An Intermediate Security Service Protection for Cloud Storage Service

Khandagale Swapneel Raosaheb[1], Khandare Jayesh Deepak[2], Rathod Aakash Ramesh[3], Patne Yashshri Bhagwat[4] and S. V. Athawale[5] (Assistant Professor, Department of Computer Engineering)

[1-5]AISSMS College of Engineering, Savitribai Phule Pune University

---

Abstract - *Malware protection is a must in all aspects of digital life, whether it be PCs, mobile devices or the cloud. Since a cloud service typically hosts data and processes of a great number of citizens, enterprises and even government agencies, its security becomes even more critical and important. Many a times, these services are compromised by uploading a malicious file, which acts as a backdoor or ransomware, via an authorized client of the cloud service. If any attacker manages to pull it off, the results can be disastrous. In this project, we have tried to address this issue by developing an intermediate security service that will scan, detect and remove all kinds of malicious files during transit itself, before it reaches its destination in the cloud. The main focus of this project will be cloud storage services. It will basically be a platform, just like a cloud service where all cloud providers can subscribe to the service and place the intermediate malware scanning servers before their own cloud infrastructure, this way every file on its way to their service will have to go through the intermediate malware scanning service, resulting in better security of the cloud infrastructure. This service can also be deployed between multi cloud servers to ensure that malwares don't propagate from one cloud network to another.*

Keywords: *Malware, Cloud, Cloud service, Ransomware, Hacker, Backdoor, Cyberattack*

1. INTRODUCTION

Cloud computing is the most trending technology in the information technology industry today. The pay-as-you-go policy of cloud providers has reduced the cost of managing IT infrastructure to minimum. New startups and also well-established multinational corporations rely on the cloud for managing their IT infrastructure.

Though cloud providers provide many services, ranging from simple storage to serverless computing and even AI building services, the storage services are the ones used the most [1]. These storage services host several petabytes of data of companies, government agencies, NGOs etc. A considerable amount of this data can be said to be confidential and critical to the functioning of these organizations.

The tremendous amount of data of various organizations in the cloud needs protection. But since security in the cloud is a shared responsibility [2], many a times mishaps occur in the form of cyber-attacks and data breaches [3]. Even though a cloud provider might secure their infrastructure to the best of their capability, it is well known in the information security industry that 100% security is a myth. A vulnerability in one of the components used in running the cloud can compromise the whole infrastructure.

Average cost of data breaches in the year 2019 was $3.86 million [4]. Thus, it is not at all advisable for cloud providers to take cloud security lightly.

One of the most well-known cyberattacks on cloud infrastructure is a malware attack. Once a malware somehow manages to enter a cloud service, the cloud service is at the mercy of the said malware. These malwares can even be ransomwares, which upon infecting the system encrypt all files on the system and demand payment of a hefty amount in exchange of a decryption key [5].

These malware threats on cloud infrastructure bring to light the need for a system to prevent infection of cloud infrastructure. Since, the service most affected and vulnerable to this attack is the cloud storage service, our solution would be primarily focusing on this service.

2. LITERATURE SURVEY

Cloud Security and Protection being a critical activity that intends to avoid or prevent disruption of cloud services has a massive research and innovation under development. Much of this work has been presented at various international conferences of various organizations and societies, published in numerous journals and also published as patents as well. A considerable amount of these works focus on zero-day exploits using malwares [6], ranging from process code injection, file upload to cryptojacking. One of the solutions that have been proposed in these conferences and journals is having an intermediate server in-between the clients and the cloud storage [7]. There have also been proposed solutions that put the intermediate servers in-between multi cloud servers [8], if a particular network employs services from more than one cloud service provider, in order to prevent the malware infection from spreading to others parts of organization IT infrastructure via monitoring. Some of these solutions also apply multi-layer protection [9] where files and traffic are scanned for malwares. A few of the patents have also been filed across the nations, the most notable being ransomware detection and protection in content delivery networks and cloud file storages [10], though each of them seemed to be using their own detection methodologies and their own proprietary algorithms and programs for detection and prevention of a ransomware attack [11].

