Sri Lanka Institute of Information Technology

Cloud Security

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20613518	Madhusanka D.N.V

Date of submission

Table of Contents

Abstract 3
1. Introduction ..... **Error! Bookmark not defined.**
2. Evolution of the topic 9
3. Future developments in the area 13
4. Conclusion 17
5. References ..... **Error! Bookmark not defined.**

Abstract

The report aims to signify however cloud security. Cloud infrastructure has become one of the foremost enticing targets for threat actors thanks to the huge quantity of sensitive knowledge that currently resides inside the cloud. In recent years, several businesses have adopted cloud-based computing services that alter users to access computer code applications, knowledge storage, and different services via an internet affiliation rather than hoping on physical infrastructure. Though selecting such a system's area unit is typically extremely useful to organizations, they have additionally become the target of cyber threats. If these systems are not properly organized or maintained, attackers' area unit a lot of seemingly to be able to exploit vulnerabilities inside the systems' security and gain access to sensitive info. [1]

Cloud services will optimize resources, save time, increase automation, associated take a range of safety responsibilities off an organization's plate. There is no surprise that today's advanced cyber-criminals are exploiting cloud technology to boost and scale their operations by considering intensive price. Taken credentials cause compromised businesses, and thus the cloud is creating that method easier than ever. [2]

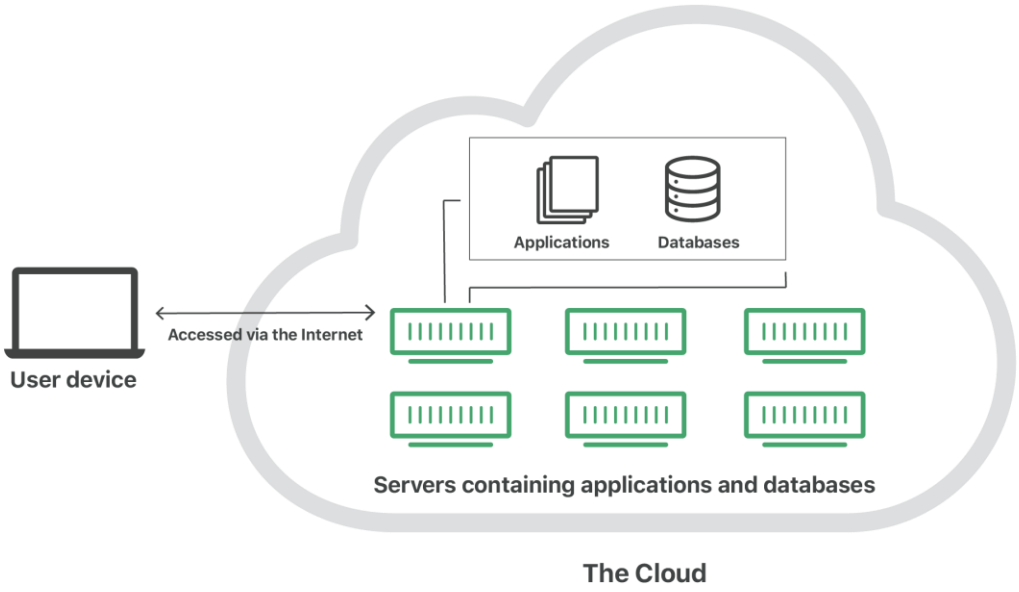
Businesses have further and further begun to embrace cloud storage choices in recent periods to store their data; among different reasons, cloud storage solutions have meant they did not ought to accept the varied prices associated with storing all their info in physical knowledge centers. Still, some businesses don't appear to understand the implicit hazards of exploitation similar as how for storing customer knowledge. Whereas the cloud has opened new borders, it's also opened a fully new world of security problems, as hackers presently have else to accept and enter people's individual and financial word. Thus, it's vitally vital that businesses process and storing customer info do their utmost to produce a positive it's secure and safe from those with minatory motives. [3]

1. Introduction

According to Kaspersky [4] "Cloud security is a guideline of cybersecurity devoted to securing cloud computing frameworks." Keeping information individual and secure across the online-based frameworks, applications, and stages are the most errands of cloud security. A person, exceptionally small to medium commerce, or undertaking utilizes this securing strategy. Securing cloud frameworks includes the endeavors of cloud providers. So, the buyers that utilize them. Have administrations are run on cloud providers' servers through always-on web associations. The cloud security models units have to keep clients' information private and securely keep since cloud suppliers depend on customer believe. Be that as it may, cloud security mostly rests inside the client's hands in expansion. Understanding each of the edges is imperative to a sound cloud security reply.

