International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Data Storage Issues in Cloud Computing

Nikhil Sreenivasan

Department of MCA SEM VI, YMT College of Management,
Institutional Area, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT

Cloud Storage is a branch of Cloud Computing, which plays an important role in IT world. Cloud providers are providing a huge volume of storage space as per the user needs. Due to wide usage of this, it also increases data security issues and threats. Hence efforts are being made to encrypt the data stored in the cloud. In this paper, we are going to look at different encryption and auditing techniques that are used to avoid data breaching in cloud storage.

KEYWORDS: *Cloud Storage, Data Security threats, Risk*

How to cite this paper: Nikhil Sreenivasan "Data Storage Issues in Cloud Computing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.906-910, URL: www.ijtsrd.com/papers/ijtsrd30194.pdf

IJTSRD30194

I. INRODUCTION

Cloud computing is an emerging IT technology that is gaining the tremendous exposure. Cloud computing is the delivery of various computing resources like CPU, RAM, Storage etc to the user over the computer network instead of physically providing at the user location. The main goal of Cloud computing is let the users take advantage of it which enables them to access and store their data with ease. Cloud security is composed of different set of policies, procedures and techniques that work in conjunction with each other to protect available resources. It includes different methods ranging from authenticating the users to managing traffic in cloud. Different cloud providers provide different security solutions depending on the user's need. A need for robust cloud security is increasing day by day. Security threats like data breaching, Phishing attacks, Viruses and Worms are affecting the data stored and hence it results in a loss of user data.

Figure 1[1]: Cloud Storage Model

A. Cloud Computing Services

The most common and widely adopted cloud computing services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[2]

Infrastructure as a Service (IaaS):
In IaaS, virtualized infrastructure is provided and handled for business organization by the service providers. It helps companies expand their storage, servers and other network units which are connected throught the internet which offers analogous functionality as that of on premises infrastructure. Some of the illustrations where IaaS is used includes website hosting, backing up of data.

Platform as a Service (PaaS):
In this model, the users rent everything which they require for developing an application, and confide on the service provider for tools, operating system and the required infrastructure. It simplifies the process of application development from the developer's point of view.

Software as a Service (SaaS):
In SaaS, the third party vendor makes use of the web to host the application which is made accessible to user's over the internet. It eradicates the need to do the installation of a particular application on an individual computer.

B. Encryption in Cloud Data Storage
As the data present in the cloud are stored in a distributed fashion, it is vital to encrypt the data. Cloud providers grant different services for encryption before the data is shipped to the cloud for storage. It includes variety of encryptions ranging from encrypting just the connections to complete end-to-end encryption. Local encryption provides an even effective security as decryption is important before using the data. Keys are used for encryption. It is neccessary to store the Encryption keys distinctly from that of encrypted data. Key backups should be kept in different place instead of keeping it onsite and examined frequently.

II. Literature Review
When user's cynical assets are not within their reach, they have to ensure that their data is safe and secured and the integrity is maintained. When user's make use of cloud computing, they store their resources in cloud provider's datacenters and hence the providers are completely responsible for ensuring the security and avoid the data from getting leaked or so. With increasing use of cloud computing, it also introduces new security threats like resource sharing, data lock in and malware attacks. All these threat prevents the users from using the facility of cloud computing and it also poses a huge risk to user's data. To determine the usefulness of building user's trust, a number of researchers have carried research to single out and evaluate the elements which plays a vital role in cloud computing, Few of the main works in this area of cloud computing are examined below.

This segment dictates a review of literature relevant to issues concerned with data security and data breaches in cloud computing. Cloud computing is not an innovation, but a means to constructing IT services that use advanced computational power and improved storage capabilities[4]. A brief analysis on different security issues and it's different countermeasures is found in [5]. There are wide range of security concerns and different case studies related to it are reviewed in [6]. How the Intrusion detection and Multifactor authentication can secure the data present has been discusses in [7].

Different security threats and related vulnerabilities are explained briefly in [8]. It is concluded that there is plenty of risk linked with cloud computing and how this risk can be avoided and assessed is discussed in [9].
When small scale companies use cloud computing, there arises an increasing risk associated. The small business are consistently looking for new tools and take up different software applications which has been discussed in [10]. Cloud Computing used with Internet of Things, trust based security, and other issues are reviewed in [11][12]. Various Qualitative measures related to information security [13], distributed type of environment and different challenges concerned with security [14], hierarchy of security in cloud computing [15], privacy, security, accountability and integrity in the field of cloud computing [16] are some of the vital areas in cloud computing security. The major vulnerabilities related to online storage facilities like Box and Drop box are discussed in [17].

