ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

ASSESSMENT OF SECURITY ATTACKS IN CLOUD

J. Mohamed Aslam*, Dr. K. Mohan Kumar#
*Research Scholar, #Research Supervisor
PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur-613005
Affiliated to Bharathidasan University, Trichirappalli, TamilNadu, India

ABSTRACT

In cloud storage, organizations records are stored with a set of distributed links which are giving lot of information about the organization. The cloud service vendors provide essential commercial records totheir clients using cloud computing technologies. Cloud service providers send information to the unauthorized users due to many reasons. This situations created by either outside attackers or the nefarious customers. Outside attackers use several mechanisms to steal the data in cloud storage. The nefarious customers take the loopholes of cloud and access others information. In multi-tenant architecture more than one customer are allowed to access the cloud. In that scenario, some customers interrupt the other customers and steal their information for their benefits and acted as a hacker. Identifying this kind of customer in multi-tenant architecture is very difficult at present. Although cloud service vendors put more effort to face these different kinds of risks from hackers, still they are in lack on these issues. This paper analyze the consequence due to the various kinds of attacks happened in cloud service environment.

Key words: Cloud service provider, cloud services, Data breaches, DoS attacks, Phishing

INTRODUCTION

Cloud computing is the term used to store the users' information and offering hosted information over the internet. The main functions of cloud service provider (CSP) are delivery of computing storages and software programs over the internet on the basis of Pay-for-use. They are providing different kinds of cloud packages to their customers based on their requirements. Now every business organization activities and publicity depends only the cloud computing. The popular business organizations like Microsoft, Amazon, Google and so forth are doing their success through cloud computing. Many business companies move to digital by embodying their work through cloud computing. CSP give the speed, storage etc. based on the packages they are having. This revolutionary version of computing breaks the need of powerful computers, electricity and space requirements of companies. The companies can avail these structures from cloud environment by paying methodology. It reduces the massive investment of the companies. They provide their service on every day basis also. While going to cloud service,a cloud person can do within 1 hour for the existing company computing activity of 1000 hours. The companies can utilize the cloud service through the authenticated net browsers only [1, 2].

Cloud Computing services [3, 4]

The three main types of cloud computing services are as follows**.**

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software program as a Service (SaaS)

Infrastructure as a Service | IaaS

IaaS is also known as *Hardware as a Service (HaaS)*. It is one kind of service of cloud computing. In this the IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources are provided to customers.Customers access these resources via Internetbased on pay-as-per use model.Previously the hosting serviceprovider gives the IT infrastructure on rental basis for a specific period of time, with pre-determined hardware configuration.Now, the clients can

dynamically scale the configuration to meet the changing requirements and are billed only for the services actually used.In this way the maintenance cost of organization is totally eliminated. IaaS is offered in three models such as public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. It will be used only by the customer. In the case of public cloud, it is located at the cloud service provider- premise and used by more than one client. Hybrid cloud is a combination of the two in which the private cloud allow the public to use their infrastructure partially.

*Examples:*DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE).

Platform as a Service | PaaS

Platform as a Service (PaaS) provides a runtime environment to the clients. It allows client side programmers to create, test, run, and deploy their applications easily. These platform will be given by the cloud service provider on a pay-as-per use basis and access them using the Internet connection. In PaaS, back end operations are managed by the cloud service provider, so the end-users need not to worry about managing the infrastructure.

PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more). It is used to support their clients during the entire life cycle of the application.

Example: Google App Engine, Force.com, Joyent, Azure.

Software as a Service | SaaS

SaaS is also known as "*On-Demand Software*". It is a software distribution model in which services are hosted by the cloud service provider. These services are available to end-users over the internet so, the end-user do not need to install any software on their devices.The following services are provided by SaaS providers.

i) Business Services - SaaS Provider provides various business software tools to the business people.. The SaaS business tools include *ERP* (Enterprise Resource Planning), *CRM* (Customer Relationship Management), *billing* and *sales*.
ii) Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.

