ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

A Study on Security and Ontology in Cloud Computing

E.Kamalakannan[1], B.Prabhakaran[2], K.S.Arvind[3]

PG Scholar, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamilnadu, India [1]

PG Scholar, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamilnadu, India [2]

Assistant Professor, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamilnadu, India [3]

Abstract: Cloud Computing is the emerging technology which is providing the effective resource management platform. There are two major types of cloud that is Public and Private cloud. In Private cloud which is formed within the organizations. So in Private cloud data will accessible only by the authorized users and also we provide more level of security inside the organization. In the case of Public Cloud the resources should publically share to all cloud users. So here the issue is security. So we have to provide the security for the data which is in the Cloud. In Cloud Computing the data will outsourced to the Third Party Storage. We need to protect our data. Providing the security for the Cloud data is challenging. And also we made a detailed study about the Ontology, and how Ontology will use in Cloud. In this paper we made the study on improving the cloud security on the outsourced data.

Keywords: Cloud Computing, Public Cloud, Private Cloud, Third Party, Ontology

I. Introduction

In Existing there are many security services is available for shielding the resources which is stored in the server. In this paper we focused how to use those security mechanisms for protecting the Cloud resources. In this paper give the idea about how the Cryptographic scheme is used for protecting the resources.

Cloud is the enormous group of linked computers, these computers are servers or personal computer, and they can be structured private or public. Amalgamating and distribution are the main characteristics of the Cloud Computing. The reason for amalgamating is to provide the service for more number of consumers like cross-platform users and enterprise users. In this paper we made detailed study about security issues [1] in cloud computing.

Cloud Computing provide three kinds of services. In General they are

- IAAS
- PAAS
- SAAS

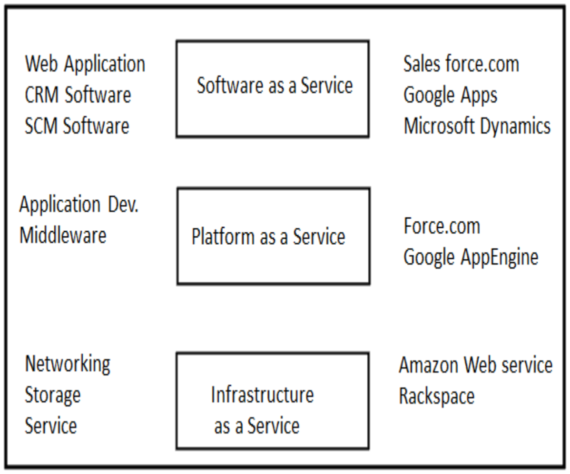

Figure1: Cloud Computing Service Models [1]

Software as a Service [2] is the service for using the service provider's applications (like Gmail, Hotmail) over the network. Platform as a Service [3] is used to provide the platform for deploy the customer created applications to a Cloud (like Sql.net, Google app engine). Infrastructure as a

Service which is provides the computational resource (like Amazon EC2, IBM smart cloud).

II. LAYERED ONTOLOGY OF CLOUD COMPUTING

In this classification methodology, the principle of compensability is used in a limited fashion. It is designed to be a stack of layers where each layer targets specific users. Each layer offers one or more cloud services [14]. The services are in the same layer if they have equal levels of abstraction. A cloud layer is said to be higher in the stack if its services can be composed from that of the underlying layer [15][16].