In this paper, we have discussed what is data breach, various data breach cases and different ways by which we can prevent data breaching in Cloud computing.

III. Research Methodology
A. Data Breaching
A data breach is a term that relates to loss of sensitive, personal and confidential data due to unauthorized access. Information that affect while data breach occurs include credit card numbers, social security number and information related to healthcare histories. Common reasons of data breach are weak passwords, unfixed, old system vulnerabilities or malware.

Data breach usually involves the following steps:
- Research: The attacker exploits the vulnerability in the organization's security.
- Attack: The attacker initially establishes a connection with the help of a network.
- Network Attack: It occurs when the attacker makes use of organization's infrastructure vulnerability to penetrate their network.
- Ex filtration: After the attacker successfully gets the access of a computer, he then infiltrate the network and can easily access personal confidential data.

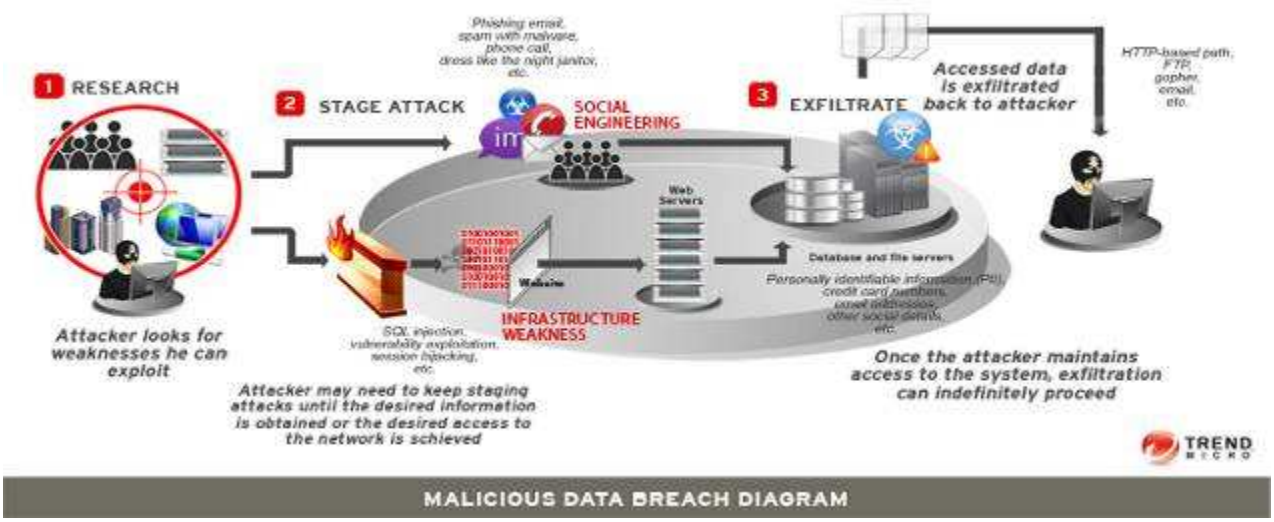

Fig 2[3] Data Breach Diagram

B. Causes of Data Breach

Security threats takes place both from outside as well as within the system. Most of the breaches occur due to faulty system or application configuration followed by the user error. Both of these error can cost the company far more than what could probably be the investment in reinforcing the defenses.

