The better Security System, Cloud Security or Antivirus

Cilla Mary Mathew
Guide: Prof. Bindy Wilson
Model College, Dombivli

***Abstract*—We are using the Internet system in every part of our day-to-day professional life. There is no task which can be done without involving the Internet or applications of the Internet. We must safeguard our computer systems from different malicious attacks that can happen at any given point of time. We can make use of different security systems to safeguard our files. Mainly these security systems are called as "Antivirus systems". We can also see that there is an inbuilt security system within Cloud Applications, mainly referred as "Cloud Security".**

A user which makes use of both the systems can get an idea of which system is having more features and which to use and why.

***Index Terms*— Cloud Security, Antivirus, Cloud System, Security, Internet Security**

I. INTRODUCTION

We are using the Internet system in every part of our day-to-day professional life. There is no task which can be done without involving the Internet or applications of the Internet. We must safeguard our computer systems from different malicious attacks that can happen at any given point of time. We can make use of different security systems to safeguard our files. Mainly these security systems are called as "Antivirus systems". We can also see that there is an inbuilt security system within Cloud Applications, mainly referred as "Cloud Security". A user which makes use of both the systems can get an idea of which system is having more features and which to use and why. A cloud user will know all features of the cloud security.

One can understand all the aspects that needs to be taken care for keeping the files and the data safe and secure. He/she can help the other fellow users to keep their data safe.

They can compare with the aspects of the Antivirus system and get the best possible combinations to keep their data safe.

Different types of cyber-attacks:

Malware refers to software programs designed to do damage to a computer, server, or computer network. Malware can decelerate or crash your device or delete files. Attackers make use of malware to send spam, obtain personal and financial information and even steal your identity.

Spyware is a sub-type of malware that attaches itself and hides on a computer's operating system without your permission to make unwanted changes to your user experience. They can be used as keyloggers to steal your information.

Phishing attackers use emails to try to cheat you into providing personal or financial information to compromise an account or steal money by posing as a trustworthy entity. Phishing can be explained as a user clicking on a URL that looks like a genuine site, but it is a fake site created by attackers.

II. OBJECTIVE

- To understand the Antivirus security system
- To understand the Cloud security system
- Compare both systems to find the best possible combinations.

III. ANTIVIRUS SECURITY MODEL

Software created specifically to help detect, prevent, and remove malicious software such as viruses.

Antivirus is software used to prevent, analyze, detect, and remove computer viruses. Once installed, most antivirus software automatically runs in the background to provide real-time protection against virus attacks.

A comprehensive virus protection program helps protect your files and hardware against malware such as worms, Trojans, and spyware, and provides

additional protection such as a customizable firewall and site blocking website.

Antivirus programs and computer protection software are designed to assess data such as web pages, files, software, and applications to detect and eliminate malware as quickly as possible.

Most offer real-time protection that shields your device from incoming threats; regularly scans your entire computer for known threats and provides automatic updates; and identifies, blocks, and removes malware and malware.

With so much activity online these days and new threats constantly appearing, it's more important than ever to have a protective antivirus program installed. Fortunately, there are many great products to choose from on the market today.

Working of Antivirus:

Antivirus software begins by checking your computer programs and files against a database of known malware types. Since hackers constantly create and distribute new viruses, it also scans your computer for new or unknown types of malware threats.

Typically, most programs use three different detection features: specific detections, which identify known malware; generic detections, which look for known parts or types of malware or patterns associated with common code bases; heuristic detections, to search for unknown viruses by identifying suspicious file structures. When a program finds a file that contains a virus, it usually quarantines it and/or marks it for deletion, making it inaccessible and eliminating risk to your device.

IV. CLOUD SECURITY MODEL

Cloud computing is one of the most demanding technologies today and organizations from small to large enterprises are starting to use cloud computing services. While there are different types of cloud deployments, templates can be used and cloud services provided as needed, such as maintaining internal and external security to ensure cloud system security. Cloud computing security or cloud security is an important issue and refers to the act of protecting cloud environments, data, information, and applications from unauthorized access, DDOS attacks, malware, hackers and other similar attacks. Cloud Computing Security Planning:

Because security is a major concern for cloud implementations, organizations should base their security planning on certain factors. The following represent the three main factors that cloud security planning is based on.

