Plagiarism Checker X Originality Report

Similarity Found: 10%

Date: Sunday, June 07, 2020
Statistics: 233 words Plagiarized / 2387 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

Data warehousing security challenges on cloud. _Student Name _ID _ _1 _???? ???? ???? ????? _20160338 _ _2 _??? ???? ????????? ????????? _2016255 _ _3 _??????? ????????? ???? ????????? _20160236 _ _ INTRODUCTION Cloud computing is a very important structure with great potential in decreasing the prices by improving and developing functionality and economic outcome which successively can increase cooperation, pace and scalability acceptance to an accessible degree .

This technology has given many opportunities to large corporations and IT companies in developed countries, however, these opportunities face with challenges like security that is one of the most important concern in the field of cloud computing . If security services misuse all parts of cloud computing face with problems like the management of private information during a public network or stored data users on the servers can provide cloud services . It can be expressed that safety may be a virtual highway to the adoption of the cloud, if the providers of this technology can destroy the obstacle from the path or minimizes it, cloud computing will be an important factor in the field of data technology, so it's easier to companies and public to simply accept and trust to use it . Today, the most concern in cloud computing is the way to make confidence in accepting, sharing applications, hardware, etc.,

in an environment that we don`t know who is liable for securing our data .So to build trust and develop the cloud computing use, it feels the need to repair the security flaws and minimize the challenges are necessary. Background Security of data storage hints to data security on storage media, which means fast or not evaporated (non-volatile) retrieving after data loss. The security should be examined by software engineers in the design phase of cloud storage. This not only includes redundancy and dynamic data, but also includes the separation as well.

Redundancy is one of the most basic measures to protect the security of data storage, and dynamic ways that the user`s information may be changed, so effective movements need to ensure the consistency of data. Separation means the time of storing user data in the platform. To guarantee the separation of the data, users can only access the data to own it, and its changing from other users won't affect current users. Cloud computing has different forms causing different meanings of them. For this reason, many consider cloud as web-based applications.

Others see it as important as parallel computing because the cloud is meant to have better efficiency in complicated and large-scaled processes. Besides different forms of cloud, the provided services are also highly incompatible. Cloud computing has various definitions that have been brought here. Cloud computing is a model for enabling appropriate, on-demand network access to a shared pool of preamble computing resources (e.g., applications, storage, networks, servers, and services) that can be rapidly purveyed and released with service provider interaction and little management effort.

Historical background Since the computer networks were created and the spread of Internet security issues of storage and data transfer, it was very important and growing more importance of the subject because the advancement of technology and the transfer of data from high-volume, high importance requires channels with a greater safety element for transferring data is sensed. Accordingly, in this point, we analyze previous researches that discussed Data warehousing security challenges on the cloud: Data Security Challenges and Its Solutions in Cloud Computing by K.

Selvamani Anna University, Chennai : Their research conclusion was although cloud computing is the new rising technology that presents a great number of benefits to the users, it faces a lot of security challenges. In this research data security challenges and solutions are provided for these challenges to beat the risk involved in cloud computing. In future solid standards for cloud computing security can be developed. To provide secure and safe data access in the cloud, advanced encryption techniques can be used for data storing and data retrieving from the cloud.

Also, appropriate key management techniques can be used to share the key to the cloud users such that only authorized persons can access the data. A Study on Data Storage Security Issues in Cloud Computing by Naresh vurukonda, B.Thirumala Rao Department of CSE, KLUniversity, Vijayawada, A.P, INDIA : Their research conclusion was: The cloud computing structure stores data and application software with the least management effort and provides on-request services to customers through the internet.

But with cloud management customers don’t have trustworthy obligations or policies. This will result in many security issues with data storage such as confidentiality, privacy, availability, and integrity. In this research, they focused on data storage security challenges in cloud computing and they first provided service models of cloud, deployment models and a variety of security challenges in data storage in the cloud environment. Then, they addressed possible solutions for the data storage challenges that provide privacy and confidentiality in the cloud environment.

DATA STORAGE SECURITY CHALLENGES IN CLOUD COMPUTING by Sajjad Hashemi Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran: Their research conclusion was: Users store their data in the cloud, so there is no point to store them locally. So, the integrity, availability and security of data files on storage shared cloud servers are guaranteed. To achieve this, the structure and security solutions of involved components in the process of data storage in the cloud environment should be examined.

About the first components: client; they suggest using an encryption mechanism from the customer like AES encryption that its high security and resistance have been proven in many testing. AES has been examined and analyzed by the NIST and its security has been accepted by this validated Institute, and this encryption is used to encrypt sensitive information in the USA. Also, they can use encryption algorithms like genetic algorithms or other dynamic algorithms in which security can increase incredibly in this way.