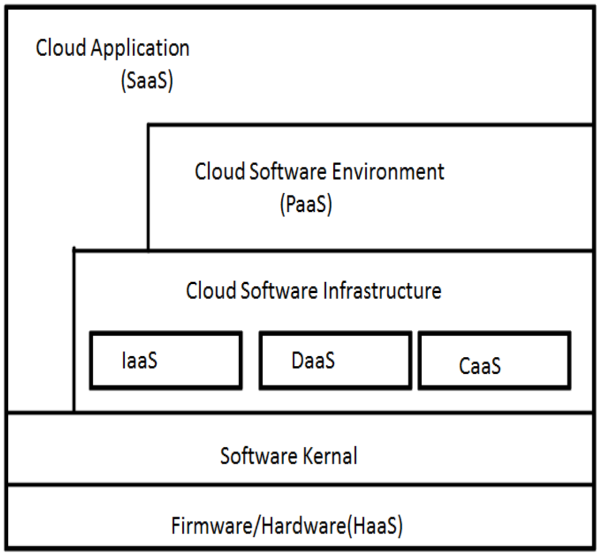

Figure 2: Layered ontology of cloud computing that shows the inter dependency and inter relations between the layers

A. *Cloud Application Layer*

This layer is visible to the end users. It is referred as the SaaS layer. One example of SaaS is Google Apps. This layer is accessed through web portals. It lessens the software maintenance and support [14]. It exports the computation work to data centers. It reduces the restriction on hardware requirements and increases performance. This layer can be developed from the software environment layer of the infrastructure components.

The cloud applications are simpler to develop and less error prone. Although it offers several advantages, it imposes limited flexibility and also poses security and availability issues. However they are currently managed by using lenient SLAs with the clients [15][16]. Other issues with SaaS are integration of legacy applications and migrating user data to the cloud.

B. *Cloud Software Environment Layer*

The users of this layer are application developers. The developers implement applications and deploy them on the cloud. This layer is referred as PaaS. E.g.: Google's App Engine. The providers supply a programming language level environment with a set of well-defined APIs [13]. The PaaS provider provides developers with the benefits of automatic scaling, load balancing and integration with other services on-demand. It also minimizes the logic faults in the Hadoop.

Deployment on the cloud can be considered as a cloud software environment. It provides its application developers with a programming environment i.e. map reduce framework for cloud computing [14]. Similarly, Yahoo's Pig is a high level language that enables processing in the Hadoop environment. It is an open source implementation of the cloud software environment layer. Cloud software environments facilitate the development process of cloud applications [13].

C. *Cloud Software Infrastructure Layer*

This layer provides fundamental resources to other high level layers. This in turn can be used to construct new cloud software environments or applications [12]. This layer can be categorized into computational resources (IaaS), data storage (DaaS) and communications (CaaS)[11].

D. *Infrastructure as a Service*

Virtual machines are the most common form of providing computational resources to cloud users at this layer. The users get finer-granularity flexibility and can use it to customize the software stack on their virtual machine. Virtualization is the enabler technology for this layer. IaaS was enabled by two virtualization techniques: Para-virtualization and hardware assisted virtualization. Both have addressed the performance isolation between VMs sharing common resources, but the performance interference between VMs could not be avoided. Amazon's Elastic Compute Cloud EC2 is one of the popular examples of commercial IaaS [13].

E. *Data-Storage as a Service*

This infrastructure allows users to store their data at remote disks and access them anytime from any location. Data storage systems need to meet several high standards of requirements, for maintaining users' information, such as reliability, availability, scalability and performance. However, all these can't be implemented in the same system [12].

DaaS providers usually implement the system such that they favour a particular feature over others. Some examples of data storage systems include GFS and RDBMS. An example of commercial DaaS system is Amazon's S3 [14].

F. *Communication as a Service*

Communication has become a vital component since the cloud systems need a guaranteed quality of service (QoS). Cloud systems are obliged to provide some communication capability that is predictable and reliable [15][16]. Towards this, the CaaS concept emerged to support network security, communication encryption and network traffic monitoring. VoIP telephone systems, audio and video conferencing are Cloud applications that can be collected of CaaS and provide compensable.

G. Software Kernel

The software kernel layer provides basic software management for the physical servers. They can be implemented as OS kernel, virtual machine or clustering middleware.