Example: Slack, Sam, epage, Box, and Zoho Forms.

Attacks in Cloud Computing [4,5,6]

The various kinds of attacks in cloud computing are listed below.

- Compromised credentials and damaged authentication
- Data breaches
- Hacked interfaces and APIs
- Exploited tool vulnerabilities
- Phishing, fraud, and software program
- Permanent data loss
- Insufficient diligence
- Cloud issuer abuses
- DoSattacks
- Account hijack
- Malicious Insiders
- Shared technology, shared dangers

Compromised credentials and damaged authentication: When the hackers damages the authentication, then any one can access the other information without any key. In some organization, they assign unnecessary data privileges to anyone for ease the access management. Sometimes the organizations also forget to remove user access when an employee's job function changedor they

leave the organization. That time the unauthorized person may damage the authentication. In this case, the organizations should use multi-factor authentication, phone-based authentication, and smart cards (digital tokens) to protect the access from the cloud.

Data breaches: Cloud environment faces similar kind attacksfor the enterprise data they are having.A cloud service provider is storing large amounts of data belonging to multiple enterprises. The threats are also magnified by significant proportions. The severity of damage depends upon the kind of data that is breached. The breached data may be health records, trade secrets or financial data. When a data breach occurs, companies may incur fines, and face lawsuits and criminal charges. More than monetary impact, reputation loss can affect organizations for many years. In this case it is important to adopt Data Loss Prevention tools as a part of cyber security plan as it will help IT department monitor and control the data sharing activity across endpoints and get alerts of any suspicious data movement.

Hacked interfaces and APIs: Almost all cloud services now provide APIs (Application Programming Interface). APIs are required by organizations to manage and interact with the cloud service they are using. Therefore, the security of the cloud service largely depends on the security of APIs. These are the most vulnerable part of attacking system because they areaccessible via the Internet. In this case designing strong attack modeling of system with secured architecture and verification of data flows in various levels will complicate the access of data using APIs.

Vulnerabilities through Malicious software: In cloud vulnerabilities are also done using malicious-software. These software exploitsmore number of bugs into the applications what they are providing to the users in cloud computing. This software also attacks the storage space of agencies by inserting bugs. So, protecting the cloud by using some strong anti-software tool will be helpful to avoid these kinds of attacks.

Phishing fraud through software program: In this kind of attack, the attackers steel user's login credentials, financial information such as credit card or bank account details or companies valuable data. These attackerslistens the activities of companies and watch the important data and do assaults through the software. Normally these phishing attackers enter into the cloud through mail. So, the cloud management should be more careful to view these kinds of fraud messages [16].

Permanent data loss: Hackers enter inside the cloud and delete or damage the business data permanently. In this case the business data should be stored in more than one zone. Also the data should be stored with encryption. In this case the hacker cannot identify the data without encryption key, easily.

Insufficient diligence:Many organizations are embracing the cloud technology without fully understanding its environment and the myriad risks associated with it. Many times, they fail to scrutinize the contract made with their cloud partner and are not aware of the provider's liability in case of a data breach. In this case understanding their requirements from cloud computing services and selecting the right cloud service provider with reviews of their contract to understand the responsibilities and liabilities will avoid the security risks.

Cloud issuer abuses: Sometimes the worst cloud service provider itself do some abuses to their customers by giving their valuable data to some other people. In this case the data should be stored with encryption techniques.

DoSattacks: DDoS (Distributed Denial of Service) is a cloud-specific attack in which attacker sends more packets with large data using multiple machines attacks. Such attacks make the resources unavailable to the user by overwhelming the network with unwanted traffic.

Account hijack: Account or service hijacking remains a serious security threat in the cloud services. Account hijacking occurs when a criminal obtains the personal data information and uses that to take over all accounts (bank account, e-mail account or social media account).

Malicious Insiders : Malicious insiders can be employees, former employees, contractors or business associates who have legitimate access to the systems and data, but they use that to destroy data, steal data or sabotage data in cloud computing.

