QUANTIFYING CLOUD MISBEHAVIOR AND MALICIOUS TRAFFIC ORIGINATING FROM CLOUD MACHINES

Abstract.

Exponential rise in the trends of Cloud security has given birth to security related issues which include detection of nefarious use of cloud machines, cloud misbehavior, cloud instances abuse etc. Clouds gained excessive adulation over the time due to the providence of on demand services with zero additional costs. It also provides superuser access which allows users to customize cloud machines according to their needs. This superuser is not always beneficial as miscreants have found out ways to violate and misuse the access. Furthermore, the miscreants can easily rent cloud machines and also hijack them to generate unwanted traffic which includes spamming, phishing, DoS, vulnerability scans etc.

In this survey paper, we aim to successfully analyze and discuss several types of malicious traffic, mitigate and quantify the misbehavior of cloud machines and identify the cloud services that generate these traffic. In this paper, we analyze different methodologies, implementation of tools, datasets and accuracy of analysis.

***Keywords-*** **Cloud, Cloud Computing, Cybercrime, Malicious Traffic, Malicious Hosting Service, Cloud Security, Quantifiable Evaluation.**

1. Introduction

The global cloud computing market size is expected to grow from USD 445.3 billion in 2021 to USD 947.3 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 16.3% during the forecast period. [1]

Cloud provides services like content hosting and renting machines to customers which more often than not are misused by conmen. These services, in turn, allow them to install and run their respective software and upload data. Although these services are paid, even the money constraint does not deter misuse of superuser access to machines. The compromised accounts, free trials or hijacking of legitimate accounts serves as fertile ground for miscreants to use them in their own favor with the help of Account Takeover Attacks, whereas other clouds host malicious contents. [2]

In the extensive research conducted by researchers around the world it was found that although cloud providers only occupy 5.4% of routable Internet address space, they generate around 50% of vulnerability scans, which are often precursor to attacks. Clouds also contribute to up to 96% of entries on blocklists, which are lists of IP addresses that participated in prior documented misbehavior.This was concluded after analyzing 13 datasets which has a comparative and thorough study of cloud and non-cloud traffic. [2][3]

Examples: BulletProof Hosting (BPH) services are services that rent out servers and networking infrastructure that provides an environment to carry out illicit activities. It provides a stable base to carry out mischievous activities ranging from DDoS attacks, phishing and hosting botnet commands etc. [4] Another example can be of the DDoS attack wherein Amazon AWS EC2 machines to carry out the attacks on a US bank and a Japanese electronics maker.[5] In another instance, it was found that Google cloud platforms were used to attack and bring down D-Link routers.[6] There are many such instances where cloud machines were used to target organizations with malicious intent[7][8]clouds

1. Review of Literature

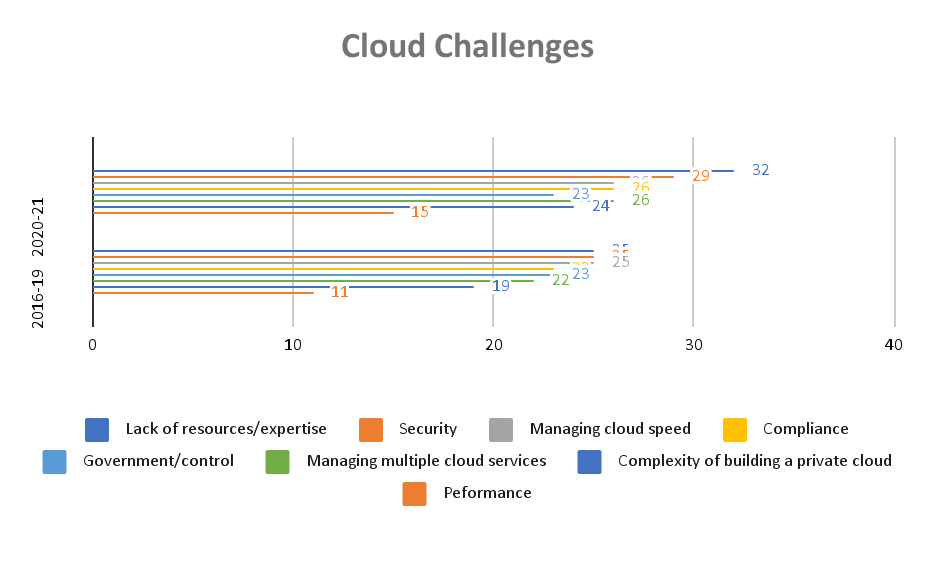
The [2] research states the analysis of 13 discrete datasets which included the study of unwanted traffic. In the study it was found that only 5.4% of the own routable IPv4 address spaces contribute to 22-96% of entries on blocklists. It was also found that the clouds produce 20-100 times more aggressive traffic (/24 prefix sending vulnerability scans) than a non-cloud. From the research metrics, it was concluded that there are 25 clouds that contribute 90percent of all cloud scans and 10 clouds contribute more than 20% of blocklist entries that are coming from clouds.