- Select resources that can go to the cloud to test sensitive risks.
- Cloud type must be considered.
- The risks of deploying a cloud depend on the type of cloud and the service model.

There are 4 types of cloud computing security controls namely:

Deterrent controls: Deterrent controls are designed to stop malicious attacks on cloud systems. This is convenient when there are initiates.

Preventive controls: Preventive controls make a system resistant to attacks by eliminating system vulnerabilities.

Detective Controls: Identify and respond to security threats and controls. Some examples of spyware are intrusion detection software and network security monitoring tools.

Corrective controls: These controls will be activated in the event of a security breach. They limit the damage an attack can cause.

The Importance of Cloud Security:

For organizations moving to the cloud, cloud security is an important consideration when selecting a cloud provider. Attacks are getting more and more powerful, so security measures must keep up. For this, it is imperative to choose a cloud provider that offers the best security and adapts to the infrastructure of the organization. Cloud security has many benefits –

Centralized Security: Centralized security leads to centralized protection. Since managing all devices and endpoints is not easy, cloud security can help.

This results in improved traffic analysis and web filtering, which means fewer policy and software updates.

Reduced Costs: Investing in cloud computing and cloud security reduces hardware expenses and reduces administrative labor.

Reduced Administration: It makes running an organization easier and there is no manual security configuration or ongoing security updates.

Reliability: It is highly reliable, and the cloud can be accessed from anywhere using any device with proper authorization.

When we think of cloud security, it includes different types of security such as access control to authorize access, network segmentation to keep data separate, encryption to encode data transmission, security controls vulnerability to patch vulnerable areas, security monitoring to focus on various security attacks, and disaster recovery for backup and data loss recovery.

Different types of security technologies are implemented to make cloud computing systems more secure, such as Secure Sockets Layer (SSL) encryption, multitenancy-based access control, security detection systems, intrusion, firewalls, penetration testing, tokenization, VPN (virtual) private network), and avoid using public Internet connections and more technology.

But things are not as simple as we imagined, no matter how much security technology is implemented, it will always involve the security of cloud systems. Since cloud systems are managed and accessed over the Internet, there are many challenges in maintaining a secure cloud.

Some cloud security challenges are:

- cloud data control
- misconfiguration
- changing workloads
- access management
- disaster recovery

Google Cloud Security Monitoring:

Google's security monitoring program is focused on data gathered from network traffic and understanding of vulnerabilities. One of Google's core principles is to collect and store all security telemetry data in one place for unified security analysis. At many points in our global network, checks internal traffic for suspicious behavior, such as traffic that might indicate a botnet connection. We use a combination of open source and commercial tools to capture and analyze traffic to perform this analysis. A proprietary correlation system built on top of Google's technology also supports this analysis. Google helps web analytics by examining system logs to identify unusual behavior, such as attempts to access customer data. Security engineers review incoming security reports and monitor public mailing lists, blog posts, and wikis. Automatic network scanning and automatic system log analysis help determine when unknown threats may occur. When an automated process detects a problem, it escalates it to security staff.

AWS Security Monitoring:

Organizations embrace the scalability and flexibility of the cloud, and AWS helps these organizations to evolve security, identity, and compliance. AWS embeds security at the heart of our cloud infrastructure, providing core services to help organizations meet their unique security requirements in the cloud. As an AWS customer, you will benefit from a data center and network architecture designed to meet the requirements of the most security-sensitive organizations. Cloud security is very similar to security in an on-premises data center but without the cost of maintaining facilities and hardware. In the cloud, you don't need to manage physical servers or storage devices. We may use software security tools to monitor and secure the flow of information to and from your cloud resources. One of the benefits of the AWS Cloud is that it allows you to scale and innovate while maintaining a secure environment and paying only for the services you use. This means we can get the security you need for less than in an on-premises environment. As an AWS customer, we can inherit all the best practices of AWS policies, architecture, and operating procedures designed to meet the requirements of our most security-sensitive customers. Get the flexibility and agility you need for security checks. This means you retain control over the security you choose to implement to protect your own content, platforms, applications, systems, and networks, just as you would in your on-premises data center. AWS provides guidance and expertise through online resources, employees, and partners. AWS advises you on current issues and you also have the option of working with AWS when you encounter security issues. Hundreds of tools and features are available to help you achieve your security goals. AWS provides security-specific tools and features in the areas of network security, configuration management, access control, and data encryption. Finally, the AWS environment is continually audited and certified by certification bodies in different regions and verticals. In an AWS environment, you can take advantage of automated tools for asset inventory and privileged access reporting.