Generally, there are is an interconnected cluster of machines in which the grid applications can run. But grid computing does not provide room for virtualization abstraction [12]. So here check pointing, migration and load balancing were complicated. This layer uses several concepts from grid computing. Currently, grid portals and gateways for grid computing are being built through various approaches and such portals can be used in the design of portals and interfaces for the cloud [13].

H. Hardware and Firmware

This is the bottom most layer of this cloud ontology. This forms the backbone of the cloud. This is generally subleased as HaaS (Hardware as a Service).

The HaaS provider operates, manages and upgrades the hardware for its customers. This provides an advantage to the users since they do not need to invest in creating and managing data centers [14]. Example of HaaS is Morgan Stanley's sublease contract with IBM.

This model has strict SLAs. However, the technical challenges in HaaS are efficiency, ease and speed of providing large scalable systems. Other issues include data center management, scheduling and optimization of power consumption. Remote scriptable boot-loaders are one solution to remotely boot and deploy software stacks on data centers [13].

III. **CLOUD SECURITY APPROACHES**

In this section we made a study about security methods
.

A. Encryption

Outsourced cloud data will stored in the third party storage, the problem is we stored our original data. So the Better way to secure our outsourced data is Encryption [6]. Providing the Confidentiality is the main theme of the Encryption.

Encryption is the best way to hide our information from service provider. We can use either symmetric encryption or asymmetric encryption i.e. Public Key Cryptography [9]. If the data is very sensitive means we need to provide more level of security for the outsourced data. Personal Health Information is the most sensitive information.

So Attribute based encryption [4] [5] is a good way to protect the outsourced data. So we need to provide separate authentication and confidentiality for both public and private domain. Increasing security level we can also use the Digital Signature for protecting the sensitive information like Personal Health Records.

B. Auditing

Third Party Auditor [7] [8] is the very good solution for protecting the outsourced cloud data. For reducing the infrastructure cost we moving to the third party cloud storage. The security issue is the service provider can distribute to the information to other distributor. So we need the help of auditor. Auditor always audits the operations on our data.

Example if we are the seller of the amazing pictures. We using cloud storage we sell our pictures. In the sense by using auditor we can audit the operations on our pictures. If any kind of error log means auditor will monitor and restrict the unauthorized operations as well as the details send to us.

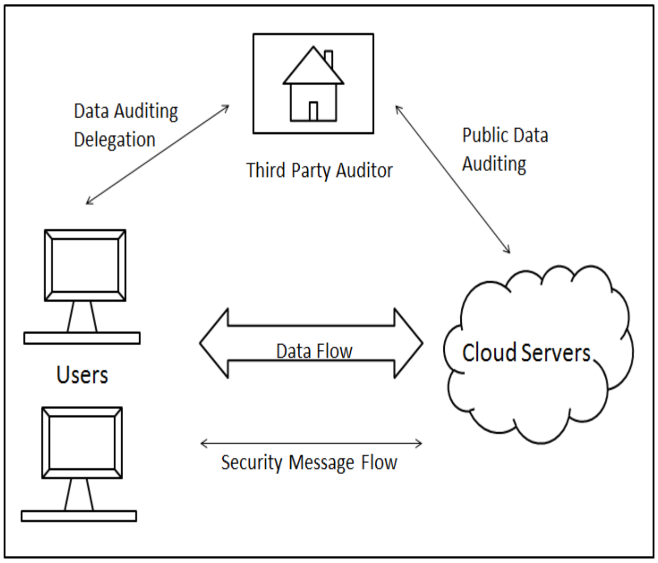

Figure3: The Architecture of Cloud Data Storage Service [7]

Above diagram used with the one Third Party Auditor. Here the data flows from users to the cloud servers are shown. With the help of the Third Party Auditor, Public Auditing is done.

So our cloud data is monitored by the Third party Auditor. My Suggestion is for this scenario we will use multiple number of third party auditor means the security level is beyond our expectation.