3. PROPOSED SYSTEM

The system we are proposing for the protection of cloud storage services is a cloud service itself, one might even term it as Security-as-a-Service [12]. The idea is to put a server in front of the cloud storage service so that all files pass through the server before being stored in the cloud storage.

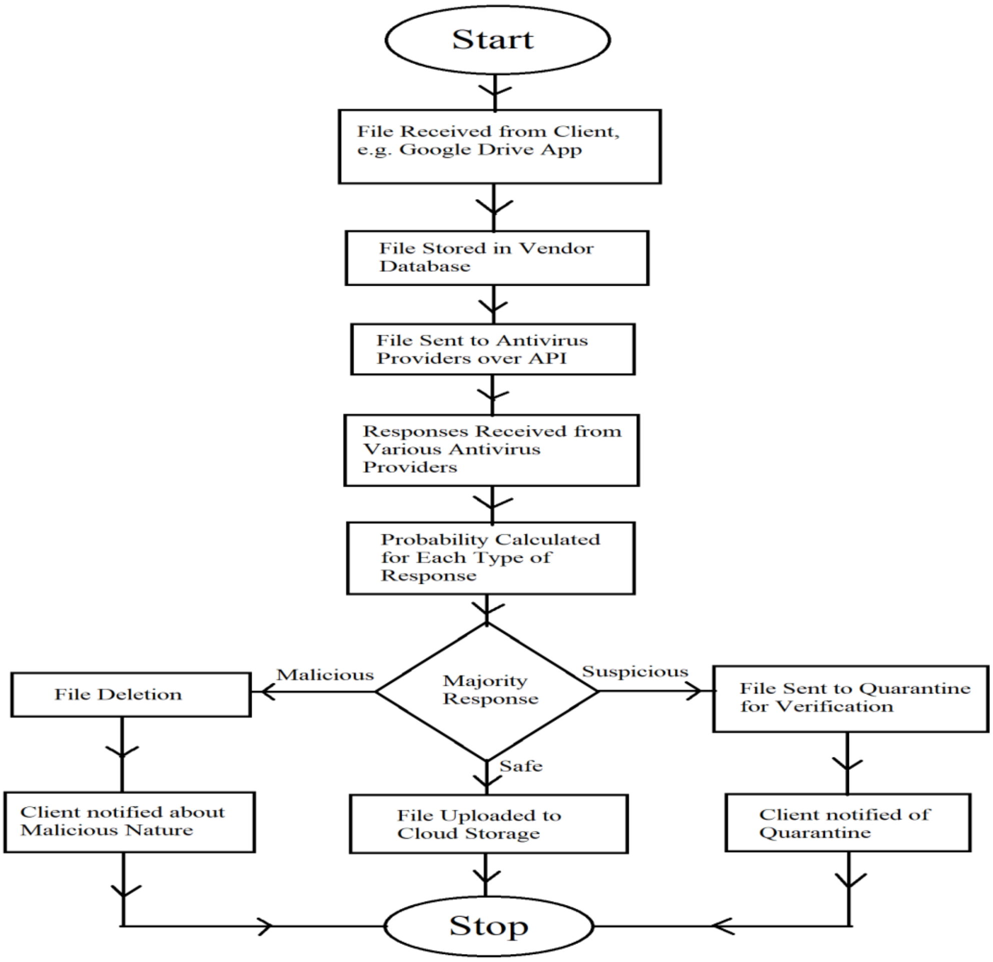
Start
File Received from Client, e.g. Google Drive App
File Stored in Vendor Database
File Sent to Antivirus Providers over API
Responses Received from Various Antivirus Providers
Probability Calculated for Each Type of Response
Majority Response
Malicious
Suspicious
Safe
File Deletion
File Sent to Quarantine for Verification
Client notified about Malicious Nature
File Uploaded to Cloud Storage
Client notified of Quarantine
Stop

Figure 1: Flowchart of Proposed System

The steps for the process are as follows:

i. Start

ii. Select a file to upload, the file can be uploaded via web, desktop or mobile clients.

iii. Click Upload to begin the uploading process.

iv. The file arrives at the intermediate server.

