Mahratta
Multi-Disciplinary Journal
ISSN No- 2581-9879 (Online), 0076-2571 (Print)
www.mahratta.org,editor@mahratta.org

Cloud Computing - Threats On Cloud Storage

Vaidehi A. Shete
shetevaidehi.95@gmail.com,

Prof. Shruti Gosavi
shruti.gosavi@tmv.edu.in
Department of Computer Science
Tilak Maharashtra Vidyapeeth, Pune.

Abstract:

Now a day in the cloud computing industry and in companies that tend to place their data on the cloud is becoming increasingly popular. IT firms feel that clouding is a major trend in their IT networks, and this increasing situation has been witnessed all over the world. Increased productivity, reduced costs and flexibility are some of the cloud benefits. Nevertheless, the basic fact is that the cloud has several disadvantages, like every IT system. The data can move and lie in the cloud world to be accessible and trustworthy and avoid user information. Several factors need to be taken into account when it comes to cloud security and privacy, yet many IT companies are fast to adopt cloud technology without addressing these issues into consideration. However, cloud service providers face problems and risks in cloud storage due to excessive data use. In recent years, security problems, such as unauthorized access, data loss, infringement of data, and account hacking have been recorded. Service providers and professionals conduct research to address these problems. This extensive research paper aims to include what are the cyber threats on cloud storage? How to avoid these attacks with the help of cyber expert-who has deep knowledge in cloud security. I reviewed Google's survey and some articles relating to cloud security in order to achieve this goal.

Keyword: Cloud computing, cloud storage, cloud security, cyber threat, cloud service provider.

I. Introduction

Cloud Computing:

Cloud computing becomes a growing term and technique in the computer industry. Cloud computing is a modern technology that allows easy access to data via internet infrastructure computing. By using frequent users, their storage system information is typically processed [5]. An program or software that takes up space on traditional hard drive storage must be installed to carry out operations such as data processing. Often customers believed it was always difficult to move their storage devices. You seek alternatives for the transportation of your files and large volumes of data and for access to information everywhere. Cloud computing is the solution for these consumers. In addition to individual users, many businesses are seeking to outsource their information to other business locations. Cloud computing gives flexibility, such as how far it is paid for, to personal storage devices. Users can access and save different apps and services using an internet-appointed gadget.

Major companies such as Google, Amazon and Microsoft are helping many customers to create and enhance cloud technology and services. The successes of companies listed above, such as Microsoft, Amazon, etc., have recently encouraged new companies to become increasingly competitive with many cloud companies. In addition, various cloud computing services are added, including SaaS, PaaS, IaaS and more. [4,5] It is not just accessible on request to attract million consumers from specialist services and from other packages such as pay-as-you-go. However, a large number of clients feel that the benefits given by cloud services require consideration and the creation of applications or the use of cloud services. There have been so many studies anticipating cloud growth, millions of customer’s adoption and expansion of various providers that offer advantages to both users and providers. Therefore, cloud computing is not only a word for computers, but for ordinary consumers of computing.

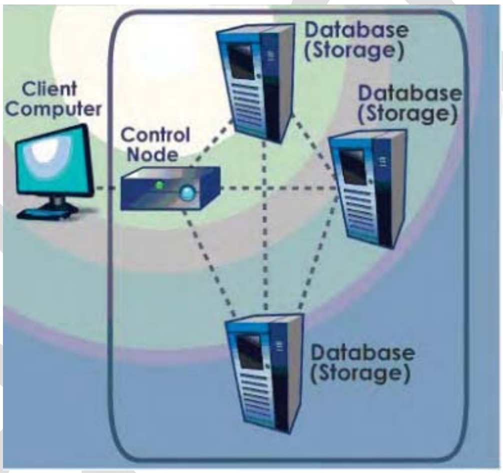

Figure: Cloud Storage System Architecture [4]

Cloud storage: Cloud storage is a service paradigm that usually offers remote backup, administration and internet access. Users pay for their cloud data storage often per gigabyte or month. For cloud storage firms, is data backup, disaster recovery, archiving, DevOps most frequently used for this purpose. [8]