Sharedtechnology and shared dangers: Cloudcomputing is a shared technology in which the computing resources are shared by many users. If the resources are shared by other people those who are not related to that particular data, security risks will occur even though they are registered users.

This paper analyze various kind of attacks happened in the last few years, loss of money through those attacks and depicts what kind of attack happened mostly.

LITERATURE REVIEW

NehaAgrawal & ShashikalaTapaswi (2019) discussed about the various DDoS attacks which reduce the capabilities of cloud computing. They analyzed the problems in low-rate and high-rate cloud providers. The author identified that in low rate purchase the DDoS attacks happened frequently. They gave some solutions to face these kinds of attacks[7].

Thirumaleshwari Devi B et. al. (2020) explained about the several attacks in cloud computing like Wrapping, Browser Malware-Injection and Flooding attacks etc… These mentioned problems occur while checking the accountability. They mainly focused on Honey pot attack happened through security breaches. Finally they analyzed account and its intrusion policies in honey pot attack[8].

M. SwathyAkshaya and G. Padmavathi (2019) discussed about the various cloud attacks using viruses and worms by the hackers and cybercrimes. Attackers are capturing private records, interrupt services, and motive harm to the corporation in cloud computing network. They provided a better solution in a scientific manner of information, identifying, and addressing protection risks from Existing taxonomies. This paper affords an outline of conceptual cloud assault and given better evaluation taxonomy[9].

Mohammad Abdelkareem et. al. (2020) explained about the DDoS issues in cloud computing. Attackers are copy the valuable data from the cloud computing server side or delete the valuable data. This paper mentioned numerous protection mechanisms for protecting DDoS. The important goal of this paper is to assess distinct mechanisms that assist to guard DDoS attacks. This paper highlights the significance of statistical anomaly and provides the tactics for detecting DDoS attacks[10].

Nalini Subramanian&Andrews Jeyaraj (2018) discussed about the benefits of cloud computing to the customers and organization in phrases of capital expenditure and financial savings in operational expenditure.Sometimes the consumers faced a lot of loss due to the lack of essential function consequences with inside the poor effects of the computing archetype. This leads to personal, ethical and economic harm to the organization[11].

This paper recognizes and discovers the safety demanding situations which might be confronted via the way of means of cloud entities.

MATERIALS AND METHODS

Data collection

In this analysis the worldwide most commonly happened attacks in cloud such as Malware, Ransomeware, Phishing, DDos and Data Breacheswere collected for the years 2015 to 2021 from various authenticated web resources[12, 13]. The following Table 1 gives the loss of different kinds of attacks type wise and year wise.

Table 1: Worldwide cloud attacks in year wise

Year	Type of attack	Loss (in billions)
2015	1 Malware	8.2
	2 Ransomeware	5.5
	3 Phishing	6.5
	4 DDos	3.2
	5 Data Breaches	10.1
	Total	**33.5**
2016	1 Malware	7.9
	2 Ransomeware	6.38
	3 Phishing	7.3
	4 DDos	4.8

	5 Data Breaches	12.1
	Total	**38.48**
2017	1 Malware	8.6
	2 Ransomeware	1.84
	3 Phishing	8.2
	4 DDos	5.1
	5 Data Breaches	14.2
	Total	**37.94**
2018	1 Malware	10.5
	2 Ransomeware	2.024
	3 Phishing	8.7
	4 DDos	6.9
	5 Data Breaches	15.5
	Total	**43.624**
2019	1 Malware	9.9
	2 Ransomeware	1.879
	3 Phishing	9.1
	4 DDos	8.1
	5 Data Breaches	16.3
	Total	**54.379**
2020	1 Malware	5.6
	2 Ransomeware	3.04
	3 Phishing	10.2
	4 DDos	9.3
	5 Data Breaches	16.8
	Total	**44.94**

Methods

The prediction of loss due to various kinds of is calculated using the linear regression formula [14] as given below.

$$Y = a + bX$$

$$b = \frac{N\sum XY - (\sum X)(\sum Y)}{N\sum X^2 - (\sum X)^2} \qquad a = \frac{\sum Y - b\sum X}{N}$$

