# Hindrances in the Security of Cloud Computing

[1]Mehul Nanda, [2]Aakarsh Tyagi
[1, 2]Department of Computer Science and Engineering
ASET, Amity University Uttar Pradesh
Noida, India
mehulnanda16@gmail.com, tyagi.aakarsh@gmail.com

[3]Karan Saxena, [4]Neeru Chauhan
[3, 4]Department of Computer Science and Engineering
ASET, Amity University Uttar Pradesh
Noida, India
saxenak96@gmail.com, nchauhan@amity.edu

***Abstract*—Cloud Computing model offers numerous advantages to the users such as flexibility, availability and less cost. This model is being adopted by large number of organizations and the list of organizations entering into Cloud Computing is growing on a large scale. The user places their data on Cloud as it provides a lot of storage area. But mounting of user data onto the Cloud demands protection of the data from malicious attacks. The Cloud providers provide various measures to protect the user data but still it is prone to attacks. This paper addresses the various security threats that might occur in Cloud Computing. A survey is being carried out to determine the awareness of these attacks among the various Cloud Computing users.**

***Keywords— Cloud Attacks; Cloud Security; Data Loss; Cloud Misuse***

## I. INTRODUCTION

The term Cloud refers to a Network or web.In other words, we can say that Cloud offers services over the Internet, whether the person is residing in a remote area. As long as he has an Internet connection he can use all the cloud services like e-mail, conferencing etc. When one stores his photos on-line rather than his disk, or use webmail or a social networking web site, he is employing a "cloud computing" service.

Now what really is a cloud computing service? Suppose if you're a corporation, and you would like to use, for instance, an internet invoicing service rather than changing the in-house one that you are using for so many years, the new on-line invoicing service would be a "cloud computing" service.

Cloud computing refers to the delivery of computing resources over the internet to all the people around the world. Rather than keeping data on one's own disc drive or, one would prefer to utilize a service over the internet, at some another location, to store his data or use his applications. Doing this could or might not bring about to sure privacy implications as there are many threats over the cloud computing.

The reason behind the interest of organizations in cloud computing is that Cloud computing will cut back the cost of owning and operating computers and networks; it will also minimize the area of working as well as cut electricity cost as well. If a company uses a cloud supplier, it doesn't have to be compelled to pay cash on data technology infrastructure, or obtain hardware or code license. Companies with low budget can use high end resources with a lower cost as compared to the cost of owning one.

When it involves cloud computing, the protection and privacy of the data is one of the factors that we cannot neglect. Provided that one's personal data is being turned over to a different organization, typically in another country, it's very important to make sure that the data is safe. The people to whom we are providing our personal data don't use it and exploit our right. There is the danger that non-public data sent to a cloud supplier may well be unbroken indefinitely or used for alternative functions. Such data may even be accessed by government agencies, domestic or foreign (if the cloud supplier retains the data outside of Canada).

For businesses that are considering employing a cloud service, it's vital to know the protection and privacy policies and practices of the supplier. The terms of service that govern the connection with the supplier typically yield rather liberal usage and retention practices [7].

### *A. Cloud Services*

Now for understanding the cloud more one should have the basic idea about the services that the cloud offers

- Platform as a Service (PaaS) :- PaaS provides the runtime surroundings for applications, development preparation tools, etc. controls their applications. User doesn't manage servers, storage and IS. So its primary aim is to facilitate the application development and related management problems and help out the customer.
- Infrastructure as a Service (IaaS) :- This service provides access to elementary resources such as physical machinery, virtual machinery, storage, etc. It does not manage the infrastructure and can manage the OS, storage, application, chosen network elements, i.e. it basically provides storage, networks, processing, and other essential resources to the user
- Software as a Service (SaaS) :-_ This model permits one to use package applications as a service to end users. User doesn't manage the network, servers, OS, storage or applications. So basically provides an environment for software distribution.

978-1-4673-8203-8/16/$31.00 ©2016 IEEE

### B. Cloud Development Strategies

Further to understand cloud we have to understand cloud development model.

