ISSN : 2231-0711

Sasanth Tummala et al | International Journal of Computer Science Engineering and Technology(IJCSET) | May 2014 | Vol 4, Issue 5,145-147

Integration of Security Issues in Multi Cloud Computing Environment

Sasanth Tummala[1], Lavanya Ganapaneni[2], Anil Kumar Jonnalagadda[3], Avinash Chanumolu[4], Manoj Kumar Tyagi[5]

[1,2,3,4] *Students, Department of Electronics and computer Engineering, K L University, India.*
[5]*Associate Professor, Department of Electronics and computer Engineering, K L University, India*

***Abstract*:- A proposed Multi-cloud computing framework allows dynamic resource sharing among cloud-based system, addressing trust, policy, and privacy issues without pre-established collaboration agreement. Multi-cloud typically consists of service providers (or admin), infrastructure providers, and service users (or clients). Service provider(or admin) delivers applications as services to the service users (or clients) and infrastructure providers provide media of communication to service providers and clients. In our project cloud service provider(CSP) gets the applications requested by the user form the cloud and Proxy service provider(PSP) provides the communication path between different clouds. Cloud computing characteristics include a ubiquitous (network-based) access channel, resource pooling, automatic and elastic provisioning and release of computing capabilities and metering of resource usage (typically on a pay-per-use basis).**

Index Terms – cloud service provider, proxy service provider, file upload, file download, hash security keys

I. INTRODUCTION

The recent survey people are more interested in using cloud computing because of its ability to provide software, infra-structure, and platform services without requiring large investments or expenses to manage and operate them. Clouds typically consist of service providers, infrastructure providers, and service users (or clients). They include applications delivered as services, as well as the hardware and software systems providing these services. Clouds typically involve service providers, infrastructure providers, and users (or clients). They include applications distributed as service, as well as the hardware and software systems providing these services. For example consider clouds like ONE DRIVE, GOOGLE DRIVE etc., cloud service offered that can be used to store large amount of data and can share the files. By using the cloud, we can completely free from problems occurred by local data storage and maintenance. Virtualization of resources such as processors, network, memory, and storage ensures scalability and high availability of computing capabilities. Clouds can dynamically provide these virtual resources to hosted applications or to clients that utilize them to develop their own applications or to store data.

As more organizations adopt cloud computing, cloud service providers (CSPs) are developing technologies to enhance the cloud's capabilities.

The major task of CSP's is to design a schema for storing the data as well as sharing the data which should be efficient and secured. The foremost challenging issue is maintaining security to the data in the cloud. Previously only the client registered to the cloud can only access the data but in this any client can request the data from all the available clouds.

Collaboration among multiple clouds can be accomplished by proxy service provider (PSP). PSP's provides the access control between the clouds and to provide secured services which opens up opportunities for CSPs to offer more-sophisticated accommodations that will benefit the next generation of clients. For example, cloud-predicated electronic medical record (EMR) management systems like Practice Fusion, Verizon Health Information Exchange, Medscribbler, and GE Healthcare Centricity Advance are emerging. In addition, government agencies are working toward building interoperable healthcare information systems that promote electronic exchange of data across multiple organizations. These developments will influence healthcare providers to interact with multiple cloud-based EMR systems in the future.

Realizing multicloud collaboration's full potential will require implicit, transparent, and on-the-fly based involving different services spread across multiple clouds that lack pre-established agreements. The research community is beginning to develop architect- ures, technologies, and standards to support collaboration among multiple cloud systems. However, these research proposals still remain constraining due to limited information in cloud computing. Multiple CSPs will provide services on an easy and standardized way of access, as this would give clients total freedom in changing providers, leading to increased open and direct competition with other providers. CSPs often offer differentiated services with specialized products and services which offer attract and maintain more clients. Cloud-based computing also introduces new security concerns that affect collaboration across multicloud applications, including the following:

- Increase in the attack surface due to system Complexity,
- Loss of client's control over resources and data due to asset migration.
- Threats that target exposed interfaces due to data storage in public domains, and
- Data privacy concerns due to multitenancy.

The research community is beginning to develop architectures, technologies, and standards to support collaboration among multiple cloud system

Some specific security issues associated with collaboration among clouds include

- establishing trust among different cloud providers to encourage collaboration.
- addressing policy heterogeneity among multiple clouds so that composite services will include effective monitoring of policy anomalies to minimize security breaches. and
- maintaining privacy of data and identity during collaboration.

