**Research on**   
**Quantifying Cloud Misbehavior and Malicious Traffic Originating from Cloud Machines**

**A PROJECT REPORT**

###### ***Submitted by***

**Shivyanshi Shukla (20BCY10027)**  
**Kartik Sharma (20BCY10044)**  
**Niture Harshwardhan (20BCY10049)**  
**Chinmay Chougule (20BCY10060)**

*in partial fulfillment for the award of the degree*

*of*

##### **BACHLEOR OF TECHNOLOGY**

***in***

**COMPUTER SCIENCE AND ENGINEERING with SPECIALIZATION in CYBER SECURITY AND DIGITAL FORENSICS**



**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRIKALAN, SEHORE**

**MADHYA PRADESH - 466114**

APRIL 2022

**BONAFIDE CERTIFICATE**

Certified that this project report titled **“Quantifying Cloud Misbehavior and Malicious Traffic Originating from Cloud Machines”** is the Bonafide work of “**Shivyanshi Shukla (20BCY10027) Kartik Sharma (20BCY10044) Niture Harshwardhan (20BCY10049) Chinmay Chougule (20BCY10060)”** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.



**PROGRAM CHAIR**   **PROJECT GUIDE**

Dr. R. Rakesh, Assistant Professor Dr. Ganeshan R, Assistant professor

School of Computer Science and Engineering School of Computer Science and Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

The Project Exhibition 2 Examination is held on 23/04/22

**ACKNOWLEDGEMENT**

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr Shishir Kumar Shandilya, Head of the Department, School of Computing Science and Engineering for much of his valuable support encouragement in carrying out this work.

I would like to thank my internal guide Dr. Ganeshan R for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computing Science and Engineering, who extended directly or indirectly all their support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**LIST OF FIGURES AND GRAPHS**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
| **1** | **Metrics based Analysis** | **11** |
| **2** | **Percentage Contribution by Clouds and Non-Clouds** | **11** |
| **3** | **Analysis based on Metrics** | **11** |
| **4** | **Cloud Challenges** | **14** |
| **5** | **SVM Kernel Performance Metric** | **17** |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | **TITLE** | **PAGE NO.** |
| **1** | **Ordered by organization wise total malscans** | **9** |
| **2** | **Ordered by organization wise total malorgscans** | **9** |
| **3** | **Ordered by organization wise total malbi** | **9-10** |
| **4** | **Ordered by organization wise total malorgscore** | **10** |
| **5** | **Datasets according to References** | **10** |

**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 this traffic. In this paper, we analyze different methodologies, implementation of tools, datasets, and accuracy of analysis.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | List of Figures and Graphs  List of Tables  Abstract | iii  iv  v |
| 1 | **CHAPTER-1:**  **PROJECT DESCRIPTION AND OUTLINE**  1.1 Introduction  1.2 Motivation for the work  1.3 Problem Statement  1.4 Objective of the work  1.5 Organization of the project  1.6 Summary | **1-2**  1  1  1  1  2 |
| 2 | **CHAPTER-2:**  **RELATED WORK INVESTIGATION**  2.1 Introduction  2.2 Core area of the project  2.3 Approaches/Methods  2.3.1 SVM (Support Vector Machine)  2.3.2 DevSecOps processes  2.3.3 Tools for automating deployment and management  2.3.4 Event prevention and Intervention  2.4 Limitations in the Existing System  2.5 Summary | **3-8**  3  3  3  6  8 |
| 3 | **CHAPTER-3:**  **ANALYSIS ARTIFACTS**  3.1 Hardware and Software analysis  3.1.1 Dataset Analysis  3.1.2 Functions Analysis  3.1.3 Metrics based Analysis  3.2 Summary | **9-12**  9  12 |
| 4 | **CHAPTER-4:**  **ANALYSIS, DISCUSSION AND ITS NOVELTY**  4.1 Security Threats  4.2 Solutions to Cloud Security Issue  4.3 Summary | **13-15**    13  14  15 |
| 5 | **CHAPTER-5:**  **PROJECT OUTCOME AND APPLICABILITY**  5.1 Significant project outcomes  5.1.1 Input  5.1.2 Output | **16**  16 |
| 6 | **CHAPTER-6:**  **CONCLUSIONS AND RECOMMENDATION**  6.1 Future Enhancements  6.2 Conclusion | **18-19**  18  19 |
|  | References | 20 |

**CHAPTER-1:**

**PROJECT DESCRIPTION AND OUTLINE**

1.1 Introduction

Over the last decade, the cloud computing business has grown by around 200 billion dollars. Cloud services such as Google Cloud, Microsoft Azure, and Amazon AWS are examples of cloud services that may be rented on demand to support a business. Despite the fact that cloud computing is quickly gaining popularity, there have been worries about its security and vulnerability. Cyber-criminals are reportedly preferring cloud service providers to wreak large-scale damage on internet services. According to recent data, cloud service providers contribute for a considerable portion of DDoS traffic. We focus on measuring the utilization of cloud resources for harmful Internet activity in this study (e.g., sending spam).

