Cyber threats to Cloud **Cyber threats for Cloud**

|  |  |
| --- | --- |
|  | Abstract  In this research paper, I will discuss some major and advanced cloud cyber threats that are taking cloud security to its meltdown point and what measures should be taken so we can stay safe from these malicious cyber-attacks.  Ashutosh Joshi  ITMS-578, Cyber Security Management |

**Thesis Statement:**

Many clouds and IT using professionals would agree and say that cloud is the most revolutionary information delivery, hardware and software model since the introduction of the internet. Cloud also provides and brings many financial and function benefits to our working environment or corporate. The cloud provides mostly all features to the cloud user's which is the best thing right, but with more power or functionality comes more responsibility and threats. The cyber threats for the cloud are little blurry at some part because the virtually unlimited amount of data and information is being published daily and continuously through the cloud.

In this research, I will discuss cyber threats for the cloud which can be of client user or system user and also some new upcoming and advanced cyber threats that can attack our cloud and how we can apply our protection mechanism and advanced tools to protect our cloud from these cyber threats.

**Contents**

1. **Cyber threats to keys (Keys to the Kingdom) 4**
2. Publicly Accessible Resources 5
3. Leaked keys or credential
4. Code repo misconfigured or hacked

C. Insider Threats  **6**

1. Untrained employee or Angry leavers
2. **Cyber threats to cloud data 7**
3. Hijacking accounts and taking or leaking important data.
4. Use of phishing and Malware
5. Data Loss **8**
6. Data Breaches  **9**
7. **Advanced cyber threats to cloud 10**
8. Denial of Service (DOS attack)
9. External Denial of service attacks
10. Internal Denial of service attacks
11. Advance Persistence threats **11**
12. Zero-day attack
13. Cryptojacking **12**
14. Man in the Cloud attack (MITC) **13**
15. Abuse or nefarious use of cloud
16. Cloud computing Malware injection  **14**
17. **How to Secure cloud from cyber threats 15**
18. Data Monitering
19. Gaining visibility
20. Manageing access **16**
21. Privileged Identity Manager system (PIM)

D. Data Loss Prevention tool (DLP) **17**

1. **Conclusion 18**
2. **Biblography 20**

1. **Cloud Keys threat (Keys to the kingdom).**

Keys play an important role in every application. We use keys to protect our data, applications and other resources on the cloud. The use of public or private keys has increased nowadays because keys provide much better security than a password that is chosen by the user. But there is some time where our data and resources can be leaked by the system fault, user fault, malicious insiders and other software or application failure which results in the venerability of cloud and our data can be seen or available to the public or the threats.

1. **Publicly Accessible Resources**

This cyber threat comes when sensitive data or resources are exposed through the misconfiguration and similar modes. This mostly happens when cloud databases or storage exposed themselves by some user or by system failure. Last year, Google cloud storage leaked 540 million Facebook user records on the exposed servers and MongoDB database led to the discovery of a huge collection of 808,539,939 email records with many of them which are containing detailed personally identifiable information (PII).

1. **Leaked Keys or credential**

To activate a cloud at run time there are many services, instances, databases, and servers that are involved, to activate all these above services we also need a credential to use or log in to our services and cloud. When there are too many keys the chances of getting them in the wrong hands can happen either they are lying around or can be any online accounts and other unsafe places. A cloud user will save these keys which can be either public or private at his GitHub account as a repo, so from there, he can easily access these keys any place and any time.

1. Code repo misconfigured or hacked:

When we save our public keys to GitHub account as a repo and we accidentally give them public access which can be fatal for our cloud security and another thing which can happen is our code repo get hacked which results in leaked keys. In October 2016 two hackers compromised Uber's GitHub which contained access keys to the Cloud and particularly they found out AWS keys and stole data of 57 million individual's data. These keys were private but somehow hackers gained access to it which result in ransom which was paid out and the whole thing was disclosed publicly in late 2017.

1. **Insider threats.**

A recent research report noted that 53% of the organizations surveyed

Confirmed insider attacks. Malicious insiders' cyber threats to an organization happens when a former employee or other business workers who have the same authorization misused their access in a negative manner that affects the integrity, availability and confidentially of the cloud user and this data that is present on the cloud. These types of threats are increasing very fast nowadays and their impact on any company or origination would be catastrophic.

1. Untrained Employees or angry leavers:

This also affected many cloud companies when they have untrained employees or angry leavers. Angry leavers affect more than we can imagine. Last year IT employee was terminated after just 4 weeks of joining and he became disgruntled and terminated 25 AWS servers and their data too. This results in $7000,000 loses to the company because the deleted data cannot be recovered. As the cloud requirement increasing some companies take unprofessional or untrained employees which can result in cyber threats if they made some bad or unknown configuration to the critical data or cloud servers. This can open a backdoor for the malicious attacker which is not good for every cloud user.