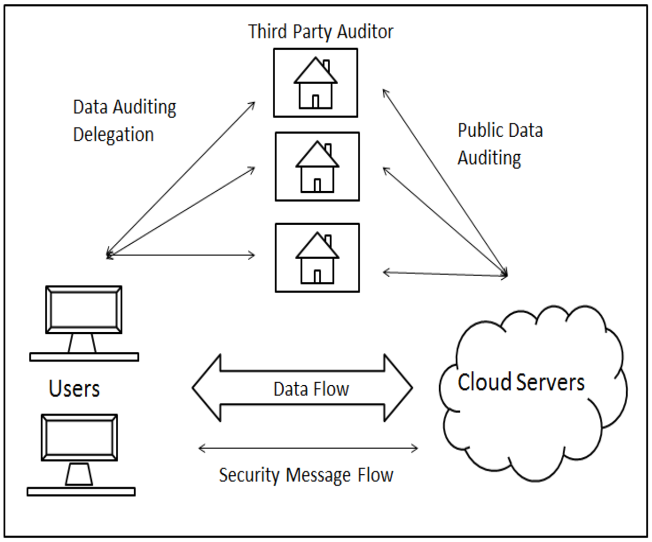

Figure4: Multiple Auditors [7]

Because in the case we are stored our data for our convenience in multiple cloud storage means there is the possible for slightly changed information will be shown for us. We can make use of the multiple auditor mechanism we can maintain our data.

C. Identity

Monitoring and confidentiality is the needed for the cloud security. But we also concentrate on the authentication also. So identity [10] is the good approach to make sure the authentication. Identity in the sense we can use the biometrics. Biometrics is the excellent identity for authentication. We suggest the IRIS is the best identity for authentication. We also integrate identity with the encryption. That is identity with encryption. IRIS based encryption. We can check IRIS for authentication. For Confidentiality we can use the encryption algorithm. So we provide the multiple level of security. These methods are used for efficiently in private cloud.

IV. CLOUD ONTOLOGY

Cloud Computing has become more popular now a day's. In Cloud Computing there is no specialized search engine to find the cloud service that is matched with the user's requirements. The agent based service search engine use Cloud Ontology for reasoning about the relations of cloud service. Though the cloud computing has great features such as on demand self-service , resource pooling and rapid elasticity there is a shortage in cloud computing because it hasn't provided a unique semantic ground as that of Semantic Web . So, in order to provide an environment for automatic searching resources ontology is used. These are all some of the areas where Ontology is used in Cloud Computing [11] [17].

- Ontology based registries are used for self-motivated discovery of cloud computing resource diagonally various cloud computing platforms.
- Ontology can be used to provide intelligent customization framework for SaaS [12].
- The design of security method by proving role based access control using ontology.

Cloud Ontology has some concepts to determining the similarity between two concepts with Cloud Ontology. There are three types of reasoning to find an exact cloud service.
1) Similarity reasoning
2) Equivalent reasoning
3) Numerical reasoning [12].

Similarity reasoning is the technique used to increase the chance of finding relevant alternatives of a service. If any exact matching service will breach the customer's requirements or price range, then the other similar services are suggested within the customer's price range [12]. Equivalent reasoning shows the similarity among two sibling concepts based on those label values [11]. Numerical reasoning will calculate the similarity among two numeric concepts based on those label values.

V. CONCLUSION

In this paper we provide the details about some security methods for secure the cloud data. And also we suggest some of the methods for provide more level of security. And we made the detailed study about the security measure and how to enhance the security levels in the private cloud as well as public cloud. In this paper we study about the how encryption used for cloud security. We suggest the Public Key Cryptography is the good for security. And we made a detailed study about auditor. Auditing mechanism is the excellent way of monitoring our data as well as monitoring and maintaining the log records. And also we suggest the multiple auditors are improving the protections of the cloud data. And we did the study on identity. And also we suggest one of the identities and also made the study about the identity based encryption.