1.2 Motivation for the work

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. 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. Hence choosing this topic will allow us to gain more knowledge about cloud computing and cloud security.

1.3. Problem Statement

* Superuser access to cloud computers is common among cloud users.
* However, without the assistance of skilled system administrators, superuser access can provide fertile ground for unintentional or purposeful exploitation.
* Attackers can hire cloud machines or take them over from their owners.
* They take advantage of these in order to create unwanted traffic
* Less awareness about cloud security.

1.4 Objective of the work

Our aim in this project is to go through the different survey papers published in the recent 5-6 years gap and extend our collective study about cloud misbehavior with reference to those papers.

1.5 Organization.

Our Project is organized by our team according to some split-ups of information and data. We gathered information about cloud misbehavior through some research papers in the recent 5-6 years gap.

1.6 Summary.

In the upcoming times or even now most of the people and industries use the cloud. Cloud security is a topic of concern. While reviewing survey papers we observed that the cloud machines are vulnerable, they can be easily taken over by attackers. So, we need to focus on cloud security.

**CHAPTER-2:**

**RELATED WORK INVESTIGATION**

2.1 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 serve 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 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 have 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.

2.2 Core area of the project

According to the study[2], 13 separate datasets were analyzed, including the investigation of unwanted traffic. Only 5.4 percent of own routable IPv4 address spaces contribute to 22-96 percent of entries on blocklists, according to the analysis. It was also discovered that cloud traffic is 20-100 times more aggressive than non-cloud traffic (/24 prefix sending vulnerability scans). According to the research metrics, 25 clouds account for 90% of all cloud scans, and 10 clouds account for more than 20% of cloud blocklist entries.

The authors of [4] examine BulletProof Hosting (BPH) services and give the first thorough investigation on this emerging trend. BPH creates an environment for conmen that is resistant to reports of illegal activity.

Omar Abdel Wahab et al. [9] introduced the Community-based Cloud Computing architecture, which intends to improve the quality and performance of cloud services. This study discovered that malicious services that undertake attacks against the entire community or against specific partners in that community constitute a threat to the architecture. This issue was then addressed and resolved using a misbehavior detection system built on the Support Vector Machine (SVM) learning approach.

In summary, numerous linked papers investigate various forms of cloud misbehavior shown by cloud computers in diverse situations. They also propose several methods for mitigating harmful traffic and cloud misbehavior. In this work, we examine the various ways for analyzing cloud misbehavior and harmful communication emanating from cloud workstations. We only look at prior research done in this subject over the course of 5-6 years.

2.3 Approaches/Methods

2.3.1 SVM (Support Vector Machine) [9].

1. 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.
2. The proposed SVM based detection framework consists of three main phases.
3. **Phase 1: Monitoring**
4. 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.
5. **Phase 2: Classification**
6. 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
7. **Phase 3: Punishment**
8. 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.

2.3.2 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.

2.3.3 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.

2.3.4 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 adaptation 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.

2.4 Limitations in the Existing System

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.

2.5 Summary

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 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 cloud machines. We only focus on the survey of previous research performed in this domain over a span of 5-6 years.

**CHAPTER-3:**

**ANALYSIS ARTIFACTS**

3.1 Hardware and Software Analysis

3.1.1 Dataset Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **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] |