Where,
N = number of observations, or years
X = a year index (decade)
Y = population size for given census years

Figure 1: Linear Regression formula

The percentage of each category of attack is calculated using the formula [15] give below.

$$P = \sum_{i=0}^{m} A \Big/ \sum_{j=0}^{n} E$$

Figure 2: Percentage calculation formula

Here, ‘P’ represents percentage of each category, ‘A’ represents sum of all kind of attacks range starts form 0 to m, and ‘E’ is sum of each kind of attacks, range starts from 0 to n.

RESULTS AND DISCUSSION

The following Table 2 shows the total loss in year wise. Even though it is not gradually increased, in total it is in increasing rate.

Table 2: Loss amount - year wise

S.No	Year	Loss amount in billions
1	2015	33.5
2	2016	38.48
3	2017	37.94
4	2018	43.624
5	2019	54.379
6	2020	44.94

The following Figure 3 clearly explains the growth of loss due to various kinds of attacks worldwide in various years.

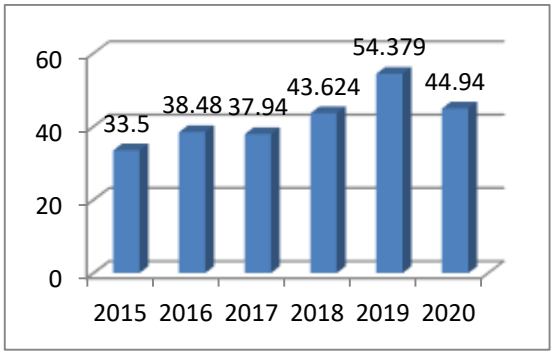

Figure 3: Loss amount in billions

Prediction

By applying the linear regression formula the prediction of loss in the year 2025 is calculated. The result is depicted in the following Table 3.

Table 3: Year and loss amount prediction

S.No	Year	Loss amount in billions
1	2015	33.5
2	2016	38.48
3	2017	37.94
4	2018	43.624
5	2019	54.379
6	2020	44.94
..	..	..
11	2025	81.663

The following Figure 4 represents the expected growth of loss in the year 2025 using the content of the above Table 3. So, this growth should be controlled anyway to minimize the loss in future by implementing new techniques or methodologies.

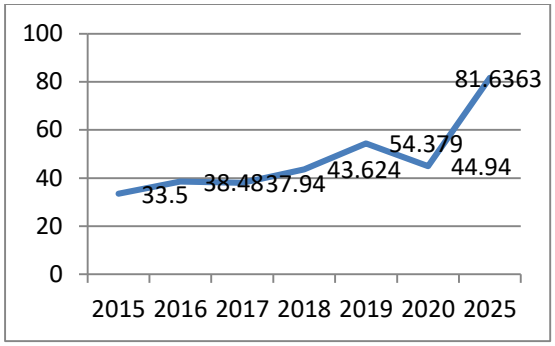

Figure 4: Year wise loss amount in billions

Percentage

The following Table 4 shows the total loss in billions in each category of attack. Here the percentage is calculated by the total loss in each category divided by the total loss of all categories.

Table 4: Percentage of different attacks

Type of attack	Loss (in billions)	%
Data Breaches	85.0	34.87
Malware	50.7	20.80
Phishing	50.0	20.51
DDos	37.4	15.34
Ransomeware	20.663	8.48

The following pie graph mentioned as in Figure 5 shows the above table's content graphically.

