International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Experimental Analysis of Data Security Challenges on Cloud

Dhruv Sirohi[1], Tanishka Shorey[2], Shivam Anand[3], Manjula R[4]

[1, 2, 3, 4]SCOPE, Vellore Institute of Technology, Vellore-632014, Tamil Nadu, India

Abstract: ***Cloud computing is in today's time an ever changing and growing phenomenon, due to its ability of global resource sharing. It is a shift towards efficient resource utilization and hence attracts such serious attention from both users and developers. It offers services related to storage, computation and networking by utilizing various types of virtualization techniques. Every coin is two faced, with its set of benefits, come the downsides of cloud computing. Security of the data is perhaps the major concern of all users (current and willing). This paper highlights the various data security challenges and their individual attributes that add up to pose the challenge. The challenges can either be consequences of loose ends or violations of direct or indirect attacks by several factors. These consequences and violations, in the paper, have been classified in terms of 1st, 2nd and 3rd party. The paper attempts to understand the factors and their attributes in depth and also tries to bring together the several factors affecting user acceptance of cloud, when it comes to the fear of security of the data stored on it. The paper can be hence used as reference by users to understand potential threats or even by developers to understand the causes of failures and the fears that are involved around wide range usage.***

Keywords: Cloud Service Provider (CSP), External Threats, Denial of Service (DoS), Disaster Recovery(DR), Virtual Machine

1. Introduction

Cloud Computing brought a significant shift in the sector of information technology. 'Cloud' here means the internet, so this internet-based computing is a model that virtually delivers hardware and software resources as services on the net. It offers several advantages like scalability, portability, flexibility, pay-as-you-use services, and manageability. Companies that have adopted cloud computing only pay for those resources that they are using, they can scale up or scale down their resources as per their market demands. For start-ups, this is a feasible option as it helps avoid investment of funds into full-scale hardware and software resources.

There are three main layers of services. – SaaS, PaaS, IaaS. SaaS (Software as a service) is the most well-known deployment model and, also represents the largest and fastest growing cloud market. It replaces the traditional on-device applications and puts all the functionalities on the web, getting rid of the installation and download hassles. PaaS (Platform as a service) as the name suggests provides the developers with a platform to build software's. This makes development, testing and maintenance of software very easy and efficient. With the commencement of the "Green Computing" wave that has flooded the IT sector, IaaS(Infrastructure as a service) deployment model is the need of the hour. It powers needs of SaaS applications and PaaS services by delivering storage (data), servers(runtime), networks(middleware) and operating systems. Companies who have volatile demand, do not have the funds for hardware, looking for scalability, this type of model is used. With such agile models that can coexist with different technologies and software designs, comes a great deal of security issues.

Data security has been one of the major concerns that have prevented an exponential growth of usage of cloud amongst the common public. Data on the cloud is remotely stored and is continuously traveling, posing a threat. Maintaining the integrity of data is paramount to cloud's success. Data outsourcing paradigm in the cloud is one of the biggest security concerns. The multi-tenant nature of the cloud often leads to resistance to use the cloud. A decade ago, data used to be physically stored in servers giving them full control of it but today with virtualization and cloud computing, data is only under the enterprise's logical control. This shift in control has added on to the data security challenges that are being faced in the sector.

This research paper examines various attributes of the data security challenges. Each attribute is then categorized under 1st party, 2nd party and 3rd party threats. These parties represent the end users, the Cloud Service Providers (CSP) and the external factors (foreign invaders, natural disasters etc.) respectively. The attributes under the data security challenges are consequences of either loose ends on the 1st and 2nd part sides or else attacks by 3rd party factors. This leads us to classify each attribute on the following lines, helping us to clearly identify the reason behind each challenge and analyse the main areas of improvement.

2. Literature Review

Cloud Computing is the future of internet based computing, it offers features like customizability and ease of access of various cloud applications all at once. It has changed the way people perceive infrastructure architectures, software delivery and deployment models [16].Cloud Computing uses basic techniques of virtualization to store and access data from anywhere by using internet [5]. This rapid shift towards cloud has fuelled a number of critical issues like the success of information systems, communication models and most importantly, data security. Inefficient data security measures for data operations,transmissions and storage can pose high risk to the data[6].Cloud Security Alliance has identified top nine cloud computing threats that mainly include threats to data such as data breaches, data loss, DoS and few others [9]. Data breaches on the cloud are constantly increasing due to hackers who are always attempting to over-ride the security set-up of the cloud [7].Data loss, which means a loss of data that occur on any device that stores data. It is a problem for anyone that uses a

computer. Data loss happens when data is physically or logically removed from the server either intentionally or unintentionally. Data Leakage refers to an unauthorized transmission of data from within an organization to an external destination [2]. Security and privacy of data arethe two main concerns of user about cloud usage. Data separation is proved beneficial to provide confidentiality, integrity, availability and trust in cloud [11]. Over the period of development of cloud, many techniques of cloud computinghave been investigated both academically and industrially, security and privacy of the data on cloud, holdmajor scope forfuture development in the field of cloud computing in view of the government, industry, and business [3].