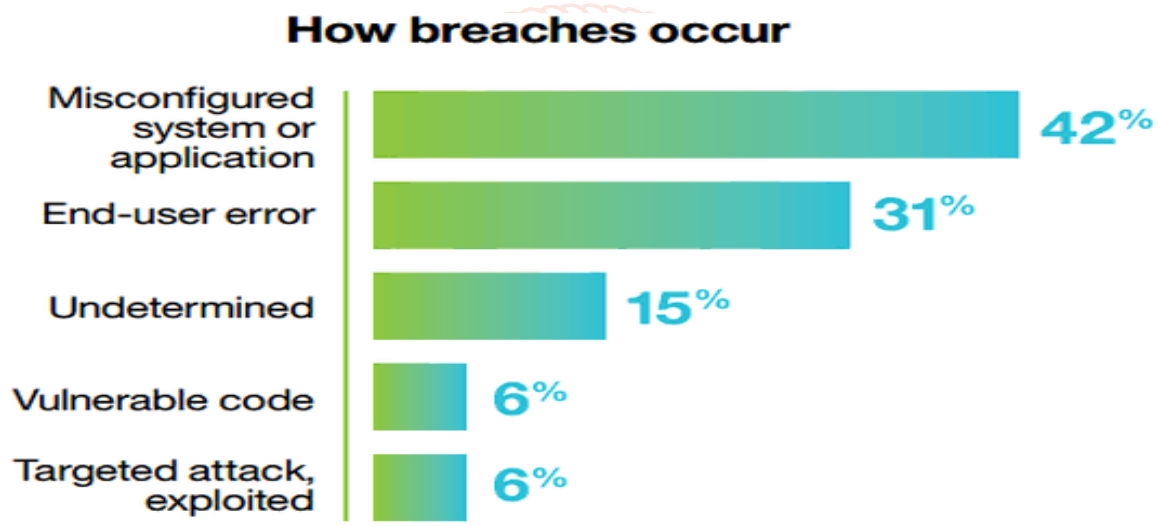

Fig 3[18] How Data Breach occur?

C. Different Ways to Avoid Data Breaches

There are multiple ways to avoid data breaches. Among all the available options, first one is spread awareness among the users. Unless and until this is done, other security measures is inadequate. Their other way is to create some kind of security policy which imposes encryption on the data which makes the stolen data as useless. It is important to have an intrusion detection system in every systems. Intrusion detection is probably the best way to prevent data breach. Drive-By downloads is one of the other way to avoid data breach. It is also possible to use susceptibility assessment programs. Most common way to avoid data breach in software application is to regularly update the patches as an when they are available. It is necessary to monitor the internal activities of the user and to take frequent backups of the data to avoid any security threat.

D. Encryption of data to avoid Data Breaches.

Encryption technologies are captious to assure the privacy of the data. It secures data which meet different compliance concerns and privacy regulations. With encryption, it is possible to provide a safe and secure place for the users to store their data. Data encryption is a techniques wherein the information is encrypted and it can only be accessed or decrypted by a person having a correct encryption key. There are different types of Encryption viz; Data Encryption Standard(DES), Triple DES, RSA, Advanced Encryption Standard(AES), Two Fish and encryption using SSL(Secure Socket Layer).

Data Encryption Standard:

It is the most popular algorithm. It is a symmetric-key algorithm. It is an implementation of Feistel Cipher. To encrypt or decrypt data it makes use of Feistel structure. It uses 64 bit of block size. It has been found as sensitive to more dynamic attacks. It is called as block cipher. It uses same algorithms for encrypting the data as well as decrypting it. It makes use of 56 bit key length. There are various kinds of modes including ECB and CBC or CFB. If each independent single bit is encrypted or decrypted individually then it is knows as ECB whereas if each data is dependent on previous one, then it is called as CBC or CFB. It includes Initial and Final Permutation after 16 rounds. Both are inverse to each other.

Process:

1. The 64 bit plain text is delivered over to an Initial Permutation function.
2. Initial Permutation is carried out.
3. It further forms two halves of the block called as Left Plain Text (LPT) and Right Plain Text(RPT).
4. Each of these blocks pass through 16 rounds of encryption procedure.
5. Finally, both of these blocks are assembled and the Final Permutation is executed on the blocks.
6. The end result of this entire procedure is a 64 bit cipher text.