II. Related Work

In the proposed system cloud collaboration is achieved by prior business agreements among the cloud providers and this limits the security to the individual cloud. Moreover our proposed cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multicloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications.This provides security to the data by providing access control to the clients.

III. System Design And Design Goals

For the proposed system there are 4 major actors namely the cloud service provider, the proxy service provider, the cloud admin and the client. The client can register, revoke and can download the file. The cloud admin upload required files into the cloud.

The cloud service provider (CSP) provides the services to the client requested. CSP's takes the request from the client and searches for the information in the cloud database. If the requested information is available in the cloud then this verifies authentication of the client by sending random security key to the register email.

The proxy service provider provides secured communication between the clouds, if the CSP can't find the requested information in the cloud this request the PSP to connect to other cloud, then PSP connects the CSP's of other clouds and request the information.

Design Goals:

Here in this section we characterize certain design goals that are taken as pre requisites for designing the proposed work. These include aspects relating to access, privacy and storage.

Access:

A client must register himself before his first login for obtaining access to the content in the cloud. The details at login are verified with the one stored in server before granting access. The rescind users will not get access as their profile is updated in the server to make him remain blocked forever.

Privacy:

The feature that a client can get the contents stored in the cloud only after the verification of the authentication of the client through the registered email. The collaboration between the clouds can only done by PSP, user or admin can't connect directly to other clouds.

Storage:

A cloud admin is provided with full freedom to access the files uploaded, download them and also can update them. But certain important data can be modified that may result in disputes. For example a mischief person in the department of a university may change the holiday schedule noticed by updating the actual notice without revealing his identity to others. So a log is maintained to resolve such disputes.

IV. Proposed Work

The Cloud Admins has full control on the file uploading, downloading and providing services to the user. The client (or user) can download the file from any of the clouds that are present. The client request the information, then the cloud service provider takes the input from the client and searches for the information in the cloud if the information is present in the cloud then the user authentication is done by registered email. CSP sends the hash security key to the registered email and when the user enters this security key the requested file is downloaded into user (or client) system. If the requested information is not present in the cloud then the CSP request proxy service provider (PSP) to connect to the other clouds that are present. PSP connects to the clouds that are available and sends the user request to CSP's present in that clouds. Then this CSP's searches for the information in their respective clouds, if the information is available then CSP sends information to PSP and PSP forwards the information to the user. A log file is created and maintained by admin. This records all the actions that are performed by the user on a file. The client passwords are encrypted by using MD5 hash for the security.

KEY GENERATION:

The ***MD5 Message-Digest Algorithm*** is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. It's very simple and straight forward; the basic idea is to map data sets of variable length to data sets of a fixed length. In order to do this, the input message is split into chunks of 512-bit blocks. Padding is added to the end so that its length can be divided by 512. Now these blocks are processed by the MD5 algorithm, which operates in a 128-bit state, and the result will be a 128-bit hash value. After applying MD5, generated hash is typically a 32-digit hexadecimal number.

Although MD5 is a widely spread hashing algorithm, is far from being secure, MD5 generates fairly weak hashes. Its main advantages are that it is fast, and easy to implement. But it also means that it is susceptible to brute-force and dictionary attacks. Rainbow tables with words and hashes generated allows searching very quickly for a known hash and getting the original word.

FILE SECURITY

It is the process which provides security to the whole data which present in the cloud environment. Clouds provide multiple services to the user such as view, edit, download, etc., and a cloud provides limited services to an individual user. In this security process an individual user gets the permission to modify the data present in cloud environment through a random key which is generated by the cloud environment using an algorithm known as SHA Hash function.

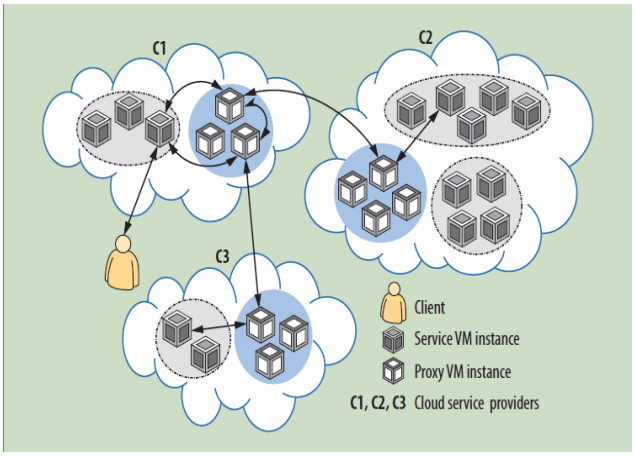

Figure:-Client sends a request to cloud C1, which dynamically discovers the need to use Services from clouds C2 and C3. C1 employs proxies to manage these interactions.