3. Data Security Challenges

Data security challenges comes with the open-environment resource-sharing nature of clouds. The different threats that come into play when it comes to using cloud services, lies in the fact that it's an upcoming technology, there are no standards that have been established. Development in the field is an ever-continuous process and there always lies more scope for improvements.

As we continue to develop and adapt more o the cloud model, it requires greater and deeper emphasis on the issues of Data Security and Privacy. To understand the reasons that provide an up-thrust to such challenges, we must list out and discuss each of it in detail. The data security challenges that have been discussed in this paper are as Disaster Recovery Challenges, Availability of Service, Data Segregation and Protection, Identity and Access Management, Data Leak Prevention in the cloud, Threat and Vulnerability Management and Physical and Personnel Security.

3.1 Disaster Recovery Challenges

a) **Dependency- 2nd party**
Along with the original data, the copy of the data backup is available only with the service provider. This creates a complete dependency for data of the users on the Cloud Service providers.

b) **Cost- 1st and 2nd party**
Minimizing the cost of a setup is the primary goal, of every business setup. Most CSP's seek cheaper ways of recovery methods to minimize operational costs. Users on the other end are unwilling to spend high costs, this creates a void of funds in the setup. Hence resulting in compromised features.

c) **Failure detection- 2nd party**
Most CSP's do not have an efficient system in place to identify the difference between service disruption and network failures. Fast and efficient detection of any sort of failure is necessary for best and most optimized DR procedure.

d) **Security- 3rd party**
There may arise threats from various external agents, these might be natural or manmade. Threats like natural disasters, cyber terrorism, hacking, snooping etc. pose threat to the data.

e) **Replication Latency- 2nd party**
Replication of the original data is the sole mean of backup. Data replication techniques may either be synchronous or asynchronous, each of which come with their own set of benefits and flaws. Synchronized replication of data is an expensive method with large overhead while a-synchronized offers cheaper and low overhead DR options. Having said that Synchronized method guarantees greater RPO(Recovery Point Objective) and RTO (Recovery Time Objective) when compared to the a-sync.

f) **Data storage- 2nd party**
Cloud storage offers greater level of flexibility and also helps save money. Cloud architecture is divided into four different layers- physical storage, infrastructure management, application interface and access layer. The data storage is centralized due to security reasons and hence results in critical challenges in terms of single point failure and data loss.

g) **Lack of redundancy- 2nd party**
In the case of a disaster, a backup site is put up while the original site is maintained and restored. The backup site may not support all sync and a-sync features and hence result in local data storage, though this is a temporary issue, all cons need to be weighed out.

3.2 Availability of Service

3.2.1 Hypervisor- 2nd party
Cloud works on the principle of virtualization and hypervisors (virtual machine monitors) allow you to create those several virtual machines and run from one hardware. A flawed hypervisor can pose serious threat to the data security. Malwares and rootkits can install themselves on the OS layer and result in hyper-jacking

.

3.2.2 Confidentiality and Data Integrity- 2nd party

Ensuring the system to be leak proof is necessary. Usage of cryptographic techniques can improve data security.

3.2.3 Single point failure- 2ndparty
As all the data is stored in one location, the data is vulnerable threats at various stages like- data centre level, application level, infrastructure level or even geographic location level. Timely identification and replacement of the failure node results in better credibility of the platform.

3.2.4 Insecure API's-2nd party
CSP's provide the customer with a number of software user interfaces (UI's) and application programming interfaces (API's) that help them with managing and interacting with service on the cloud. An insecure API will directly.

3.2.5 Unauthorized access- 3rd party
Malicious attacks such as XSS (Cross Site Scripting) attacks, Cookie Poisoning, DoS attacks and many more pose a serious threat to the services available on the cloud. A secure design and coding pattern should be adopted to make it difficult for the foreigners to hack into the system.