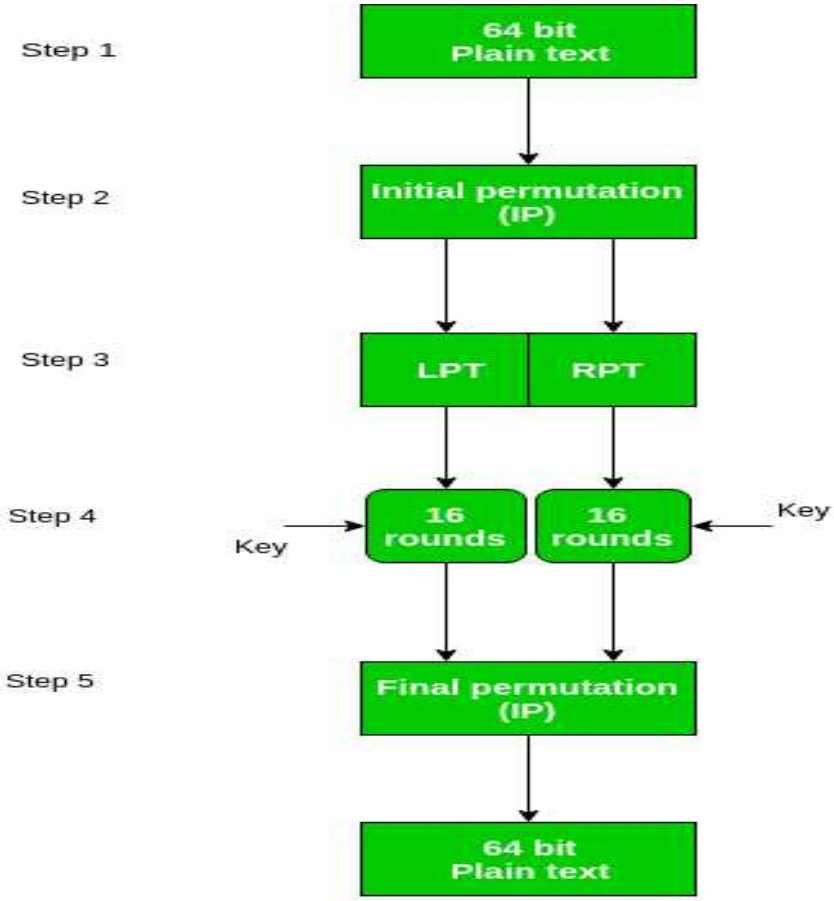

Fig 4[21] DES Process

Hence, DES plays a vital role in preventing data breach in cloud by encrypting the data so that it can't be easily accessible to unauthorized users. It makes the data more secure. With increasing use of Cloud Computing, public and private organizations using Cloud services are also facing the issues of data theft, privacy and security issues. The use of such security algorithms and assuring it's proper implementation helps in safeguarding end user security in an efficient way.

E. Auditing

A Remote Data Auditing is a technique which allows public audit ability of the stored data in the cloud. It is useful to check the integrity and the reliability of the data which is present. Remote Data Auditing for single server does not support data recovery. The remote auditing approach in distributed cloud environment are critically assessed and are further categorized into three classes; replication-based, erasure coding based and network coding based[19]. A data security audit is a process of auditing what all data is present in cloud, how it functions and who has the rights to access the data present and creating a plan to document it. After taking all the initial steps to protect the data, a security audit is vital to evaluate the cloud provider's present security systems so that a better future recovery plans can be made. Security audit should be performed regularly even when no data breach occurs. There's a difference between a post-data breach audit and a routine audit[20]. An audit conducted after data breach incident occurs is required to find and implement new fixes and security policies. A routine audit which refers to as DNS Audit, will help the cloud service provider to secure it's entire infrastructure and also to administer the systems. An outdated DNS server can cause more harm. Inspecting the provider's network, servers, open ports and IP blocks can help the organization with a complete audit of data which is already exposed and accessed by the attackers.

F. Results

Due to an increasing use of cloud computing facility the threat to data stored are also increasing which is a major threat to the user's data. Due to weak security policies, data breach can takes place. Data breaching is a type of incident which leaks user's confidential, sensitive data into an unsecured environment. It is becoming an increasing threat to the data present or stored in the cloud. It is possible to avoid data breach by taking different preventive measures. The graph below depicts the number of data breach incidents in respective years till date since 2005.