How cloud storage works: Some of the options for cloud storage exist, while others are available to digital data of all kinds. Some little cloud operating system, while some are so big that the mechanical equipment consumes a full warehouse. The region where cloud storage systems are operated is considered the basic level of data centers where one data violation is enough for a cloud storage system. An internet copy of the files from a customer subscribing to the cloud storage will be sent to the Data Server, and cloud storage data is then entered. If the client wishes to get the information, he can visit the data server via a web-based interface. The server either returns the file to the client or lets the client find and manage the files on the server itself. Cloud security relates to network security, computer security, and data security. Losses of governance [11, 15 and 16] are a major danger for cloud security. Customers and suppliers can share responsibility for various components of cloud security, but the policy must specify this. There are numerous concerns with customer security and providers in the move from local computing to distant computing. The trustworthy third party provides a number of cloud services which lead to new safety issues. The cloud providers provide online their services and use numerous web technologies to generate new security issues. In short, the future cloud will be stronger and stronger than ever before. Complex, automated and more sophisticated cloud safety driven by advances in IT, engineering, quantum computing and other transformative technologies. [15,16]

Objective of the Study:

- Current threats and ways to prevent the cloud.
- Through this survey, we learn about the many assaults that have occurred thus far.
- This article highlighted the need of maintaining a solid cloud security position that enables companies gain well known advantages of cloud computing.

II. Different Types of Security Challenges In Cloud Computing

The main security issues of any firm are increasing attacks on stolen private data. The perceived loss of control over the corporate data is another key obstacle to widespread acceptance by the cloud. The Cloud Security Alliance (CSA) report describes the major security issues that the IT sector has to address via cloud technology. [2, 7]

Data security: The most important problem is data security. The major targets and victims of data breach are cloud service providers. Any unauthorized party is here susceptible to sensitive information. [2]

Non-compliance with regulatory mandates: The second question is how compliance with regulations is guaranteed when data is maintained on the cloud. If the regulations are not complied with, there may be considerable money loss, criminal fines, legal proceedings, and corporate loss.

Loss of control: The data is available in many administrative sectors; therefore companies fear that their data will be lost control. For comprehensive data management, it must be transmitted to the service provider. The firms have to rely on and trust the service provider.

Expertise of IT and business managers: All IT and business personnel must be able to shift to cloud computing with the technical ability. We need further experience in negotiations with and benefitting from the firm of the SLA cloud service providers.

Compromised accounts or insider threats: 92 % experience an issue with affected accounts passwords through darknet according to survey. There are also significantly higher levels of insider risks.

Disaster management: The second big issue is data retrieval if the supplier quits the organization unexpectedly. There should be an extensive disaster recovery strategy for the company not to lose all data and detect alternate data storage.

The following problems need to be solved before using cloud technology for any firm.

SECURITY ISSUES:

The Internet is an infrastructure for communication utilized by a cloud provider's well-established TCP/IP protocol that identifies IP addresses of users on the Internet. Like an actual IP address on the Internet, an IP address is likewise included on the Internet virtual machine. You may also find this IP address for a malicious user, internal or external, like a genuine user. In this case, the actual server the victim uses can be determined by malicious individuals using a malicious virtual machine. Because all users using the same virtual machine as an infrastructure are able to access all users' data if a hacker robs or controls the virtual machine. So the hacker can move them into its local system before the cloud provider realizes it's not in place. Then the hacker can reveal vital data when examining the data. [2,15]

1) Attacks in cloud

A lot of IT assaults are presently ongoing. As the cloud offers service to legal consumers, it may also serve malicious people. A cloud hacker can host harmful software, which might be a cloud attack or a cloud user. For instance, if a victim knows that his victim uses a typical cloud provider, an attacker can utilize the same cloud provider to plan an attack on his victim. The attackers as well as the victim are on the same network, but they do not really use a real network but they use virtual computers. That is a comparable case.

a) DDoS attacks against Cloud

Distributed denial service (DDoS) assaults frequently focus enormous amounts of IP packets on some components in the input network; hardware that works on a blacklist is overridden quickly and is out of service. DDoS attacks may have a considerably greater impact in the cloud computing than just single tenured systems, because an important number of customers share the infrastructure. If you don't have the capacity to deliver services to your consumers, unwelcome DDoS attacks may occur.

