RESEARCH ON :

Quantifying Cloud Misbehavior & Malicious Traffic Originating from Cloud Machines

Team - 22

Team Members

Guide:
Dr. Ganeshan R

01 Shivyanshi Shukla
20BCY10027

02 Kartik Sharma
20BCY10044

03 Harshwardhan Niture
20BCY10049

04 Chinmay Chougule
20BCY10060

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 utilisation of cloud resources for harmful Internet activity in this study (e.g., sending spam).

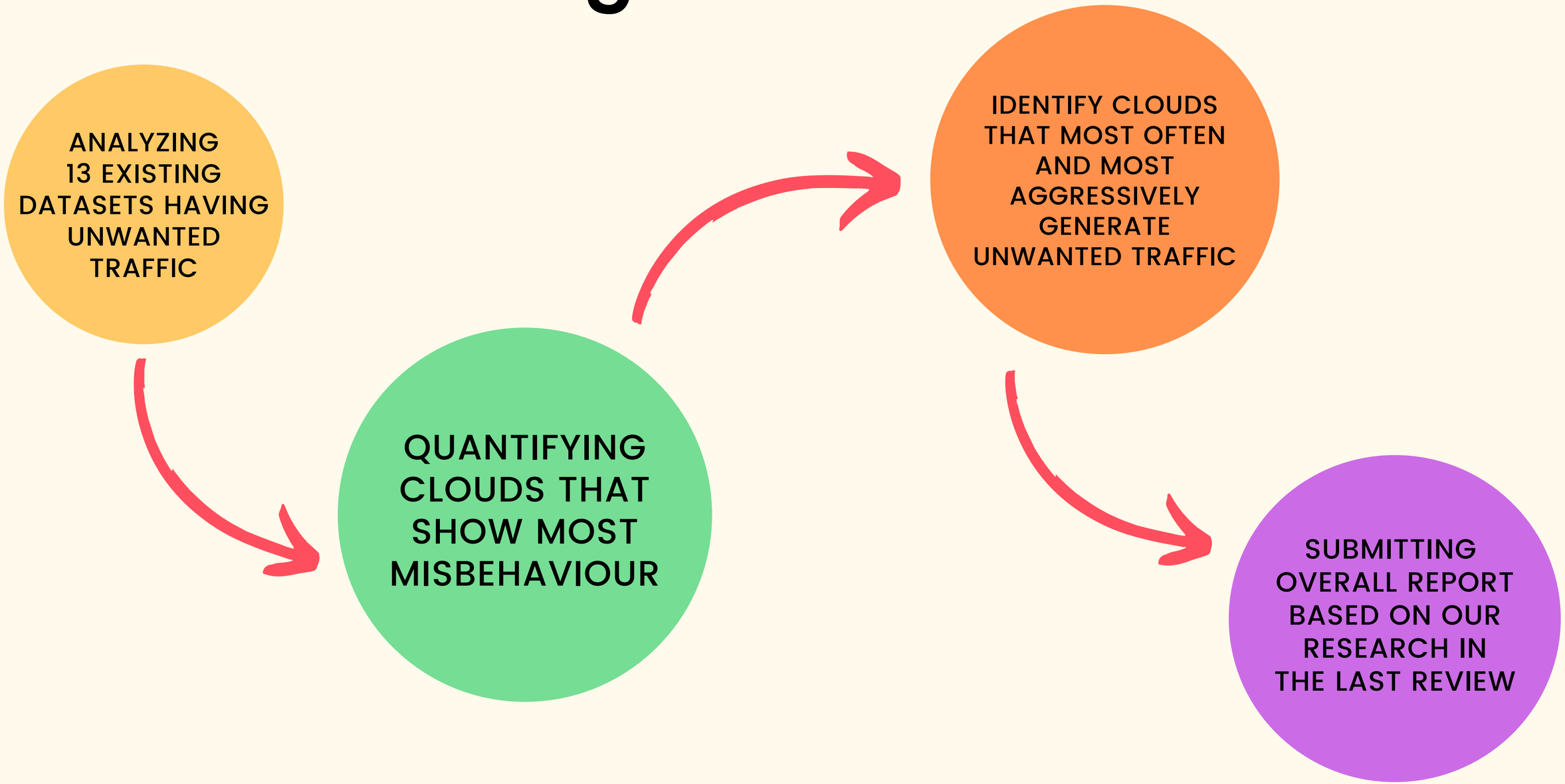
PROPOSED WORK

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.

Real Time Usage

- Clouds may offer content hosting (e.g. Wordpress) or may rent virtual machines to customers, giving them the liberty to install and run their own software and upload their own data (e.g. Amazon AWS).
- Cloud services are increasingly popular among businesses and organizations (e.g, NGOs, government), as a way to scale their infrastructure as demand increases or obtain access to special hardware (e.g., GPUs). Google Cloud, Microsoft Azure and Amazon EC2 are all examples of cloud services one can rent on demand to support their business.

