IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Cloud Computing with Data Confidentiality Issues

Dr. S. S. Manikandasaran

Dean, Department of MCA, Christhu Raj Institute of Computer Applications, Christhu Raj College, Trichy, India.

Abstract: Cloud computing is a key enabling technology for fast wide-area networks and it has more powerful server computers. Cloud operates on a high-performance virtualization. Cloud provides wide range of users like individuals, businesses and governments to provide virtual resources such as CPUs, memory, hard drives, bandwidth, platforms, and applications in an on-demand environment. Every day, the data is growing at a rapid rate in enterprises. To store data, a large number of processing units, hard drives, network infrastructure and other resources are required. Cloud satisfies this entire computational requirement to any enterprises by its infrastructure, but, at the same time, cloud is step-down by some of the security related issues. Maintaining confidentiality of data in the cloud is the most important security issue. This paper describes the cloud computing architecture, data management in cloud environment and data confidentiality issue in cloud. Cloud has many issues among that security is the top most issue. This paper opens the confidentiality problem in cloud data storage and also helps the researcher to kick start their research to address data confidentiality issues in the cloud environment.

Keywords: Cloud Computing; Data Confidentiality; Security Issues; Cloud Storage;

I. INTRODUCTION

This Cloud computing is an internet based computing. It is evolved from grid computing, utility computing, parallel computing, distributed computing and virtualization [1]. It has more powerful computing infrastructure with a pool of thousands of computers and servers [2]. It provides computational resources like server, storage, software, memory, network etc., as on-demand services [3]. It helps to reduce the computational infrastructure investment and maintenance cost of IT requisite for Small and Medium scale Enterprises (SME) [4]. It provides Everything (X) as a Service (XaaS) where 'X' denotes software, OS, server, hardware, storage, etc [5]. Cloud services are scaling up and down based on the users' demand [6]. Cloud has multiple datacentres placed in different geographical locations in the world to provide reliable services to the users [7]. It provides unlimited service provisioning without any human intervention. Cloud automates the service provisioning by way of running a number of Application Programming Interface (API) in the cloud storage environment.

The major feature of cloud computing is that it allows sharing and scalable deployment of services as needed by the users from any location. Cloud computing saves time and money during software up-gradation; cloud services are updated by the provider; so users are always working on the latest platform [8]. Cloud minimizes the amount of wasted computing resources and can also reduce energy consumption significantly.

The main core area of Cloud computing is Virtualization [9]. Virtualization empowers the cloud as a scalable and elastic service environment. It enables a dynamic datacentre where servers provide a pool of resources that are connected as needed, where the relationship of applications to compute, storage, and network resources changes dynamically in order to meet both workload and business demands. Cloud is mainly used for storing data in the remote cloud server. SMEs are not having enough infrastructure to keep their data on-premises, so they outsource their databases to the cloud storage. Outsourcing helps SME to grow up in their business .

Outsourced data of SME are controlled and maintained by the Cloud Service Providers (CSP) and user don't have any right on their data when data are in cloud storage. This scenrio makes some security issues in the cloud storage. The confidentialial data in cloud must be secured from the unwanted threats. Protecting data confidentiality is cloud storage is the open problem in cloud environment.

II. CLOUD COMPUTING ARCHITECTURE

The current cloud computing system mainly consists of three service models, Software as a Service (SaaS), which provides online software to users and it is controlled by CSPs. Platform as a Service (PaaS), which enables the web application developers to easily host their online web application on the cloud platforms and user only control the application whatever they are hosted in the cloud. Infrastructure as a Service (IaaS), provides computing infrastructure in virtualized manner based on the users demand [10].

The cloud system is deployed in four models, Public cloud, which is operated and controlled by third party service providers and it is accessed by any internet users. It is more cost effective and adaptable to all levels of IT users but it has some security related issues. Private cloud, which is maintained by individual organization or institution, is lunched for their computing needs. It is more expensive and secured cloud model. Community cloud is used for specific community of users such as Government, Medical and Education. Hybrid cloud is the integration of any two or three clouds for maintaining

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

sensitive and insensitive data.