3.3 Data Segregation and protection

3.3.1 Multitenancy- 2nd and 3rd party
Multitenancy refers to the multi-user attribute of cloud computing which leads us to question the confidentiality and integrity of the data stored. several clients on the cloud access the data in several ways, making the cloud environment unsafe.

3.3.2 Cost- 1st and 2nd party
Customers constantly look for cheaper options to meet their needs, at the same time CSP's work on increasing profit margins. Data can be separated physically or logically, physical separation further required purchase of storage arrays. Data segregation comes with huge costs as data security application techniques like encryption and decryption need to then be applied to each segment, to ensure data security.

3.3.3 Secure Technology- 2nd party
SSL (Secure Socket Layer) is the sole encryption technology to be practiced for data communication between the server and the browser. Ensuring all data communication to occur only via SSL protocol is important.

3.3.4 Cloud storage- 2nd party
The sheer basis of cloud storage is the abundant replication of the server data to ensure anytime access of all data to the users. This replication constantly requires more storage space which entails greater cost.

3.3.5 Data mobility- 2nd party
Segregation of data of two organizations onto different storage arrays may ensure greater level of data security and integrity. The process of data transfer from one array to the other must also be carefully secured and encrypted to prevent any sort of data leakage.

3.3.6 Different levels of security- 2nd and 3rd party
The biggest advantage of segregation of data on cloud is the ability to provide varied level of security for each data set based on the customers need. Maintaining and monitoring all these levels efficiently is essential. Moreover, hackers and intruders may take advantage of this varied level of security and find a breakthrough to the data from any weak point.

3.4 Identity and Access management

3.4.1 Legal regulations- 2nd and 3rd party
Laws related to personal information, data positioning, audit regulations etc. are not complied to. Most laws are redundant and obsolete.

3.4.2 Data- 1st, 2nd and 3rd party
Loss or theft of data can occur at multiple levels due multiple issues. These may include insecure authentication, incompatible authorisation management, direct access to the hardware, lack of monitoring and efficient auditing and even incorrect deprovisioning.

3.4.3 Technology- 2nd and 3rd party
Technological risks such as incompatible authentication mechanisms, SSO (Single Sign on Computing) and technology to update or store user data poses threat to IAM (Identity and Access Management). Power or internet outage can discontinue cloud services for the users. Users can further be unable to access cloud services due to incorrect provisioning and inability of the CSP's to monitor the services.

3.4.4 Operational- 2nd party
Weak ends on the side of the CSP's results in the inability to efficiently monitor and control IAM. These weekends may be described in lines of inability to manage control changes to the server along with the quality and frequency of monitoring and auditing. It may also include inabilities such as verification of all access holders of the data and server, successful updates of all accounts and the execution of authorisations along with authorisation of errors.

3.5 Data Leak Prevention in the Cloud

3.5.1 Physical- 1st, 2nd and 3rd party
Data can be leaked by human error at several waypoints. Users and employees both can leak data knowingly or unknowingly by cutting the original data from the source file while making a copy, transferring data using external storage devices, taking printouts of data or even transferring data using e-mails or other unprotected means. Hackers can take advantage of any such slip-ups and get access to sensitive information.

3.5.2 Application- 2nd party
Most cloud applications ensure encryption only at the end user level of data transfer. Database security and inter-application security is ignored. Most cloud applications can also be accessed wirelessly today, data encryption can be broken in the absence of proper connectivity, leaving the data unprotected while connection is re-established. The extent of employee access and interference with data is not specified as part of the business model. This leaves scope for inappropriate use and frauds.

3.5.2 Process- 2nd and 3rd party
Migration of technology by the CSP requires creation of temporary backup during the transition process. Chances of data loss increases during this data transfer. CSPs sometimes outsource their work for specific requirements, this may require sharing of sensitive user data. This endangers data integrity and the complete protection of data is unknown as outsourcer can miss use the available data.

3.6 Threat and Vulnerability management

Data threat mainly refers to the attacks and abuses that a data faces while data vulnerability aims at the system flaws that allow the above attacks to be successful.

3.6.1 Types of data threats

3.6.1.1 Data breaches- 3rd party
Identified as the number one threat by CSA, it is the stealing of sensitive or personal data by malicious individuals by breaking into a corporate's network.

3.6.1.2 Data loss- 2nd party
A serious security threat to all CSP's is the loss of all the data on their servers through accidental deletion or corruption of storage device.

