JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Are cloud applications secure and protects our privacy?

Surya Nair

Guide: Asst. Prof Gauri Ansurkar

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

suryanair.model@gmail.com

***Abstract*— Cloud computing is a type of computing which is Internet based and the users can obtain the resources within the enterprise of user either on a third party server or in private own cloud. The characteristics of cloud computing includes self service, scalability, pay per use model. Cloud Computing provides us with many benefits of technology which includes cost efficiency, enhanced scalability and computing elasticity. Cloud Computing reduces our need to maintain hardware, software and the space required for the IT infrastructure. Many industries such as education, healthcare, banking, business are adopting cloud technique due to the efficiency of services which helps us in accessing storage, server, network, application without acquiring them physically. However the cloud computing services provided by the cloud providers can poses various security threats. Cloud applications stores sensitive data which includes personal information, credential etc of various users. In this research a survey is conducted in order to understand the awareness of security and privacy in cloud among 101 users. This study aimed to examine the awareness of users about cloud based applications and to understand if users consider security as important concern while using cloud based applications.**

***Keywords*— cloud computing, characteristics, security threats, security and privacy in cloud, security issues**

I. INTRODUCTON

Cloud Computing and storing data on cloud has become very popular in the past few years where the users prefer to store their data such as personal documents, images, music files, etc on the cloud servers. Cloud computing reduces the cost of storing and sharing of data. Organisations can use cloud in order to port their data so that The stakeholders can use data. Google Apps is considered as an example of cloud computing. Due to the advancement in technology, the Internet usage has increased in a wide range and the hardware and software cost has also rose. In order to compensate with the cost of hardware and software by providing services when the user demands, the concept of cloud computing has been successful and again popularity in a very little span of time. Cloud is build on the grid based architecture using the grid services and other technologies which include virtualization. Cloud services are generally defined as XaaS, where X can be software or platform or infrastructure. The backbone of cloud computing is virtualization. Virtualization is used for efficient and effective management of resources which includes processor, network devices, hard disks, memory, etc. The process of cloud storage includes four layers. The storage layer stores the data on cloud data centre, management layer ensures the privacy and security of cloud storage, application interface layer provides cloud application service platform and the cloud access layer provides access ability to the cloud user. Security layer implementation is an essential component in the management layer. It is important to understand the challenges in cloud security to address the issues. It is necessary to inspect vulnerabilities, risks and threats associated with cloud computing. It is important to clearly identify security requirements and understand how various cloud deployment models which includes public, private, hybrid and community cloud are affected by the security challenges and threats. This research paper provides an overview of the awareness of users on cloud based attacks and counter measures used by cloud service providers.

II. MODELS OF CLOUD

- Software as a Service

This service is also known as cloud application services. It utilises the internet in order to deliver the applications that are managed by the third party and whose interface is accessed on the side of customers. the applications are accessible in various platforms like desktop, mobile, mainframe and servers using a web browser. In this service, the user do not have the capability to control the underlying impressed after of cloud which includes operating system, network devices, storage, applications. users also cannot modify the hosting environment where the applications are hosted. The users that instructed to manage and modify only the application specific settings in order to customise their own profiles. Examples- Citrix, Google Apps, Go- To Meeting, Cisco, Webex, Sales force workday, concur.

- Infrastructure as a Service

This service allows users to dynamically request for data storage, computing, computing resources and networking. It also provides the users to run operating system using virtualization technology. the users have the capability to control and monitor the usage of diploid applications,

networking capabilities, computational requirements, etc. Examples- Joynet, Amazon Web Services (AWS), Computer Compute Engine (GCE), Cisco Meta-pod Microsoft Azure.

- Platform as a Service

This service allows the users to deploy the application tools that are provided by the cloud providers. Unlike Infrastructure as a Service, in Platform as a Service users do not have the freedom to manage underlying cloud infrastructure. In this service, the deployed applications and the hosting environment provided to the application can be controlled by the users. Example- Apprenda

III. TYPES OF CLOUD

- **Private Cloud**

Private cloud infrastructure is provided and operated by private organisation. The cloud infrastructure management can be done by the organisation or a third party. The infrastructure of cloud can be hosted off premise or on premise.

- **Community Cloud**

This type of cloud infrastructure is shared among several users. It is used to support a specific community that has concerns like security requirements, missions. The community cloud is managed by third party or an organisation. It can exist off premises or on premises. This is a platform that allows many users or organisations to work on the same platform provided that they should have similar requirements and concerns. Example of community cloud include Google Apps for government, Microsoft government community cloud.