Using the identity based encryption we achieve the authentication as well as confidentiality. So if we using these three methods i.e. encryption, auditing, identity means definitely we will successfully achieve cloud security without any threats. Thus Ontology plays a very important role in the cloud computing technology by consolidating view of computing resources present across disparate Clouds, given that the ability to safeguard penetrating information from illegal access, customization of SaaS and by improve the overall efficiency.

REFERENCES

[1] Aderemi A. Atayero, Oluwaseyi Feyisetan, “Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption, Journal of Emerging Trends in Computing and Information Sciences”, VOL. 2, NO. 10, October 2011

[2] Bhaskar P., Admela J·, Dimitrios K·, Yves G.: Architectural Requirements for Cloud Computing Systems:An Enterprise Cloud Approach. J. Grid Computing 9(1), 3-26 (2011)

[3] Boniface, M., Nasser, B., Papay, J., Phillips, S., Servin, A., Zlatev, Z., Yang, K. X., Katsaros, G., Konstanteli, K.,Kousiouris, G., Menychtas, A., Kyriazis, D. and Gogouvitis, S.,“Platform-as-a-Service Architecture for Real-time Quality of Service Management in Clouds”, FifthInternational Conference on Internet and Web ApplicationsAnd Services, ICIW 2010, May 2010, Barcelona

[4] Ming LiShucheng Yu, Yao Zheng,Kui Ren, and Wenjing Lou,Scalable ,” Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013

[5] L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Records by Applying Attribute-Based Encryption,” technical report, Univ. of Twente, 2009.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007.

[7] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou,” Privacy-Preserving Public Auditing for Secure Cloud Storage”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ’10, Mar. 2010.

[9] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107,Dec. 2008.

[10] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-Based Encryption with Efficient Revocation,” Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008. P.P. van Liesdonk, Anonymous and Fuzzy Identity-Based Encryption MASTER'S THESIS, Eindhoven, Augustus 2007

[11] J. Kang and K.M. Sim, “Cloudle: An Agent-Based Cloud Search Engine that Consults a Cloud Ontology,” Proc. Int’l Conf. Cloud Computing and Virtualization, pp. 312-318, May 2010.

[12] Pankaj Arora* Rubal Chaudhry Wadhawan Er. Satinder Pal Ahuja,” Cloud Computing Security Issues in Infrastructure as a Service”. Volume 2, Issue 1, January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[13] Wei-Tek Tsai*, Xin Sun, Janaka Balasooriya,”Service-Oriented Cloud Computing Architecture”. 2010 Seventh International Conference on Information Technology.

[14] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma,” Cloud Computing: Different Approach & Security Challenge” .International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[15] Rajkumar Buyya Saurabh Kumar Garg, and Rodrigo N. Calheiros,“SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions” 2011 International Conference on Cloud and Service Computing.

[16] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang,”A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches”. Accepted in Wireless Communications and Mobile Computing – Wiley.

[17] Kwang Mong Sim,,"Agent-Based Cloud Computing".IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 4, OCTOBER-DECEMBER 2012

BIOGRAPHIES

E. Kamalakannan is a Second year M.E CSE Student of Kalaignar Karunanidhi Institute of Technology, Coimbatore. He received B.TECH IT Degree in Chettinad College of engineering and Technology, Karur. He is doing Project in the area of Cloud Computing.

B.Prabhakaran is a Second year M.E CSE Student of Kalaignar Karunanidhi Institute of Technology, Coimbatore. He received B.TECH IT Degree in Kalaignar Karunanidhi Institute of Technology, Coimbatore. He is doing Project in the area of Cloud Computing.

Arvind. K.S is working as Assistant Professor in Kalaingnar Karunanidhi Institute of Technology. He had received his Bachelor of Technology from Pondicherry University, Master of Engineering from Anna University Chennai and currently pursuing Research in Anna University Chennai. His field of Research is Cloud and Information Security.