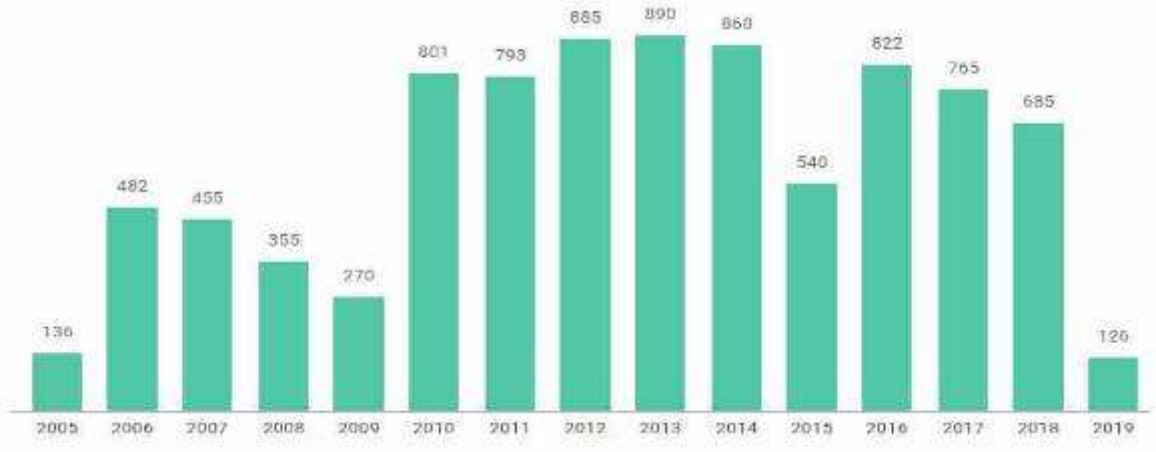

Fig 4[22] Number of data breaches since 2005 till date

IV. Conclusion

In this paper, we conferred the understanding related to data breach in cloud computing. Cloud computing has many pros and cons. However the cons directly effects the security of the data. Data breach is caused by many factors like human error, improper system and application configuration, unauthorized access, hacking etc. Data breach caused due to theft is more. Hence, it is vital to keep confidential and sensitive data secret. Since 2011, the number of data breach incidents has increased. Data breach caused due to vulnerable code is less as compared to human errors. In this paper, we have also discussed about the methodology of how data breach can be avoided successfully by using different security policies and techniques like Intrusion Detection System, encryption etc.

V. Future Enhancement

In our future work, we consider other means of forbidding data breaches and recommend a broad framework that marks all kinds of data breach in cloud computing. By making use of more effective encryption algorithms and strict policies it will be possible to completely eradicate data breach issues from cloud making cloud a reliable storage for the users.

References:

[1] https://www.researchgate.net/publication/306071422_A_Study_on_Data_Storage_Security_Issues_in_Cloud_Computing

[2] https://www.trianz.com/insights/revolution-that-is-cloud-computing#5

[3] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

[4] https://pdfs.semanticscholar.org/4ce8/91731f0dc7352d329b1f2dcc5b56cb8f6190.pdf

[5] https://pdfs.semanticscholar.org/8ee8/7566633ae84d3289ffdee687b3df08940b27.pdf

[6] http://www.iaeng.org/publication/WCE2013/WCE2013_pp1287-1291.pdf

[7] https://www.researchgate.net/publication/335243297_Data_Breach_a_Cyber_Security_Issue_in_Cloud

[8] Te-Shun Chou. (2013). SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES. International Journal of Computer Science & Information Technology. 5 (3), p79-88.

[9] Nathalie Brender and Iliya Markov. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. International Journal of Information Management. 33 (5), p1-17.

[10] https://aic.gov.au/publications/tandi/tandi456

[11] Alessio Botta , Walter de Donato, Valerio Persico and Antonio Pescapé. (2016).Integration of Cloud computing and Internet of Things, A survey. elsever, p684–700.

[12] Ahmad Rashidi and Naser Movahhedinia. (2012). A Model for User Trust in Cloud Computing. International Journal on Cloud Computing, Services and Architecture. 2 (2), p1-8.

[13] Mouna Jouini, Anis Ben Aissa, Latifa Ben Arfa Rabai and Ali Mili. (2012). towards quantitative measures of Information Security, A Cloud Computing case study. International Journal of Cyber-Security and Digital Forensics, p248-262.

[14] Mr. G. Nanda Kishor Kumar and Mr. M. Naresh. (2017). SECURITY THREATS IN CLOUD COMPUTING. International Journal of Application or Innovation in Engineering & Management, p983 -992

[15] Seyyed Mohsen Hashemi and Mohammad Reza Mollahoseini Ardakani. (2012). Taxonomy of the Security Aspects of Cloud Computing Systems-A Survey. International Journal of Applied Information Systems. 4 (1), p1-8.

[16] Sultan Aldossary and William Allen. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing, Issues and Current Solutions. International Journal of Advanced Computer Science and Applications. 7 (4), p485 -498

[17] https://acadpubl.eu/hub/2018-119-14/articles/1/3.pdf

[18] https://heimdalsecurity.com/blog/corporate-security-checklist-a-ceos-guide-to-cyber-security/

[19] https://www.semanticscholar.org/paper/Remote-Data-Auditing-in-Cloud-Computing-A-Survey%2C-Sookhak-Gani/6c09c92841e254b4169401405620478703a2804f

[20] https://securitytrails.com/blog/top-5-ways-handle-data-breach

[21] https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

[22] https://www.comparitech.com/blog/information-secusrity/biggest-data-breaches-in-history/