- **Public Cloud**

The public cloud is owned and managed by an organisation that is selling or providing the cloud services to users. It is readily available to public. Examples of public cloud include Sun Cloud, Amazon Elastic Compute Cloud(ES2), Windows Azure, Google's App Engine, IBM's Blue Cloud. Another simple example of public cloud is electronic mail.

- **Hybrid Cloud**

Hybrid cloud infrastructure uses mix of Cloud computing platform like public, private and community clouds. Whereas these different platform of cloud are binded using the standards and technologies. To make application compatible and portable on these mix platforms, a business application designed for the hybrid cloud by an organisation to connect to mixed environment like private community or public cloud as they were a single environment and it provides transparent services to its users by hiding the underlying details. This cloud is not called as a hybrid cloud if a few programmers of an organisation uses the public cloud for testing of the application prototype which is completely disconnected from data centre or private cloud. Hybrid cloud means an organisation exchanges the data between application environment or private cloud.

IV. FEATURES OF CLOUD COMPUTING

- **Flexibility**

Cloud computing allows users to dynamically request computer resources which include memory, storage, process is as needed without human intervention. Automatically resources are rapidly allocated and assign to the users based on the requirements of scaling up or down.

- **Infrastructure scalability**

Based on the requirements of the organisations or applications, new servers are computing resources in the form of new notes can be easily added or removed from the network without any disruption and human intervention in exiting services. According to the demand the cloud architecture allows scaling Vertically or horizontally.

- **Broad network access**

Cloud computing resources and services are available to the users or organisation to access over network using heterogeneous platforms like laptops, mobile phones.

- **Location independence**

Cloud computing stores data of different locations around the world. users do not get the freedom to choose the exact location of the resources it just provided like data centre, country, state.

- **Reliability**

Using application of data on multiple servers which are located at same or different site provide reliability to users. This feature makes cloud computing popular among the users and helps in disaster recovery. It ensures to make secure logical compartments with the security cheques to ensure the isolation of users data present on the same server or multiple servers located at same or different sites. The threat increases in cloud due to Large number of users accessing same resource on cloud. Therefore it is necessary to create secure compartment which provides isolation of data, ensuring an auditing security strengths in timely manner is important in cloud computing. it is also important to establish the policy in order to perform regular security cheques to validate that the users data is confidential. to ensure the confidentiality, various encryption techniques are proposed by the researchers which are adopted in cloud.

- **Sustainability**

It is provided in order to improve resource utilisation and build more efficient systems.

V. GENERAL REQUIREMENTS ON CLOUD SECURITY

- **Confidentiality**

Confidentiality refers to authorised users and the application they can access. It is shows that unauthorised users or applications will not be available to store or access data on cloud. In cloud computing, the data is stored on remote servers that are owned by the cloud service providers an which are shared to multiple users. There are two types of algorithms namely symmetric and are symmetric algorithms. the key management and key length in symmetric cipher are important

characteristics of an encryption algorithm. This is dependant on the algorithms adopted by the cloud service provider. The cloud service provider should also ensure deployment of encryption standards using NIST standards.

- **Integrity**

It is a critical security property in cloud. integrity means that data that is stored on cloud can be modified only by the authorised parties or only in authorised ways allowed by an application. it is associated with application, hardware and data. data integrity refers to protecting the data off users from modification by unauthorised people. The integrity protection techniques and methods provides the information about who may have altered the data and what is the data that is altered.

- **Availability**

It means that the system should be accessible to authorised users upon their demand. In other words, it means that the user should have access to complete setup cloud resources allow catered to them at all times. Availability can be temporarily or permanently affected. A loss occur due to the unavailability of the resources could be partial or complete. The threats to this include equipment outages, denial of service attack. Natural disasters can also be a threat to availability. Cloud computing also needs sensors part machine learning based techniques to ensure that the users have availability to resources. The concerns of availability extends to the need to change another provider, up time the period present provider.

- **Trust**

This is important factor in cloud computing. It depends on self assessment and the reputation of cloud service provider. various tools, models, techniques have been proposed in order to establish trust. However there are only few research efforts to analyse the relation of trust among cloud users and cloud service providers.