In [4], the researchers discuss BulletProof Hosting (BPH) services and present the first systematic study on this new trend. BPH provides an environment to the conmen that is resilient to complaints of illicit activities.

Omar Abdel Wahab et. al. [9], proposed the architecture of Community-based Cloud Computing which aims to improve the quality and performance of the cloud services. In this research it was found that malicious services that perform attacks either against the whole community or against some partners prevalent in that community, pose a threat to the architecture. This problem was then addressed and solved by the means of a misbehavior detection framework based on the Support Vector Machine (SVM) learning technique.

In summary, the different related works analyze various types of cloud misbehavior portrayed by cloud machines in different environments. They also suggest various methodologies used to mitigate the malicious traffic and cloud misbehavior. In our work, we analyze the different methods used for the analysis of cloud misbehavior and malicious traffic that originates from the cloud machines. We only focus on the survey of previous research performed in this domain over a span of 5-6 years.

1. Analysis and discussion.



A. The security service level agreement (SLA) is assigned to the location of the information, data safeguarding, distinction, and information recovery.

B. The Information Technology Infrastructure Library has a number of security administration standards.

C. The most serious problem with cloud computing is a Denial-of-Service attack based on HTTP or XML. These sorts of offenses are simple for the hacker to carry out; nevertheless, they are twice as difficult to stop.

The biggest issues for businesses, on the other hand, are a lack of transparency, high-speed internet access, and standardization. Keeping records of users' privacy, awareness, and privacy habits creates major data security risks.

D. Lack of Control: On the one hand, you won't have to manage your data, but your data will be managed by someone else in the cloud. Because you have no control over your data storage, anything that affects your vendor's storage capabilities also affects your data access. Being locked out of your own storage platform is one of the most serious risks in cloud storage. As a result, selecting a safe and secure vendor is critical.

E. Shared Servers: On-site servers contain data in cloud-based storage systems, and servers retain data from numerous users. While consumers cannot access these servers directly, the sort of data exchanged on them might pose a concern. If your data is shared on the same server, unusual data uploads might pose a security risk.

F. Data Leakage: One aspect of security is ensuring that no unauthorized users have access to your organization's data; another is ensuring that your data is not transferred to anybody outside your business (without proper care in terms of checks, etc.). External sources might be exposed to sensitive and private data if data is leaked. Even if an organization's data security standards are in place, the cloud equivalent is heavily reliant on the storage provider's security controls.

G. API and Storage Sinks: Migrating to the cloud is a time-consuming procedure that is typically made easier by utilizing the cloud's storage APIs and storage gateways. However, because these technologies act as a middleman between the user and the platform, they might be a security risk. Data leaks can be caused through an insecure API or gateway, thus only utilizing services that have robust comprehensive security during data transport.

H. Account Control: Attackers can acquire access to sensitive/private information through hijacking. Subscription accounts or cloud service accounts are the accounts that are most vulnerable in cloud settings.

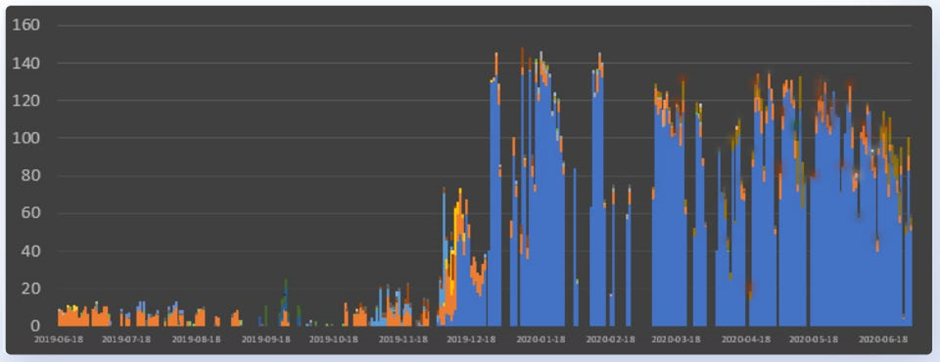
I. Malicious Insiders: Because insiders don't have to hack past firewalls, VPNs, or other security barriers, they can access networks, data, and systems on a trusted level. A bad insider might sell or utilize this knowledge for personal benefit or the target user's collective loss (s).