3.6.1.3 Account hijacking- 3rd party
Malicious intruders can break into cloud computing services using stolen credentials. They can then enter on other's transactions, insert false information, and divert users to explicit and malicious web sites which results in legal issues for CSP's.

3.6.1.4Insecure API's- 2nd party
The API's used by the users to communicate must be efficiently secured by the CSP's. Any weak point in it can be misused and compromised by intruders to harm the data or the system.

3.6.1.5 Denial of service- 3rd party
A relatively newer and serious threat, for organisations depending on the cloud services 24/7. This involves attacking the CSP server by sending server requests in thousands, this makes the server unable to respond to regular clients, denying them of the service temporarily.

3.6.1.6 Malicious insiders- 2nd and 3rd party
It is any person that intends to enter the cloud network to the confidential data and assets of the organization or its users.

3.6.1.7 Abuse and nefarious use- 3rd party
Network hackers are constantly working on new ways to extend their reach by propagating malwares and sharing pirated software, avoid detection and improve their effectiveness. The primary target of these attackers being CSPs that have weak security measures.

3.6.1.8 Insufficient due diligence- 2nd party
Due diligence is the care a person or an organization that must be taken before entering into an agreement or transaction with another person or organization. Parties planning to set up CSP environment must ensure they have sufficient resources and are also well aware of every aspect of the cloud infrastructure.

3.6.1.9 Shared technology issues- 2nd party
Cloud computing is a mix of several technologies, hence making it very difficult to obtain a strong isolated multitenant architecture. The CSP is responsible for providing a scalable service to the user without interfering with other clients of the system.

3.6.2 Types of data vulnerabilities

3.6.2.1 Session riding and hijacking- 3rd party
Hackers can break into the web applications by providing hacked session ID's and hence gain unauthorized access over user session. Hackers can also delete all of user's data and information by sending commands over web applications. This is simply done by redirecting current user session to harmful and malicious websites.

3.6.2.2 Reliability and availability of service- 2nd party
The cloud infrastructure is highly dependent on several other technologies, failure of any can result in outage of cloud services temporarily or permanently.

3.6.2.3 Insecure cryptography- 3rd party
Cryptographic algorithms can be decrypted by attackers. This converts a strong cryptographic method into a weak one, requiring constant effort to alter and improve the existing cryptographic algorithms and techniques.

3.6.2.4 Data protection and portability- 1st and 2nd party
This is a serious matter of concern that evolves when a user discontinues the service of the CSP. A similar threat evolves when a CSP discontinues to offer its services in the sector. the question that arises in both these cases is, what happens to the data of the user?

3.6.2.5 Virtual machine escape- 3rd party
Type 2 hypervisors can be compromised by malicious and virus contents, known as hyper-jacking. The virus is able to directly interact with the OS of the host device by breaking the isolation layer between the host OS and the VM's.

3.6.2.6 Vendor lock-in- 2nd party
The clients are unable to change over or discontinue with the existing CSP because of the exiting legal bond or understandings, even though the CSP may not be able to provide all necessary or promised services.

3.6.2.7 Internet dependency- 3rd party
The cloud service is an online service, and can only be accessed through an active internet connection. This increases service liability on an external factor.

3.7 Physical and Personnel Security

3.7.1 Background check- 2nd party
The CSPs must carry out, -pre, -para and -post background checks on employees. This ensure the safety of the data of the several clients of the CSPs.

3.7.2 Accesscontrol-2ndparty
The CSPs must ensure stringent security for the network hardware and ensure the server are not exposed to any stranger. Even for employees at the CSP, strict rules and supervision must be maintained during access to the hardware or database.

3.7.3 Surveillance- 2nd party
The systems of the CSP must be monitored round the clock with cameras, intrusion detection sensors, heat and smoke monitoring systems and notification systems.

4. Experimental Analysis and Discussions

The various challenges and their attributes are mapped based on the cause party of it and simulated on SPSS to generate

results and to clearly understand the major source of threat to all our data on the cloud.