- **Audit and compliance**

Auditing is the mechanism to examine all records and attempts of the cloud resources authentication and authorization to check compliance with security policies and standards. Cloud service provider need to have policies in order to inspect and ensure the user needs and security of cloud infrastructure. A cloud service provider needs to perform external audit and security certification.

VI. SECURITY ISSUES IN CLOUD PLATFORMS

There are many security issues in cloud applications as it consists of systems, virtualization, working framework, asset planning etc. Some threads in cloud are listed below.

1. Data breaches

Due to the technology improvement, cloud servers contain huge information that acts like the target to hackers. More the data exposed greater is the damage to users. Breaches involve trading secret, health information, etc that can cause destruction.. Do cloud providers provide security controls to protect the environment enterprises are responsible for securing the data. Multi factor authentication, encoding of data is used so that only the authorised users can access the information.

2. Sand broken authentication and compromised credentials

Information breaches and other attacks frequently result from slack authentications, powerless passwords, destitute key or certificate management. In some cases, not as it were organizations indeed we forget to remove our access after our work is done. Example is the Gmail account in case we login within the public places of accessing(web cafes) and bymistakely forget to logout after our utilize, it can cause exposure of our own private information to others. It is our responsibility to keep in mind everything and beware . To maintain a strategic distance from these issues, Multi-factor authentications such as one-time passwords, phone-based authentications, security questions would make the hacker harder to login from stolen passwords. The use of cryptographic keys frequently will keep the records secure and also make the data difficult for the hackers who utilize keys without authorization.

3. Hacked Interfaces and API

Nowadays every cloud service providers gives APIs. It is used to manage monitoring, orchestration, management, cloud services. The APIs and interfaces which are weak Can explosive security components like confidentiality, integrity, availability. CSA Has recommended two focus on threat modelling applications which include architecture or design which are the primary concept for future developments and also to understand the flaws in the security coding reviews.

4. Exploited System Vulnerabilities

The problem of bugs have been faced by users since a long time. as the usage of technology has increased these vulnerabilities can cause big issues. The databases, sharing off memory and other data in the organisations can lead to data crash. To get rid of these bugs the system must be scanned regularly and need to find the solutions from reported bugs.

5. Account hijacking

One of the most common issues at present is account hijacking. There may be various attacks that can result when sharing data to third party vendors during transaction occuring online, sharing credentials to others etc. The hackers who hijack over data can manipulate it, change the transaction details or they can even use other cloud applications connected to the account to cause further more attacks. the only thing user can do is to be cautious well sharing credentials and always follow up whenever things go wrong and report them.

6. Malicious Insiders

These threats generally occurs to the people who work in organizations such as employees, business associates and they have the valuable information regarding the organizations which are to be maintained securely and privately. By limiting the accessing time in the computer systems during working

hours and by encrypting the routine job such as any malicious we can avoid these insider threats to certain extent . Any sensitive information regarding the users if by mistakely is provided in the servers can affect their reputation and business for many years. Thus, proper training needed to be given to the people manage those sectors.

7. The APT parasite:

The APT is considered as a continuous hacking process, made by a person or group of persons targeting a specific organization . It is well known for attacking the private organizations for business motives. This process uses a malware to cause vulnerabilities like virus, bugs, installations in the system. Consider an example, The Stuxnet computer worm, which was used to attack the Computer hardware of Iran's nuclear program . The Iranian government considered this as an APT because it had used a malware program code which spreads itself to all the other computers using a computer Network causing security failures. In the recent years, the threats consisted of direct attacks, USB drives preloaded with malware coding etc.

8. Inadequate diligence:

Organizations that adopt the cloud without fully understanding its nature and its related dangers may experience business, money related, specialized, legitimate, chances. Due to the constancy applied, the organization is attempting to relocate to cloud or combining with another organization in the cloud. For instance, organizations that neglect to investigate an agreement may not know about the service providers obligation if there could be an occurrence of information rupture. Operational and building issues emerge if an organization's improvement group cloud advancements as applications are later sent to a particular cloud.

9. Cloud service abuses:

Cloud abuse is considered as one of the top most threats. The main concept of cloud service abuse is that the hacker use the social media services to understand and extract various codes. This can disturb the cloud environment. Once if this occurs, the organizations may face the issues like shut down of computers, erasure of the important data. To avoid this issue, we must keep a track on identifying the assets, analyzing the critical information, analyzing the threats and vulnerabilities, risks when accessing and finally fix the issue with the defense layers that keep application safe.