Benefits of AWS Security:

- Protecting your data – The AWS infrastructure implements strong security measures to help protect your privacy.
- Meeting Compliance Requirements - This means your compliance part is complete.
- Save Money: — Reduce costs by using AWS data centers. Maintain security standards without having to manage your own installations.
- Scale quickly - Security scales with your use of the AWS cloud. Regardless of the size of your business, the AWS infrastructure is designed to keep your data secure.

V. RESEARCH METHODOLOGIES

A model can include both descriptive and analytical components. A descriptive model's logical relationships can be examined, and conclusions can be drawn. The logical analysis draws quite different conclusions than the quantitative investigations of the properties. We conducted an online poll utilizing an online form creator and data collection service to acquire information regarding people's awareness.

VI. PUBLIC SURVEY

We deployed our data gathering facility, to a variety of people of all age ranges to collect information on various faces of their understanding of which security monitoring model will help to make their life better.

VI.I QUESTIONNAIRE

- What is your age range?
- Are you aware of Cloud Security?
- Do you think Cloud security will be more helpful?
- What do you think which is better? Cloud Security or any Antivirus
- Do you believe that cloud security would be more secure than manual process?

VI.II RESPONSES

The major age group who responded id from 18-40 years (71%) followed by 40-65 years (16%) and people less than 18 years (7%)

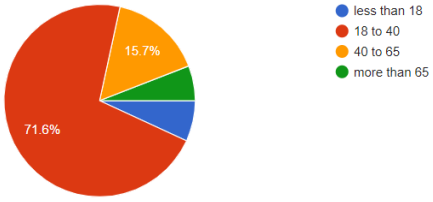

Chart 1: Age group

The respondents who knew about Cloud Security were 71% of the total and 15% were somewhat aware of Cloud Security and the rest were not aware of Cloud Security.

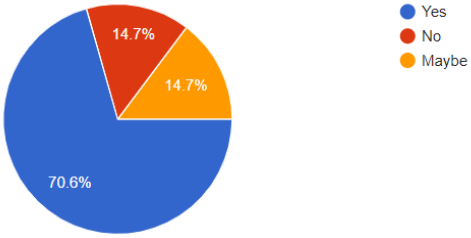

Chart 2: Cloud Security awareness

73% of the respondents thought that Cloud Security was more secure than Antivirus and the rest favored Antivirus being more secure.

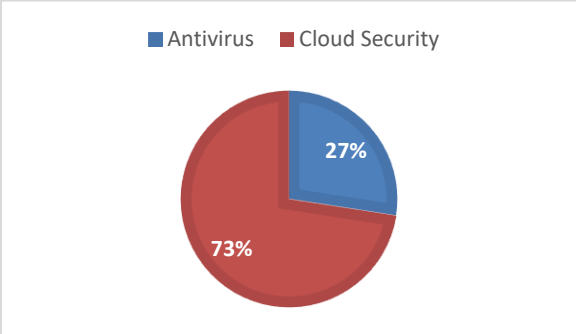

Chart 3: More secure

64% of the respondents believed that Cloud security would be more helpful whereas 32% were unsure about it.

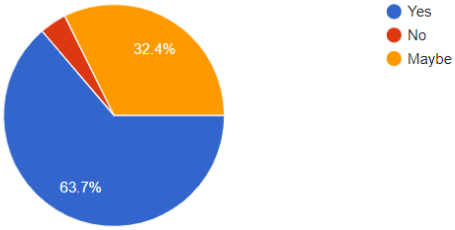

Chart 4: Cloud security being more helpful.

67% of the respondents thought that Cloud Security would be more secure and 27% thought that Antivirus would be more secure.