The next component must consider its security is a server because its data stores on the server and they have storage space virtually as a user. So, the accuracy and availability of data and IR are very important and should provide the necessary security to accomplish this on the server-side. The third component that its security is important in the storage and transmission of data is the connection channel between cloud service providers and users.

In this case, we can refer to the protocols and establishing or retrieving more secure transmission channels that they give to using new sciences and methods in computer science. A survey on security challenges in cloud computing: issues, threats, and solutions by Hamed Tabrizchi & Marjan Kuchaki Rafsanjani : Their research conclusion was: Cloud services are now an important part of corporate life, bringing a critical opportunity to speed business through their ability to quickly grow, allowing us to be smart with our resources, and providing new opportunities for collaboration. actually, the cloud brings many uses to organizations, companies, and even countries.

regardless of bringing many advantages, the cloud still is vulnerable to many security challenges. This is the reason for the security is the major challenge in the adoption of the cloud. The customer and sellers are well aware of security threats and the main aim of the current study is to show all possible security challenges in the cloud computing environment and provide an appropriate solution to solve these challenges. In fact, this research attempted to show several security attacks, challenges attacks, vulnerabilities, and threats that restrain the adoption of cloud computing.

this research provided a survey on cloud security issues and challenges that emerge from the unique characteristics of the cloud. A generalized view of these challenges has been given here to improve the importance of understanding the security errors of the cloud computing framework and plan suitable countermeasures for them. This research proposes a review of recent security frameworks in the condition of reducing vulnerabilities to prevent possible attacks.

this research categorizes security challenges and performs a relative analysis of security issues and the countermeasures suggested to deal with these issues. What Security Challenges to Expect When Migrating to the Cloud by GiladMaayan IBM developer This research was about the challenges that faces the security when migrating to the cloud Which was: Data breach: Its solution is investing in data encryption, threat prevention and tokenization tools to protect the data like intrusion detection and threat intelligence. Data loss: Its solution is companies need to invest in a cloud data loss prevention solution to make sure that hackers don't steal their information.

Insider threat: Its solution is to combine ID management and automated user access to encourage safe and smart data access practices and to prevent poor security awareness, phishing and social engineering thefts. DDoS attacks: Its solution is investing in DDos protection to service to provide protection for advanced DDoS threats at every network layer. API Security: Its solution is to implement Secure Socket Layer encryption to create secure communication based on components like IP address, geography and incoming device identification.

4-Gaps in previous studies There are some Problems in the previous studies about Data warehousing security cloud, So, in this topic we will show some of that problems. -Data Breach: In local environments, Information Technology security professionals have control over the hardware and network infrastructure. In environments based on cloud computing, part of this control is transferred to a third-party partner, which makes the environment prone to attacks. Professional hackers can exploit vulnerable cloud environments to steal confidential data from companies.

-Data Loss: Many Companies have no idea about happens to their own data when it is stored in the cloud, when many end-users work in the cloud at the same time, it's easy to lose some data. the major benefits of cooperation and sharing become a weakness for cloud administrators of cloud. Things like accidental files deletion, use of own devices without any passwords, password sharing are the causes to lose data in cloud. - DDoS attacks: When cloud computing first became popular for all users, DDoS attack against cloud computing platforms were unthinkable.

Cloud is based on shared distributed computing resources and using different kinds of virtualization technology, which makes the DDoS security more complex and harder to control. A successful DDoS attack can make a website useless for days. This can result in a money loss, a decrease in customer trust. - API Security: Application Programming Interfaces (APIs) require authentication and access to any application they communicate with, so, they become a security threat to cloud. So, With APIs growing, The vulnerabilities for a security breach. - Locality: the data in cloud is distributed over the regions and very difficult to find the location of data.

When the data is moved to different geographic location the laws on that data may also change. So, there are an issues of data privacy laws in cloud-computing. All Customers must know their data locations. 5- Suggested idea(s) to enhance any of previous researches gaps we will show Our solutions for the above gaps, In Data breach the best solution is Encryption like RSA algorithm, RSA is the first algorithm that used to providing data. RSA can encrypt messages without the need to exchange a separate secret key. The RSA can be used for public key encryption and digital signature.

Its security is based on the difficulty of factoring large integers, So, invest money in data encryption, threat prevention tools and tokenization to protect the data. Solutions like intrusion detection and threat IA can easily identify and mitigate a threat. In data loss we can use DLP solutions and recovery tools, as well as some dedicated systems to prevent any attacks, in addition, protect our personal network layer, including the application layer too.