This method is a standard strategy that enhances the number of vital resources. However, when a rogue individual has deliberately attacked bot-net with a DDoS, the major problem is.

Many network countermeasures cannot be protected against DDoS assaults as they can't prevent traffic flooding and generally cannot discriminate between good and bad traffic. Intrusion prevention systems (IPS) are effective when attacks have been identified and signatures are existing; nonetheless, their content is lawful or with malevolent intents. Intrusion Prevention Systems (IPS).Such firewalls are, sadly, vulnerable and ineffective in DDoS attacks as IPS solutions, because an attacker can quickly bypass firewalls and IPS because they can handle legitimate traffic and generate traffic attacks on a number of different hosts in order to prevent traffic from being managed via a server or its cloud connection.

It is maybe more accurate that DDoS prevention is not server virtualization, but part of the virtualization layer of the Network. For example, spoofing in the ARP network can be defeating virtual machines-having cloud systems, which involve layer security via multi-computer networks, firewalls, and load balancing. [1]

b) Cloud against DDoS attacks:

In particular in botnet operations using a large variety of zombie machines, DDoS assaults are among the world's most serious hazards. A big packet flood is transmitted from multiple sources to a Web server when a DDoS assault is begun. In this scenario, the cloud can form part of the solution. Notice that DDoS websites that have server resource restrictions might utilize Cloud to withstand these attacks. It is important to note this. On the other side, cloud technology offers the flexibility to deploy resources almost quickly to prevent website collapse. [1]

III. Analysis

Threats on cloud storage

1.Data breaches

Any event involving confidential or sensitive information without consent is an infringement of the information. Violations are created by a cyber-attack in which thieves have unlicensed access to a network or a computer system have stolen private, sensitive, or confidential, personal and financial data contained inside them. Typical cyber hazards include extortion, data loss and denial of information in data violations.

Analysis:-

Adobe:-Adobe originally reported that hackers have stolen nearly 3 million encrypted customer credit card records, as reported in early October 2013 by security blogger Brian Krebs, plus login data for an unknown number of user account. The report says over 150 million usernames and hashed Adobe password pairs. The investigation shows user identification, passwords, credential information.

Canva: Canva is an Australian graphic design tool website. According to sources in May 2019, 137 million of users were attacked, with email addresses, usernames, names, cities of residence and crypto passwords exposed and hacked (for users who do not use social logins — around 61 million). Canva discovered the assault and shut down its server infringement.

E-Bay:In May 2014 a hack disclosed its full bank account information of 145 million customers, including names, addresses, dates of birth and cryptographed passwords, an American multinational e-commerce business, e-Bay. The online auction company claimed hackers have accessed its network using credentials of three companies and had full access over 229 days – time to jeopardize the customer database. If the firm knows the threat at the time, it asks consumers to update their security passwords.

Bigbasket: BigBasket, a prominent online food company in India, experienced a huge data break in October, which exposed data of 20 million members. The infringement took place on 14 October, and made public on 7 November when personal data such as complete names, email addresses, date of birth and IP addresses of user devices were compromised and put for sale via the dark web. The infringement happened according to sources.

LinkedIn: LinkedIn has become an appealing offering to attackers who want to engage in assault on social engineering as the main social network of business people. However, leakage of user data in the past has also been affected.

In 2012, the firm said 6.5 million related passwords were stolen and released on the Russian Hacker Forum (unsealed SHA-1 hatches). The whole nature of the tragedy was not, however, known until 2016.The same hacker that sold My Space information was found to offer almost 165 million LinkedIn members' email addresses and passwords for only five bit coins (about 2.000$ at the time). The same hacker was identified to provide My Space data. LinkedIn said it was notified of the infringement and stated that the impacted accounts have reset their passwords.