- **Disaster Recovery Challenges**

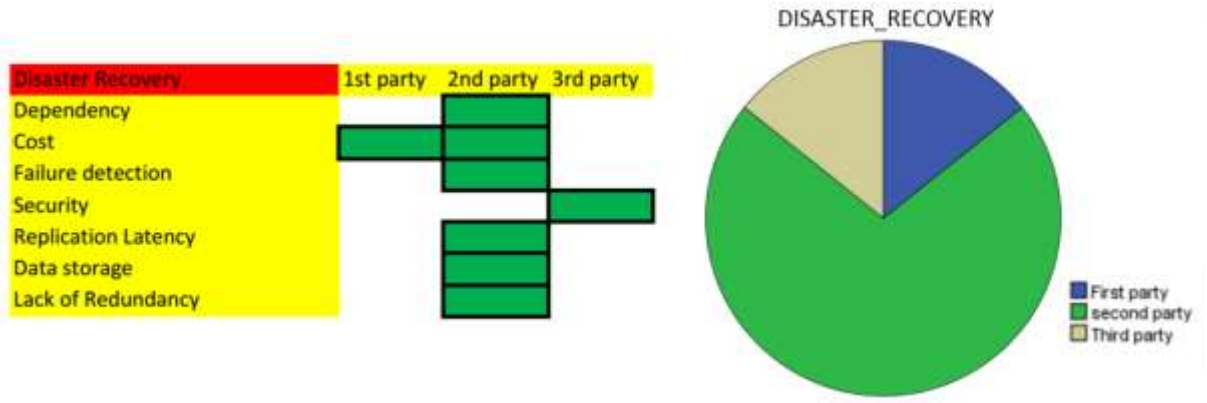

Figure 1: Attributes of Disaster recovery

Inference *(Fig. 1)*- Disaster recovery mainly occurs in three layers. The first one being Data Level which aims at security of application data. Second one being System Level which aims at reducing recovery time of the application as short as possible. Third one being Application Level which should ensure uninterrupted execution of the application. As visible, DR challenges mainly revolve around the functionalities of the application developed, hence, 2nd party being the major contributor. 1st party only comes into play when we consider the cost factor of the application, i.e. demand for a full-service application at a lower price. Shielding the application from external threats account for the 3rd party ratio.

- **Availability of Service**

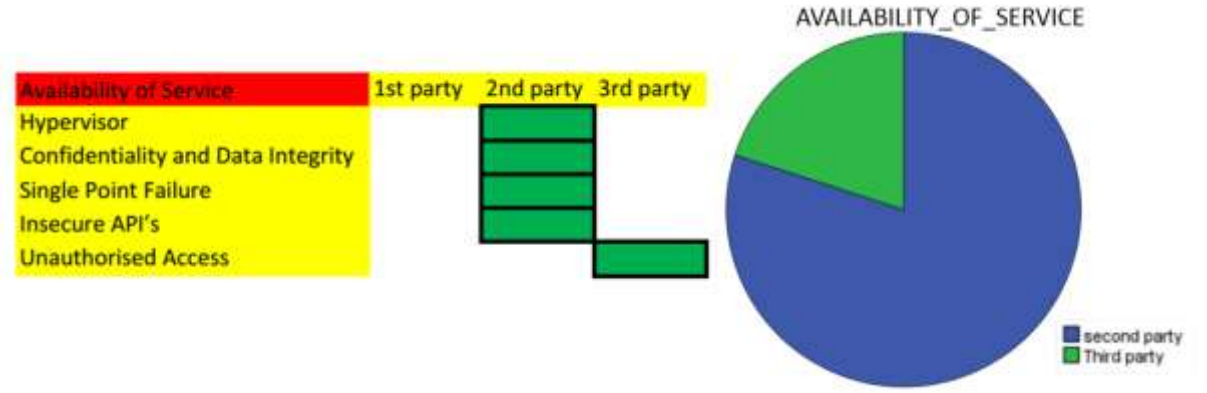

Figure 2: Attributes of Availability of Service

Inference *(Fig. 2)*- The system should be available to the user at all given time, irrespective of any intervention from external threats (3rd party). So, it's the job of the system designer to ensure that the cloud is available at all times to an authorized user which is why the major portion of the pie-chart falls under the domain of the 2nd party.