10. DOS attacks:

These attacks can affect the performance of the system. The system may run out of time and may also becomes slower than the usual. The DOS attacks may consume more power due to which the billing expenses also increases. The solution for this is to anticipate the threats before occuring and only provide access to the necessary resources.

11. Shared Technology and Shared Dangers:

Cloud service provides share infrastructure, applications, platforms. If a bug arises in any of the these layers, it can affect the secured data which can directly affects the users. A defense-in-depth technique is suggested by CSA which includes the multi-factor authentication on all of the hosts, network based systems.

VII. RESEARCH CHALLENGES IN CLOUD COMPUTING

Although cloud computing has rapidly come into the existence, the researches regarding cloud computing are still in an early stage. Many issues have not yet been resolved and new challenges are emerging in industry day-by-day. The following are few research challenges occuring in cloud computing.

1. Service level agreement (SLA):

If needed then several instances of one application are replicated on multiple servers on basis of priority. Most of the vendors create SLAs which acts as a protective shield against the legal issues, which offers minimum assurance to cloud users. Few important issues like data protection, outages and price structures are important to be considered before signing the contract with the organizations. Some of the questions regarding SLAs are as follows: Does these services provide 99.9 percent security? Will there be problems like leakage of our private data during the servers downtime and breakdowns? Are they going to store our data? if yes, then where do they store and how long? Can we get an assurance that our data are safe with them without any misuse? Is there any SLA that is associated with backup, preservation of our data? There are a lot of scope and research to do on SLA and is surely an important area of research in cloud computing.

2. Cloud data management and security:

Cloud data security concept is an important research topic in cloud computing. Cloud data can be a large data, unstructured or semi structured with rare cloud updates. The cloud infrastructure provider, in this context, need to achieve the objectives like confidentiality, transfer and auditability. Confidentiality is for securely accessing data while transfer and auditability are for checking whether the applications has been altered or not. Cryptographic protocols are used in order to achieve the confidentiality, whereas auditability can be achieved through remote attestation techniques. The file systems like GSF and HDSF are different from traditional distributed file systems especially in their storage structure, accessing patterns and application programming interface. Due to this, there may be compatibility issues occuring with long-lasting files, systems and applications.

3. Data Encryption:

It is a key technology in data security. Security can range from small, medium or high (whether in cost, issue). We can consider APIs as an example . When an object arrives at the cloud the data gets decrypted and stored. The questions include

are there any options to encrypt the data before storing it? Is there any possibility to study cloud computing and take the required measures for making it secure? These type of questions are still not yet understood and a clear knowledge is not available in cloud computing which are needed to be resolved.

4. Virtual machine migrations:

To balance the load across the datacenter virtual machine migration can be enabled in cloud computing. It is evolved from the techniques of process migration. Xen and VMWare have implemented live migration of VMs that includes extremely short down times ranging from milliseconds to a second. The major benefits are avoiding hotspots but this has not been implemented . Detection of work load hot spots, initiating migration and the time taken to respond to a sudden workload changes has been implemented.

5. Access Controls:

The identity and authentication process are very important in managing the security in cloud. The control of these access managers would help us to build the security of the users but also cause some research challenges like how to improve the security? How strong is the password strength and what is the change frequency that provider assure us? What are the recovery methodologies that should be implemented if the password and username become corrupted? How are logs and messages secured without even displaying? How are the changed passwords delivered to the users again? All these are not new things. But we still need to do a lot of improvements and gain knowledge so that we can implement new security measures which brings more clarity to the future scope.

6. Multi-tenancy:

The unique nature of Multi-Tenancy in Cloud Computing is that both the hacker and the user share the same server . Such a setup cannot be mitigated by the traditional security techniques because it is not designed to penetrate through the servers and the monitoring techniques are limited to the network layer. From the past researches it has been found that there is no way to eliminate the Multi-Tenancy effect as it provides us with key benefits. But the effect could be minimized by using a smart resource allocation technique. What is interesting regarding Multi-Tenancy is that in order to achieve the targeted users, the hacker needs to invest a lot of cost, effort, time. So by making Multi-Tenancy difficult to achieved by users, thereby restricting the number of potential attackers. The proposed technique to challenge this is threat model and attack model which bring in the advancements and increase the efficiency of multi-tenancy.