Sina Weibo:-Sina Weibo is China's response to Twitter with more than 500 million users. In March 2020, however, genuine identities, website usernames, gender, location and – for over 172 million people – telephone numbers on black market were published. Passwords were not included, indicating why just €1,799 ($250) was available for the data (INR18,554.85)

Weibo admitted that the company's data were sold but said that the data were obtained by matching contacts with its API address book. It also says consumers should not be worried since they don't save passwords in plaintext. This does not, however, reflect that some of the information, such as location data, is not available through the API. The social media giant reported notifying the authorities and the Ministry of Industry and Information Technology's Chinese Cyber Security Administration stated it is investigating.

Companies	Month-year	User data affected(in millions)
Adobe	Oct-2013,Aug-15	153
Canva	May -2019	412
e-bay	May-2014	145
Linkedin	2012-2016	165
Bigbasket	2020	20
Sina Weibo	2020	538

Preventions:

- Authentication multi-factor – The user has to submit more than proof of identification and access authorisations. For example, type in your password and receive a notice with an active single-use number string randomly created over a short period of time on a cell phone. It's now one of the standards for cloud security.
- Encryption Data-at-Rest. Data-at-rest is a form of data saved but not actively used on various devices on the system. This involves logs, databases, and datasets and so on.
- Percentage of firewall between private and public systems that regulates system traffic; internal firewall for traffic monitoring and anomalies in allowed traffic.

2. Denial of service

Cloud companies have security challenges digitally to ensure consumers are safe from harmful websites due to the overuse of cloud apps. During a DoS assault, the system resources are diluted. Because of the shortage of resources leads to different speeds and issues with general stability. Sometimes, the program is running slowly or cannot be properly loaded. It appears like users are being picked up in a gridlock. The company commits itself to more efficiently discovering and neutralizing the causes, as well as to spending resources.

DDOS attack: Distributed denial of service attacks are a cyber-assault that overloads or disrupts network services through access requests. The hacker behind DDoS delivers malware to several computers and may remotely control certain (or all) of the system's functions when successfully installed in order to conduct the assault.

Analysis:

Amazon Web Services (AWS):- "Amazon announced that its AWS Shield service has neutralized the greatest ever recorded DDoS assault and ended a 2,3-Tbps onslaught," says a February 2020 report by ZDNet. Before this assault, a record of 1,7 Tbps (Terabits per second) for the most recorded DDOS attack replaced the record for the next GitHub attack.

The ZDNet report doesn't name the AWS client, but it mentioned "three days of 'high threats' to [Amazons] AWS Shield personnel were attacked by hijacked CLDAP web servers." This CLDAP is a protocol to log, search and change shared directories on the internet for Connection-less Lightweight Directory Access Protocol.

ZDNet further states that "the servers of CLDAP are recognized as a 56 to 70 times largest initial DDoS travel extension," which "are misused for DDoS assaults since the end of 2016."

GitHub:GitHub has been utilized by millions of developers as a popular online code management tool for heavy traffic. The record of 1,3 Tbps of traffic that overwhelmed its servers with 126,9 million packets each second was not prepared. At the time, the attack was the largest DDoS assault, yet just 20 minutes were taken down by GitHub. This is mainly due to the fact that DDoS was used by GitHub to identify the assault and take rapid actions to reduce its damage.

The GitHub assault did not cover botnets, unlike a number of recent DDoS operations. Rather, the DDoS attachers have utilized the so-called memcaching method to transmit a faked request to a susceptible server, which subsequently inundates a target victim with amplified traffic. Memcached database is used to accelerate web sites and networks, however recently DDoS attackers have been armed.