- Public cloud :- It is a traditional computing approach, in which a facility supplier makes resources like storage and applications and make it available to the community over the internet. Cloud infrastructure is accessible to the overall public, closely-held and managed by organization commercialism cloud services. A public cloud is made so as to supply cloud services to a diversity of third-party clients.
- Private cloud :- The cloud infrastructure is operated alone for a particular organization, and is managed by the organization.
- Community cloud :- The service is shared by many organizations and created accessible solely to those teams. The infrastructure could also be closely-held and managed by the organizations or by a cloud service supplier. Community cloud to some extent is overlay with Grids.
- Hybrid cloud :- Hybrid clouds mix each public and personal cloud models. The important activities area unit performed exploitation personal cloud whereas the non-critical activities area unit performed exploitation public cloud.

In this research paper, Section II consists of the literature review which sheds light on the various theories elaborated by different number of authors. Section III accounts for the full explanation of the various security threats that have been categorized as internal and external threats. In order to understand this from the prospective of a cloud user and non user, a survey is thus an essential component of our research. A questionnaire was thus prepared and sent out to numerous people, mostly university students. The questionnaire contained questions that would appeal to a cloud user and non user and make us understand the various reasons for them to approach cloud computing and frequently use it. The results were then analyzed. Section IV describes the analysis of the survey conducted by us. Section V is the conclusion of our findings. the current designations.

## II. Literature Review

Louai A. Maghrabi et al. investigates on the concept of cloud computing explained the various security threats and attacks in cloud computing. The author rightly states that Cloud Security is indeed being compromised with reference to the near future. New and improved threats are arising day by day and causing chaos amongst users who are already using the service and even spreading doubt within the minds of the people who would like to use the cloud service [1].

Sajjad Haider et al. define the threats to cloud computing into categories such as internal and external threats. These threats have an adverse effect on the cloud service. A culmination of both threats is also applicable under certain set situations[2].

Ray Hunt et al. describe as to how people are unsure as to whether they should approach cloud computing. This debatable issue is supported by the various threats that are prevalent in cloud computing and to the numerous advancements that are arriving on the scene. Hence cloud users and non users are skeptical about the idea and concept of cloud computing in totality[3].

Sugam Sharma et al. describes how cloud computing is being widely accepted beyond the range of IT communities as well. It is thoroughly explained as to how cloud computing may not be a potential solver for all the problems that one might encounter, however in a specified problem such as handling of large amounts of data called Big Data, it is the best possible solution. One then also realizes the close proximity between Big Data and Cloud Computing by real life examples such as Netflix, which is a video streaming website that access library of videos that are stored on cloud handled by the Amazon Web Services[11].

Johnny Wong et al. also illustrate the fact that cloud computing is a new, highly flexible, pay per view or free delivery and provisioning system. It also being noted that cloud computing is closely linked with the upcoming Internet of Things age that is the use of sensory systems to make use of everyday objects. With the increase in the senses that can be identified and the ever increasing population and need of the world, the sensory systems need a large amount of storage and backup in order to work flexibly. The data that is used is also of great sensitivity and is collected from highly sparse geographical environments thus it needs proper handling and care. Hence Cloud Computing can be used as a tool to manage this varied range of data[12].

## III. Threats to Cloud Computing

### A. Internal Threats

- Rogue Administrator: A very unaccounted for internal threat is that of a rogue administrator. What this implies is that there is every possible chance of the cloud service administrator to be of malicious character and use every possible means of exploiting the info that is stored on the cloud. Sensitive information stored on the cloud is at the most risk. An administrator can sabotage the files or data stored on the cloud service as he has unchallenged access to all the data on the cloud service. He can also use brute-force passwords to gain access to certain inaccessible files and can also download the data that is present on the cloud of the particular victim that is being targeted. Such an attack is brought about by grudges that may be prevalent amongst individuals within an organization[4]. Not only is the theft of data at stake, also data availability is jeopardized. The administrator can restrict certain sections of the files or data uploaded to be accessed thus causing problems for the user of the service. It can also lead to the hosting system to not respond to the customer requests.
- Cloud Vulnerability: Mostly overlooked, such type of a threat is very dangerous as it can be accidental as