7. Reliability and availability of services:

The concept of reliability comes into the picture when the cloud provider delivers on-demand services to users. The users mainly depend upon the network services when it comes to reliability and availability. One good example for this is Apple's Mobile Me cloud service that stores and synchronizes data across multiple devices. It was initially not up-to the mark output as many users were not able to synchronize the data correctly. Considering the implementation of software like 3D gaming applications and video conferencing systems, reliability has progressed up to a certain extent in the past five years but still acts as a challenge to achieve for an IT solution that is based on cloud computing.

VIII. PURPOSE OF STUDY

1. To identify whether users are aware of the security in cloud based technologies.
2. To know if they are familiar with any of the security breaches occuring in cloud based platforms, security measures used by cloud providers in order to prevent threats or attacks.
3. To identify if the users feel security as the biggest concern when accessing cloud based application.

IX. RESEARCH METHODS

The research method which was used is questionnaires as it is the best way to obtain information from a large number of people. The goal of the current research is to explore if security is affected in cloud computing and the user awareness of security breaches occuring in cloud based platforms from 15-65 age group. The survey of people were carried out and data were collected. The collected data was then analysed for the research purpose.

X. PUBLIC SURVEY AND EXPERIMENTS

A. Public Survey

After creating the questionnaires, it was sent to various people from age group between 15-65 and data was collected on various aspects of security in cloud computing among people.

B. Questionnaires

• Do you access or use cloud based applications? (Eg: Facebook, Gmail, Netflix, Instagram, Google Drive)

• Would you prefer to host your sensitive data on cloud platform?

• When you delete your file from cloud account what do you think will happen?

• Have you seen service level agreement of cloud service providers?

• Does your cloud service provider has the right to disable your account?

• Are you aware of any security threats in cloud computing?

• Do you feel attacks and security incidents should be reported by cloud service provider to it's users?

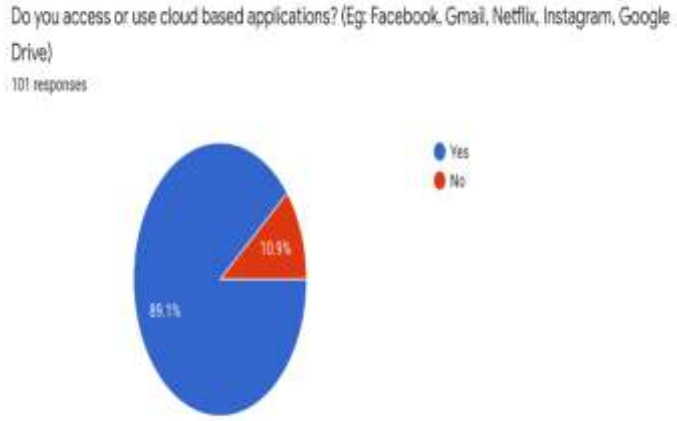
• Are you familiar with countermeasures applied by various cloud service providers to protect against attack?

• What are your main concerns in your approach to cloud computing?

• Which from the following cloud service providers option would you take into consideration?

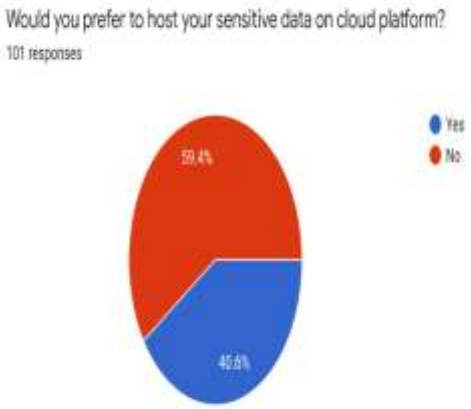
C. *Results*

101 people participated in the online survey. The age groups were divided into three categories like 15-30, 31-50, 51-65. The people were classified into three sectors like studying, working and others. From 15-30 age group, there were 72.3% responses, from 31-50 there were 13.9% responses and from 51-65 there were 13.9% responses. Out of 101 people, 42.6% people are students, 42.6% people are employees and 14.9 belong to other sector.