Cloud has five essential characteristics which provide unique features to the cloud than other computing [11]. On-Demand Self-Service, It enables users to use cloud computing resources without human intervention between the users and the Cloud Service Providers (CSP). Broad Network Access, High-bandwidth communication links must be available to connect to the cloud services. High-bandwidth network communication provides access to a large pool of computing resources. Location-Independent and Resource Pooling, Computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to users' demand. Applications require resources. However, these resources can be located anywhere in the geographic locations physically and assigned as virtual components whenever they are needed. Scalability, it enables new nodes to be added or dropped from the network like physical servers, with limited modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to users'demand. Measured Service, Users are billed automatically based on the usage of cloud resources. Cloud systems automatically control and optimize resource usageby leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). The cloud computing architecture with these layers is shown in Figure 1 [12].

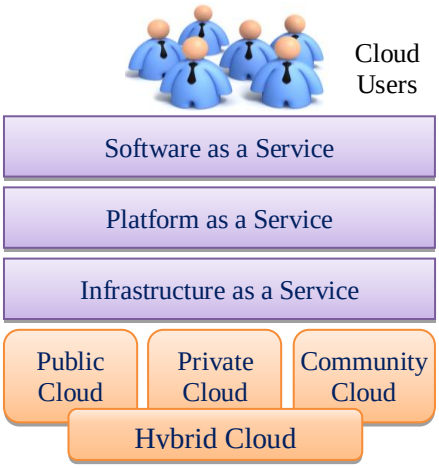

Fig. 1 Current Cloud Computing Architecture

A cloud is structured in seven layers on the basis of Cloud Security Alliance: 1) Facility Layer, 2) Network Layer, 3) Hardware Layer, 4) OS Layer, 5) Middleware Layer, 6) Application Layer and 7)The User Layer [13][14][15]. The CSPs or the cloud users can manage these layers.

A. The Facility Layer

The facility layer provides physical security. A high priority should be considered in controlling and monitoring physical access to the hardware. Closed-circuit cameras and patrolling security guards, alarm system, administrator logging, authentication, confidentiality agreements, background checks, and visitor access should be incorporated into surveillance of physical security. Also, an architectural security should be adequate enough to guard the data center from any kind of physical attack.

B. The Network Layer

The provider furnishes the network access to the users to access the customer data across the Internet on cloud. Hence, the network defense devices should collect information about security events on the networks. The provider should maintain, monitor and audit network flow data. Also, the customer should request these audits for verification.

C. The Hardware Layer

As the customer accesses services from virtual machines, the provider should maintain and monitor that the hardware is tamper-free. The provider should have appropriate protocols to monitor the connection topology, memory use, bus speeds, processor loads, and disk storage and so on.

D. The OS Layer

The vital important factor to be considered in cloud environment is securing the host OS. If it can be accessed by the illegal users, the customer data would be compromised. The provider should deploy an OS that manages to identify where the security policy or configuration might be lacking and prevent future invasions.

E. The Middleware Layer

Middleware involves virtualization management tools, data format conversion, performance of security functions, and access controls management.

The middleware mediates between the applications and the OS. It should monitor and secure communication between various systems. So, the provider should ensure that the middleware will accept and transmit only encrypted data and protect it against malicious manipulation.

F. The Applications Layer

The providers provide the application as a service to the public. So the code can be exposed to potentially malicious users. Hence, secure coding and secure software development should be an important factor to be considered. Customers should prefer applications in which the source code and business logic can be carefully examined by neutral third parties for potential flaws. Also, applications should sufficiently monitor to detect viola-tions in web based applications. The provider should widely deploy stricter security policies in application layer.