well intentional. Cyber Crimes are an active part of this threat. Services such as Facebook, WhatsApp etc. display personal information such as date of birth, gender, name etc. and digital media such as photos, music, videos etc. on them and these details are stored on the server of the website or application. The entire storage system may be a target for such an attack. An employee of the organisation may unintentionally initiate the attack by the prompting of an outsider. Malicious outsiders often provoke internal employees into accessing certain encrypted files that may harm the service itself. Thus they are able to track the path taken by the data from the user to the storage device or service and hence cause damage to the system. In such a case, the outsider may use any sort of information such as stolen passwords, or downloaded files for their own purpose without the proper knowledge of the organization[5].

### B. *External Threats*

- Data Loss: Data loss is often the one of the most popular and common threat for any sort of storage computing technology. Data loss can occur due to improper storage of data, attacks on the cloud database such as hacking, or due to measures implemented by the developers of the cloud service. Often such measures are taken for effective cost saving and valuable data may be compromised. An example to justify this is absence of criteria for modifying of a file and saving it or restoration of data after system failure etc. Data loss occurs generally due to corrupted storage, insufficient storage space, inadequate partitions for storage, and poor policies for backing up of data[6].

- Abuse and Misuse of cloud computing **:** Cloud Security Alliance(CSA) notes that some of the Infrastructure-as-a-Service providers(IaaS) do not have enough domination over spammers, crackers, hackers and other people engaged in various other criminal activities that are taking benefit of the opportunities offered in the cloud. Easy registration processes offered by Cloud Computing Service providers allows hackers to misuse their infrastructure and use them for their own advantage. For example, brute force attack or a DoS attack can be successfully launched by abusing cloud computational services[9].

  Technique used to break passwords and keys is called brute force attacks. The greater the computing capability of the system more is the success rate of this attack. Thousands of passwords and key combinations are targeted to the client's account until the right combination matches the password and cloud computing system provides excellent platform to do so.

  DoS attacks blocks users of their access to use cloud as a service by messing up a host or network resource. DoS attacks are of three types namely: consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, and physical destruction or alteration of network components.

- Sessions and services hijacking :- These types of spasms with embezzled credentials material are generally perpetrated. There are different methods of attack to steal credentials information such as phishing, fraud, DoS (Denial of Service), exploring vulnerabilities and account hijacking. In a Cloud surroundings, if an attacker can access to credentials of a person's session, it can spy on all activities, make connections and alter data. There are four types of attacks that correspond to this kind of threat. These are: the middle attacks (man-in-the-middle), phishing, spam and DoS attacks. Some scholars have proposed defensive actions to deal with such threats. The most important points are the following: robust encrypted authentication of system and Cloud operators, increased protection against sessions hijacking at the application level and allow one reliable party of system belonging to the company to access and manage the Cloud resources for a given customer[8].

The current scenario is as such that majority of Cloud Computing systems use digital identity of their consumers to access specific services, this could be a potential drawback particularly for Hybrid Cloud.

## IV. ANALYSIS AND FINDINGS

The results of the survey thus conclude: 88.46% of the students were vaguely aware of Cloud Computing services while the others are still unaware of the concept of cloud computing. Only 11.53% of students believe they are thoroughly familiar with the concept of Cloud Computing.

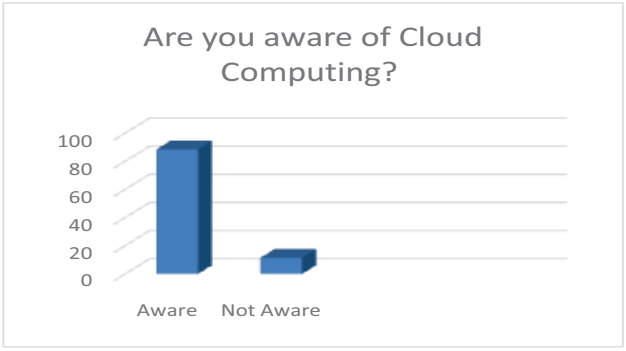


Fig. 1. Familiar with the concept of Cloud Computing

84.61% of students are frequent users of cloud computing services while the rest are unaware of what services are categorized as cloud computing services. Amazon, Google Drive and iCloud are amongst the most popular cloud computing services.

