International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

# Cloud Based Data Security

**Arundhati A. Dudhgaokar, Ajay J. Bidla**

Master of Computer Application, Jawaharlal Nehru Engineering College, Aurangabad, India

## ABSTRACT

It is study of data in the cloud and aspects related to it concerning security. Data security and private protection issues are reverent to both hardware and software in cloud architecture. This study is review of different attacks& security techniques from both software and hardware aspects for protecting data in cloud and aims at enhancing the data security privacy protection for the trustworthy cloud environment.

**Keywords :** Data Security, Cloud Computing, Data Integrity.

## I. INTRODUCTION

Cloud computing provides services over the internet, in that user can utilize the online services of different software instead of purchasing or installing them on their own computers. Data security is a major concern for users who want to use cloud computing. This technology needs proper security principles and mechanisms to eliminate users concerns. Most of the cloud services users have concerns about their private data that it may be used for other purposes or sent to other cloud service providers.

It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data. Security and privacy are the critical aspects in a cloud computing environment due to the sensitive and important information stored in the cloud for customers. The appearance of the title and author block, the appearance of section headings, document margins, column width, column spacing and other features.

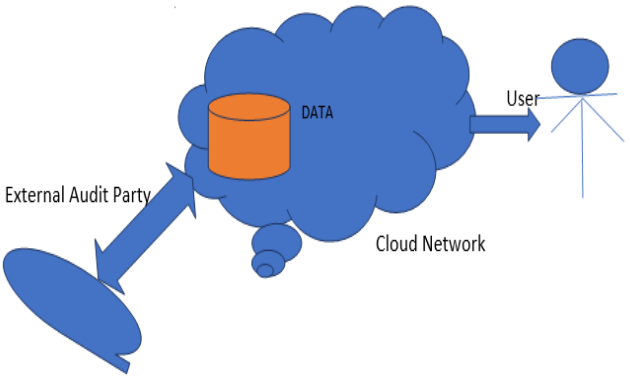



**Figure 1.** data security in cloud computing

## II. ATTACKS VECTORS ON CLOUD

As more companies move to cloud computing, look for hacker to follow. Some of the potential attack vectors criminals may attempt include following four attacks

### A] Denial of Service (Dos) attack

It is one type of attack where the attackers attempt to prevent legitimate users from accessing the service. In this attack the attackers usually send excessive

message asking the network or the server authenticate requests that have invalid return address.

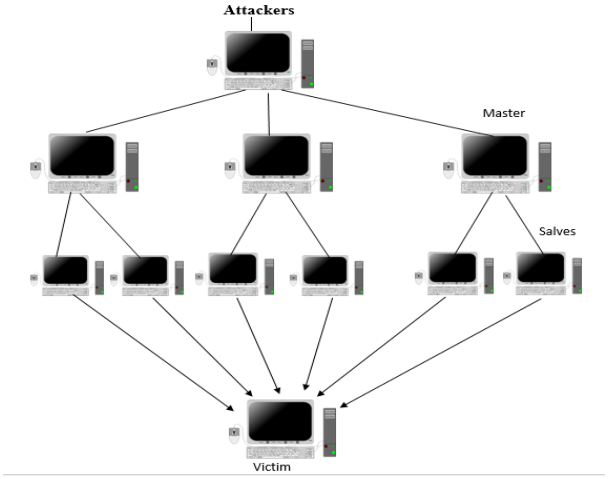



**Figure 2**

E.g.: -

1) An Attacker can target first large amount of data then they can consume the network bandwidth and resources for example UDP floods ICMP floods.
2) They can also make HTTP request in large amount data. It cannot be handled by the server for example HTTP DDOS attack DDOS attack etc.

**Security**

On the basics of authorization, we can classify the traffic for restricting DOS attack. For this firewall can be used to allow or deny the traffic on the basics of IP addresses and access protocol.

**B] Cloud Malware Injection Attack: -**

In this type of an attacker tries to inject malicious service or virtual machine into the cloud. Here hackers add an infected service implementation module such as SaaS, PaaS or a virtual machine instance ( IaaS). If the cloud system is successfully deceived, then Malware injection attacks are done to take control of a user's information in the cloud. For example, In the case of SQL injection, attackers target SQL servers with vulnerable database application.