J. Data Control: Any attack or occurrence in which sensitive information is taken, read, or utilized by an unauthorized person is considered a data breach. Lack of data control may be seen in insecure data storage containers, excessive permissions, unpatched systems, and so on.

K. Management Console Security: The most exposed parts of a system are the user interfaces and APIs. From authentication to access control, everything must be built to prevent security breaches.

L. Multi-tenancy Issues: A cloud service provider's key priority should be data isolation, traffic bandwidth, and so on. To address this, logical security, trust, access control, and encryption of both keys and data are essential.

4.1 Based on tools used for implementation.



1. SVM (Support Vector Machine) [9].

It is a tool used to analyze the training set of the classifier and predict the final classes of the cloud services. When assigning tasks to the appropriate cloud services, master[9] acts as a watchdog to monitor the behavior of members of the community. The result is a data set consisting of a representative set of statements. Later, master uses SVM to analyze this dataset and classify cooperative or malicious service.

The proposed SVM based detection framework consists of three main phases.

**Phase 1 : Monitoring**

Master[9] monitors the behavior of the services that belong to its community. It allows the master to collect a set of representative pieces of evidence that span over a period of time.

**Phase 2 : Classification**

Master[9] constructs the training set of the SVM classifier based on the set of evidence collected in Phase 1. It then analyzes the training data using SVM to get the properties of data by pairing each set of inputs with the expected output. Using the learned classifiers, finally it predicts the final class of the cloud

**Phase 3 : Punishment**

In this phase of punishment master[9] of the community detects the malicious clouds and services from the classified set in phase 2 and hence it blacklists them from the community.

2. DevSecOps processes: DevSecOps and DevOps are constantly monitored in order to reduce vulnerability and exploitation possibilities, improve code quality, deliver new features, and increase the application's pace. Including security procedures, advances, and quality assurance in the units of the business/applications team rather than relying on a single security verification team is critical for today's enterprises' operations.

3. Tools for automating application deployment and management: The increase in the pace and number of security threats, along with a lack of security-related skills, means that even the most experienced security expert will be unable to keep up. Ordinary jobs may be automated, and it can also augment human labor advantages with those of machines, which is a fundamental feature of sophisticated IT operations.

4. Assessing cloud framework:To guard against unwanted access, all businesses must monitor connected devices, update current accessible devices, and delete obsolete / useless devices. The ability to map data flows across systems, apps, and devices will allow for a more thorough examination of cloud utilization. Many cloud providers provide services to help with this.

5. Security Encryption:Understanding how data is safeguarded (particularly during transit between data centers, servers, and other devices) is a key component of any cloud storage infrastructure. Additional security is provided by robust user management and machine-learning algorithms that verify geo-locations and IP addresses of visits. The addition of a layer of abstraction for the cloud engineer monitoring services is provided by learned filters regarding typical regions of access and their display in event logging.

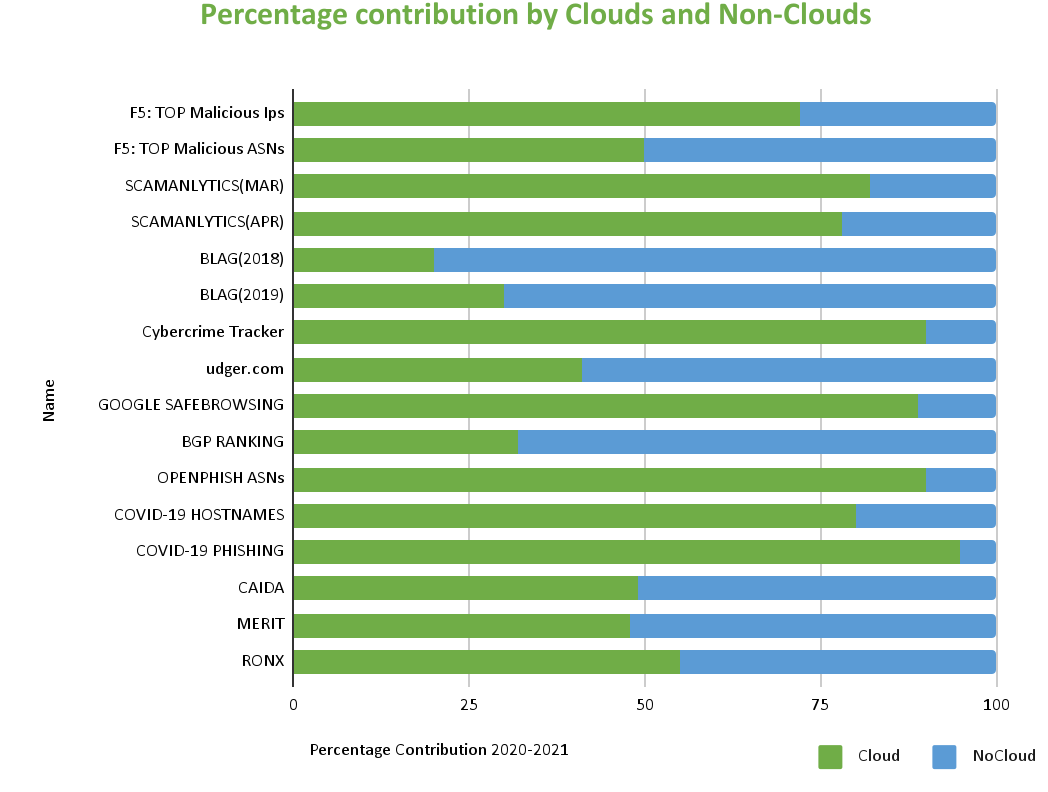
6. Event prevention and Intervention: One of the most significant parts of cloud security, like with other IT disciplines, is to uncover issues and vulnerabilities that exist in the cloud; nevertheless, it is more vital to apply the most convenient reaction to any issue you find. In summary, the cloud system is built on a unique set of storage engines that are managed by a bespoke distributed transaction coordinator, and it provides high availability. Cloud providers must solve these difficulties in the areas of adaptation, workload analysis, and prototyping in order to maximize the flexibility, scalability, and efficiency of available resources.