Fig. 2 describes the users using Cloud Computing services.

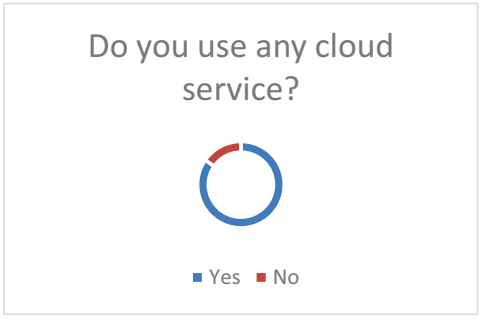


Fig. 2 Frequent use of Cloud Computing

42.30% of students consider security as the most important factor for choosing a cloud security service. 38.46% believe that performance of the cloud service in terms of reliability is a much more important factor. Reputation of the cloud service is also regarded by 7.6%.

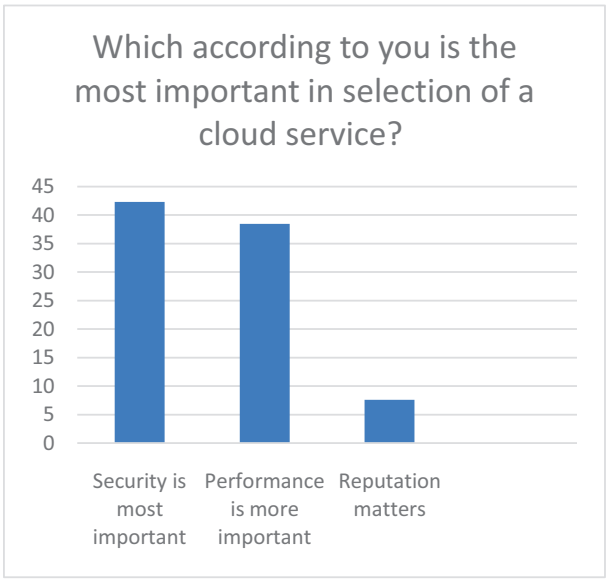


Fig. 3 Criterion in Selection of Cloud Computing Services

92.30% of the students use cloud computing services for Email, 57.69% for E-Commerce purposes and 34.61% for office tools.

42.30% of students use private cloud strategies, while 34.61% of students use public cloud strategy and the rest use hybrid cloud strategy.

88.46% of students are reluctant to adopt cloud computing services due to security reasons as they believe that security is compromised to a high extent in such a storage policy. 26.92% students believe that system performance is an essential pre-requisite for any sort of application and the absence of this on cloud computing makes them reluctant to use these services. Lack of Standards with reference to evolving times is regarded as a reason by 26.92% of students, while Implementation of the service itself is given 30.76%.

Fig. 4 shows the functional areas of cloud computing services used by the different users of Cloud Computing according to the survey being conducted.