v. The file is scanned by several scanners provided by their respective vendors.

vi. The percentage of scanners flagging the file as malicious/suspicious is calculated.

vii. If even one of the scanners flags the file as "Malicious", the file is deleted and an error saying "Malicious file detected" is returned.

viii. If the percentage of scanners flagging the file is "Suspicious" is more than 50% and none of them flags it as "Malicious", it is put in quarantine in the server itself and the support team is notified by an email to verify the file to be malicious. The users are returned a notification saying "File might be a Potential Threat".

ix. If all scanners flag the file as "Safe", the file is forwarded to the cloud storage service and the users are returned the notification saying "Upload Successful".

x. Stop.

This system ensures greater probability in detection of malware and securing the cloud storage services. Since the system is a cloud service, it is more affordable and doesn't require onsite installation at datacenters.

To connect the security service to a cloud storage service, one just has to access our web platform that provides the control panel for our security service and connect it to their own cloud storage service. Our security service connects to the cloud storage service via software defined network, ensuring fastest possible communication between the two services [13]. In case of heavy data traffic, our systems are able to scale out to meet the heavy traffic demand. This ensures that multiple end users can upload their files simultaneously and the storage providers can still rest assured that their infrastructure is secure.

A report of all the malwares detected and files uploaded is shared with the storage providers fortnightly. In case a storage provider finds that a file detected as malware is actually harmless or a file deemed to be safe is actually a malware, the provider can raise a ticket on our platform for resolution of the issue. If the issue is found to be valid, our database is updated accordingly to improve our detection capabilities and filter out false positives.

The monitoring servers are setup with a cron job that audits the server regularly for any unnecessarily open ports or unrecognized connections that might have turned up due to the servers being affected themselves by malware or any other reason. Regular auditing by a cron job and the subsequent alert sent to the security team ensures the security of our platform, which in turn ensures the security of the infrastructure owned by storage providers.

Thus, we have removed the drawbacks of the current security services used for cloud storage services that have been explained in the previous section.

4. IMPLEMENTATION OF THE SOLUTION

4.1 Frontend

The frontend of our solution is a web application for registration of the vendors that would be using our solution for protection of their cloud storage service, and also for management of the service they have signed up for.

Once signed up, they can log into their dashboard and connect or disconnect our proxy servers from their storage buckets. The option is given via a button on the screen to connect their bucket to our server. The next page that opens up on pressing the button asks for the bucket URL. On pressing the Submit button, a set of credentials (a user ID and password) are generated that the vendor can use for the storage service clients like Digiboxx app, Google Drive app, Mega app etc for authentication with our server, in order to allow the server to accept the files from the cloud storage client. The URL of our protection server is displayed to the client as well. These details can be used by the vendor to enable authentication from their cloud storage client on our server for smooth functioning of operations.

4.2 Backend

With the smooth experience provided to the vendors, there also comes the complexity of all the processes running in the backend ensuring the experience.

a. Authentication:

We are using simple email and password authentication. The vendor enters the email and password, our web application checks whether the vendor exists and verifies the password from our vendor database, upon which the vendor is successfully authenticated and given access to their dashboard.

In case of an authentication request from a cloud storage client, the credentials are verified by our database service, namely MySQL, and the file being uploaded is accepted in the vendor's database.

b. Generation of Credentials:

When the vendor signs up for our protection service, a user ID and password is generated for their applications to use, so that the vendor's storage service client can authenticate themselves. In addition, a table is created in the web application database for handling of files to be scanned for malware.

c. Scanning for Malware:

When a file is uploaded by the cloud storage client, it goes to the vendor's table in the database. A program detects the addition of the new record and forwards the uploaded file for scanning to multiple antivirus and antimalware providers via their APIs and waits for response. On receiving the response, the response is recorded in the table.

From the responses received, the response that is in majority is generally taken to be the correct one.