This key is send to respective mail which is suggested by the user. User has to report this key in the respective column presented by the cloud and the cloud compares the key which they send and user entered in the respective column and gives the permission for modification. All the users have only view permission but only a few has permission to modify the data present in the clouds. An user who does not have permission to modify the data file has requested for that then the cloud shows an information that he has no right to access this right. A Cryptographic Hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digests.

V. Performance Evaluation

Performance: The user once clicked on download link, a hash code is generated and sent to registered email. When the user enters this security key in required space the file is downloaded into users system. Collaboration between the clouds done only by the proxy service provider, this increases the security.

Security: In the proposed system the security is provided in two ways, one is providing the security at base level i.e. encrypting the passwords of the user by MD5. Two providing security at file level i.e. the hash code is generated when user clicks on file and sent to mail. This increases the security to the data that is stored in the cloud.

VI. Conclusion

In this paper, we proposed a secure multicloud computing which provides collaboration between clouds and gives the user opportunity to download the files from different cloud that are present. This also provides the security to the user's password and also to the files and data present in the cloud.

References

1. P. Meill and T. Grance, The NIST Definition of Cloud Computing, special publication 800-145, Nat'l Inst. Standards and Technology, 2011, p. iii + 3.
2. D. Bernstein and D. Vij, "Intercloud Security Considerations," Proc. 2nd Int'l Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.
3. R. Buyya et al., "Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing as the 5th Utility," Proc. 9thIEEE/ACM Int'l Sympi. Cluster Computing and the Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.
4. B. Rochwergeri et al., "Reservoir—When One Cloud Is Not Enough," Computer, Mar. 2011, pp. 44-51.
5. M.P. Papazoglou and W. van den Heuvel, "Blueprinting the Cloud," IEEE Internet Computing, Nov./Dec 2011, pp. 74-79.
6. S. Ortiz Jr., "The Problem with Cloud Computing Standardization," Computer, July 2011, pp. 13-16.
7. P. Mell and T. Grance, "Perspectives on Cloud Computing and Standards, NIST Information Technology Laboratory," Nat'l Inst.Standards and Technology, 2008; http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud computing standards_ISPABDec2008_P-Mell.pdf.
8. W. Jansen and T. Grance, Guidelines on Security and Privacy in Public Cloud Computing, special publication 800-144, Nat'l Inst. Standards and Technology, 2011, p. x + 70.
9. S. Chandrasekhar et al., "Efficient Proxy Signatures Based on Trapdoor Hash Functions," IET Information Security, Dec. 2010, pp. 322-332.
10. C.M. Ellison et al., SPKI Certificate Theory, IETF RFC 2693, Sept. 1999; www.ietf.org/rfc/rfc2693.txt.
11. E. Hammer-Lahav, ed., The OAuth 1.0 Protocol, IETF RFC 5849, Apr. 2010; http://tools.ietf.org/html/rfc5849.
12. Y. Zhang and J.B.D. Joshi, "Access Control and Trust Management for Emerging Multi domain ii Environments," Ann. Emerging Research in Information Assurance, Security and Privacy Services, Emerald Group Publishing, 2009, pp. 421-452.
13. J. Jin et al., "Patient-Centric Authorization Framework for Electronic Healthcare Services," Computers & Security, Mar.-May 2011, pp. 116-127.
14. R. Wu, G.J. Ahn, and H. Hu, "Towards HIPAA-Compliant Healthcare Systems," Proc. 2nd ACM Int'l Symp. Health Informatics (IHI 12), ACM, 2012, pp. 593-602.
15. N.R. Adam and J.C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," ACM Computing Surveys, Mar. 1989, pp. 515-556.
16. L. Xiong, S. Chitti, and L. Liu, "Preserving Data Privacy in Out sourcing Data Aggregation Services," ACM Trans. Inter- net Technology, Aug. 2007, p. 17.
17. D.J. Abadi, S. Madden, and M. Ferreira, "Integrating Compression and Execution in Column-Oriented Database Systems," Proc.ACM SIGMOD Int'l Conf. Management of Data (SIGMOD 06), ACM, 2006, pp. 671-682.