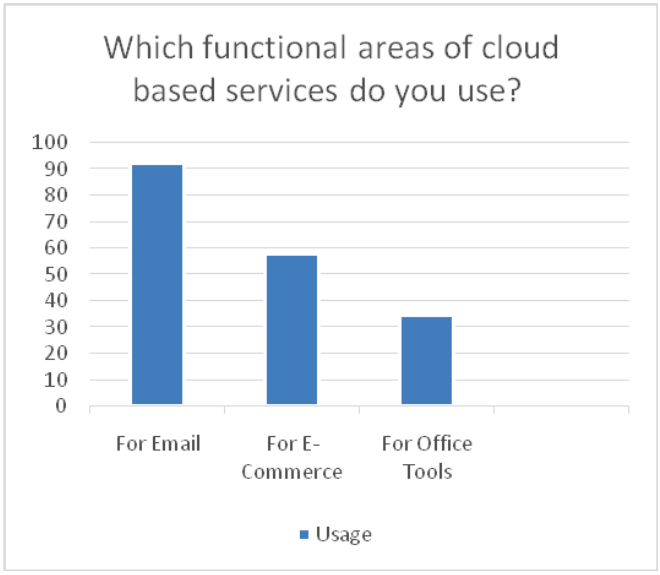


Fig. 4 Functional areas of Cloud based Services used by users

Fig. 5 shows the type of cloud computing model used by the different users of Cloud Computing.

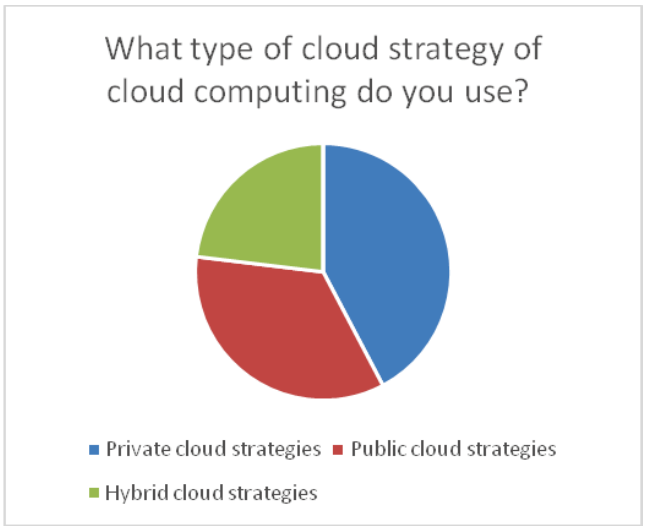


Fig. 5 Functional areas of Cloud based Services used by users

70% of students are aware of the various security threats that affect cloud computing. Amongst this 57.69% are familiar with Abuse and Misuse of Cloud Computing service, 38.41% are familiar Internal Mischief that may be caused in the cloud computing service, 73.07% are familiar with the threat of Data Loss within the cloud service.

In terms of familiarity with cloud classifications: 65.38% are familiar with Software as a Service, 34.61% are familiar with Platform as a Service and 34.61% are familiar with Infrastructure as a Service. Fig. 6 shows the obstacles in adopting the Cloud computing services being faced by the different users of Cloud Computing according to the survey.

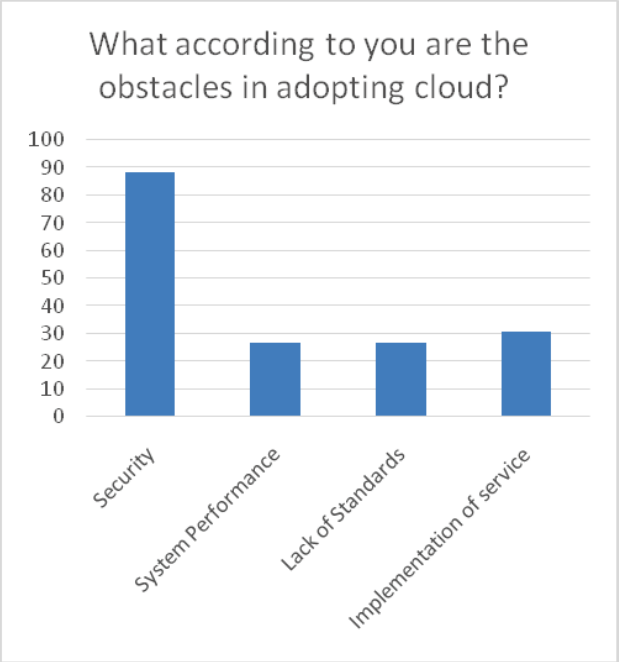


Fig. 6 Obstacles in adopting Cloud Computing Services

Fig. 7 shows the awareness of the attacks on Cloud Computing by the different users of Cloud Computing according to the survey being conducted.