1.1) What's Cloud?

According to Cloudflare, [5] "The cloud" is the servers that unit accessed over the net. Laptop code and databases are run on those servers. Cloud server units are located everywhere in the world. Clients and organizations ought to not oversee physical servers themselves or run composing applications on their machines by misusing cloud computing.



1.2 What is Cloud computing?

According to AWS, [6] Cloud computing is the on-demand conveyance of IT assets over data superhighway with pay-as-you-go valuation. You'll get to innovation administrations, like computing control, capacity, and databases, on AN as-needed premise from a cloud supplier like Amazon Web Administrations (AWS), instead of buying, owning and keeping up physical information centers and servers. Cloud computers are utilized to perform method errands for cloud computing. Information reinforcement, calamity recuperation, e-mail, virtual desktops, coding framework improvement, and testing, expansive information analytics, and customer-facing web applications are utilized by Organizations of each sort, measure, and commerce unit hone the cloud for legitimate sensibly cases. As a case, computer amusement producers unit

hone of the cloud to provide online recreations to numerous players around the world. There are four primary assortments of cloud computing.

- ## Private clouds

  The private cloud environment is utilized for these clouds. The environment by and large runs behind completely committed to one client, or a cluster, or a group's firewall. Private clouds don't get sourced from on-premises IT framework. Organizations' range units are by and by building private clouds on lease. Which makes any area and ownership rules out of date seller on the off chance that claimed information centers are put off-premises. [6]

- ## Public clouds

  Public clouds are more often than not made from IT foundation not in hand by the most elevated client to the unit of measurement cloud situations. Alibaba Cloud, Amazon net Administrations (AWS), Google Cloud, IBM Cloud, and Microsoft Purplish blue are the well-known fundamental open cloud providers. Old open clouds ceaselessly ran off-premises. Be that as it may, today's open cloud providers have begun giving cloud administrations to clients' on-premises data centers. This has made area and possession distinctions out of date. Once the situations area unit apportioned off and decentralized to numerous inhabitants, all clouds got to be open clouds. Since a few cloud providers allow inhabitants to utilize their clouds for the complimentary charge so, these structures are not fundamental characteristics of open clouds any longer. The bare-metal IT framework utilized by open cloud providers can too be preoccupied and oversubscribed as IaaS, or it squares degree more often than not created into a cloud stage oversubscribed as PaaS. [6]

- ## Hybrid clouds

  Capacity, mixed computing, and administrations landscape made up of on-demesne, private cloud administrations, and an open cloud is known as crossover clouds. Open clouds, private clouds, and on-premises computing combination in the information center can be called crossover cloud foundation. Nimbleness is the essential advantage of these clouds. Advanced trade should alter and alter the course rapidly. Undertaking moreover ought to combine open clouds, private clouds, and on-premises assets. At that point, the endeavor can pick up the nimbleness. This needs a competitive advantage.

  Virtual surroundings are associated with a least one open cloud or non-public cloud. be that as it may, once apps will move in and out of numerous isolated however associated situations at that point, each IT framework gets to be a

crossbreed cloud. A modest bunch of those situations must be compelled to be sourced from solidified IT assets that can scale on request. [6]