Datasets according to References

3.1.2 Functions Analysis

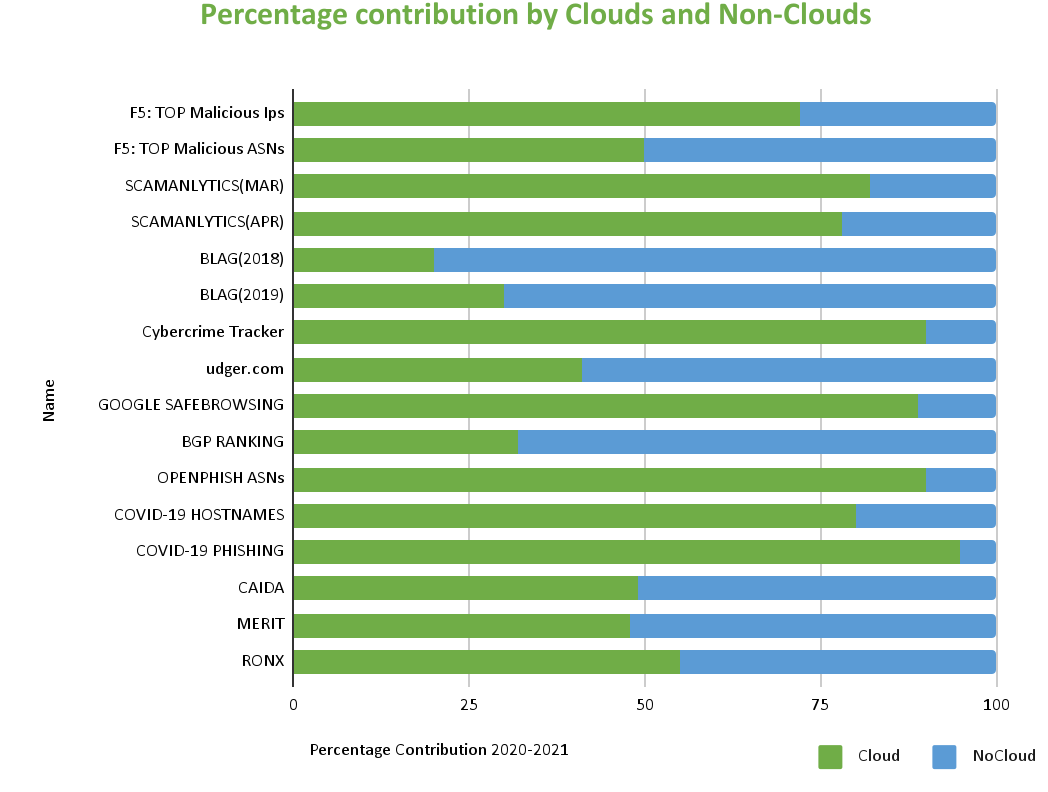
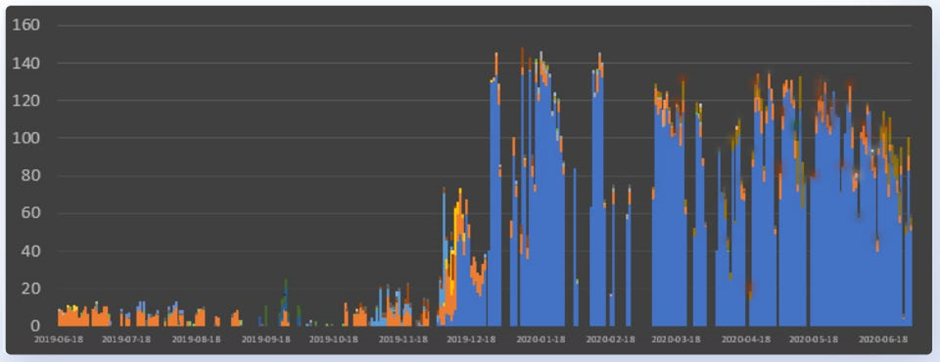
1. Network Traces

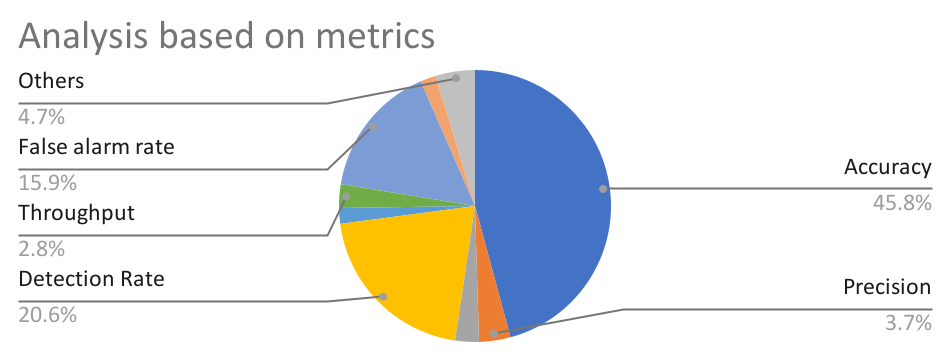
* CAIDA real-time network telescope data
* Merit network real-time network telescope data
* Regional optical network RONX dataset

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

3.1.3 Metrics based Analysis





3.2 Summary.

We have organized the data in the form of tables and divided the organizations into clouds and non-clouds. The data tables have different organizations in cloud and in non-clouds and we arranged the information according to the average ranking calculated based on various parameters like mal-scans, mal-scores etc. We also represented the data in the form of graphs and figures. The data analyzed is based on the different datasets we collected from the different research papers.