Fig. 7 Awareness to Cloud Attacks by the users of Cloud Computing Services

## V. CONCLUSION

Cloud Computing as we now know refers to the advanced and sustainable storage and sharing of data over the internet. It enables one to create a connection over the internet with as many individuals as possible. It also allows one to privately store data as per their needs. As elaborated, these needs are satisfied by the various computational methods and strategies for the functioning of cloud computing. However, the concept of cloud computing is still in its early stages and is not effectively used by all the people who access the internet. The root cause of this is many threats to the entire concept of cloud computing are prevalent which raises doubts in one's mind regarding using the service or not. A survey thus conducted highlights the major causes of concern for as to why the use of cloud computing services is still debatable. Security threats tend to be a major issue in this. Such security threats may be insider threats or outsider threats, both being equally malicious in nature. New security techniques have to be devised in addition to the already existing ones, in order to deal with the advanced computational problems that might occur today or even in the near future. We hope that our work gives a much better understanding of the challenges one might have to go through in order to support cloud computing and pave the manner for additional analysis during this space.

## REFERENCES


[1] Louai A. Maghrabi , "The Threats of Data Security over the cloud as perceived by experts and university students", in Proceedings of IEEE World Symposium on Computer Applications & Research(WSCAR), 18-20 January 2014, pp. 1-6.

[2] Sajjad Haider and Engr Farhan Bashir Shaikh, "Security Threats in Cloud Computing",in Proceedings of IEEE 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, UAE, 11-14 December 2011,pp. 214-219..

[3] Ray Hunt and Jill Slay, "A New Approach to Developing Attack Taxonomies for Network Security- Including Case Studies",in Proceedings of 17th IEEE International Conference on Networks(ICON), 14-16 December 2014, pp. 281-286.

[4] Amir DJENNA and Mohamed BATOUCHE, "Security Problems in Cloud Infrastructure", in Proceedings of IEEE International Symposium on Networks, Computers and Communication,17-19 June, 2014, pp. 1-6.

[5] Te-Shun Chou, "Security Threats to Cloud Computing", in Proceedings of IEEE International Journal of Computer Science & Information Technology (IJSCIT) , Vol 5, No 3, June 2013, pp. 79-88..

[6] William R Claycomb and Alex Nicoll, "Insider Threats to Cloud Computing: Directions for new Research Challenges", in Proceedings of IEEE 36th Annual Computer Software and Application Conference (COMPSAC), 16-20 July 2012, pp. 387-394.

[7] D. Shin, Y. Wang, and W. Claycomb, "A policy-based decentralized authorization management framework for cloud computing," in Proceedings of ACM Symposium on Applied Computing (ACM SAC), 2012.

[8] A. Mladen et al., "Cloud Computing–Issues, Research and Implementation," International Journal of Computing and Information Technology - CIT 16, 2008.

[9] E. Grosse et al., "Cloud computing roundtable, Security & Privacy," IEEE 2010.

[10] Sugam Sharma, U Sunday Tim, ShashiGadia, Johnny Wong(2015) , "Proliferating Cloud Density through Big Data Ecosystem, Novel XCLOUDX Classification and Emergence of as-a-Service Era".Available: "http://www.public.iastate.edu/~sugamsha/articles/Cloud%20Density%20in%20Big%20Data%20Ecosystem,%20Novel%20XCLOUDX%20Cla

ssification%20and%20Emergence%20of%20aaS%206%2014%202015.pdf."

[11] Sugam Sharma, "Evolution of as-a-Service Era in Cloud", Cornell University

Available: "http://arxiv.org/ftp/arxiv/papers/1507/1507.00939.pdf".

[12] Sugam Sharma , U Sunday Tim , Shashi Gadia, Johnny Wong, "Growing Cloud Density & as-a-Service Modality and OTH-Cloud Classification in IOT Era. Available: "http://www.public.iastate.edu/~sugamsha/articles/OTH-Cloud%20in%20IoT.pdf .".