- **Multiclouds**

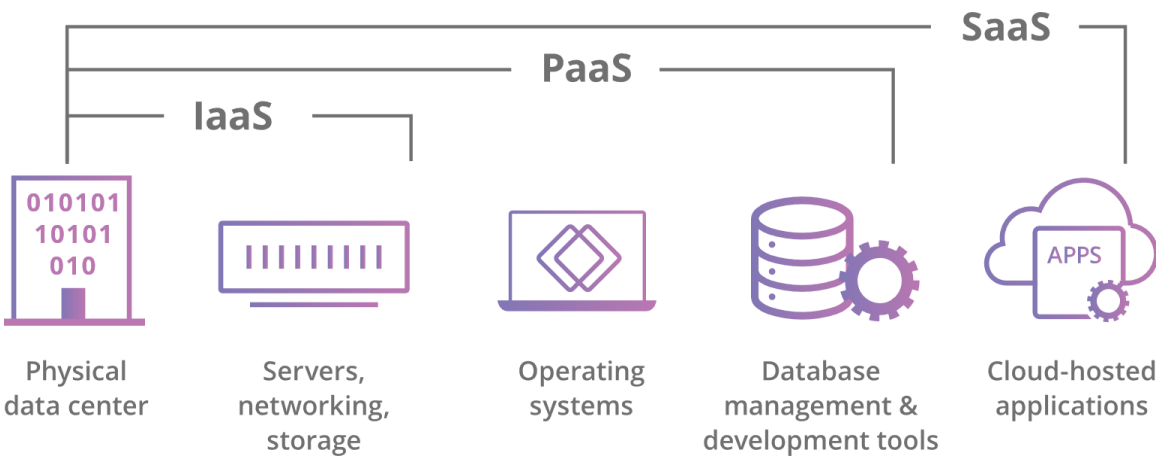
  From moderately one cloud vendor- open or nonpublic, Multiclouds unit of measurement a cloud course created of generally one cloud benefit. All half-breed clouds unit multi-clouds. But not all multiclouds units of measurement half breed clouds. Multiclouds that have once different clouds area unit associated by integration or solidarity get to be crossover clouds. A multiclouds environment would live designedly or inadvertently. Numerous clouds can turn into more common endeavors that get to boost security and execution through an extended portfolio of environments.[6]

1.3 What are Cloud services?

According to Citrix, [7] "Cloud services" are assortment of administrations conveyed on-demand to enterprises and clients over the net. These administrations are planned to deliver straightforward, cheap get to applications and assets, whereas not the prerequisite for inside framework or equipment. Most staff individuals utilize cloud administrations all through the workday, whether they're tuned into it or not from checking mail to collaborating on records.

The stream of client data is encouraged by cloud administrations from front-end buyers, through the net, to the provider's frameworks, and back. Clients get to cloud administrations without very pc, OS, and net property or virtual non-public organize (VPN). [8]

Cloud computing services have three varieties. These are called as Infrastructure as a service, Platforms as a service, and Software as a service.



- **IaaS**

  In IaaS, Service supplier of cloud oversees the frameworks a bit like the real servers, organize, virtualization, and data storage—through a web alliance. The client has got to through Relate in Nursing API or dashboard and essentially rents the infrastructure. The client oversees things just like the OS, apps, and middleware while the provider takes care of any equipment, organizing, depleting drives, data capacity, and servers; and has the obligation of taking care of blackouts, repairs, and equipment issues. Usually frequently the quality preparation shows of cloud capacity providers. [9]

- **PaaS**

  PaaS is the equipment Relate in an application-software stage is unit given and overseen by an out-of-doors cloud benefit provider, be that as it may, the client handles the apps running on prime of the stage and thus the data the app depends on. PaaS gives clients a shared cloud stage for application advancement and administration (a necessary DevOps component) fundamentally for designers and software engineers whereas not having to make and keep up the framework now and then related to the method. [9]

- **SaaS**

  Delivers a coding system application, that the cloud benefit provider oversees to its clients in SaaS. Typically, SaaS apps unit net applications or mobile apps that clients will get to by means of an online browser. Code updates, bug fixes, and elective common coding system upkeep unit is taken care of for the client, which they interface with the cloud applications through a dashboard or API. SaaS moreover kills the necessity to have a relate in Nursing app put in locally on each person user's portable workstation, allowing bigger ways of cluster or group get to to the computer code. [9]

1.4 What is Cloud storage?

According to Amazon, [10] Cloud computing show that stores information on the Web. IT called as cloud storage. It oversees and works information capacity as a benefit. It's conveyed fetched and dispenses with overseeing and buying users' information capacity framework on-demand with just-in-time capability. This gives "anytime, anywhere" information gets to. Cloud capacity can get from a cloud vendor. Capability, security, and quality to make information available to applications is overseen by merchants of Cloud Capacity all around the world. Applications get to cloud capacity through ancient storage conventions or straightforwardly by means of scholarly degree API. Cloud administrations planned to help collect, oversee, secure and analyze information at a gigantic scale by sellers offer complimentary.