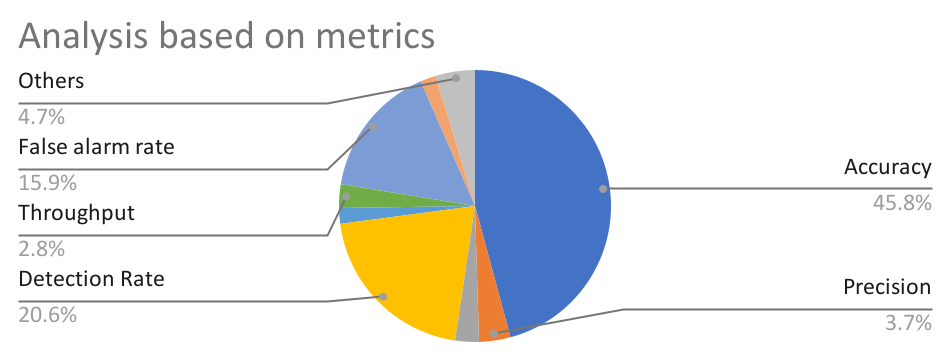
1) Partitioning: To enable values to be multiplied over numerous computers, data must be divided into pieces that improve speed and searches.

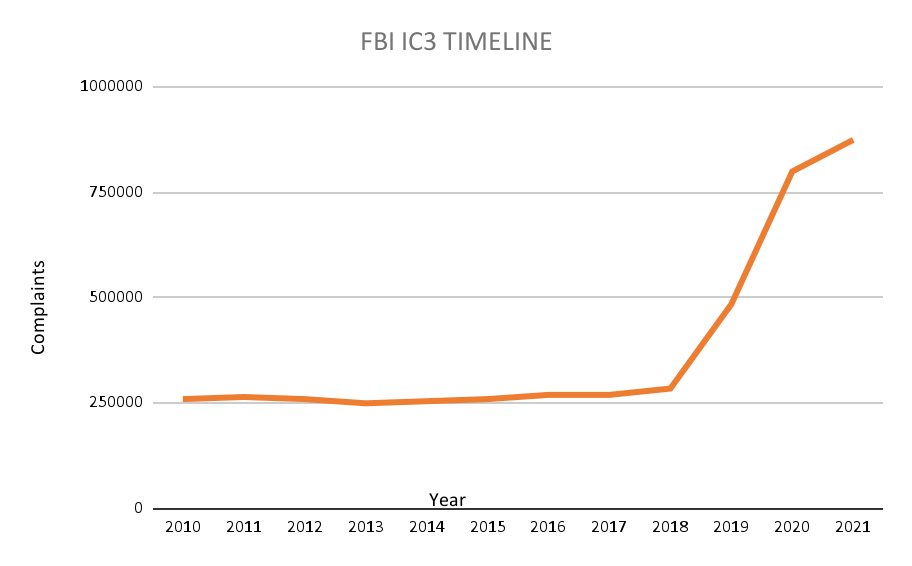
2) Migration: The cloud's capacity to be adaptable is one of its most basic characteristics. Flexibility in a cloud service refers to allocating resources where they are most required. With the volume of data that has to be moved for reintegration, this is especially problematic in a database context. During migration, the proper strategy should estimate the adaption time and aim to avoid overloading cloud fragments and activities like breaking down data into little parts and retaining the capacity to do operations while executing transactions.