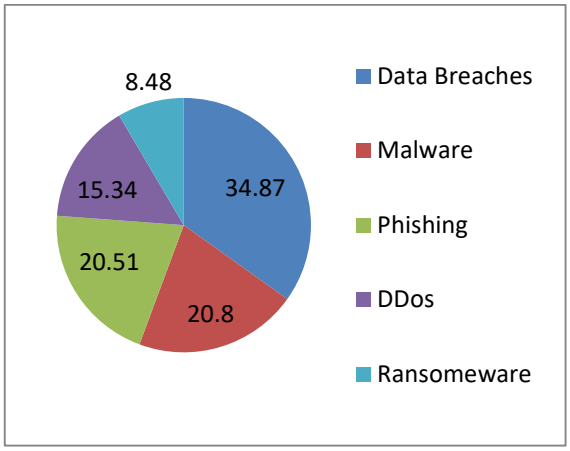

Figure 5: Percentage of different attacks

In this data breaches occupies 34.87%, malware occupies 20.8% and phishing occupies 20.5%. These three categories plays major role in cloud attacks. So, the necessary action should be taken to control these attacks.

CONCLUSION

Cloud computing is built for built for present and future generation for its various service with minimum investment of cost and accessed through internet. This technology used to reduce the investment for the beginners. While going for shared technology for its clients, many problems are accruing due to different kinds of attacks. In that major attacks are done through

data breaches attack, malware attack and phishing attack. So, this kind of attacks should be controlled by implementing new techniques or updating in the existing techniques at some extent.

REFERENCES

1. Michael Armbrust, Armando FoxandRean Griffith, Anthony D. Josephand Randy, H. Katzand Andrew Konwinski, Gunho Lee, David A. Pattersonand Ariel Rabkin and Ion StoicaandMateiZaharia., "Above the clouds: A Berkeley view of Cloud Computing", *UC Berkeley Reliable Adaptive Distributed Systems Laboratory*, February 10, 2009, pp: 1-23.
2. Lizhe Wang, Jie Tao andKunze M, Castellanos A.C, Kramer D and Karl W,"Scientific Cloud Computing:Early Definition and Experience", *10th IEEE Int. Conference on High Performance Computing and Communications*, Dalian, China, September, 2008, pp: 825-830.
3. Xiaojun Yu and Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle," *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference*, 10-12 December 2010, pp:1-4.
4. Kangchan Lee, "Security Threats in Cloud Computing Environments,International Journal of Security and Its Applications", *International Journal of Security and Its Applications*, Vol. 6, No. 4,October 2012, pp: 25-32.
5. Sachin Kumar Singh and Devendra Kumar Singh,Cloud Computing: Security Issues And Challenges,International Journal of Advances in Engineering & Technology,Vol. 10, Issue 3, June, 2017, pp: 338-343.
6. Danish Jamiland Hassan Zaki, "Security issues in cloud computing and counter measures", International Journal of Engineering Science and Technology, Vol. 3 No. 4, April 2011, pp: 2672-2676.
7. NehaAgrawal and ShashikalaTapaswi, "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges", IEEE Communications Surveys & Tutorials, Volume: 21, Issue: 4, Aug 2019, pp: 3769 – 3795.
8. B. Thirumaleshwari Devi, S. Shitharth and M A Jabbar, "An Appraisal over Intrusion Detection Systems in Cloud Computing Security Attacks", *2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) IEEE Xplore*, April 2020.
9. M. SwathyAkshaya and G. Padmavathi, "Taxonomy of Security Attacks and Risk Assessment of Cloud Computing", Springer Nature Singapore Pte Ltd, 2019, pp:37-59.
10. Mohammad Abdelkareem, Alarqan1 and ZarulFitri Zaaba1 and AmmarAlmoman, "Detection Mechanisms of DDoS Attack in Cloud Computing Environment: A Survey", *Springer Nature Singapore Pte Ltd*, 2020, pp:138–152.
11. Nalini Subramanian and Andrews Jeyaraj, "Recent security challenges in cloud computing", Computers and Electrical Engineering: Elsevier Ltd, June 2018, pp :28-42.
12. https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide
13. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide
14. Sarah Boslaugh, "Statistics in a nutshell: A desktop quick reference" , *O'Reilly Book publishers*, Second edition, 2012.
15. S.C. Gupta and V.K. Kapoor, "Fundamentals of Mathematical statistics", *Sultan & Sons book publishers*, Twelfth Edition, 2020.