1.5 What is Cloud security?

Secure the whole innovation, conventions, and hones that guard the cloud computing environment, operations are running, and dominance among the cloud is known as cloud security. Framework viewpoints that have to be overseen. So, securing cloud administrations start with understanding what accurately is being secured, conjointly. Backend advancement is essentially among the cloud benefit suppliers to security vulnerabilities. Buyers have to be compelled to center inside and out on correct benefit arrangements and securely utilize propensities separated from selecting a security-conscious provider. Buyers got to be compelled to certify any end-user equipment and systems unit of estimation legitimately secured to boot. Cloud security implies security these things.

- Secure routers, electrical power, cabling (Physical networks)
- Secure hard drives (Data storage)
- Secure main network computing hardware and code system (Data servers)
- Secure computer virtualization frameworks
- Secure OS
- Secure API management,
- Secure runtime environments
- Secure data
- Secure applications
- End-user equipment -computers, mobile devices

Ownership of those components can change broadly with cloud computing. These things can deliver the scope of client security duties vague. Cloud security conveyance way can depend on the cloud supplier or the put. Still, Between the trade proprietor and the result supplier execution of cloud security forms ought to be a common obligation. [4]

1. Evolution of the topic

Cloud computing has changed from an unrelated degree to an inventive conception into the only endeavor over a long time. Within the cutting edge world, cloud computing may moreover be a booming exchange all through those organizations, and analyst still pushes the boundaries of what is doable and give modern and moved forward arrangements for imperative issues.

1.1 A Brief History of Cloud Computing

According to Dataversity, cloud computing began in almost the mid-1940s. After Alan Turing's 1930, ENIAC was presented. By controlling components like vacuum tubes and transfers, these sorts of computing included gigantic, shared, and costly machines competent of performing computations mechanically. [11]

Software engineers not required consistent get to to the machine in those days, as they are doing nowadays, numerous different individuals and groups would program and run the centralized computer. Clients had get to once they required it to form beyond any doubt that, "time-sharing" plans were made. Clients seem enter the centralized computer from any associated stations or " idiotic terminals" and utilize the computing control of the centralized server from a fastened show. Programs would create to enable these things. Whereas this is often frequently exceptionally distinctive from cutting edge cloud computing, the essential premise is that the same. The division of cloud computing in some decades afterward progressed once more when an interconnected framework of computers proposed by J.C.R. Licklider, a scientist. In 1969, this thought was created into the Progressed Investigate Ventures Organization Arrange (ARPANET), a primitive adaptation of the net. ARPANET was the essential organize that empowered advanced information to be shared between inaccessible computers. the thought behind ARPANET and Licklider's vision was to create a framework where everyone inside the world can be interconnected, and information was all around open. [11]

Counting the release of IBM's Virtual Machine (VM) OS in 1972, numerous progressions came inside the taking after decades. These OSs empower to create virtual computers that worked a bit like a physical one. Comparable consumer-grade advances would show up along the way. Parallels for Mac was a well-liked equipment virtualization stage. Nowadays, parcels of Linux clients accept instruments like Wanderer for proportionate usefulness. In the long run, this was getting to be the creation of "virtual" private systems utilized by businesses. At that point, an advanced cloud computing framework was created within the 1990s Salesforce got to be the essential company to supply a software-as-a-service over the net made conceivable by cloud computing. Amazon Web Services (AWS) was made and thus the Flexible Compute Cloud (EC2) benefit was discharged in 2006. This benefit empowers clients to lease virtual machines as foundation for his or her information and applications. This was an comparable year that Google discharged Google Docs, a presently well-known cloud benefit that won't make, alter, and share reports inside the cloud. At that point, Google, IBM, and several other colleges worked together to form a server cultivate with assets devoted to inquire about ventures inside the cloud in 2007.[11]

Moreover, Netflix started propelling gushing administrations in 2007. Advances supporting information started to appear, beginning with the 2004 MapReduce paper from Google around the same time. A few of a long time afterward after the presentation of Hadoop, it got to be conceivable to oversee greatly expansive datasets on production equipment. Apache Cassandra made it to disseminate information amid a dialect exceptionally nearly like standard SQL. This will store and disseminate information. [11]

