Survey on Security Issues and Security Storage in Cloud

Dakshayani Seemakurti[1], S. Venkateswarlu[2], N. Parashuram[3]
[1,2,3]*Computer Science and Engineering, G. Pullaiah College Of Engineering and Technology.*

Abstract— *Cloud computing is an emanate technology, flexible, cost-effective for providing services over the internet. Different storage services are provided by the cloud they are Platform-as-a-Service, Infrastructure-as-a-Service, Software-as-a-Service, Storage-as-a-Service. The services mentioned above supports secure and efficient data storage in the cloud. With the use of Storage-as-a-Service, users store data in related manner which has new security risks of data in the cloud. Several cloud based services helps the service providers to provide sensitive information and to protect the data from unwanted parties. This paper deals with the security issues and secures storage in cloud using internet and providing the access to the users.*

Keywords— **Cloud users, cloud service, security issues, secure computing, secure storage, security.**

I. INTRODUCTION

Data can be stored in the cloud and can be frequently updated, inserted and deleted by the users who have given permissions to modifications on the data stored in the cloud. From the perspective of cloud computing the security issues has been a important aspect of quality of service. Now-a-days every company is associated with the service providers in order to store their data in cloud. By taking that into consideration different service providers are providing the service with security and privacy on pay-as-per-use basis. In some cases, it is required for a person to store the data in the remote cloud servers.

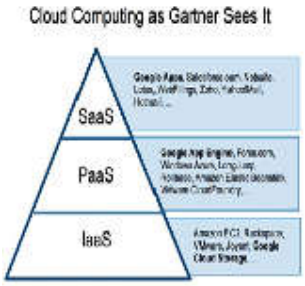

Fig. 1.Services provided by cloud

II. SAFETY ISSUES IN CLOUD

Safety issues in the cloud come with both possibilities and limitations. Different security issues are there and security challenges for cloud computing are vast. Data location is the crucial factor and transparency in location is one of the rugged flexibility of cloud as well as a security threat. It will severely affect customers if they are unaware of the data stored location. Trust is the another security issue in the cloud, the establishment of trust might become a key establishment of better relationship among the users and service provider in the cloud computing. There are some myths regarding the data storage in the cloud, thinking that these are less secure than traditional approaches.

Fig. 2.Safety issues in cloud

Trust in cloud is not a technical security issue and it depends on several factors like policies, human factors etc. Distributes Denial of service is another security issue in the cloud which has no option to relieve it and some threats like man-in-middle attack, phishing and sniffing attacks. There are some myths regarding the data storage in the cloud, thinking that these are less secure than traditional approaches.

III. SECURE STORAGE IN CLOUD

Cloud computing uses deployment models for providing network, platform, infrastructure as service and there are three deployment models they are hybrid, private, public. The secure storage in cloud provides security to the users by encrypting the data and file which is going to be stored in the cloud is splited in to small blocks. Secure storage in cloud gives the access to the user over their data so that they can ensure that the data is secure and not corrupted. The customers in the cloud do not own physical infrastructure besides that they rent the storage from third party i. e; service providers. The resources are provided to the users and they pay only to the resources they use.

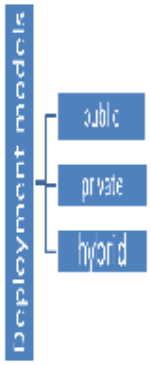

Fig. 3.Deployment models in cloud

The cloud users has large amount to store in cloud and cloud server has significant data storage managed by the cloud service providers. Third party auditor is given permission to access the cloud service, storage security upon request from user. The basic algorithm can be generated to ensure data integrity and confidentiality.

Step 1: Generate a random session key kr and compute the key hashed value h(data,kr)

Step 2: Encrypt data h(data ,kr) with kr.

Step 3: Encrypt kr using the key KUV.

Step 4: Store data<={data ,h(data, kr) } kr, {kr} KUV> and destroy kr.

IV.AUTHENTICATION IN CLOUD

Security is the most important aspect for any form of computing and making it an obvious expectation that security issues are crucial for cloud environment as well. As the cloud computing helps in storing the easily affected data in both cloud server and the client server [2]. Identity management, privacy, physical security and personnel security plays a crucial role in cloud computing.

Every user will have their own identity management system to control their sensitive data and resources. Making use of this identity management the data is encrypted to avoid potential attackers gain access to any easily affected data or even they can gain access contents of the individual.

Physical security secures the hardware parts like routers, servers, cables against unauthorized access. It gives the total details about the materialistic area of data stored in the cloud to the users by the service providers.

Fig. 3 .Authentication in cloud

In the above figure it is clear that user access the data by using internet service provider (isp), authentication management provider and third party authentication server. The cloud server provider network routes the data from cloud.

V. CLOUD STORAGE ARCHITECTURE

Files which are said to be stored in remote servers are easily accessible from anywhere through internet, including smartphones, tablets etc. Every platform is easily accessible through a web browser and also provides apps for ease access.

Fig.4.Cloud storage architecture

VI. ADVANTAGES

The companies which are using cloud storage need to pay only for the storage they are using and it acts as a proof backup from natural disaster there are normally 2 or more servers are located around the world. Cloud server can function as a central file server for organisations in different locations[5].

It provides users with a immediate access to the resources and applications via a web server interface and it is possible to move the virtual images between user accounts to data centres. Data loss is less in a cloud and cloud provider have better control over the threats as it provides integrity, confidentiality, availability.

VII. ARCHITECTURES

1) *Privacy manager in the client:* It helps the user to store the sensitive data and also protects privacy from accessing of cloud services, it allows the user to express privacy preferences[3].

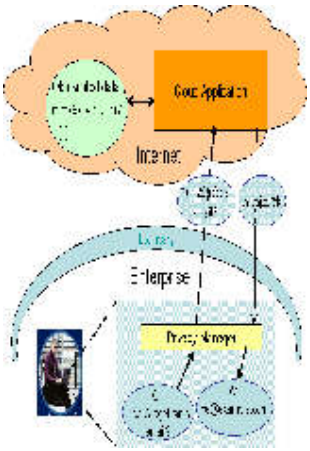

Fig.5.Cloud Architecture

2) *Privacy manager in hybrid cloud:* Privqacy manager may be deployed in a local network, to protect information relating to multiple parties. Advantages to this approach include that the benefits of the cloud can be repeated within the private cloud, including the most.

VIII. CONCLUSION

This paper dealt with different security issues with both limitations and challenges and secure storage architectures which helps the users to store the sensitive data from the third party users. The issues of security in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints. This paper also dealt with the deployment models which helped the user in storing the secure data and also cloud storage architectures with both privacy in the cloud and privacy manager in hybrid cloud.

REFERENCES

[1] Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," https://www.sun.com/offers/details/sun_transparency.xml, White paper, Nov. 2009

[2] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[3] Agarwal , A(2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1(Special Issue on CNS), 257-259

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory Applications of Cryptographic techniques (Eurocrypt '03), pp. 416-432, 2003.

[5] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy- Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008

[6] S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.

[7] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[8] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. IEEE INFOCOM pp. 954-962, Apr.2009.

[9] A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010