DDoS attack is very real threat, So, we suggest invest in DDoS protection services that save time protection for difficult DDoS threats at each network layer including Layers 3, 4 and. In API, implement SSL [Secure Socket Layer] encryption to establish more secure communication based on incoming device IP address, geography and identification. Conclusion: Although cloud computing is a new emerging technology that offers a large number of benefits to users,It faces many security challenges.

In this paper, data security challenges and solutions are provided Challenges to overcome the risks involved in cloud computing. In the concrete future standards of cloud computing Security can be developed. To provide secure access to data in the cloud, advanced encryption technologies can be used Storage and retrieval of data from the cloud. Key management techniques appropriate for major distribution can also be used Cloud users so that only authorized people can access them.

We suggest using the encryption mechanism from The client is like AES encryption which has proven safe and high resistance in many Tests. The National Institute of Standards and Technology has investigated and analyzed AES and its security has been approved By this accredited institute, this encryption is used to encrypt sensitive information United States of America. We can also use the encryption algorithm by new methods such as Genetic algorithm or other dynamic algorithm that security can greatly increase in it The Road.

REFERENCES: [1] Cloud computing security issues and its solution: A review - IEEE Conference Publication. (2020). Retrieved 6 June 2020, from https://ieeexplore.ieee.org/document/7100438 [2] Tianfield, H. (2012). Security issues in cloud computing. 2012 IEEE International Conference On Systems, Man, And Cybernetics (SMC). doi: 10.1109/icsmc.2012.6377874 [3] Cloud Computing Challenges & Security Issues. (2017). International Journal Of Modern Trends In Engineering & Research, 4(3), 57-61. doi: 10.21884/ijmter.2017.4079.cfbgf [4] Nadeem, M. (2016). Cloud Computing: Security Issues and Challenges. Journal Of Wireless Communications, 1(1). doi: 10.21174/jowc.v1i1.73 [5] (2020). Retrieved 6 June 2020, from https://www.researchgate.net/publication/273135379_A_Study_of_the_Issues_and_Security_of_Cloud_Computing 6-H.Takabi, J.B.D.Joshi, G.Ahn., “Security and Privacy Challenges in Cloud Computing Environments”, IEEE Security Privacy Magazine, Vol 8, pp.24-31, 2010. 7-Raj H, Nathuji R, Singh A, England P. “Resource nmanagement for isolation enhanced cloud services.”, Proceedings of the 2009 ACM workshop h on cloud computing security, Chicago, Illinois, USA, pp. 77–84, 2009. 8. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou.

Achieving vsecure, scalableg and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9. 9-M.B. Mollah, K.R. Islam, and S.S. Islam. Nextf generation of computing through cloudf computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.

INTERNET SOURCES:

<1% -
https://www.businessinsider.com/10-essential-data-security-measures-every-business-s

hould-take-2010-6

1% - http://sistemas-humano-computacionais.wdfiles.com/local--files/capitulo%3Asistemas-de-servico/Dillon2010.pdf

3% - https://www.sciencedirect.com/science/article/pii/S1877050915006808

<1% - https://textbooks.elsevier.com/manualsprotectedtextbooks/9780124046276/cloud_computing_solutions.pdf

1% - https://www.slideshare.net/ijeei-iaes/a-secured-cloud-data-storage-with-access-privilages

1% - https://www.sciencedirect.com/science/article/pii/S1877050916315812

1% - https://www.x-mol.com/paper/1233483931059245056

<1% - http://shodhganga.inflibnet.ac.in/bitstream/10603/15084/15/15_%20chapter%207%20solving%20the%20security%20issues%20with%20e.pdf

1% - https://www.sciencedirect.com/science/article/pii/S1084804516301990

<1% - https://link.springer.com/article/10.1186/s13174-014-0015-z

<1% - https://digitalguardian.com/blog/enterprise-data-security-breaches-experts-how-companies-can-protect-themselves-big-data

<1% - https://www.cwps.com/blog/cloud-computing-security-issues

<1% - http://docshare.tips/essentials-of-cloud-computing_574a864ab6d87fb8468b4655.html

<1% - https://crypto.stackexchange.com/questions/61197/how-can-i-securely-encrypt-the-same-message-multiple-times

<1% - http://www.connellybarnes.com/documents/factoring.pdf

<1% - https://www.ijert.org/a-detailed-study-on-security-threats-and-issues-in-cloud-computing-and-its-reduction-techniques

<1% - https://searchcloudcomputing.techtarget.com/tip/Secure-data-in-the-cloud-with-encryption-and-access-controls

<1% - https://www.afcea.org/content/tags/national-institute-standards-and-technology

<1% - https://www.researchgate.net/publication/261073370_Security_issues_in_cloud_computing

1% - https://link.springer.com/chapter/10.1007/978-3-319-77839-6_7