3) Workload analysis and allocation: To correctly collaborate on workloads on virtual machines, you must first analyze your resource requirements and determine how to assign them to your virtual machines.

4.2 Based on evaluation of metrics.

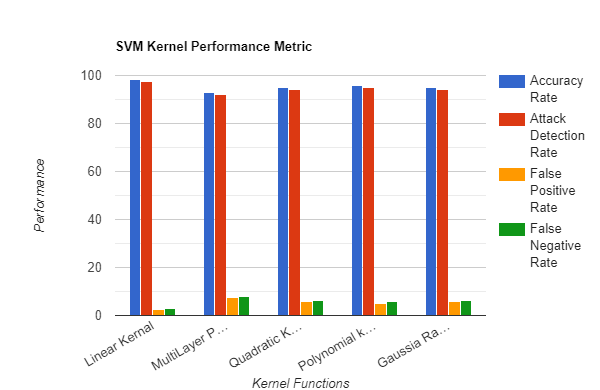






4.3 Based on Accuracy.

Following metric shows the accuracy rate, attack detection rate, false positive rate and false negative rate with respect to five. SVM kernel functions[9].



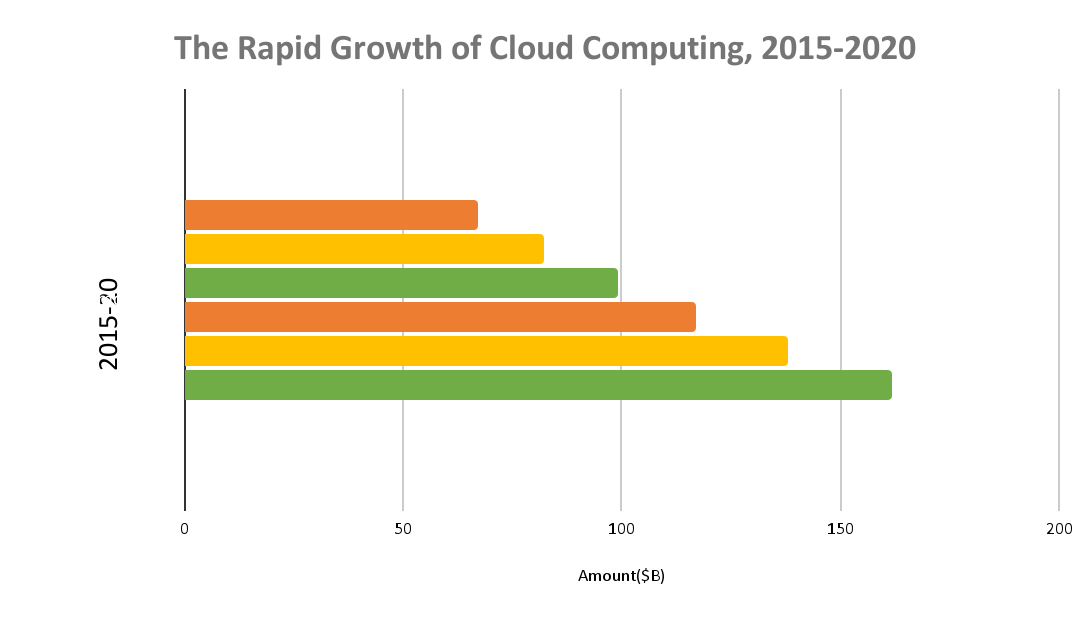
4.4 Based on datasets.

| **Clouds** | | **Non-Clouds** | |
| --- | --- | --- | --- |
| ***Organizations*** | ***AVG RANK*** | ***Organizations*** | ***AVG RANK*** |
| SELECTEL | 1.33 | SSNET.BG | 1.00 |
| IPVOLUME | 2.00 | MEGA VOLTAGE | 3.33 |
| PERHOST | 2.67 | CHINA UNICOM | 4.00 |
| INTER-HOST.NET | 3.33 | CHINA TELECOM | 5.33 |
| NOVOGARA | 5.00 | CENSYS.IO | 6.33 |
| DIGITALOCEAN | 5.33 | CHINA MOBILE | 6.67 |
| RM-INJINERING | 8.33 | AS62355 | 7.33 |
| OVH | 8.67 | DM AUTO EOOD | 9.33 |
| COLOCROSSING | 9.00 | VITOX TELECOM | 9.33 |
| RELIABLESITE | 9.67 | WENZHOU GLASSES | 11.00 |