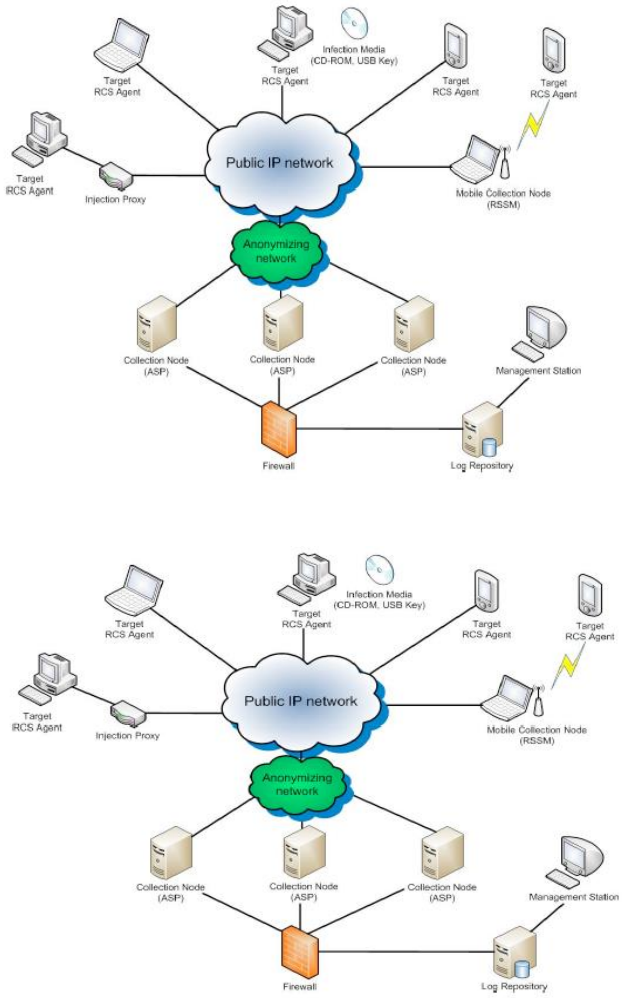



**Figure 3**

**Security**: -

To prevent the cloud from malware injection attack we can use hardware and file allocation table system for integrity purpose be it is difficult to invader in the Iaas level for an attacker.

**C] Distributed Denial of Service Attack**

When cloud computing first became popular, Distributed Denial-of-Service (DDoS) attacks against cloud platforms were largely unthinkable the sheer amount of resources cloud computing services had made DDoS attacks extremely difficult to initiate. But with as many Internet of Things devices,

smartphones, and other computing systems as there are available now, DDoS attacks have greatly increased in viability. If enough traffic is initiated to a cloud computing system, it can either go down entirely or experience difficulties.

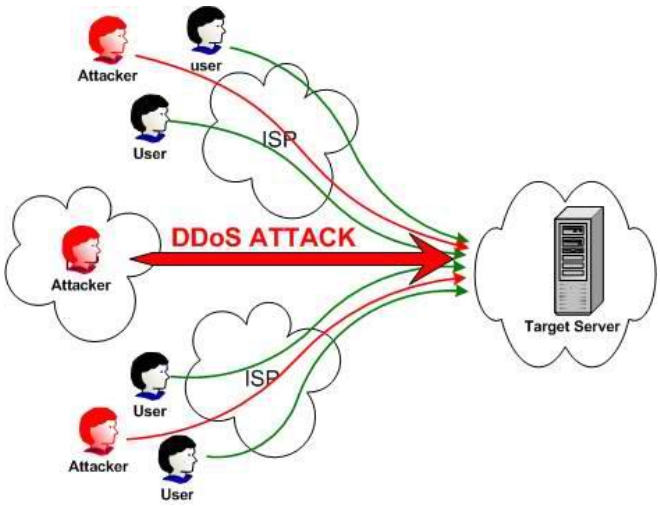



**Figure 4**

**Security Techniques**: -

1) **Challenge Response**: - here we use Effective methods using puzzle to differentiate human and bots.
2) Hidden server: - here Service is being offered authorized user while no direct connection is established with real the server.
3) **ingress Filtering**: - This process stops the incoming packets with a non-authorized source address.
4) **Restrictive access:** - Here admission control responses are prioritized for different class of user.