Dyn: Dyn, a major DNS provider, was vital to the Netflix, PayPal, Visa, Amazon and The New York Times network architecture. Unidentified hackers established a vast botnet using the virus Mirai to perform what was the biggest documented DDoS assault at that time. The attack has been significant, as several Dyn clients find Dyn's servers to be paralyzed by DNS problems. While the problem has been resolved and service resorted before the end of the day, the fragility of network infrastructure is frighteningly reminiscent.

BBC:-A 600 Gbps attack was conducted by the organization "New World Hacking" on the final day of 2015 with their BangStresser application tool. For almost three hours, the attack seized the BBC sites, including the on-demand iPlayer service. Apart from the fact that the tool used to boot it was used by two Amazon AWS servers to really employ cloud computing resources. It was the greatest DDoS assault record at that time but it was noted most of the BBC attack. The idea that DDoS attackers found a method to use the bandwidth of a public cloud computing service to power their assault was particularly alarming for IT security professionals who had long trusted Amazon's reputation for protection.

Companies	Month-Year	Attack (in Terabits per second)	Impact
Amazon Web Service(AWS)	Feb-2020	2.3tbps	hijacked CLDAP web servers
GitHub	Feb-2018	1.3tbps	Due to high traffic and usage, flooded its servers
Undisclosed NETSCOUT client	Mar-2018	1.7tbps	memcached reflection/amplification attack
Dyn	Oct-2016	-	Malware-mirai attack
BBC	Dec-2015	600gbps	Attack on the BBC site

Preventions:

- Intrusion Detection System Up-to-date. Anomalous traffic should be recognized and early warning should be provided based on credentials and compartmental characteristics. It's a break-in alert for cloud security.
- Firewall Traffic Type Inspection functions for inspection of incoming traffic's source and destination, and evaluation of probable type using IDS technologies. The function helps to resolve good and bad traffic and quickly eliminate harmful traffic.
- Source Rate Limiting - one of DoS's key objectives is bandwidth consumption.
- It helps to keep the issue under control if IP addresses are blocked as a source of an attack.

3. Insecure API:

Cloud providers give their APIs to enable developers to construct the app to connect to their cloud. The developer community may make them available and can be used easily. However, the provided APIs were determined to be not cloud-protected enough as needed. This vulnerability has been detected by third parties utilizing Cloud APIs. False APIs so expose many attackers to the cloud. The communication between apps is the vulnerability of an API. Despite the possibility of programmers and corporations, they are also left behind vulnerable security issues.

4. Malicious insiders:

Any company's insider threats are a major safety concern. A malicious insider has already provided access and some of his essential resources to a company's network. Attempts to achieve these levels show that a hostile inside for an unprepared organization is difficult for most attackers to identify. A hostile insider is more difficult to uncover on the cloud. Cloud deployments reduce the efficiency and control of many of the traditional security solutions. This, in turn, makes it harder to detect harsh insiders, as cloud-based technology is easy to access from the Internet and is normally misconfigured.

5. Misconfigured cloud storage:

False cloud storage services are common in the vast majority of cloud deployment. Cloud malfunction is a set-up susceptible to cloud server infringements (for saving or computer reasons).The results were made by security operators Accuracy who claim that 93 percent in their present DevSecPos condition of cloud installations have been examined and that most of them have a networking exposure of at least one where a security group remains open. Control of server access and cloud security data availability standard, Incompliance with access management—if an unauthorized person access to sensitive information unintentionally. Access to altered data- When private content aren't available and no permission are required.

Prevention: Many third-party programs such as cloudsploit can monitor the scheduled status of security settings and discover problems before it is too lengthy.

6. Insider threats:

The threats of trusted insiders, like with local systems, are severe in the cloud. Anyone who does not have to break past the defenses of a corporation for access to its systems may be current or former workers, contractors or trustworthy business partners. An insider does not have to be malevolent in order to inflict harm; he might involuntarily endanger data and systems. CSA cites Cost of Insider Threats 2018 from the Ponemon Institute which says that 64% of all insider events recorded were attributable to carelessness of employees and contractors. That failure may involve misconfigured cloud servers, the storage of sensitive data on a personal device, or a phishing email victims.