1. **Cyber threats for cloud data.**

Data is one of the important things in the cloud. This data can be of a single image as well as large data sets which are governing a large company or an individual. If a cyber threat happens to our cloud than our sensitive, protected and confidential data or information is released, viewed, stolen or used by an unauthorized individual which involves any kind of information that was not intended for public release, including information, personal information, trade secrets, and intellectual property.

1. **Hijacking accounts and taking or leaking important data.**

Account Hijacking happens in cloud happens when an individual or organization cloud account is being stolen or hijacked by an attacker. This is the greatest cybersecurity threat to the cloud that is account hijacking. In this attack, the attacker uses the stolen account information to conduct malicious or unauthorized activity. The hijacking account involves many attacks which can lead to the accounts being compromised.

1. Use of Phishing and malware:

Phishing is the most pressing threat to the cloud cybersecurity after data breaches. The use of phishing and malware attacks has stormed back into the cybersecurity radars. In these attacks, the cloud user gets some suspicious emails from time to time also known as phishing scams to lower the user into those emails and try to get some personal or financial information. Sometimes they also put some malware with the emails as the cloud user clicks on these links or any sites which the attacker sends their security is being compromised.

1. **Data loss**

The data loss in the cloud for consumers and businesses user is terrifying and it's harder to predict and even harder to handle the data which is lost. There could be many reasons for data losses in the cloud-like cloud alteration, unreliable storage medium failure, data breaches, accidentals data deletion which cannot be recovered in some cases. The data is the most important thing that is stored on the cloud.

1. Data lock-in: Data lock-in problems come in when a cloud user wants to switch to a different vendor. This threat arises because of many cloud companies that provide cloud service at low rates according to the other cloud company. The moving of data from one cloud to another cloud opens many doors to the cyber threats which should not be done if the data is more critical.
2. **Data breaches**

The risk of data breaches is not unique to cloud security, this cyber threat has been ranked as a top concern for cloud security.

The inadvertent exposure of protected data to the public or any unwanted person can be called a data breach in the cloud. Data breaches occur when a business is attacked by cybercriminals who are able to gain unauthorized access to the cloud network or utilize your programs or cloud data to view, copy and transmit data. There are many examples of data breaches in cloud this can happen due to misconfiguration of AWS cloud instance and by any user which configured wrong authentication permissions. Last year Instagram had a data breach which resulted in almost 50 million records from its users. The data contained shared bios, publicly pictures, profile pictures, numbers of followers, etc. Once the cloud providing company know about the exposure, they immediately pulled the database offline to contain the breach and save many data breach as possible.

1. **Advanced cyber threats to cloud**
2. **Denial of service**

Denial of service attack is one of the major cybersecurity challenges or concerns for cloud services. In DOS or Denial of service attack in which the attacker will try malicious attempt to make online cloud services unavailable to the users, the attackers try to mitigate temporarily or suspending the cloud services of its hosting cloud server. Currently, there are many numerous types of Dos attack are conducted against the various cloud services and its resources. which target their availability, running services and performance. There are two types of Denial of service attacks in cloud

1. External Denial of Service attacks: In this attack, the attacker tries to attack the client's running services in the cloud such as virtual machines, web-based application or any other particular services. This attacker tries to load some trojan horses on the victim's cloud services and these contain hundreds or thousands of trojan horses which will create a catastrophe on the system health and it's services.
2. Internal Denial of service attacks: These attacks are more serious than it looks. In these attacks, attackers try to attack internal cloud infrastructure which results in the breakdown of cloud infrastructure.

**B. Advances persistence threats**

An advanced persistence threat (APT) is a cloud cyberattack in which malicious attackers or cyber attackers with the intent to steal your data or they monitoring your every cloud activity over an extended period of time. This comes under advances threats because in this the attacker has some specific target and goals which he wants to exploit. The attackers have spent time and resources to gained particular vulnerabilities that he can exploit or which he is looking for there. The advanced persistence threats are undetected for a long time when the cloud security experts know about these attacks it's already too late. The motive of these attacks can be either financial gain or someone whos' trying to steal some government or industrial secrets. Advanced persistence threats nowadays mostly used to steal data or intellectual property that they can sell or otherwise monetize. Let's discuss an advanced persistence threat and see how it works and how we can stop it from harming our cloud cybersecurity.

