdf.

[10]. Cognism (2022) what is a go-to-market strategy? (Complete Guide for 2022), Cognism. Cognism. Available at: https://www.cognism.com/blog/what-is-a-go-to-market-strategy (Accessed: November 20, 2022).

[11]. Dodig-Crnkovic, G., 2015, September. Preparing the next generation of software engineers for future societal challenges and opportunities. In Proceedings of the 7th International Workshop on Social Software Engineering (pp. 49-52).

[12]. Donald, A.C., Oli, S.A. and Arockiam, L., 2013. Mobile cloud security issues and challenges: A perspective. International Journal of Engineering and Innovative Technology, 3(1), p.401.

[13]. Editor, B.B. and S. (2009). Defining Cloud Security: Six Perspectives. [online] CSO Online. Available at: https://www.csoonline.com/article/2124412/defining-cloud-security--six-perspectives.html [Accessed 3 Nov. 2022].

[14]. Gupta, S. and Kumar, P. (2013) “Taxonomy of Cloud Security,” International Journal of Computer Science, Engineering and Applications, 3(5), pp. 47–67. Available at: https://doi.org/10.5121/ijcsea.2013.3505.

[15]. Ibikunle, Francis. (2011). Cloud Computing Security Issues and Challenges. 2011-247.

[16]. Islam, T., Manivannan, D. and Zeadally, S., 2016. Classification and characterization of security threats in cloud computing. International Journal of Next-Generation Computing, pp.01-17.

[17]. Jaiswal, P.R. and Rohankar, A.W., 2014. Infrastructure as a service: security issues in cloud computing. International Journal of Computer Science and Mobile Computing, 3(3), pp.707-711.

[18]. Jangjou, M. and Sohrabi, M.K., 2022. A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, pp.1-22.

[19]. Kumar, P.R., Raj, P.H. and Jelciana, P., 2018. Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, pp.691-697.

[20]. Lurie, Y. and Mark, S., 2016. Professional ethics of software

engineers: An ethical framework. Science and engineering ethics, 22(2), pp.417-434.

[21]. Mell, P. and Grance, T., 2011. The NIST definition of cloud computing.

[22]. Mills, J. and Birks, M., 2014. Qualitative methodology: A practical guide. Sage.

[23]. Patel, N.S. and Rekha, B.S., 2014. Software as a Service (SaaS): security issues and solutions. International Journal of Computational Engineering Research, 4(6), pp.68-71.

[24]. Pimple, K.D., 2002. Six domains of research ethics. Science and engineering ethics, 8(2), pp.191-205.

[25]. Prasad, C.S.S., Yadav, B.P., Mohmmad, S., Gopal, M. and Mahender, K., 2020, December. Study of threats associated with cloud infrastructure systems. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022055). IOP Publishing.

[26]. Rosian, M., Hagenhoff, P. and Otto, B., 2021. Towards a Holistic Cloud Computing Taxonomy: Theoretical & Practical Findings. In AMCIS.

[27]. Sabahi, F., 2011, May. Virtualization-level security in cloud computing. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 250-254). IEEE.

[28]. Sadooghi, I., Martin, J.H., Li, T., Brandstatter, K., Maheshwari, K., de Lacerda Ruivo, T.P.P., Garzoglio, G., Timm,

[29]. S., Zhao, Y. and Raicu, I., 2015. Understanding the performance and potential of cloud computing for scientific applications. IEEE Transactions on Cloud Computing, 5(2), pp.358-371.

[30]. Saurabh Singh, Young-SikJeong and HyukParkaPerson, J. (2016) A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications. Academic Press. Available at: https://www.sciencedirect.com/science/article/pii/S1084804516301990 (Accessed: November 23, 2022).

[31]. Shajan, A. and Rangaswamy, S. (2021) ‘Survey of Security Threats and Countermeasures in Cloud Computing’, United International Journal for Research & Technology, 02(07, Al Nafea, R. and Almaiah, M.A., 2021, July. Cyber security threats in the cloud: A literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779-786). IEEE.2021).

[32]. Shakir, M., Hammond, M. and Muttar, A.K., 2018. Literature review of security issues in saas for public cloud computing: a meta-analysis. International Journal of Engineering & Technology, 7(3), pp.1161-1171.

[33]. Sharma, A., Singh, U.K., Upreti, K., and Yadav, D.S., 2021, October. An investigation of security risk & taxonomy of Cloud Computing environment. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1056-1063). IEEE.

[34]. Shea, S. (2021) Top 11 cloud security challenges and how to combat them, SearchSecurity. TechTarget. Available at: https://www.techtarget.com/searchsecurity/tip/Top-11-cloud-security-challenges-and-how-to-combat-them (Accessed: November 20, 2022).

[35]. Simmonds, P., Rezek, C. and Reed, A., 2011. Security Guidance for Critical Areas of Focus in Cloud Computing V3. 0 (No. 3.0)(p. 177). Cloud Security Alliance.

[36]. Soni, M., 2018. Practical AWS Networking: Build and Manage Complex Networks Using Services Such as Amazon VPC, Elastic Load Balancing, Direct Connect, and Amazon Route 53. Packt Publishing Ltd.

[37]. Soofi, A.A., Khan, M.I., Talib, R. and Sarwar, U., 2014. Security issues in SaaS delivery model of cloud computing. International journal of computer science and mobile computing, 3(3), pp.15-21.

[38]. Sridhar, S.D.S.S. and Smys, S., 2016. A survey on cloud security issues and challenges with possible measures. In International conference on inventive research in engineering and technology (Vol. 4).

[39]. Thabit, F., Alhomdy, S.A.H., Alahdal, A., and Jagtap, S.B., 2020. Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques. Journal of Information and Computational Science, 12(10).

[40]. Tianfield, H., 2012, October. Security issues in cloud computing. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 1082-1089). IEEE.

[41]. Tissir, N., El Kafhali, S. and Aboutabit, N. (2020) 'Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal', Journal of Reliable Intelligent Environments, 7(2), pp. 69–84. Available at: https://doi.org/10.1007/s40860-020-00115-0.

[42]. Wu, H., Ding, Y., Winer, C. and Yao, L., 2010, November. Network security for the virtual machine in cloud computing. In 5th International conference on computer sciences and convergence information technology (pp. 18-21). IEEE.

[43]. Yan, X., Zhang, X., Chen, T., Zhao, H. and Li, X., 2011. The research and design of cloud computing security framework. In Advances in Computer, Communication, Control and Automation (pp. 757-763). Springer, Berlin, Heidelberg.

[44]. Yasrab, R., 2018. Platform-as-a-Service (PaaS): The Next Hype of Cloud Computing. arXiv preprint arXiv:104.10811.