IV. Solution Against Cloud Security Problems

There are a number of traditional methods to reduce security issues in the internet environment as cloud architecture, however the cloud is particularly vulnerable to security flaws in the cloud. Standard countermeasures for significant Internet security concerns are also offered for cloud use, although some of them need to be improved or modified properly in the cloud.

Access Control: Access control mechanisms are mechanisms meant to ensure authorized users may access and prevent unlawful access to information systems. Formal mechanisms should thus be in place to regulate the allocation of access rights for information systems and services. The procedure should include all user access cycle phases from the first recording of new users through the eventual break-down of user access systems and services that no longer need access. When appropriate, extra attention should be made to distributing privileged access privileges, which enables users to avoid system checks. In order to guarantee the effective administration of access control, the following six control statements should be considered:

1. Control access to information.
2. Manage user access rights.
3. Encourage good access practices.
4. Control access to network services.
5. Control access to operating systems.
6. Control access to applications and systems.

The cloud provider usually administers all parts of the SaaS models' network, server and applications architecture. As a service given to end users under this paradigm, network-based monitoring is typically less essential via a web browser and is supplemented or replaced with user access limitations such a single password authentication. The customer's priorities should thus be user access control (authentication, federation, privilege management, provisioning, etc.) to protect SaaS-hosted data. [8]

In the PaaS delivery model, the Cloud provider is responsible for the management of the network, servers and application platform access control. Nevertheless, the customer is responsible for managing access to PaaS programs. Application access control is enduser access management that provides and authenticates users. Application access control IaaS customers are responsible for all access control components in cloud management. The clients will need to access on-line servers, virtual networks, virtual storage, and apps on an IaaS platform for customer design and management.Access management is part of an IaaS delivery model in one of the next two categories. Host, network and management apps must be managed in a cloud provider and user control system by controlling access to its virtual server, VSS, virtual networks and virtual server applications. [1,4]

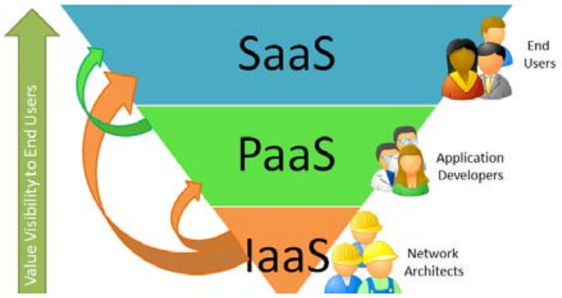

Figure. SPI model with services (Source-http://cloudcomputingarena.blogspot.com)

Cloud Storage Security:

In this section, we outline the life of the data cycle and the procedures necessary to guarantee that it is carried out at all times. The second section gives an overview of novel data security technologies that have been offered in Cloud in recent years.

A. Data Cycle life security:

The life cycle of the datas is: data are first sent to the cloud and stored, and finally recovered and removed. At each stage of this life cycle several actions may be done for ensuring data security, as indicated below.

Data transfer: Data from internal systems or local users of the firm is transmitted to the cloud. At this level, security is not a major concern because the technologies employed are trustworthy such that data may be encrypted in advance. Include a transport layer that has this encryption function as another means of employing one of two prevalent ads, IPSEC and SSL, to securely transmit data to the cloud.

Storage phase: When the data is submitted, it is automatically stored. According to some publications, the cloud storage architecture is a layered design that consists of a front component with an API for storage access. Here you may also find the front ends, files and other typical web service components (such as Internet SCSI or iSCSI). The front end of the storage is a logical layer (internal software). This layer offers numerous features, including replication and data decrease in typical data placement procedures (considering the geographic location).The back of the system stores the physical data. Despite the speed of this design, the security module is considerably more sophisticated, which is why customers are concerned about the data they save. Some cloud-based data security solutions have been proposed, such as encryption, access control, authentication or security as a service module.