G. The User Layer

The cloud users can be of two types: Web-based application cloud users and members of customer organization user. The former accesses cloud information in insecure environment, while the latter uses information which has security policy. However, access patterns can be monitored for malicious behavior. For example, Google Apps monitors login behavior such as the time and IP

address, makes this information available to the user, and notifies the user of aberrant behavior. This idea could be extended to make digests of such alerts available to IT managers about the accounts for which their organization is responsible. In addition, the customer might access sensitive data in public areas.

The authorized users can demolish many security policies in a few clicks because of carelessness and web browsers have many vulnerability than can be manipulated. So, user education is the best way to avoid such problems in cloud environment.

III. DATA MANAGEMENT IN CLOUD STORAGE

The data management is a critical aspect for Enterprises [16]. The Enterprises are interested in getting the benefits from the cloud paradigm, to outsource their data to cloud database service providers and to access their data via internet. This data management model is referred to as Database as a Service (DaaS) [17]. DaaS is one of the most important applications of SaaS delivery model. DaaS model provides many benefits to enterprises as it saves the cost of database administration, and offers reliable storage[18].

In DaaS model, enterprises store data through internet into the database that is managed by Data Base Administrators (DBA) of the Service providers. DBA sought to have full control over the database to perform responsibilities of DBA like database backup, database restore, and recovery of database in case it is crashed and also to achieve performance and tuning of the database [19]. This situation results in two types of attacks on the cloud data; attacks are either by CSP or other users of cloud services. Although DaaS model is attractive, it is not successful since the DBA can look into the data and can transfer business sensitive information to the competitors [20].

IV. CONFIDENTIALITY OF OUTSOURCED DATA

Data sent to the cloud are not stored in a single cloud storage server. It is replicated to different cloud data centers located in different places in the world. Data centers are controlled and maintained by different experts from CSPs. The data can be hacked from any datacentre [21]. In cloud storage, maintaining the confidentiality of the data is the primary issue.

In [22], confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or devices. Hence, it must make sure that the users' confidential data, which the users do not want to be accessed by CSPs, are not disclosed to CSPs in the cloud computing systems, including applications, platforms, CPU and physical memories.

It is noted that users' confidential data are disclosed to a CSP only if all the following three conditions are satisfied simultaneously [23]:

1) *The CSPs know where the users' confidential data are located in cloud computing systems.*
2) *The CSPs have the privilege to access and to collect the users' confidential data in cloud computing systems.*
3) *The CSPs can understand the meaning of the users' data.*

The above three conditions arise from the following reasons, in order to collect users' data. The CSPs must know the location of the data in cloud systems and have the privilege to access the data.

Even if the CSPs could collect users' data successfully, they may not be able to understand the meaning of the data unless the CSPs have at least some of the following information to understand the meanings of the data: Types of data, Functionalities and interfaces of the application using the data and Format of the data.

Hence, it is needed to prevent the CSPs from satisfying all the above three conditions, and then protect the confidentiality of users' data in cloud storage.

V. MAJOR PROBLEMS OF DATA CONFIDENTIALITY IN CLOUD

The current cloud computing system consists of three layers: software layer, platform layer and infrastructure layer. The software layer provides the interfaces for users to use CSPs' applications running on a cloud infrastructure. The platform layer provides the operating environment for the software to run using system resources. The infrastructure layer provides the hardware resources for computing, storage and networks [24].

Platforms or infrastructures could be provided as virtual machines. The following are the major problems of current cloud computing system:

- Each CSP has a software layer, a platform layer and a infrastructure layer. When users use a cloud application from a CSP, then the users are forced to use the platform and infrastructure provided by the same CSP. Hence the CSP knows where the users' data are located and has full access privilege to the data.
- The users are forced to use the interfaces provided by the CSP, and users' data have to be in a fixed format specified by the CSP. Hence, the CSP knows all the information required for understanding the data.

