RESEARCH ARTICLE OPEN ACCESS

Conceptual Oriented Investigation on the Improvement of the Cloud Data Storage Security

Dr.K.Sai Manoj [1], K. Mrudula [2]

CEO [1], Innogeecks Technologies and Amrita Sai Institute of Science and Technology, Vijayawada, AP, India

Managing Director [2], Innogeecks Technologies, Vijayawada, AP, India

ABSTRACT

Cloud Computing reflects Efficiency, Flexibility and also savings in the cost as per the IT industry Point of View. As more and more companies are focusing on the cloud computing technology that is why the reason research on the cloud data storage security plays very important role. More users rely on cloud storage as it is mainly because cloud storage is available to be used by multiple devices (e.g. smart phones, tablets, notebooks, etc.) at the same time. These services often offer adequate prostection to user's private data. However, there were cases where user's private data was accessible to other users, since this data is stored in a multi-tenant environment. These incidents reduce the trust of cloud storage service providers; hence there is a need to securely migrate data from one cloud storage provider to another. This research Paper Point out on the investigation to provide Security as a Service for cloud brokers in a federated cloud. This scheme allows customers to securely migrate from one provider to another.

Keywords:- Cloud Computing, Security, IT Industry, Multi-Tenant Environment

I. INTRODUCTION

Cloud storage is a new business model for delivering virtualized storage to customers on demand. The formal term proposed by the Storage Networking Industry Association (SNIA) for cloud storage is Data Storage as a Service (DaaS) - as "Delivery over a network of appropriately configured virtual storage and related data services, based on a request for a given service level." [1] Allocation of costs is important for DaaS. Providing virtualized storage on demand does not require organizations to pre order a defined amount of storage capacity. This enables organizations to save a significant amount of capital because storage costs depend only on the actual amount of storage space used. This business model is extremely cost efficient for start-ups and small organizations. However, it is not cost effective for organizations that know (or can predict) the amount of storage that they actually need. Capital cost savings for organizations are very tempting. However, this simply shifts the challenge to the cloud providers. Cloud storage services require deployment of accurate metering and billing mechanisms. Additionally, cloud providers have to meet the potential user's peak demands without expanding existing facilities and at a price that is less than or equal to the non-cloud alternative. [1] A cloud storage service presents a container for data, and the user does not really care how the cloud provider implements, operates, or manages their resources within the cloud. Although seemingly abstract and complex, cloud storage is actually rather simple. Regardless of the data type, cloud storage represents a pool of resources that are provided in potentially small increments with the appearance of unbound capacity. [1]

II. MAIN CONCEPTUAL ORIENTED ANALYSIS IN THIS RESEARCH PAPER

Existing Cloud storage services Security should be a top priority when it comes to choosing a cloud storage service. Cloud storage services should employ robust security measures to safeguard the customer's data during transmission and when stored in the cloud. The most basic protection is Secure Socket Layer (SSL) encryption of the data during transit, password-protected accounts, and multi-level security in the cloud.

DropBox:

Dropbox encrypts data in transit with Secure Socket Layer (SSL), while stored data is protected with Advanced Encryption Standard (AES)-256 bit encryption. Data file names are in their original (plain

text) form. Dropbox uses Amazon's Simple Storage Service (S3) for storage. S3 has a robust security policy of its own. The overall service design has security flaws and is a subject to known attacks [2]. Dropbox states that their employees are allowed to see only metadata, but not the data itself. However, when legally required to there are some employees who are allowed to view the customer's data. Although the user's data is encrypted, [2] states that Dropbox employees are capable to decrypt any data. Those who are interested in protecting their data should consider adding an extra layer of encryption before synchronizing data with Dropbox, as described in [3].

Amazon Cloud Drive

Amazon's Cloud drive offers no encryption at all. Amazon's Cloud Drive "Terms of Use" [4] states that the provider can do whatever he likes with the user's data. Providing a free cloud audio player encourages users to upload music to their storage. However, all that music is periodically inspected for illegal (i.e. unlicensed content). As stated in [4], Amazon is able to access, retain, use, and disclose any account information and files. In other words if a user wants to use this cloud storage service he has to give up all privacy or protect the data himself or herself.

III. CLOUD SERVICE BROKERS AND CARRIERS

Although the terms cloud broker and cloud carrier are not new in areas such as real estate and telecommunications, in cloud computing these two roles are relatively new. Since so many cloud providers have entered the market, it is hard for a customer to choose a suitable cloud provider for their needs from the many cloud service providers (CSPs). It is even harder to integrate cloud solutions across different providers. Thus, cloud brokers and cloud carriers will arise in the near future, in order to provide customers simplified methods to adopt and utilize cloud services.