Let's look at the algorithm a bit in detail.

i. Start
ii. Select a file to upload, the file can be uploaded via web, desktop or mobile clients.
iii. Click Upload to begin the uploading process.
iv. The file arrives at the intermediate server.
v. The file is scanned by several scanners provided by their respective providers.
vi. The percentage of scanners flagging the file as malicious/suspicious is calculated.
vii. If even one of the scanners flags the file as "Malicious", the file is deleted and an error saying "Malicious file detected" is returned and the same is noted in the table in the database.
viii. If more than 50% scanners flag the file as "Suspicious" or "Potentially Harmful", the file is deleted and an error saying "Malicious file detected" is returned.
ix. If the percentage of scanners flagging the file is "Suspicious" is lower than 50% and none of them flags it as "Malicious", it is put in quarantine in the server itself and the support team is intimated by an email to verify the file to be malicious. The users are returned a notification saying "File might be a Potential Threat".
x. If all scanners flag the file as "Safe", the file is forwarded to the cloud storage bucket and the users are returned the notification saying "Upload Successful".
xi. Stop.

d. Quarantine:

When a file needs to be quarantined, it is moved from its original location to a hidden location within the server, so that the team can take a look later and verify whether it is a malicious file or not.

5. COMPARATIVE STUDY

Features	**Existing Systems**	**Proposed System**
Architecture	Utilizes Intermediate Servers	Utilizes Intermediate Servers
Detection methodology	Signature verification or reverse connection activity of malware based on datasets provided by vendor's own threat intelligence platform	Several detection tools are used from various vendors, some utilizing signature verification and others their own various approaches

Handling malware	Deletion of the carrier files along with malware	Deletion of the carrier files along with malware
Approach	Definitive approach, it is determined for certain by a vendor whether a file is malicious	Probabilistic approach, a file is determined to be malicious based on results given by several antimalware solutions
Accessibility	The systems need to be installed by the cloud storage providers on their own, at times it is really costly	The cloud storage service can be connected to our intermediate security service anytime, since it is a cloud service itself

6. RESULTS

We compared the efficiency of our solution with the current antivirus providers with the latest definitions. The rate of detection of malware is as shown in Graph 1, where, “Server” refers to our intermediate server.

Since our solution employs multiple antivirus engines for scanning malware, few of which are part of the comparison, the rate of detection of our solution is same as that of the antivirus engine with the greatest rate of detection.