1.2 Cloud Computing Over the Past 10 Years

Moreover, Netflix started propelling gushing administrations in 2007. Advances supporting information started to appear, beginning with the 2004 MapReduce paper from Google around the same time. A few of a long time afterward after the presentation of Hadoop, it got to be conceivable to oversee greatly expansive datasets on production equipment. Apache Cassandra made it to disseminate information amid a dialect exceptionally nearly like standard SQL. This will store and disseminate information. Within the once 10 times, all businesses sizes have upheld pall administrations promptly in interest of bettered administrations and long-term took a toll investment funds. Concordant with Gartner, over a 3rd of affiliations consider pall calculating together of their best three speculation priority. Due to this relinquishment, software-as-a-service (SaaS) immolation utilized by affiliations multiplied between 2015 and 2017. Moreover, various new companies joined the ask. SaaS companies were enhanced in 2017. Still, structure-as-a-service (IaaS) has been the foremost imperative region of development. In 2018, Ask of IaaS was overwhelmed by five suppliers Google, Amazon, IBM., Alibaba, and Microsoft. Assiduity values reflect this beginning at around $12 billion in 2010, profit was prognosticated to surpass $623 billion by 2025. [11]

1.3 Why need security for cloud?

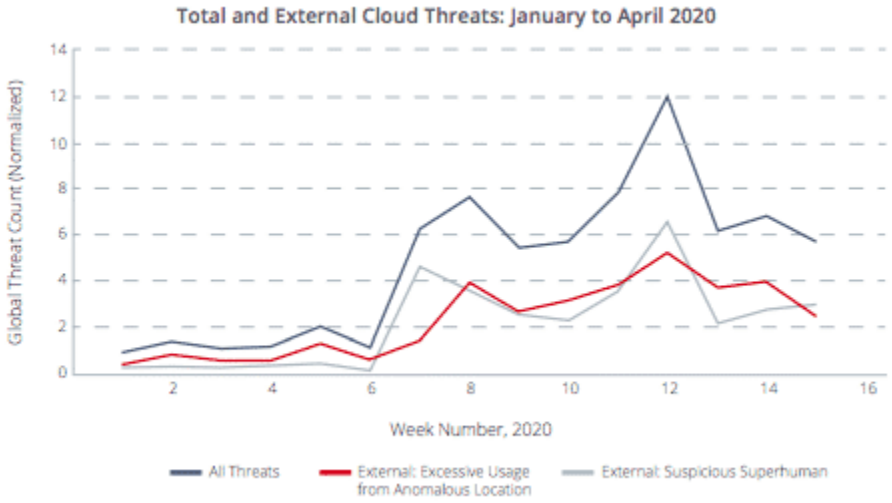
Cloud security is crucial since most organizations at already exploiting cloud computing in one kind or another. This high rate of adoption of public cloud services is mirrored in Gartner's recent prediction, [12] that the worldwide marketplace for public cloud services can grow in the future, with code as a service (SaaS) remaining the foremost vital market section. Per Gartner analysis chairperson Sid Nag, "At now, cloud adoption is thought." however as corporations move a lot of information and applications to the cloud, IT professionals stay involved concerning security, governance, and compliance problems once their content is held on inside the cloud.

Users worry this sensitive business data and property might even be exposed through accidental leaks or because of progressively refined cyber threats. A vital element of cloud security is targeting protective information and business content, like client orders, secret style documents, and monetary records. Maintaining customers' trust and shielding the assets that contribute to competitive advantage is important. So, preventing leaks and information stealing is crucial. Maintaining a sturdy cloud security posture helps organizations accomplish the currently wide far-famed edges of

cloud computing: lower direct prices, reduced current operational and body prices, straightforward scaling, multiplied reliability, availableness, and a whole new method of operating. There's an exceptionally small address that the cloud has the potential to be more secure than old on-premises arrangements. The watchword here is potential. Fair since the cloud is more often than not more secure, doesn't cruel businesses until the end of time savor greater security once they make the move. In numerous words, that's what clients do with the cloud that things.