Use of Data: Data is kept and available at this level for cloud usage. Security of data is based on established control methods of access to data: This applies to both external and cloud administrators and operators' access. It is important thus to trust your source when you store your data, irrespective of the data format (files, pictures, applications, etc.).

Destruction: It is important that data in the cloud be preserved in the owner's life and removed from the cloud. The supplier shall delete all data traces. The previously employed encryption methods help to make data unique, albeit not eliminated from the source.

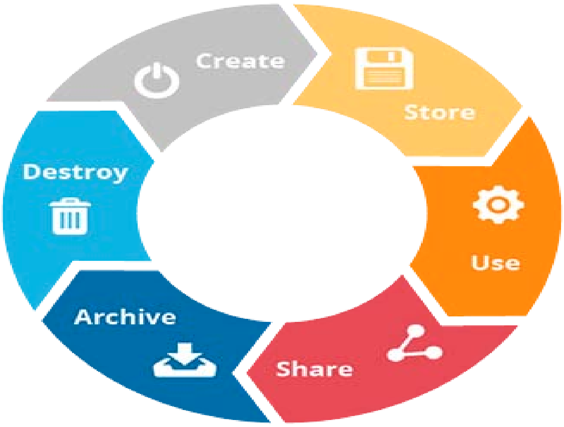

Figure: Data cycle life security (Source:Sunflower-CISSP.com)

B. Data security threats

In this section, the hazards influencing the recorded information that are listed below are important to us. The Cloud Security Alliance research offers a list of nine more prevalent and more important cloud security problems.

Data Breaches: Target was one of the most amazing robs while processing and saving data, which caused personal and credit card information losses of up to 110 million individuals. "While loss of data and data leakage are both important cloud computing issues, measures to mitigate the risk might exacerbate the risk," stated the report. Encryption protects data at rest but loses the encryption key to lose the data. Double data is generally made by the cloud to prevent loss due to an unforeseen death of the server.

Data Loss: Data loss can occur when a disk dies without the owner's backup. When the owner loses the key to open the encrypted data, this happens. Amazon Web Service users have lost minor amounts of data during a "emerging storm" from their EC2 cloud following an Easter weekend mistake in 2011. And a data loss might occur deliberately in case of a malicious attack.

Account or Service Traffic Hijacking: In general, stolen credentials remain a significant concern. In general, attackers access key segments of deployed cloud services using stolen authorizations to compromise their confidentiality, integrity and availability. Phishing with software vulnerabilities can cause user account loss of monitoring, such as buffer overflows and loss of passwords and credentials. A user-controlled intruder can eavesdrop transactions, change data, offer false and damaging replies to customers and turn them to the website and inappropriate places of the competitors.

V. Conclusion

Cloud computing allows sensitive consumer data to be stored on cloud servers in a wide range of unsecured areas. Different issues related to cloud security must be recognized and solved in order to safeguard and secret user data from unauthorized cloud access. Cloud security comprises proper authentication, strong encryption and protection against data loss. In this context, it is necessary to consider all modes of delivery of services and cloud deployment. The paper covers security issues at several levels in the cloud environment. For hosts, launched apps and networks, security measures must be employed. When providing protection to data, the proposed safety framework should encompass data saved in transit and also traces of deleted data. It also requires a proper access control system to guarantee access to cloud resources exclusively for valid users. The paper addresses various issues, safety requirements and mitigation techniques at every level. On all three levels, we offer a new security architecture that interconnects security. There are three classification levels of security suggested: application level, cloud level and infrastructure level. Cloud-based computing businesses need to modify their in-house applications software development process. Organizations should address important problems which contribute to the creation and use of multi-tenancy and security capacities of programming standards.

References:

[1] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting Webbased DDoS Attack using MapReduce operations in CloudComputing Environment," no. 8111, pp. 28–37.

[2] D. Jamil and H. Zaki, "Security Issues in Cloud Computing andCountermeasures," *Int. J. Eng. Sci. Technol.*, 2011.