**CHAPTER-4:**

**ANALYSIS, DISCUSSION AND ITS NOVELTY**

4.1 Security Threats

1. The location of the information, data protection, distinction, and information recovery are all covered by the security service level agreement (SLA).

2. A variety of security administration standards can be found in the Information Technology Infrastructure Library.

3. A Denial-of-Service attack based on HTTP or XML is the most critical problem with cloud computing. These types of violations are simple for the hacker to do, but twice as difficult to detect and stop.

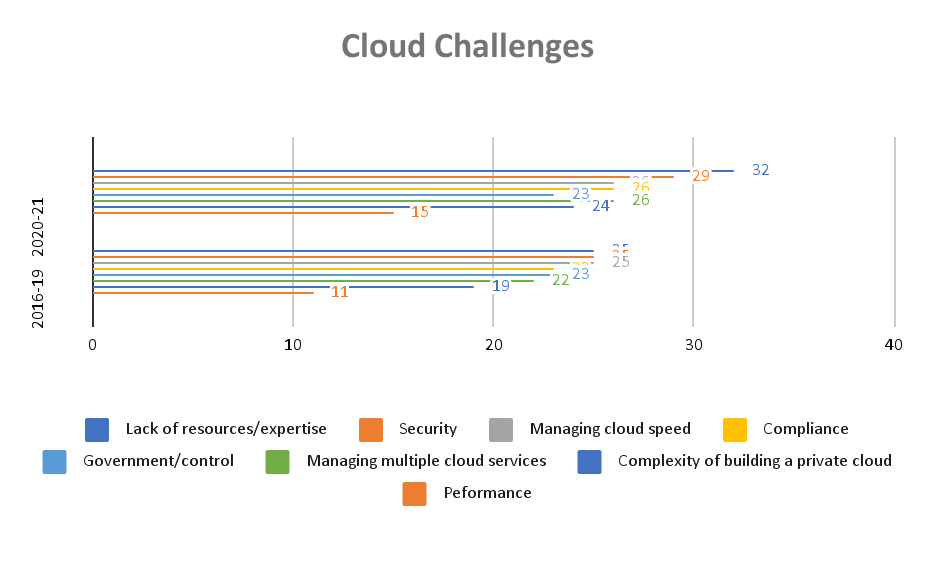
Lack of transparency, high-speed internet access, and uniformity, on the other hand, are the most pressing concerns for enterprises. Data security hazards arise from keeping records of users' privacy, awareness, and privacy practices.

4. Lack of Control: On the one hand, you won't have to handle your data, but it will be managed in the cloud by someone else. Because you have no control over your data storage, anything that affects the storage capacities of your provider also affects your data access. One of the most critical concerns in cloud storage is being locked out of your own storage platform. As a result, choosing a trustworthy and secure vendor is essential.

5. Dedicated Servers: Data is stored on-site servers in cloud-based storage systems, and servers store data from multiple users. While users cannot directly access these servers, the type of data that is transferred on them may be of concern. Unusual data uploads may constitute a security concern if your data is shared on the same server.

6. Data Leakage: Ensuring that no unauthorized persons have access to your organization's data is one part of security; another is ensuring that your data is not shared to anyone outside your firm is another (without proper care in terms of checks, etc.). If data is released, external sources may be exposed to sensitive and private information. Even if an organization's data security requirements are in place, the cloud equivalent is primarily reliant on the security controls of the storage provider.

7. Sinks for APIs and Storage: Migrating to the cloud is a lengthy process that can be sped up by employing the cloud's storage APIs and storage gateways. These technologies, however, may pose a security risk because they function as a mediator between the user and the platform.

 4.2 Solutions to Cloud Security Issue

A. Access Control: An access control mechanism allows an authenticated user to access an information system while preventing unauthorized access. However, suitable processes for overseeing the allocation of access to information systems could be followed. These methods must cover all phases of the user access life cycle, from initial registration of new users to the last registration of users who no longer require access to the most up-to-date information systems and services.

The user's requirement to govern the assignment of privileged access, which can override system controls as needed, should be given special consideration. For appropriate access control management, consider the following five control statements:

Users' access rights can be managed.

Encourage the use of relevant resources.

Examine network service access.

Verify that you have access to the operating system.

Keep an eye on the software and systems you're using.