1. Zero-day attack: A zero is a cyber-attack that occurs when a weakness is discovered in hardware or software that is working on the cloud. When a zero-day attack occurs, some malware is released before the weakness is discovered and can be resolved by the security experts. To provide protection from these kinds of threats a cloud user can use "CipherCloud CASB" which integrates on-premises of the sandbox. Sandboxes are used as a threat prevention system, which tests software, attacks, and vulnerabilities that look or are potentially malicious.

**C. Cryptojacking**

Cryptojacking is the new form of cyber-attack to the cloud and it also can go easily under the radar. These kinds of attacks become famous after the popular practice of mining for the cryptocurrencies like Bitcoin. Cryptojacking involves the hijacking of the CPU power of a visitor website to perform CPU-intensive cryptocurrency mining. The rise of these types of attacks is because it can be very tricky to spot and deal with. When a hacker performs cryptojacking at our particular cloud system, the operation will be slowed down but it will continue to work. This means that we think it just our system struggling with the processing power or with the bad internet at the moment but something malicious is happening at the same time. Many experts think these kinds symptoms of cryptojacking is a flaw with the update or need some patch but it needed much longer time to establish the real problem.

**D. Man in the cloud attacks (MITC)**

This attack aims to access victim's accounts without the need to obtain compromised user credentials beforehand. MITC attacker takes advantage of the synchronization token system used by the cloud applications. Most cloud companies use these such as Dropbox, OneDrive, and Google. Whenever a user login into the cloud with its proper user device with proper credential the login become successful to the cloud. These authentication tokens are saved so that users don't have to enter their password every time they attempt to access the cloud. As the benefit of cloud service, the user can access the cloud anytime and anywhere which means the same token can grant access from any device and any place. If an attacker is able to access that copy of a token which he can use to infiltrate the user cloud remotely. The discovered MITC attacks were the easiest, in which attackers get access to the authentication token copy of the cloud credential through the social engineering tools such as Switcher. In Switcher, the attacker uses an exploit to execute the Switcher. Then Switcher plants the attacker's synchronization authentication token keys into the drive application. The drive application is synchronized with the attacker account which can be on cloud or any local device. Once the attacker possesses working keys, he's ready to exploit the user cloud account with full access.

1. Abuse or nefarious use of cloud

This is becoming the new cybersecurity threat to the cloud because most of the cloud providers do not force any strong registration process where any cloud using a person with a valid credit card can register to receive cloud services. Some companies also provide a free limited trial period of cloud services which presents a perfect opportunity and time for cybercriminals to join the cloud services and possibly misuse and abuse their free access privileged to the cloud services. Attackers launch many instances and services in a very short time without proper security and privileges. Many services and applications running suddenly make the system slow and the advances security tools have to process more data so it can find malicious attackers which sometimes he can't which results in attackers using private cloud data and information from malicious activity.

1. Cloud computing Malware injection:

In this attack, the attacker gained access to the cloud services mostly by free trial version period, which most of the cloud hosting companies provide. When a malicious hacker is already in the cloud environment and then tries to implements he own module or malware attack within the cloud, and then he tricks the cloud security experts or advanced security tools that he's just launching some application or instances to his own cloud which he was using to creating an attack for the other cloud users. The hackers host malicious data on the cloud and run images or instances named "Amazon-core" or "Fedora-core" which looks like they are official cloud users. They create many virtual machines or images so they can possibly locate and identify a real cloud user machine and if they were able to locate one the hacker can easily compromise that virtual machine and do some malicious work or can leak its data or information.

**VI. Securing cloud from cyber threats**

The best cybersecurity for any application or cloud is there should be a security incident team working to protect your data from any threats that are coming or about to happen or any malicious activity notices by the user. This security team will take action about the attacks and stop them so they cannot happen again. This team will thwart attacks and restore system health as soon as possible. The security of the cloud is done in three phases which involves

1. **Monitoring Data**

Monitoring data involves monitoring the data which comes and goes through the cloud. These monitoring tools use advanced machine learning techniques that build a detailed model of the system behavior and flags any deviation to these models. These tools and models have insight-built features for most of the hacking techniques and malicious tools which rapidly alert our response team and if any unauthorized user or any unusual database is started or taking place without user permission of the user.

But what happens when someone passes our first security step, for example, we can say that a new tool or method has been created by the attacker and they passed our insight and try to enter the cloud. Then come other important security aspects for the cloud.

1. **Gaining visibility**

Gaining visibility in cloud is very important because everyone is an outsider in a cloud. By gaining visibility in the cloud means we have to figure out who is a normal user and who is malicious users from the millions of cloud users. This is done by a variety of sophisticated software or virtual software appliances that detects multiple events that are happening at the current time or happened. Then these events are analyzed and summarized why these events are happening and who's responsible for these events. The software looks for the pattern and event which doesn't look normal to the cloud system behavior and if the system analyses that than it provides the visibility to quickly pinpoint the threat and who's trying to gain unwanted access to the cloud users account. By gaining visibility means we are able to see which malicious user is trying to get into our cloud without his proper credentials and if he's doing

some suspicious activity to the cloud servers than we are able to see that activity.