[3] T. Moyo and J. Bhogal, "Investigating security issues in cloudcomputing," *Proc. - 2014 8th Int. Conf. Complex, Intell. Softw.Intensive Syst. CISIS 2014*, 2014.

[4] A. S. Thakur, "Framework to Improve Data Integrity in Multi CloudEnvironment," vol. 87, no. 10, pp. 28–32, 2014.

[5] G. Kulkarni, R. Waghmare, R. Palwe, V. Waykule, H. Bankar, andK. Koli, "Cloud storage architecture," in *2012 7th InternationalConference on Telecommunication Systems, Services, andApplications, TSSA 2012*, 2012, pp. 76–81.

[6] S. A. Weil, S. A. Brandt, and E. L. Miller, "CRUSH: Controlled,Scalable, Decentralized Placement of Replicated Data," *SC 2006Conf. Proc. ACM/IEEE*, vol. 1, no. November, p. 31, 2006.

[7] T. Threats and W. Group, "The Notorious Nine Cloud ComputingTop Threats in 2013," no. February, 2013.

[8] V. Varadharajan and U. Tupakula, "Security as a Service Model forCloud Environment," *IEEE Trans. Netw. Serv. Manag.*, 2014.

[9] Q. Vu, A. Sajjad, T. Dimitrakos, M. Colombo, and R. Asal, "SecureCloud Storage: A Framework for Data Protection as a Service in theMulti-cloud Environment. In IEEE Conference on Communicationsand Network Security (CNS), 28-30 September, 2015, Florence,Italy." 2015.

[10] I. KMeenakshi and V. Sudha George, "Cloud Server StorageSecurity Using TPA," *Int. J. Adv. Res. Comput. Sci. Technol. IssueSpec.*, 2014.

[11] X. Ma, "Study on Access Control for Cloud Storage Security," no.Csic, pp. 333–336, 2015.

[12] Y. Yu, Y. Zhang, J. Ni, M. H. Au, L. Chen, and H. Liu, "Remotedata possession checking with enhanced security for cloud storage,"*Futur. Gener. Comput. Syst.*, vol. 52, pp. 77–84, 2015.

[13] L. Chen, "Using algebraic signatures to check data possession incloud storage," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp.1709–1715, 2013.

[14] D. S. Lorunser Thomas, Thomas Grob, Thomas Langer, Mathieudes Noes, Henrich C. Pohls, Boris Rozenberg, “Towards a NewParadigm for Privacy and Security in Cloud Services Thomas,” *Commun. Comput. Inf. Sci.*, vol. 530, pp. 14–25, 2015.

[15] S. Singh, Y. S. Jeong, and J. H. Park, “A survey on cloud computingsecurity: Issues, threats, and solutions,” *J. Netw. Comput. Appl.*, vol.75, pp. 200–222, 2016.

[16] I. M. Khalil, A. Khreishah, M. Azeem, ”Cloud Computing Security: ASurvey,” *In Journal of MDPI Computers*, vol. 3, no. 1, pp. 1-35, 2014.

[17] Tilak, G. (2020). Utilization of Cloud Computing in Higher Educational Institutions.

Website References:

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

https://www.securityroundtable.org/future-of-cloud-security/

https://www.malwarebytes.com/data-breach

https://www.hfsrecords.com/2020/09/16/largest-data-breaches/

https://www.netacea.com/blog/the-rise-of-social-media-data-breaches

https://inca.ie/blog-page/canva

https://monin-it.be/2020/06/23/protectingyourdata/

https://trixter.in/the-10-biggest-baddest-data-breaches-of-the-21st-century/

https://indiancybersecuritysolutions.com/the-10-biggest-data-breach-happened-in-21st-century/

https://www.ct.co.uk/blog/defence-against-the-dark-web

https://ethhack.com/2020/04/the-15-biggest-data-breaches-of-the-21st-century/

https://www.vxchnge.com/blog/recent-ddos-attacks-on-companies

https://www.academia.edu/23500285/Cyber_Attacks_in_Cloud_Computing_A_Case_Study

https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/