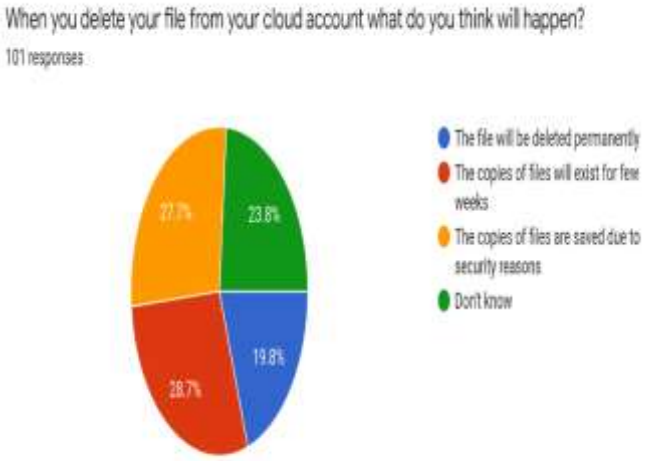


When the question was asked as do you access cloud based applications, 89.1% of people responded that they use and 10.9% people responded that they don't have access to cloud applications.

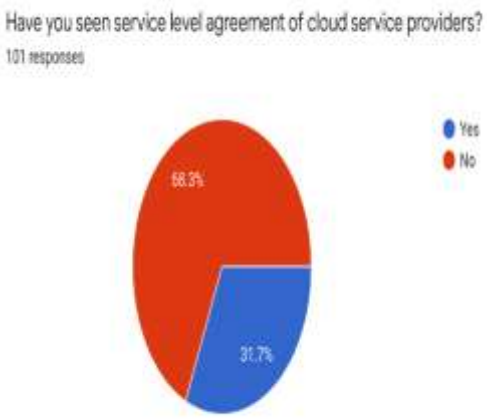
When the question was asked as would they prefer to host their sensitive data on cloud platform, 59.4% of users responded that they do not prefer sharing their sensitive data while 40.6% of users prefer sharing their data on cloud platform.

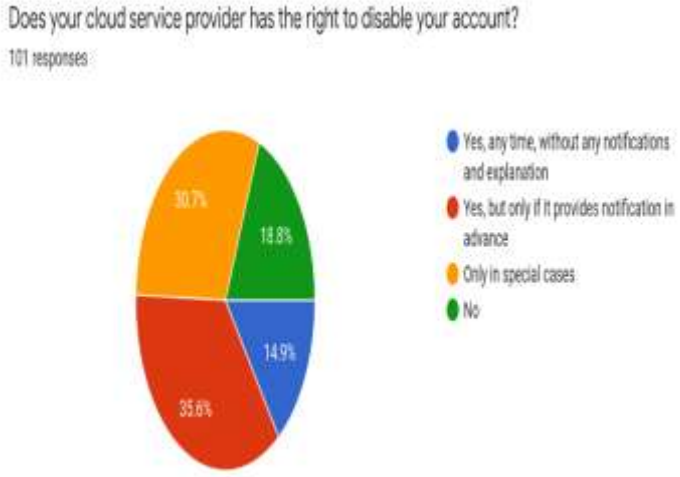


When the question was asked as when you delete your file from cloud account what do you think will happen, 28.7% of users responded that they think the copies of files will exist for few weeks, 27.7% of people responded that they feel that the copies of files are saved due to security reasons, 19.8% of people responded that the files will be deleted permanently. 23.8% of people don't know what will happen if they delete file from their cloud account.

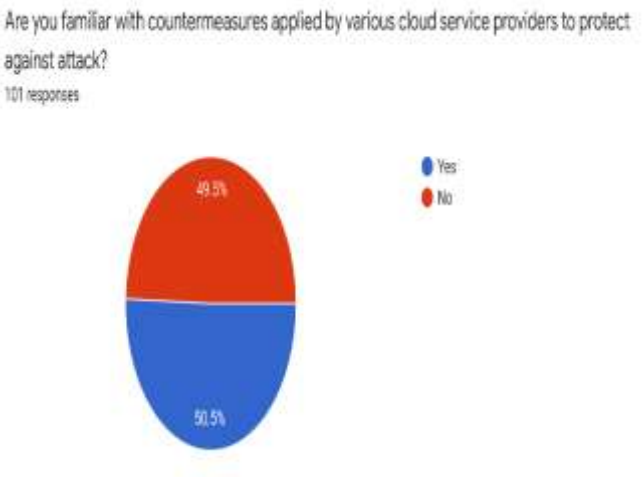


When question was asked as if they have seen the service level agreement of cloud service providers, 68.3 % of people responded that they have not seen the agreement while 31.7% of people responded that they have seen and aware of service level agreement.