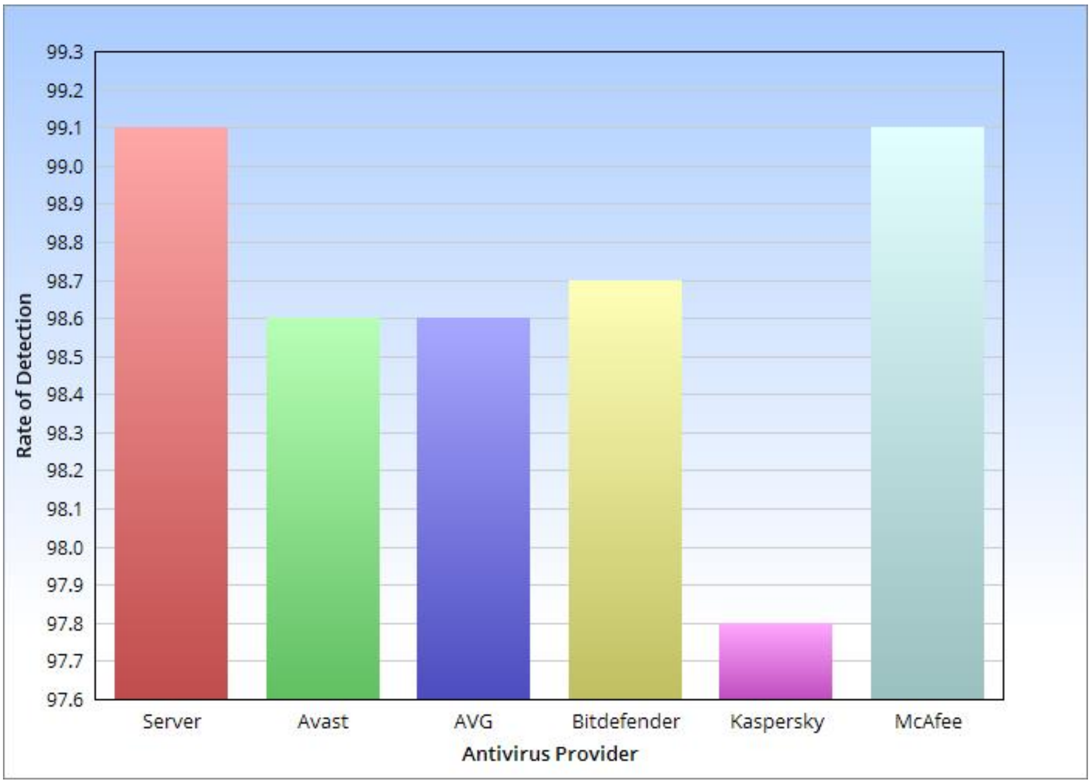

Chart 1: Rate of Detection of various Antivirus Providers

7. CONCLUSION

The system is more efficient and employs a probabilistic mechanism for detection of malware. This system is an integration of various scanners on an intermediate server that acts as an intermediate security service for the cloud storage service. This service is cheap, easily accessible and enables integration with the cloud storage services without heavy spending on hardware.

In further future work, we plan to expand this service to other kinds of cloud services and also employ advanced strategies for improvement in efficiency of this system

ACKNOWLEDGEMENTS

We are grateful to Asst. Prof. S. V. Athawale for his insight, feedback and support in this project. Also, we would like to thank several open access platforms for their resources without whom this project could never have taken form.

REFERENCES

[1] Rakesh Kumar and Rinkaj Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey", Computer Science Review, **(2019)**, pp. 3.
[2] Michael Lane, Anup Shrestha and Omar Ali, "Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation", Proceedings of the Bright Internet Global Summit, Seoul, South Korea, **(2017)** December 8-10.
[3] R. Barona and E. A. Mary Anita, "A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats", Proceedings of the International Conference on Circuits, Power and Computing Technologies (ICCPCT), Kollam, India, **(2017)** April 20-21.
[4] "Cost of a Data Breach Report 2020", IBM Security, New York, **(2020),** pp. 5.
[5] Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Ransomware.
[6] Kiran Radhakrishnan, Rajeev R. Menon and Hiran V. Nath, "A Survey of Zero-day Malware Attacks and its Detection Methodology", Proceedings of the IEEE Region 10 Conference (TENCON), Kochi Belgatti, Kerala, India, **(2019)** October 17-20.
[7] Simon Hunt and Sean Tiernan, "Ransomware Protection for Cloud File Storage", U.S. Patent 20180007069A, **(2018)** January 4.
[8] N. Moses Babu and G. Murali, "Malware Detection for Multi Cloud Servers using Intermediate Monitoring Server", Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017), Chennai, India, **(2017)** August 1-2.
[9] Saad Khan, Simon Parkinson and Andrew Crampton, "A Multi-layered Cloud Protection Framework", Companion Proceedings of the 10th International Conference on Utility and Cloud Computing", Queensgate, Huddersfield, UK, **(2017)** December 5-8.
[10] Dhawal Kumar Sharma, Manoj Apte and Patrick Foxhoven, "Content Delivery Network Protection from Malware and Data Leakage", U.S. Patent 10,237,286, **(2019)** March 19.
[11] Jithin Chandra Mohan and Renuka Kumar, "On the Efficacy of Android Ransomware Detection Techniques: A Survey", International Journal of Pure and Applied Mathematics, Volume 115, No. 8, **(2017)**, pp. 115-120
[12] Mohamed Hawedi, Chamseddine Talhi and Hanifa Boucheneb, "Security as a Service for Public Cloud Tenants(SaaS)", Proceedings of the 9th International Conference on Ambient Systems, Networks and Technologies, ANT-2018 and the 8th International Conference on Sustainable Energy Information Technology, Porto, Portugal, **(2018)** May 8-11.
[13] Jacob H. Cox Jr., Joaquin Chung, Sean Donovan, Jared Ivey, Russell J. Clark, George Riley and Henry L. Owen, "Advancing Software-Defined Networks: A Survey", IEEE Access, vol. 5, **(2017)**, pp. 1-40