1. **Managing access**

This security process involves managing access which means which specific user can access the cloud servers or services. If a hacker tries to enter our cloud system through any other unauthorized or authorized credentials and now what hacker do in most cases that he will try to create new rules so he can gain access to all the services of the cloud and with these new rules a hacker can or will change all cloud credential and passwords for a current user. So, what we can do here is, we can shut down this particular access of the hacker from the cloud or can terminate the specific malicious account and it's related services to the specific time until everything's backs to normal. To apply more security to our cloud access control list tools are applied like.

1). Privileged Identity Manager system (PIM)

Privileged Identity Manager system checks current login user to the cloud each time any user login or logout from the cloud. Which provides additional security to the cloud. Privileged Identity Manager system which controls the access list to the critical cloud resources which store the sensitive information and confidential information on the cloud. So, if any suspicious privilege is seen than security experts terminate or stop that user to login to the cloud.

1. **Data Loss Prevention tool (DLP)**

Data loss prevention tools help us to protect data at rest and in motion. DLP is driven by regulatory compliance such as HIPPA, PCI-DSS, etc. DLP applies an encryption and other security measures so that our data is safe if somehow loss of data happened through unsecured storage or taken by a malicious user. The main role of the DLP is that to ensure that critical or business data is secured stored in the first place and the next step is that correct data with the correct individual have the right permission for the right data. If the data is too critical than it's stored with hashes and some impurity is being mixed by some advanced tools. Some of the examples of the data loss prevention tools are SolarWinds, Teramind DLP, Clear swift DLP, Secure Trust DLP. These all tools contain advances machine learning languages and models which helps to secure our data in the cloud and provide a good defense for our cloud services and applications

**VII. Conclusion**

Cloud technology is growing at a rate of 17% and its estimated total will be 266.4 billion. Cloud taking over the way companies or a user share and store their information. As the cloud provides many technology capabilities such as availability, capabilities, services, more resources available than ever before. As the cloud services increase the cyber threats also increases to our cloud. This research paper raises awareness about the most of the cybersecurity threats to the cloud such as data breaches, keys misuses, malicious insiders, vulnerable APIs, interfaces and other every aspect of cloud that makes it easier target than we think. All these threats mentioned have a major impact on the cloud using a user or any organization, this will create more attention to the cloud security experts which manages the security of clouds and create more advanced security to the data and cloud securing tools.

**VIII. Bibliography**

CHESTER AVEY, 2019, 7 CYBERSECURITY THREATS TO CLOUD COMPUTING. https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/

Fahmida Y. Rashid, 2016, The top 12 cloud security threats.

https://www.networkworld.com/article/3042610/the-dirty-dozen-12-cloud-security-threats

Takahiko Kajiyama 2012, CLOUD COMPUTING SECURITY: HOW RISKS AND THREATS ARE AFFECTING

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.9097&rep=rep1&type=pdf

Wagner's Ring, 2018 Spectre, and Meltdown. https://www.lightreading.com/enterprise-cloud/security-and-compliance/spectre-and-meltdown--andndash-what-cloud-users-need-to-know/a/d-id/739483

Chris Pedigo, 2019, The biggest cloud breaches of 2019. https://www.lacework.com/top-cloud-breaches-2019/

https://linkinghub.elsevier.com/retrieve/pii/S1877050916318257

Yasir Ahmed Hamza1, Marwan Dahar Omar, 2013 Cloud Computing Security: Abuse and Nefarious Use of Cloud. http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-4666-8387-7 Fred Bals, 2018, 10 critical cloud security threats in 2018 and beyond.

https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/

System Vulnerabilities, Exploits and cybersecurity on the cloud.

https://www.whoa.com/system-vulnerabilities-exploits-and-cybersecurity-on-the-cloud/

Dimitra A. Georgiou, 2017, Security Policies for Cloud Computing, Page-27, 54

Jon-Michael C. Brook, 2019, Top threats to cloud computing. https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/aug/cs2019f

Ramakrishnan Krishnan, 2017, SECURITY AND PRIVACY IN CLOUD COMPUTING

CHESTER AVEY, 2019, 7 KEY CYBERSECURITY THREATS TO CLOUD. https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/

James condon, 2019, Top 10 security threats to cloud.

**Ashutosh Joshi**

**ITMS 578 Spring 2020**

**Cyber Security Management in Information Technology**

**Professor Ray Trystad**

**Illinois Institute of Technology**

**Date: 04/09/2020**