1.4 Recent cloud security challengers

Agreeing to McAfee inquire about, cloud administrations to figure out in case there has been an increment in assaults since the COVID-19 widespread. Since Jan 2020, the comes about were amazing, uncovering a 630% rise in cyber-attacks on cloud administrations. This revelation is overwhelming to say the most modest amount with an increment of fifty interiors the business of cloud administrations and a 600% increment beside administrations. [13]



- **Data Breaches**

Where that information is gotten or get absent from a framework whereas not the data or authorization of the cloud system's proprietor. This is what happen in Data breaches. A little company or giant organization could suffer a knowledge breach. Taken knowledge could involve sensitive, proprietary, or hint like master card numbers, client knowledge, trade secrets, or matters of national security. [14]

- **Lack of IT experience**

Most organizations hop into the cloud whereas no right IT information like plan and methodology. Sometime recently making the jump to the cloud, clients ought to see the dangers they're uncovered to, a way emigrate to the cloud solidly note, it isn't a lift-and-

shift strategy additionally the ins and outs of the shared obligation model. This risk is modern to the list and is that the obligation of the client. Whereas not redress coming up with, customers are inclined to cyberattacks that will conclude in financial misfortunes, reputational hurt, and legitimate and compliance problems.

- **Use weak cryptography methods**

Cryptographic calculations are utilized to secure information in capacity by cloud suppliers. So, they utilize constrained sources of entropy. That naturally makes self-assertive numbers for information encryption. Linux- grounded virtual motors make purposeless keys as they were from the precise millisecond for this. Linux- grounded isn't sufficient for solid information encryption. Assailants too utilize modern interpreting methods. Thus, cloud creators ought to assume how to secure information sometime recently it moves to the cloud.

- **Cloud Migration problems**

Cloud relocation is when a company moves a few or all of its information center capabilities into the cloud, for the most part, to run on the cloud-grounded structure. Cloud movement has to be taken care of appropriately. Something else, it can be a hazard. There are four greatest challenges in cloud migration. They are businesses' unit perceivability into foundation security (43 percent), compliance (38 percent), setting security approaches (35 percent), and security coming up short to stay up with the pace of adjustment in applications (35 percent). Most clear relocation strategies can encourage businesses to oversee moves cleanly. [15]

- **Unsecured APIs**

Cloud suppliers show computer program bundle client interfacing (UIs) and APIs to allow clients. At that point, they can oversee and move with cloud administrations. With the security of those APIs, the security and comfort of the common cloud administrations unit captivated. These interfacing ought to be planned to watch against each coincidental and pernicious makes an endeavor to bypass the security arrangement from get to administration and confirmation to mystery composing and action observes. Broken, uncovered, or hacked application program interfacing that have caused a few major data breaches. Organizations ought to see the security necessities around arranging and showing these interfacing on the net. [15]

- **Insider Threats**

The dangers related to specialists and others working inside associations organize aren't constrained to the cloud. Whether careless or intentional, interposers counting current and previous laborers, temporary workers, and mates can generate information mislaying, framework time-out, decreased client affirmation, and information breaches. [15]

- **Bounded Cloud Operation Visibility**

bounded cloud operation permeability happens when an affiliation doesn't hold the capability to fantasize and dismember whether the cloud benefit utilized inside the

affiliation is secure or horrendous. This conception is broken down into two significant challenges. Un-sanctioned app utilization This happens when specialists are utilizing pall operations and coffers without the particular authorization and bolster of commercial IT and security. This script comes about in a tone-back demonstration called Shadow IT. When uncertain pall administrations effort doesn't meet commercial rules, this activity is hazardous. Particularly, when matched with touchy commercial information. Gartner predicts that by 2020, one-third of all fruitful security assaults on companies will come through shadow IT frameworks and coffers.

- **Open source**

The open-source package is free for everyone. This provides unlimited access to the source code and is developed and maintained by massive numbers of contributors. So, users can modify it as they need. Like all packages. One in 10 open supply package downloads are vulnerable, and on average there are thirty-eight identified open supply vulnerabilities per application in step with Sonatype 2020 State of the package offer Chain Report.