B. Provide more security at minimum cost: Follow these measures to make cloud computing safer and more convenient for reducing computer costs:

• When a user enrolls in a cloud computing service, stringent validation of the user's background is required.

• Cloud service providers and users must sign an SLA that clearly defines the parties' obligations and functions in relation to the contracting parties' contractual conditions.

• You shall be responsible for data loss owing to cloud service providers and data backup measurements (if any).

• Cloud providers must give their staff transparency and tried-and-true solutions.

• Cloud service providers should be able to search for each other.

• A minimal standard for cloud computing should be established, and cloud service providers should be accredited.

C. 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 adaptation 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.

4.3 Summary

In this chapter we have listed out the major security threats to clouds based on the research papers we have been through. A major security threat to cloud based on our discussion is DDoS. Based on the security threats we prepared a graph which shows comparison of cloud challenges then in 2016-19 and now 2020-21. It is observed that cloud security has improved over the years.

**CHAPTER-5:**

**PROJECT OUTCOME AND APPLICABILITY**

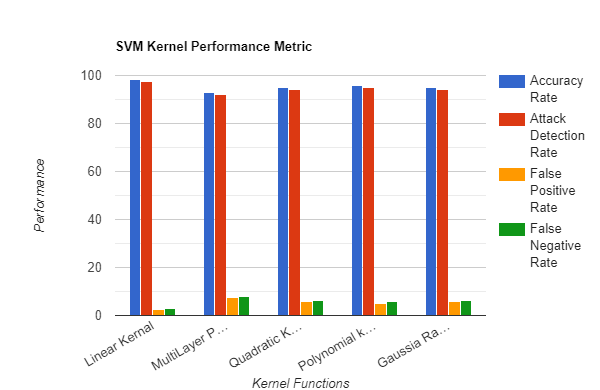
5.1 Significant project outcomes

5.1.1 Input

We have gathered and studied research and survey on the cloud security domain within the gap of 5-6 years. While reading the papers we got to know about the different methodologies used to analyze malicious services in cloud machines. We collected data sets which contain information about the cloud machines and their malicious behavior in different sections.

5.1.2 Output

The output of the work we did showed us that many people are not aware about cloud computing and its security. We have differentiated the cloud machines which are malicious in nature based on accuracy, implementation tools that been previously used, different datasets from the different papers and evaluation of the metrics. The graphs are already mentioned in this paper in chapter 3 of this report. Metric which shows accuracy rate, attack detection rate, false positive rate, and false negative rate with respect to five SVM kernel functions is as follows



**CHAPTER-6:**

**CONCLUSIONS AND RECOMMENDATION**

6.1 Future Enhancements

People and professionals were unsure how to deal with faulty cloud services and computers in the early days of the cloud. Miscreants found it easier to gain access to cloud machines by compromising existing accounts because there was no prior awareness. As previously stated in the research article, attackers can rent cloud computers or take them over from cloud customers and utilize them to produce unwanted traffic such as spam and phishing, denial of service, vulnerability scans, and drive-by downloads, among other things. For instance: Yahoo suffered the most serious security breach of 2013. The attack began with a spear-phishing email sent to a Yahoo employee in early 2013. In late 2017, the FBI identified four suspects, two of them were Russian spies.[18]

Many security flaws were uncovered in the following years after considerable research into "cloud misbehavior and malicious traffic originating from cloud machines." It was discovered that as technology progressed, the vast amount of data held on cloud servers may become a target for hackers, resulting in compromised accounts.

Weak interfaces and APIs subject authorizations to security risks such as confidentiality, integrity, availability, and accountability. The exchange of memory, databases, and other data between corporations could result in data failures or reports of larger flaws, and eventually, the virus could harm them as well. Breach of health-related information, trade secrets, or intellectual property rights might be disastrous.[19]

Multi-factor authentications like one-time passwords, phone-based authentications, OTPs, and security questions make it more difficult for an attacker to log in with stolen credentials. Using multi-factor authentication and encrypting data or information so that only authorized users can access it necessitates the development of a disaster recovery plan, the construction of secure infrastructure, and the investment in prevention and detection technology.[19]

Due to the epochal shift to online, the gradual and steady movement from the early days of cloud computing to the exponential expansion of cloud services. The security flaws were fixed, but con artists discovered new ways to take advantage of these services as technology advanced. As a result, research is still ongoing to overcome these obstacles and establish a safe and secure cloud.

6.2 Conclusion

Clouds can be misused, either via carelessness or because they actively allow it. In our work we analyzed the ways in 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 of 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.

**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”