Ordered by organization wise total malscans

| **Clouds** | | **Non-Clouds** | |
| --- | --- | --- | --- |
| ***Organizations*** | ***malorg Score*** | ***Organizations*** | ***malorg***  ***score*** |
| PERHOST | 5.19 | SSNET.BG | 9.18 |
| INTER-HOST.NET | 4.24 | CHINA UNICOM | 0.97 |
| RM-INJINERING | 0.99 | CHINA TELECOM | 0.96 |
| NOVOGARA | 0.92 | DM AUTO EOOD | 0.68 |
| DIGITALOCEAN | 0.57 | VITOX TELECOM | 0.44 |
| IPVOLUME | 0.51 | MEGA VANTAGE | 0.23 |
| SELECTEL | 0.31 | CHINA MOBILE | 0.23 |
| OVH | 0.22 | VNPT | 0.20 |
| LINODE | 0.16 | VIETTEL GROUP | 0.18 |
| NFORCE | 0.13 | TELEKOM.CO.ID | 0.16 |

Ordered by organization wise total malorgscans



| **Non-Clouds** | | **Clouds** | |
| --- | --- | --- | --- |
| ***Organizations*** | ***Average Ranking*** | ***Organizations*** | ***Average Ranking*** |
| CHINA TELECOM | 5.0 | OVH | 5.0 |
| VNPT | 6.0 | DIGITALOCEAN | 5.3 |
| ROSETELECOM | 6.3 | AMAZON AWS | 7.7 |
| AIRTEL | 6.8 | GODADDY | 8.0 |
| PTCL | 8.0 | CLOUDFLARE | 8.3 |
| CHINA UNICORN | 8.0 | HETZNER | 11.3 |
| ER-TELECOM | 8.7 | UNIFIED LAYER | 12.7 |
| VEITTEL GROUP | 12.5 | QUADRANET | 13.3 |
| CHINA MOBILE | 13.7 | GOOGLE CLOUD | 18.7 |
| FPT CORP | 17.6 | NAMECHEAP | 19.0 |

Ordered by organization wise total malbi

| **Clouds** | | **Non-Clouds** | |
| --- | --- | --- | --- |
| ***Organizations*** | ***malorg Score*** | ***Organizations*** | ***malorg***  ***score*** |
| DIGITALOCEAN | 0.27 | AIRTEL | 0.22 |
| LANSET | 0.22 | PTCL | 0.23 |
| OVH | 0.20 | ROSETELECOM | 0.21 |
| NAMECHEAP | 0.19 | VNPT | 0.21 |
| UNIFIED LAYER | 0.18 | CHINA TELECOM | 0.21 |
| HOSTMAZE | 0.14 | ER-TELECOM | 0.19 |
| GODADDY | 0.13 | VIETTEL GROUP | 0.16 |
| COLORCROSSING | 0.10 | TOT PCL | 0.15 |
| QUADRANET | 0.10 | FREGAT.NET | 0.12 |
| NOCIX | 0.10 | UFANET | 0.11 |

(d) Ordered by organization wise malorgscore

| **Dataset** | **Source** | **Dataset** | **Source** |
| --- | --- | --- | --- |
| CAIDA | [19] | Cybercrime Tracker | [10] |
| Merit | [17] | Google Safebrowsing | [14] |
| RONX | Anon. | COVID-19 Hostnames | [8] |
| Scamalytics | [35] | COVID-19 Phishing | [7] |
| udger.com | [15] | Openphish | [20] |
| BLAG (2019) | [47],[38] | BGP Ranking | [3] |
| F5 Labs: Attack Traffic | [18] | BLAG (2018) | [47],[38] |

1. Network Traces

* CAIDA real-time network telescope data
* Merit network real-time network telescope data
* Regional optical network RONX dataset

1. Blocklists

* Scamalytics: IP fraud risk lookup tool
* F5 Labs
* BLAG
* Google Safe Browsing
* COVID-19 phishing URL’s list from maltiverse.com
* COVID-19 malicious hostnames/URL’s List from maltiverse.com
* Openphish
* Cybercrime Tracker
* Udger.com
* BGP Ranking

1. Limitations

1. SQL Injection Attack.

This is a virtual attack on a computer that mostly harms SaaS. Because of the application's bad architecture, SaaS suffers the most damage from this assault.

2. Cloud Computing Abuse and Malicious Use

Hackers take advantage of flaws in the process of authenticating cloud registrations. They also have access to SaaS, PaaS, and IaaS services. Hackers may make their move by engaging in dubious activities such as phishing and/or spamming.