The main reason behind the vulnerability of open supply lies precisely in its public nature. various developers will get entangled with very little vetting - together with unhealthy actors. Open supply is, well, open and designed by typically unaccountable contributors. Whereas security awareness inside the open supply community is slowly up and there are initiatives to handle security problems (e.g., GitHub Security Lab), the shortage of central management provides many opportunities for attackers to search out holes and vulnerabilities. [16]

2.5 7 Most Common Types of Attacks on Cloud

Getting unauthorized get to information and avoiding getting to cloud administrations are the most objectives of cyberattacks against the cloud computing. Programmers have numerous ways that can assault to cloud. They attempt to urge unauthorized access, then they can utilize users' information. These are the foremost common sorts of assaults to cloud.

- **Malware injection attack**

  Malware infusion assaults are propelled to urge the operation at interims within the cloud. Programmers include a related contaminated benefit execution module to a SaaS or PaaS reply for this reason. In any case, it's reaching to the cloud user's demands to the hacker's module or case, starting the indictment of horrendous law, On the off chance that the cloud framework is with victory hoodwinked. Also, the assailants can start their horrendous effort like spying or controlling or taking information. Cross-site scripting assaults additionally SQL infusion assaults are cases of the common sorts of malware infusion.

Programmers include horrendous scripts to a defenseless site through cross-site scripting assaults. German experimenters organized a related XSS attack against the Amazon net Administrations cloud computing stage in 2011. Assailants target SQL servers with powerless information operations at interims within the case of SQL infusion. Sony's PlayStation site turned the casualty of an SQL infusion assault in 2008. [17]

- ## Abuse of cloud services

  Hackers will use low-cost cloud services to set up DoS and brute force attacks not of course users, companies, and even different cloud suppliers. By exploiting the capacities of Amazon's EC2 cloud infrastructure in 2010, security specialists Bryan and Anderson organized a DoS attack. They managed to make their shopper out of stock online. By Thomas author in 2011, Black Hat Technical Security Conference brute force attack was incontestable. Hackers will use powerful cloud capacities to send thousands of doable passwords to a target user's account by transaction servers from cloud suppliers. [17]

- ## Denial of service attacks

  DoS assaults are especially perilous for cloud computing frameworks. These assaults are planned to stack a framework and deliver administrations out of stock to its clients. Cloud frameworks start to allow more machine control by including more virtual machines and frame cases for cases of tall business. The cloud framework makes it another ruinous. In the long run, the cloud framework moderates down, and bona fide clients lose any comfort to penetrate their cloud administrations. DDoS assaults can be without a doubt more perilous at interims within the cloud climate in the event that programmers dispatch numerous zombie machines to assault-related enormous run of frameworks. [17]

- ## Side-channel attacks

  Hackers put a horrendous virtual machine on an indistinguishable have owing to the target virtual machine in the side-channel assault. Programmers target framework executions of shrewdness calculations all through a side-channel assault. Nowadays moreover, Side-channel assaults inconvenience is by and largely dodged with a secure framework fashion. [17]

- ## Wrapping attacks

  Cloud framework is defenseless to these sorts of assaults. So, Clients connect with cloud administrations through an internet browser. Man-in-the-middle assault is one of example wrapping assaults within the cloud. Relating XML

signature is imperative since it employments to ensure users' accreditations from unauthorized get to. However, at interims, this signature doesn't secure the positions within the record. So, XML signature part wrapping licenses assailants to control related XML reports. For a moment, interims within the Cleanser interface of Amazon Flexible Cloud Computing (EC2) in 2009 were established. This could permit aggressors to alter the relate listened to stealthily messages since of a profitable signature wrapping assault. [17]

- **Man-in-the-cloud attacks**

  Hacker's intercept and reconfigure cloud services during this type of attack by exploiting vulnerabilities. With a relief bone that provides, access to the bushwhackers, the synchronization commemorative goes to get replaced. Users might seize that their accounts malware injection attacks are done to bear control of a user's information within the cloud. [17]

- **APTs (Advanced persistent threats)**

  This assault lets hackers endlessly take the delicate data held on inside the cloud or abuse cloud administrations whereas not being recognized by lawful clients. The length of those assaults licenses programmers to acclimatize to security measures against them. Once unauthorized get to is set up, programmers will move through data center systems and work arrange activity for his or her horrendous workout.

2. Future developments in the area

Cloud protection needs to be improved in future as the threat to cloud security is currently increasing. So that cloud security needs to develop below things.

- **improve security policies**

  Software merchandisers ought to constrain the compass of their obligation for protecting client information and operations inside the cloud in their security approaches when conveying cloud administrations.