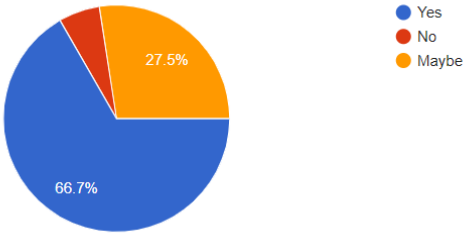

Chart 5: more secure

VII. HYPOTHESIS TESTING

Hypothesis testing is a systematic process of determining whether research findings support a particular theory that applies to humans. The hypothesis test uses sample data to test a population-based opinion.

The hypothesis testing examines how rare the outcome is, whether the variance is reasonable or whether the outcome is too extreme to be considered a variance of luck.

There are two types of hypotheses:

a) Null Hypothesis (denoted H0)

b) Alternate or Research Hypothesis (denoted Ha)

For this paper,

H0: Cloud security can improve security.

Ha: Cloud security cannot improve security.

VIII. TEST(STATICS)

There are three tests available to determine if the null hypothesis is to be accepted or not. They are:

1) Chi-squared Test

2) T-Student test (T-test)

3) Fisher's Z Test

In this paper, I'll be using the Two-Tailed T-student test.

A t-test is an inferential statistic that determines if there is a significant difference in the means of two groups that are related in some manner.

➔ Level of Significance

The chance of rejecting the null hypothesis when it is true is the significance level (also known as alpha or α). A significance level of 0.05, for example, means there's a 5% probability of discovering a difference when there is none. Lower significance levels indicate that more evidence is required to reject the null hypothesis.

➔ Level of Confidence

The Confidence level indicates the probability that the location of a statistical parameter such as the arithmetic means measured in the sample survey is also true for the entire population.

Sr. No	Data
1	71.6
2	70.6
3	72.5
4	63.7
5	66.7
Mean (x)	69.02
Standard Deviation (s)	3.706

Level of Significance =0.05 i.e. 5%

Level of Confidence= 95%

A t-score (t-value) is the number of standard deviations away from the mean distributions.

The formula to find the t-score is:

$t=(x-\mu) / (s/\sqrt{n})$

where x is the sample mean,

μ is the hypothesized mean,

s is the sample standard deviation,

and n is the sample size.

The Probability value, also known as the p-value, indicates how probable your data is under the null hypothesis. Once we have the value of 't', we can calculate the p-value. If the p-value is less than the alpha level, then we can reject the null hypothesis and conclude that Cloud Security cannot improve security.

➔ Calculating 't' value:

Step 1: Determine the Null and Alternate hypothesis.

Null Hypothesis (H0): Cloud security can improve security.

Alternate Hypothesis (Ha): Cloud security cannot improve security.

Step 2: Find the test statistic:

In this case, the hypothesized mean is considered 0.

Therefore,

$t=(x-\mu) / (s/\sqrt{n}) = (69.02-0)/(3.706/\sqrt{5})$

$=41.644$

t-value=41.644

➔ Calculating p-value:

Step 3: Calculate the test statistic's p-value.
The t-distribution table with n-1 degrees of freedom is used to calculate the p-value. In this paper, the sample size is n=5, so n-1=4.
By feeding the observed value into the calculator, we got the p-value which is 0.00000198. The p-value is less than 0.00001.
Since this p-value is less than our selected alpha level of 0.005, we can reject the null hypothesis. Therefore, we can conclude that we have enough evidence to say that Cloud security cannot improve security.

IX. CONCLUSION

Cloud Security alone might not improve the security but it can help us detect and prevent all possible threats and which would help us in making our organizational or personal systems more secure.

REFERENCE

[1] https://www.verizon.com/articles/internet-essentials/antivirus-definition/#:~:text=Antivirus%20is%20a%20kind%20of,time%20protection%20against%20virus%20attacks.
[2] https://www.verizon.com/articles/internet-essentials/antivirus-definition/#:~:text=Antivirus%20is%20a%20kind%20of,time%20protection%20against%20virus%20attacks.
[3] www.wikipedia.com
[4] Security and compliance - Overview of Amazon Web Services
[5] Google security overview | Documentation | Google Cloud
[6] Cloud Computing Security - GeeksforGeeks