- **Data Segregation and Protection**

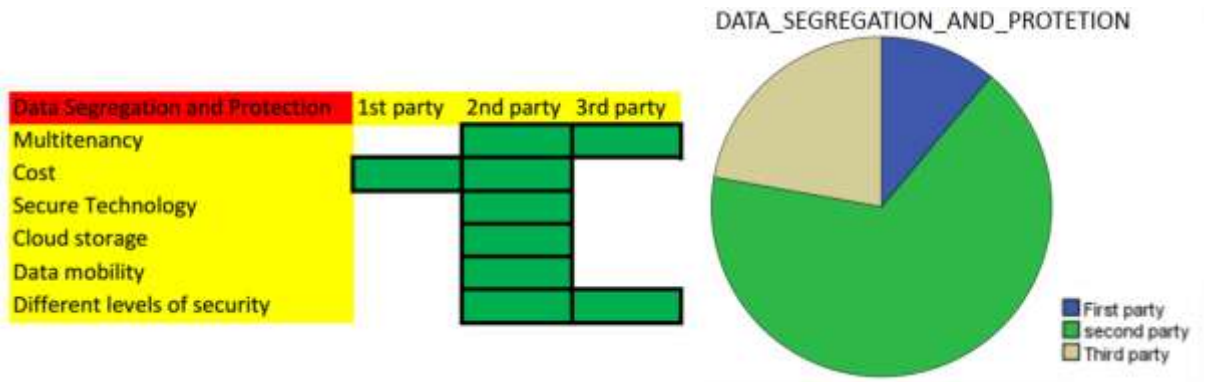

Figure 3: Attributes of Data Segregation and Protection

Inference *(Fig. 3)*- This challenge is a cumulative of many challenges such as data loss, unauthorized access due to poor software design and concurrent modification by multiple users. 2nd party plays a major role in affirming data segregation and protection followed by 3rd and finally the 1st party.

- **Identity and Access management**

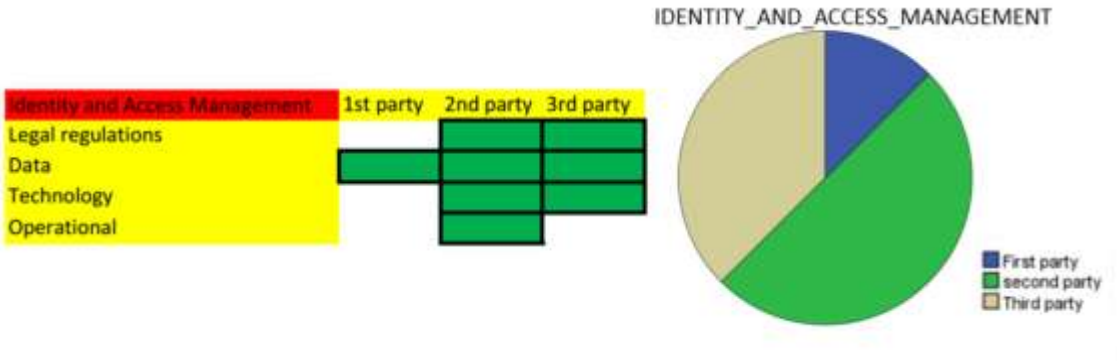

Figure 4: Attributes of Identity and Access management

Inference *(Fig. 4)*- This is one of the most upcoming threats in the world today as the criminals have gone up one level by selling stolen and fabricated accounts, which in turn pose a major threat to sensitive data stored in the cloud. Due to unavailability of updated standards and regulations, the general public are reluctant to use cloud. 50% of the causes account for 2nd part while 40% account for 3rd parties and 10% or the 1st party.

- **Data Leak Prevention in the Cloud**

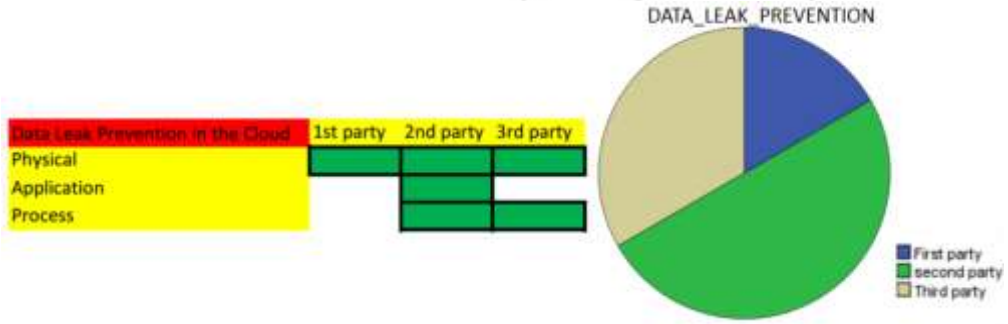

Figure 5: Attributes of Data Leak Prevention

Inference *(Fig. 5)*- Data leakage can occur due to multiple reasons such as service abuse by 3rd party. With the boon of wireless technology comes its downfalls too because each aspect of the cloud system is heavily dependent on the wireless connectivity, even the slight loss of connectivity can lead to data loss. That is why this aspect is highly dependent on the kind of service the 2nd party provides giving it half of the share on the pie chart. Frivolous behaviour of the 1st party often leads to data leakage too, by tampering the data that is provided.