3. Net Sniffers

It is also a danger that comes with SaaS. The hacker obtains access to the system via programmes in this form of danger. This allows them to collect packets as they move over a network, as well as data if it is transmitted unencrypted through the intercepted packets.

4. Attacks by Flooding

This is a form of "denial of service attack" that is used to increase network connectivity by flooding the network with a significant number of different types of data. This form of attack occurs when hackers overload services or networks with data packets.

1. Software as a Service (SaaS):

The cloud service provider gives database and application software access using this paradigm. SaaS (Software as a Service) is a high-demand software. The challenges with this application are around its security, which is naturally oriented around access and stored information because practically all of the models that are responsible for data sharing security issues leave these two issues to the SaaS customers. Every user must be aware of the type of information they share with the cloud and who else is permitted to utilize that information. Users must be aware of the level of protection given by the service provider.

The following are the top ten cloud application security vulnerabilities that SaaS users face:

i. Cloud apps do not give a clear visual image of what data is included inside them.

ii. A malicious actor steals data from a cloud application.

iii. There is insufficient control over sensitive data accessibility.

iv. Inability to monitor data in the movement of data from/to cloud apps.

v. Provisioning of cloud apps outside of IT visibility (e.g., shadow IT)

vi. The available workforce is insufficient and inexperienced for resolving difficulties and developing cloud application security.

vii. Inability to prevent hostile data usage or data theft on the inside.

viii. High-tech fires and risks to service providers.

ix. Inability to analyze the cloud application's operational security.

x. Incapacity in terms of ensuring regulatory compliance

2. Infrastructure as a Service (IaaS):

IaaS is a method of supplying users with virtual or physical computers that run virtual machines, such as Hyper-V or virtual box. In IaaS, data protection is a difficult issue.

As the user's responsibilities for the operating system, network traffic, and applications grow, so do the dangers. Organizations should not put off evaluating the evolution of assaults that have gone beyond the data, which is at the heart of the IaaS danger.

Below are the top 10 cloud security vulnerabilities experienced with IaaS:

i. Workloads and accounts in the cloud are generated outside of IT's view (e.g., shadow IT)

ii. Lack of total control over who has access to critical information

iii. Malicious insider theft or misuse of information hosted in cloud infrastructure

iv. Lack of staff with the skills to secure cloud infrastructure

v. Lack of visibility into what data is in the cloud

vi. Inability to prevent malicious insider theft or misuse of information

vii. Inconsistent security controls across multi-cloud and on-premises environments

viii. Advanced threats and attacks against cloud infrastructure

ix. Inability to check for vulnerabilities in cloud workload systems and apps.

x. An attack can extend laterally from one cloud task to another.

3. Platform as a Service (PaaS)

This model's provider gives the user access to the operating system, web servers, and programming language execution environment. This paradigm serves as a link between the IaaS and SaaS worlds.

1. Research Gaps Identified.

In the initial days of the cloud, people and technicians were unaware of how to face the malfunctioning cloud services and machines. As there was no prior knowledge, miscreants found it easier to get into cloud machines by compromising existing accounts. As mentioned previously in the research paper, attackers can rent cloud machines or hijack them from cloud users and leverage them to generate unwanted traffic, such as spam and phishing, denial of service, vulnerability scans, drive-by downloads, etc. For example: In the year 2013, Yahoo witnessed the most devastating breach. The hack started with a spear-phishing email that was sent to an employee at Yahoo early in 2013. Later in the year 2017, the FBI identified four suspects out of which two were Russian spies.[18]

In the coming years and after extensive research regarding "cloud misbehavior and malicious traffic originating from cloud machines", many security lapses were discovered. It was found that as the technology advanced, the large amount of data stored in cloud servers could become a target for the hackers which in turn would lead to compromised accounts.

The interfaces and APIs which are weak would expose the authorizations to security issues like confidentiality, integrity, availability and accountability. The sharing of memory, databases and other data among the organizations would lead to data crashes or reports of larger bugs and later on, even may be affected by the virus too. Breaches involving health information, trading secrets, and intellectual property rights would bring destruction. [19]

Multi-factor authentications such as one-time passwords, phone-based authentications, OTPs, and security questions would make it harder for the attacker to log in from stolen passwords. Using multi-factor authentication and encoding the data or information so that only authorized users can access it means creating a disaster recovery plan, building infrastructure that is as secure as possible, and investing in prevention and detection technologies. [19]

The slow and steady transition from the initial days of cloud computing to the exponential growth of cloud services due to the epochal shift to online. The security lapses were overcome but with advancements, conmen found new ways to exploit these services. Hence, the research still continues to date to overcome these challenges and create a safe and secure cloud.