- **Use strong verification framework**

  Taking passwords is that the common much obliged to get to users' information and administrations inside the cloud. So, cloud innovators ought to apply solid confirmation and personality operation. Multi-factor confirmation can be built up for strong.

- **Make access management system**

Cloud creators ought to let cloud clients dole out portion- grounded warrants to distinctive chiefs in arrange that client as it were have the capabilities relegated to them. This will grant more security for cloud.

- **Safeguard data**
  Data within the cloud terrain must be encrypted in the least platforms of its transfer and storage.

- **Discover intrusions**
  Give cloud grounded result with a completely managed intrusion discovery system which will discover and inform about the vicious use of cloud services by interferers. Use an intrusion discovery system that gives network monitoring and notifies about the abnormal actions of insiders.

- **Secure APIs and access**
  Cloud creators ought to make certain that clients can enter the apparatus as it were through secure APIs. This might need to constrain the extent of IP addresses or conveying get to as it were through commercial systems or VPNs.[17]

- **Secure cloud services**
  Cloud sellers will constrain to get to cloud services. It'll halt assaults on cloud administrations. Minimize the occasion handler consents to exclusively those fundamental for the execution of operations once coming up with the cloud benefit plan. Moreover, Cloud security providers will restrain security choices that are a unit of measurement beyond any doubt by clients. So will oversee their data security.

And cyber security professionals need to handle situations and secure cloud. Therefore, cybersecurity jobs will be increase in future.

3. Conclusion

In modern world, cloud computing is more popular among users. Today, most of the people work from home due to Covid 19 pandemic situation. They use cloud services to do their tasks. So, this is good opportunity to hackers to do attacks. Attackers search vulnerabilities in cloud to do attacks. By understanding vulnerabilities how

vulnerabilities perform and increase security controls cloud developers can protect platforms.

References

[1] K. Burnham, "Cybersecurity Trends Emerging in 2021," 14 May 2021.

[2] infosecurity, "How Hackers Use Cloud Services to Make Cybercrime More Profitable," 28 April 2021.

[3] cloudcomputing-news, "How cloud storage became a target for hackers – and what can be done about it," no. https://cloudcomputing-news.net/news/2016/oct/20/how-cloud-storage-became-target-hackers-and-what-can-be-done-about-it/.

[4] Kaspersky, "What is Cloud Security?," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security. [Accessed 25 09 2021].

[5] Cloudflare, "What is the cloud? | Cloud definition," Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/. [Accessed 25 09 2021].

[6] Aws.Amazon, "What is cloud computing?," Aws.Amazon, [Online]. Available: https://aws.amazon.com/what-is-cloud-computing/. [Accessed 25 09 2021].

[7] Citrix, "What is a cloud service?," Citrix, [Online]. Available: https://www.citrix.com/solutions/digital-workspace/what-is-a-cloud-service.html. [Accessed 25 09 2021].

[8] Redhat, "What are cloud services?," Redhat, [Online]. Available: https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-services. [Accessed 26 09 2021].

[9] Red hat, "Types of cloud computing," Red hat, [Online]. Available: https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud. [Accessed 26 09 2021].

[10] Aws, "Cloud storage," Amazon, [Online]. Available: https://aws.amazon.com/what-is-cloud-storage/. [Accessed 26 09 2021].

[11] G. D. Maayan, "How the Cloud Has Evolved Over the Past 10 Years," 06 04 2021.

[12] Box, "What is Cloud security?," Box, [Online]. Available: https://www.box.com/resources/what-is-cloud-security. [Accessed 27 09 2021].

[13] Mcafee, "Cloud Adoption and Risk Report," Mcafee, santa Clara, 2020.

[14] Trendmicro, "Data Breach," [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/data-breach. [Accessed 02 11 2021].

[15] Checkpoint, "The Biggest Cloud Security Challenges in 2021," Checkpoint, 2021.

[16] B. Portnoy, "The threats of open source software in cloud native," 12 October 2020. [Online]. Available: https://www.itproportal.com/features/the-threats-of-open-

source-software-in-cloud-native/. [Accessed 02 November 2021].
[17] A. Katrenko, "Cloud Computing Attacks: A New Vector for Cyber AttacksIt," www.apriorit.com, 2020.