- **Threat and Vulnerability management**

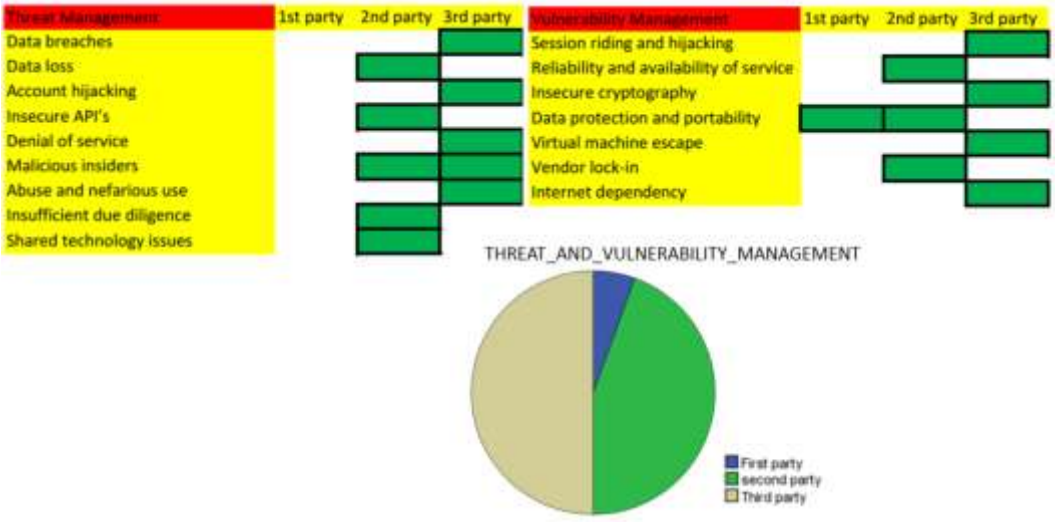

Figure 6: Attributes of Threat and Vulnerability management

Inference *(Fig. 6)*- This is one of the broadest challenge as the attributes that lead to this challenge share a common point with many other challenges. This also means that as a developer, one should carefully look upon all the attributes and as a user, one should consider all the attributes before using the cloud. Data breaches by malicious individuals, account hijacking, denial of service by overloading of requests, service abuse are the main reasons why the 3rd party contribute a major part of the pie chart shown above.

- **Physical and Personnel Security**

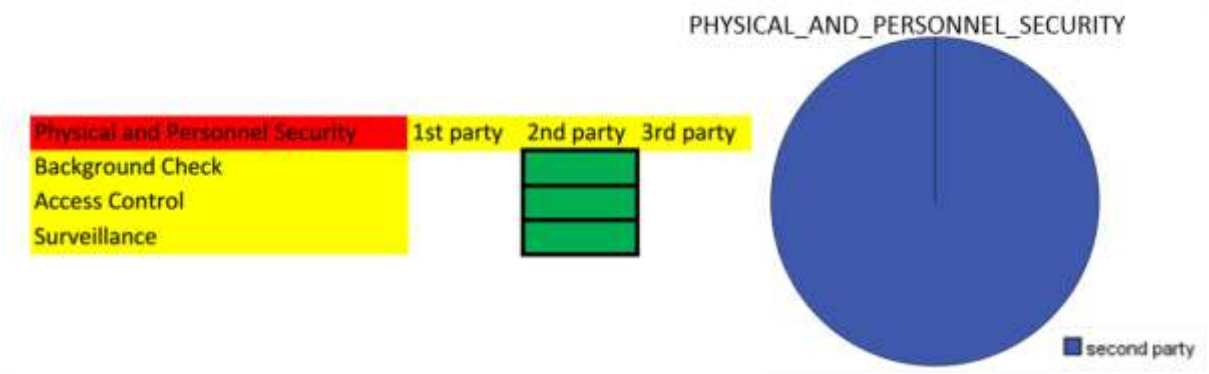

Figure 7: Attributes of Physical and Personnel Security

Inference *(Fig. 7)*- This involves safeguarding the interest of the users by conducting timely checks on the CSPs, strengthening the physical sites against accidents or any break throughs. Any sort of disaster recovery system should be tested periodically to ensure efficient performance. So, such factors purely lie under the domain of the 2nd party as shown in the pie chart above.