Securing the data

The Internet is not a safe place for sensitive private data to travel. Additionally the cloud model does not define what security measures should be taken in order to secure the data while it is inside the cloud. All security related decisions depend upon the specific policies and actions of each cloud service provider (CSP). This raises security risks both in the protection of data and in the safeguards applied to this data. According to [5], recent studies show that CSPs have tended to provide their services without strong security solutions. However, Christopher Soghoian recommends that CSPs should use the kind of encryption which is currently used by on-line banks. Moreover, data protection should be applied to data at rest, in transition, and while processing it.

IV. CONCLUSION

The aim of this research paper was to identify cloud storage security and privacy risks and propose a Security as a Service design which could securely migrate data from one cloud service provider (CSP) to another. The motivation behind this research lies in the fact that for many organizations the final barrier to adopting Cloud computing is whether it is sufficiently secure.

DECLARATIONS:

Availability of data and material:

Not applicable.

Competing interests

Not applicable.

Funding:

No funding was applicable.

Authors' contributions:

The other of the paper do all the work, the environment for research work is done by my best of my knowledge and supporting my family members.

Acknowledgements:

First of all, I am thankful to Honorable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

Authors' information:

Dr K Sai Manoj, Founder and Executive Director of Innogeecks Global Services Pvt Ltd, Founder and CEO of Innogeecks Technologies and Founder of 3 start-ups based on IOT and Cloud Computing, is an Enthusiastic learner, Excellent Financial Advisor, Innovative and Visionary Leader, Insightful team builder and strategic planner, who has 10+ years of experience in Financial Services, Equity Research and IT- ITeS services to his credit. He has worked in Reputed Companies like WIPRO Technologies, Fidelity Inverstments.etc.,

He is Proud of achieving many laurels in the field of Computers and Research. He is a Certified Ethical hacker, Certified Computer hacking forensics Investigator, Certified Security Analyst, Charted Engineer from IEI (India), Certified Blockchain Expert, Microsoft Certified Technology Specialist, AWS Certified Solutions Architect-Associate, Google Analytics Individual Qualification, IBM Block chain Certification, Certified EC Council Instructor and so on.

He has a proven record of having 10+ certifications from the most sought after software giants such as Microsoft, IBM, Google, Face book, EC Council & Amazon besides this he has acted as a reviewer for the Journal of Super Computing (Springer) , Journal of Big Data (Springer) and Journal of the Institution of Engineers (India) – Series B (Springer). And also with his solid financial advice 21 start-ups of Kochi, Bangalore and Vijayawada have tread the success track.

Talking about his research excellence, it is exciting to know that he has filed 3 patents and 4 more are in pipeline and has Published more than 25 research papers in reputed journals like Thomas Reuters, IEEE, Scopus etc., and shows keenness in researching on Cyber Security, Cloud Computing, Big Data / Hadoop, Block chain and Data Analytics.

Ms. K.Mrudula working as a Director for the Innogeecks Technologies. She was completed M.Tech from IIIT Hyderabad .She has more than 6 years of experience in academics and research. She published more than 5 research papers in various International and national research journals. She attended 2 FDP, and 1 workshop.

REFERENCES:

[1] SNIA, Advanced Storage a Information Technology. Implementing, Serving, and Using Cloud Storage. Cloud Storage Initiative. October 2010, http://www.snia.org/sites/default/files/2010-10-WP-ImplementingServingandUsingTheCloud.pdf

[2] Bruce Schneier. Dropbox Security. Schneier on Security. May 23, 2011, http://www.schneier.com/blog/archives/2011/05/dropbox_securit.html

[3] Melanie Pinola. How to Add a Second Layer of Encryption to Dropbox. Lifehacker. June 20th, 2011, http://lifehacker.com/5794486/ how-to-add-a-second-layer-of-encryption-to-dropbox

[4] Steven J. Vaughan-Nichols. No Privacy on Amazons Cloud Drive. ZDNet networking Blog. March 2011, http://www.zdnet.com/blog/networking/ no-privacy-on-amazons-cloud-drive/882

[5] Privacy Issues related to Cloud Computing. Office of the Privacy Commissioner of Canada. March 2010, http://www.priv.gc.ca/information/pub/cc_201003_e.asp

[6]A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli,International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11

[7] Satish, Karuturi S R V, and M Swamy Das. "Review of Cloud Computing and Data Security." IJAEMA (The International Journal of Analytical and Experimental Modal Analysis) 10, no. 3 (2018): 1-8, 2018.