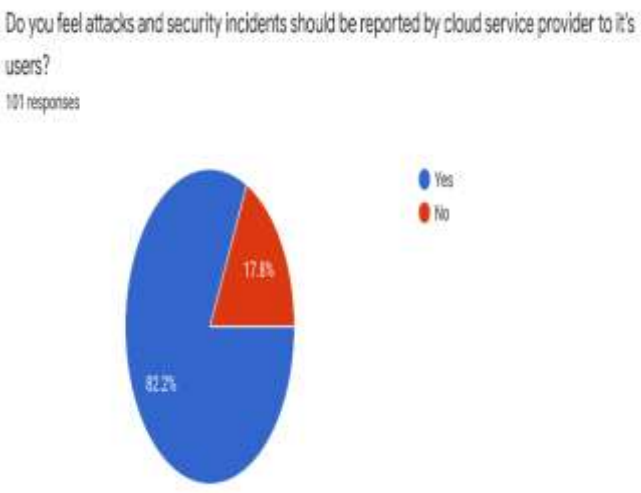


When the question was asked if their cloud services provider has the right to disable your account, 35.6% of people responded that they can disable but need to provide notifications in advance, 30.7% of people responded that only in special cases they can disable the account, 18.8% of people feel that the cloud service providers don't have the right to disable their account, 14.9% of people feel that the cloud services provider can disable the users account without any notifications in advance.

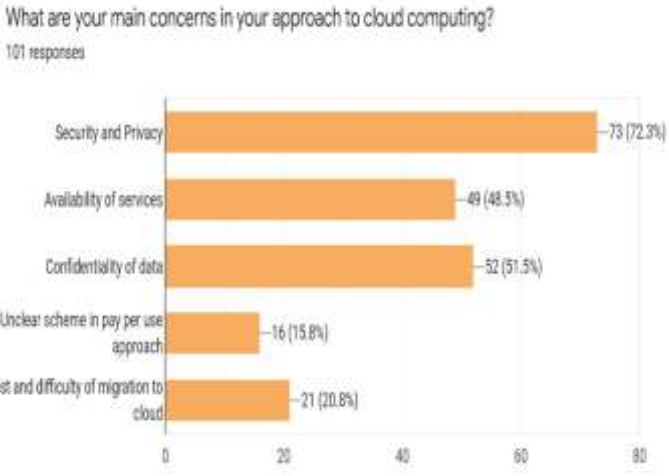


When the question was asked if they are familiar with any countermeasures used by cloud service providers to protect against attacks, 50.5% of people are aware of the countermeasures applied by cloud service providers while 49.5% of people are not aware of any countermeasures used by cloud service providers.

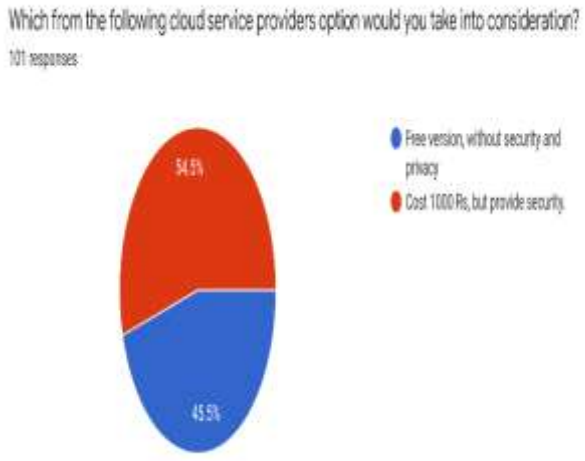
When the question was asked if the users are aware of any security threats occuring in cloud platforms, 60.4% of people responded that they are not aware of any threats while 39.6% of people responded that they are aware of threats occuring in cloud.



When the question was asked if they feel that attacks should be reported by cloud service provider to users, 82.2% of people feel that the service providers should mention about threats to it's users, while 17.8% of people responded that they do not need to be aware of security threats.



When the question was asked what are the major concerns they feel regarding cloud computing, 72.3% people responded security and privacy as the major concern, 48.5% people responded availability of service as the concern, 51.5% people feel confidentiality as the biggest concern, 15.8% people responded that unclear scheme in pay per use approach as their main concern, 20.8% people feel cost and difficulty of migration to cloud as the major concern.