**Cloud services for data security: -**

The basic security services for information security include assurance of data Confidentiality, Integrity, and Availability (CIA). In Cloud Computing, the issue of data security becomes more complicated because of the intrinsic cloud characteristics.

1) **Secure data access: -**

This security service is to limit the disclosure of data content to authorized users. cloud users may need fine grained data access control in the sense that different users may have access to different set of data. This security service is applicable to most of the data objects addressed above.

2) **Security audition: -**

This service provides a way for cloud users to monitor how their data are accessed and is critical for compliance enforcement. In Cloud Computing, however, it requires the service provider to support trustworthy transparency of data access. In the case of local storage

3) **Guaranty of data: -**

This service assures that data stored in the cloud are available on each user retrieval request. This service is particularly important for data at rest in cloud servers and related to the fulfillment of Service Level Agreement. Data availability assurance is of more importance because of the increasing possibility of data damage or loss over the time.

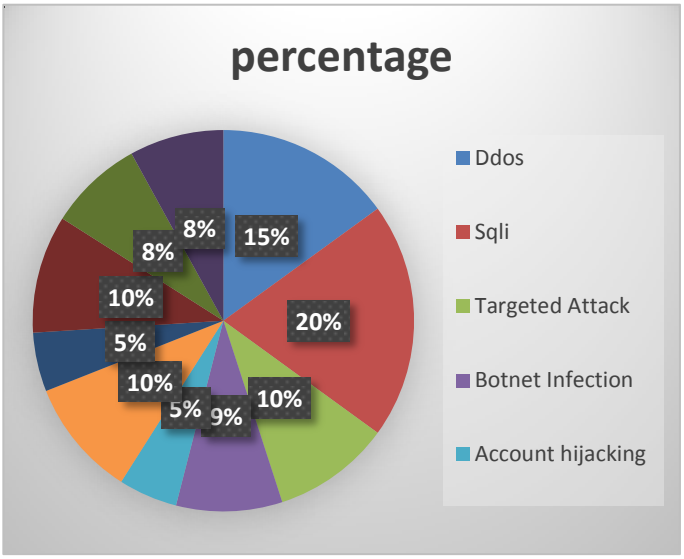
4) **Data integrity protection: -**

This service protects data from malicious modification. Such a security service would be of the core value to cloud users.it is also critical to guarantee that all the audit data are authentic since these data would be of legal concerns. This security service is also applicable to other data objects discussed above.

**Cloud Computing Attacks Statistics: -**

The results of the review are presented in this section. A year wise result representation is presented and frequency of papers with respect to sources is shown. The results are characterized with respect to the questions posed earlier.

Figure 6




| Attack Technique for 2017 | Percentage |
|---|---|
| Ddos | 15% |
| Sqli | 20% |
| Malware | 10% |
| Vulnerable wordpress | 5% |
| Targeted attack | 10% |
| Malicious | 10% |
| Local File Inclusion | 8% |
| Unauthorised Access | 8% |
| Botnet Infection | 9% |
| Account Hijacking | 5% |

## III. CONCLUSION

As cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. This paper gives a first step towards classifying them, thus making them more concrete and improving their analysis. Using the notion of attack surfaces, we illustrated the developed classification taxonomy by means of four up-to-date attack incidents of cloud computing scenarios. Being a work-in-progress, we will continue with the collection and classification of cloud-based attacks and vulnerabilities in order.

## IV. REFERENCES

[1]. Priyanka Chouhan, Rajendra Singh Jaipur Engineering College, Kukas, Jaipur, Rajasthan, India.

[2]. Robert Walters, Gary Wills School of Electronics and Computer Science University of Southampton ,United Kingdom.

[3]. Arundhati A. Dudhgaonkar Jawaharlal Engineering College, Aurangabad, India.

[4]. Mohammed A. AL Zain, Ben Soh and Eric Pardede Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.

[5]. Fazal-e-Amin Department of Software Engineering College of Computer and Information Sciences King Saud University, Riyadh, KSA.

[6]. Aized Amin Soofi, M. Irfan Khan College of Computer Science and Information studies Government College University Faisalabad, Pakistan.

[7]. Ahmed Albugmi School of Electronics and computer Science, University of Southampton, United Kingdom.

[8]. Denial Of service attack Defence Techniques.