5. Summary

Table 1: Percentage breakup of Data Security Challenges and their Causing Parties

	1st party	2nd party	3rd party
Disaster Recovery Challenges	12.5%	75%	12.5%
Availability of Service	0%	80%	20%
Data Segregation and Protection	11.1%	66.7%	22.2%
Identity and Access Management	12.5%	50%	37.5%
Data Leak Prevention in cloud	16.6%	50%	33.4%
Threat and Vulnerability Management	5.5%	44.4%	50.1%
Physical and Personnel Security	0%	100%	0%

6. Conclusion

Cloud development is still in its growing phase and a perfect and standard Cloud system is still a distant vision to reality. The division of data security threatson the basis of causing parties, carried out in this paper should help users clearly understand the risks involved in the acceptance of cloud services. The paper can also be used by CSPs as a tool to analyse downsides in their existing frameworks and hence, properly shape the cloud applications and systems that they offer to their users. 2nd Parties can get a clear idea of which security aspect of the cloud is totally dependent on them and what steps can lead to greater efficiency in handling these data security concerns. The 1st parties of the cloud services must also learn about their sense of responsibilities in preventing loss of data on their end. Our research is able to accurately pinpoint the major areas that require attention, manging them efficiently can lead to a safer cloud experience. Even if the 1st and 2nd parties are careful on their respective ends, the external threat of 3rd parties still exist. This paper talks about the various data security threats that can be exploited by a hacker. The 2nd parties can utilize this information and knowledge, to make necessary improvements and safeguard the users and he system from such threats. A safer cloud experience can only be achieved by the collective efforts of 1st and 2nd parties.

References

[1] Prof.Sushilkumar N. Holambe, Dr.UlhasB.Shinde, Archana U. Bhosale (2015). Data Leakage Detection Using Cloud Computing. *International Journal of Scientific & Engineering Research,* 6(4), pp. 1255-1260.

[2] BijayalaxmiPurohit, Pawan Prakash Singh (2013). Data leakage analysis on cloud computing. *International Journal of Engineering Research and Applications*, 3(3), pp. 1311-1316.

[3] YunchuanSun , Junsheng Zhang, YongpingXiong and Guangyu Zhu (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*.

[4] DipaliPattanayak and Amarinder Kaur (2016). Effectiveness of Data Loss Prevention in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, 6(2), pp. 364-368.

[5] Anand Padwalkar, SulabhaPatil and Neha Mogre (2015). Designing an Application for Recovery of Data in Cloud Environment: A Problem Definition. *International Journal of Advance Research in Computer Science and Management Studies, 3(2),* pp. 291-295.

[6] R. Velumadhava Rao, K. Selvamani (2015). Data Security Challenges and Its Solutions in Cloud Computing. *International Conference on Intelligent Computing, Communication & Convergence*, pp. 204-209.

[7] Te-Shun Chou (2013). Security Threats On Cloud Computing Vulnerabilities. *International Journal of Computer Science & Information Technology*, 5(3), pp. 79-88.

[8] Mohammad Ali Khoshkholghi, Azizo Abdullah, RohayaLatip, ShamalaSubramaniam& Mohamed Othman (2014). Disaster Recovery in Cloud

Computing: A Survey. *Computer and Information Science*, 7(4), pp. 39-54.

[9] S. Venkata Krishna Kumar, S.Padmapriya (2014). A Survey on Cloud Computing Security Threats and Vulnerabilities. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, 2(1), pp. 622-625.

[10] Rajarshi Roy Chowdhury (2014). Security in Cloud Computing. *International Journal of Computer Applications*. 96(15), pp. 24-30.

[11] Seema Singh Solanki, Shaikh Nabeel (2014). Cloud Computing: Data Separation Issues. *International Journal & Magazine of Engineering, Technology, Management and Research*, 1(11), pp. 155-160.

[12] Hussain AlJahdali, AbdulazizAlbatli, Peter Garraghan, Paul Townend, Lydia Lau, Jie Xu (2014). Multi-Tenancy in Cloud Computing. *White Rose Research*.

[13] Edwin Sturrus (2011). Identity and access management in a cloud computing environment. *Master Thesis Economics & Informatics*, pp. 1-55.

[14] http://searchsecurity.techtarget.com/magazineContent/Challenges-with-data-protection-in-the-cloud

[15] http://searchsecurity.techtarget.com/definition/physical-security

[16] http://www.sciencedirect.com/science/article/pii/S0167739X10002554

[17] http://www.techrepublic.com/blog/it-security/understanding-risk-threat-and-vulnerability/