At last when question was asked as what cloud services option would users take into consideration while using cloud platforms, 54.5% of people responded that it should provide security but cost is 1000 Rs. These users feel security and privacy is the biggest concern while accessing cloud based application. It may cost a few rupees but security is considered important while using cloud applications. 45.5% prefer free version of cloud which donot provide security and privacy

HYPOTHESIS TESTING

Hypothesis testing is a sort of statistical reasoning that includes analysing data from a sample to derive inferences about a population parameter or probability distribution. First, a hypothesis is created regarding the parameter or distribution. This is known as the null hypothesis, abbreviated as H0. After that, an alternative hypothesis (denoted Ha) is defined, which is the polar opposite of the null hypothesis. Using sample data, the hypothesis-testing technique determines whether or not H0 may be rejected. The statistical conclusion is that the alternative hypothesis Ha is true if H0 is rejected. For this paper

Null hypothesis (H0): Cloud applications are secure and protects our privacy.

Alternative hypothesis (Ha): Cloud applications are not secure and cannot protect our privacy.

TEST (STATISTICS)

There are 3 tests available to determine if the null hypothesis is to be rejected or not.

They are:

1. Chi-squared test

2. T-student test (T-test)

3. Fisher's Z test.

For this paper, we will be using a 2 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 isn't one. 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 mean) measured in a sample survey is also true for the entire population.

Sr.no	Data
1	89.1
2	59.4
3	71.5
4	68.3
5	85.1
6	60.4
7	82.2
8	50.5
9	72.3
10	54.5
Mean(x)	69.33
SD(s)	13.21876192

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 t-mean. distribution's.

The formula to find 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 p-value, also known as the probability value, indicates how probable your data is to have happened under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are .01, .05, and .10) then we can reject the null hypothesis and conclude that cloud applications are not secure and cannot protect our privacy.

Calculating t-value:

Step 1: Determine what the null and alternative hypotheses are.

Null hypothesis (H0): Cloud applications are secure and protects our privacy.

Alternative hypothesis (Ha): Cloud applications are not secure and cannot protects our privacy.

Step 2: Find the test statistic.

In this case, the hypothesized mean value is considered 0.

$t = (x-\mu) / (s/\sqrt{n}) = (69.33-0) / (13.218/\sqrt{10})$

$= 16.58565267$

t-value = 16.58565267

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 = 10, so n-1 = 9. By plugging the observed value in the calculator, it returns a p-value. In this case, the p-value returned is less than 0.00001.Since this p-value is less than our chosen alpha level of 0.05, we can reject the null hypothesis. Thus, we have sufficient evidence to say that cloud applications are not secure and cannot protect our privacy

XI. FINDINGS

1. Most people access cloud based applications for various purposes.
2. Many of the users don't prefer to host their sensitive data on cloud.
3. Most users feel that the copies Which they have deleted would exist for a few weeks with the cloud service provider.
4. The service level agreement is very important when using cloud based applications but many people has not even seen the service level agreement.
5. Many people feel that their service providers can disable their account if it provides prior notification.
6. Users are aware of the security threats occurring in cloud computing
7. The attacks must be reported by cloud service providers to the users.
8. Users are aware of the countermeasures applied in cloud applications.
9. Many people prefer using secured versions of cloud even though the cost is high.
10. Most of the people feel that security and privacy as the important concern well choosing cloud based platforms.

XII. CONCLUSION

The cloud applications are used by many people all over the world. The users store their sensitive data on cloud. Therefore it is important to secure the data in cloud. Cloud providers use various techniques in order to prevent attacks. The users need to be provided with the secured versions of cloud. The security in cloud can never be achieved fully. There may be some breaches happening in cloud. The users have the right to know about the attacks occuring in cloud platforms. These attacks can be also reduced from the users end up to a certain limit. Service level agreement is something which needs to be read before agreeing to the terms and condition of cloud service providers. But many people are not even aware of the service level agreements. But data cannot be fully trusted and stored in cloud applications.

REFERENCES

1. Syam Prasad, G. and Gaikwad, V., 2018. A Survey on User Awareness of Cloud Security. *International Journal of Engineering & Technology*, 7 (2.32) (2018) 131-135.
2. Mijuskovic, A. and Ferati, M., 2016. Cloud Storage Privacy and Security User Awareness. *International Journal of Human Capital and Information Technology Professionals*, 7(3), pp.1-18.
3. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. and Al-rimy, B., 2021. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. *Applied Sciences*, 11(19), p.9005.
4. Widjaja, A. and Chen, J., n.d. USING CLOUD COMPUTING SERVICE: A PERSPECTIVE FROM USERS' INFORMATION SECURITY, PRIVACY CONCERN, AND TRUST.