Overall Working Architecture



Literature Review

01 Clouds play a vital role in spreading malware and supporting phishing. Some small clouds misbehave more per /24 prefix than larger clouds, which may indicate lack of security resources, or higher inclination to allow malicious activities

02 Cloud machines can be misused either because of:
The negligence in adopting the security practices by their users
Or because they explicitly permit malicious traffic generation

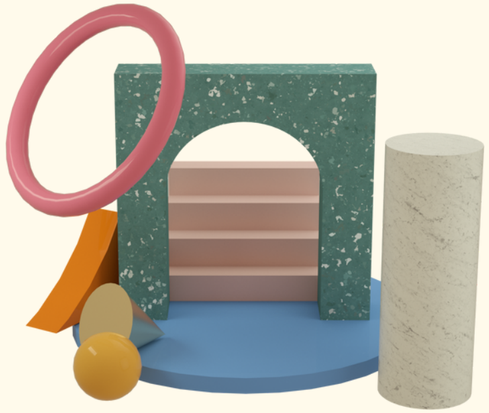
01 Rakotondravony, N., Taubmann, B., Mandarawi, W. et al. Classifying malware attacks in IaaS cloud environments. J Cloud Comp 6, 26 (2017). https://doi.org/10.1186/s13677-017-0098-8

02 Quantifying Cloud Misbehavior
Rajat Tandon, Jelena Mirkovic, Pithayuth Charnsethikul
University of Southern California
Information Sciences Institute

03 Security Challenges from Abuse of Cloud Service Threat Ishrat Ahmad1 and Humayun Bakht 1 1 School of Management, Cardiff Metropolitan University, UK Received 19 Aug. 2018, Revised 7 Dec. 2018, Accepted 17 Dec. 2018, Published 1 Jan. 2019

Attack Tactics

Module Description



The survey paper is divided into the following modules under the name Analysis and Discussion:

- **Analysis based on implementation of tools/techniques:**
  - SVM (Support Vector Machine)
  - DevSecOps processes
  - Tools for automating application deployment and management
  - Event prevention and Intervention
  - Security Encryption
- **Analysis based on performance analysis**
  - Based on datasets
  - Based on accuracy
- **Analysis based on evaluation of metrics**

Result:

THE RESULTS FROM THE SVM KERNEL FIVE FUNCTIONS ARE:
LINEAR KERNEL FUNCTION SHOWED ACCURACY RATE OF 98.14% AND 97.38% ATTACK DETECTION RATE WHEREAS FALSE POSITIVE AND NEGATIVE RATES ARE 2.61% AND 2.98% RESPECTIVELY. SIMILARLY, IN CASE OF MULTILAYER PERCEPTION KERNEL ACCURACY RATE WAS 93.05% AND IT SHOWED ATTACK DETECTION RATE OF 92.25%. FALSE POSITIVE RATE IN CASE OF MULTILAYER PERCEPTION KERNEL WAS 7.69% AND FALSE NEGATIVE RATE WAS 8.02%. THERE ARE FIVE DIFFERENT SVM KERNEL FUNCTIONS WHICH SHOWED DIFFERENT ACCURACY RATE, ATTACK DETECTION RATE, FALSE POSITIVE RATE AND FALSE POSITIVE RATE. AMONG THE FIVE SVM KERNEL FUNCTIONS LINEAR KERNEL SHOWED THE MOST ACCURACY RATE OF 98.14% WHILE IT ALSO SHOWED ATTACK DETECTION RATE OF 97.38% WHICH IS HIGHEST AMONG ALL THE FIVE.

Discussion:

The security service level agreement (SLA) is allocated to the information's placement, data protecting, differentiation, and information recovery. A variety of security administration standards are available from the Information Technology Infrastructure Library. A Denial-of-Service attack based on HTTP or XML is the most critical issue with cloud computing. These types of violations are simple for the hacker to commit; nevertheless, they are twice as difficult to detect.
Choosing a trustworthy and secure provider is essential. Everything that impacts the storage capacity of your provider also affects your data access. On-site servers contain data in cloud-based storage systems, and servers retain data from numerous users. If your data is shared on the same server, unusual data uploads might pose a security risk.
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. 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

Conclusion:

Clouds may be abused, either by negligence or by purposefully allowing it. We investigated how clouds misbehave and the mitigating measures employed by experts to quantify cloud misbehavior and harmful traffic emanating from cloud devices in our research.
Internet assaults can be considerably decreased if efforts are concentrated on safeguarding these clouds.

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] 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.
- [3] “Cybercriminals Abuse Amazon Cloud to Host Linux DDoS Trojans” https://www.securityweek.com/cybercriminals-abuse-amazon-cloud-host-linux-ddos-trojans
- https://www.link11.com/en/blog/threat-landscape/public-cloud-services-increasingly-exploited-to-supercharge-ddos-attacks-new-link11-research/
- [4] Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, Azzam Mourad “ Misbehavior Detection Framework for Community-Based Cloud Computing”.
- https://ieeexplore.ieee.org/document/7300816
- [5] 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.
- [6] 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.
- [7] 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.
- [8] “Top 5 Security Risks of Cloud Computing” https://securityscorecard.com/blog/top-security-risks-of-cloud-computing
- https://www.trendmicro.com/en_in/research/20/e/is-cloud-computing-any-safer-from-malicious-hackers.html
- [9] https://blog.storagecraft.com/7-infamous-cloud-security-breaches/

Thank You !

Team 22