1. Conclusion

Clouds can be misused, either via carelessness or because they actively allow it. In our work we analyzed the ways by which clouds misbehave and also the mitigation techniques being used by specialists to quantify cloud misbehavior and the malicious traffic originating from cloud machines. In the process of analysis we also tried to identify the research gaps within a time frame of 5-6 years and stated the limitations from each era. After thorough analysis of 20 different research papers and doing a comparative study on the basis of four distinct variables namely : analysis on the basis of implementation of tools, performance analysis ( accuracy and dataset) and on the basis of metrics. It can be concluded that from the 13 datasets used in the survey the CAIDA stands to be the most accurate followed by the RONX dataset. Also from all the cloud organizations used in the survey, it can be said that the OVH and Digital Ocean have proven to show the most malicious activity. Thus, if efforts are focused on securing these clouds, Internet attacks can be greatly reduced.

1. References

[1] “Cloud Computing Market by Service Model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), Deployment Model (Public and Private), Organization Size, Vertical, and Region - Global Forecast to 2026.” https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html

[2] Tandon, Rajat & Mirkovic, Jelena & Charnsethikul, Pithayuth. (2020). “Quantifying Cloud Misbehavior.” 10.1109/CloudNet51028.2020.9335812.

[3] “Cloudy With a Chance of Misbehavior”: Researching Malicious Traffic originating from CloudMachines <https://viterbischool.usc.edu/news/2021/05/cloudy-with-a-chance-of-misbehavior-researching-malicious-traffic-originating-from-cloud-machines/>

[4] S. Alrwais et al., "Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks," 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 805-823, doi: 10.1109/SP.2017.32.

[5] “Cybercriminals Abuse Amazon Cloud to Host Linux DDoS Trojans” <https://www.securityweek.com/cybercriminals-abuse-amazon-cloud-host-linux-ddos-trojans>

[6] “Hackers Abuse Google Cloud Platform To Attack D-Link Routers” <https://www.tracesecurity.com/blog/daily-breach-1/hackers-abuse-google-cloud-platform-to-attack-d-link-routers>

[7] “Azerbaijan and the fineproxy DIY DDoS Service (Region40/ Quality network)”

<https://www.qurium.org/alerts/azerbaijan-and-the-region40-ddos-service/>

[8] “Public Cloud Services Increasingly Exploited to Supercharge DDoS Attacks”

<https://www.link11.com/en/blog/threat-landscape/public-cloud-services-increasingly-exploited-to-supercharge-ddos-attacks-new-link11-research/>

[9] Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, Azzam Mourad “ Misbehavior Detection Framework for Community-Based Cloud Computing”.

<https://ieeexplore.ieee.org/document/7300816>

[10] F. Doelitzscher, M. Knahl, C. Reich and N. Clarke, "Anomaly Detection in IaaS Clouds," 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2013, pp. 387-394, doi: 10.1109/CloudCom.2013.57.

[11] Liao, Xiaojing & Alrwais, Sumayah & Yuan, Kan & Xing, Luyi & Wang, Xiaofeng & Hao, Shuang & Beyah, Raheem. (2018). Cloud repository as a malicious service: challenge, identification and implication. Cybersecurity. 1. 14. 10.1186/s42400-018-0015-6.

[12] M. K. Sasubilli and V. R, "Cloud Computing Security Challenges, Threats and Vulnerabilities," 2021 6th International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 476-480, doi: 10.1109/ICICT50816.2021.9358709.

[13] A. Syed, K. Purushotham and G. Shidaganti, "Cloud Storage Security Risks, Practices and Measures: A Review," 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp. 1-4, doi: 10.1109/INOCON50539.2020.9298281.

[14] Z. Balani and H. Varol, "Cloud Computing Security Challenges and Threats," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116266.

[15] “Top 5 Security Risks of Cloud Computing” <https://securityscorecard.com/blog/top-security-risks-of-cloud-computing>

[16] Rakotondravony, N., Taubmann, B., Mandarawi, W. et al. Classifying malware attacks in IaaS cloud environments. J Cloud Comp 6, 26 (2017). https://doi.org/10.1186/s13677-017-0098-8

[17] “Is Cloud Computing Any Safer From Malicious Hackers?”

<https://www.trendmicro.com/en_in/research/20/e/is-cloud-computing-any-safer-from-malicious-hackers.html>

[18] <https://blog.storagecraft.com/7-infamous-cloud-security-breaches/>

[19] “Cloud Computing: Security Issues and Research Challenges”