Protecting data from the CSP is more difficult process in the cloud environment. Because, they are privileged admins have rights to monitor users' data [25]. They are easily compromised the confidentiality of data stored in the cloud. So, maintaining confidentiality of data is more essential in cloud environment. Ensuring confidentiality helps all types of cloud users to securely store and maintain their data in the cloud.

VI. CONCLUSION

The unique and attractive features of cloud computing have been fuelling the integration of cloud storage in the enterprises. The mixture of pay-as-you-go with on-demand elastic operation of cloud makes the transition of on-premises storage to off-premises storage. The cloud storage reduces the capital expenditure and operational expenditure of users, as the users delegate the responsibilities to the cloud environment.

Regardless of it benefits, it has many security concerns and issues. Confidentiality is the main issue to be addressed by the researchers.

There are many confidentiality issues are described in the paper, researchers could take this issues for their research and address a proper solution for the issues in the cloud environment.

REFERENCES

[1] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg and Ivona Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility", Elsevier Science Publishers, Volume 25, Issue 6, 2009, pp. 599-616.

[2] Borko Furht, "Cloud Computing Fundamentals", Handbook of Cloud Computing, Chapter-1, Springer Science, Business Media, LLC, 2010, pp.1-17.

[3] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", Technical Report-800-145, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[4] Ali Khajeh-Hosseini, Ian Sommerville and Ilango Sriram, "Research Challenges for Enterprise Cloud Computing", Proceedings of ACM Symposium on Cloud Computing, 2010, pp. 1-11.

[5] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Elsevier Journal of Advanced in Control Engineering and Information Science, Procedia Engineering, 2011, pp. 2852-2856.

[6] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", Proceedings of IEEE International conference on High Performance Computing and Communications, 2008, pp.5-13.

[7] Sudha M and Monica M, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications, Volume 1, Issue 1, 2012, pp. 32-37.

[8] Armbrust M, Fox A, Griffith R, Joseph A. D, Katz R. H, Konwinski A, Lee G, Patterson D. A, Rabkin A, Stoica I, and Zaharia M., "Above the clouds: A Berkeley View of Cloud Computing", EECS Department, University of California, Berkeley, Technical Report, 2009, pp. 1-23.

[9] Zhang Q, Lu Cheng, and Raouf Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges", Springer Journal of Internet Service Application, Volume 1, Issue 1, 2010, pp. 7-18.

[10] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong, The Characteristics of Cloud Computing, IEEE International Conference on Parallel Processing Workshops, 2010, pp. 275-279.

[11] Dr. L. Arockiam, S. Monikandan, G. Parthasarathy "Cloud Computing: A Survey", International Journal of Internet Computing, Volume 1, Issue 2, ISSN: 2231 – 6965, October 2011, pp. 26-33.

[12] Ilango Sriram and Ali Khajehhosseini, "Research Agenda in Cloud Technologies", Proceedings of ACM Symposium on Cloud Computing, 2010, pp. 1-11.

[13] Jonathan Spring Software Engineering, "Monitoring Cloud computing by layer part 1" Security & Privacy, IEEE vol 9, Issue 2, pp 66-68, Mar 2011

[14] Jonathan Spring Software Engineering, "Monitoring Cloud computing by layer part 2" Security & Privacy, IEEE vol 9, Issue 3, pp 52-55, May 2011

[15] Cloud Security Alliance Web site, http://www.cloudsecurityalliance.org/.

[16] Waleed Al Shehri, "Cloud Database Database as a Service", International Journal of Database Management Systems, Volume 5, Issue 2, 2013, pp. 1-12.

[17] Carlo Curino, Evan P. C. Jones, Raluca Ada Popa and Nirmesh Malviya, "Relational Cloud: A Database-as-a-Service for the Cloud", Proceedings of Biennial Conference on Innovative Data Systems Research, 2011, pp. 235-240.

[18] Atiq ur Rehman and M. Hussain, "Efficient Cloud Data Confidentiality for DaaS", International Journal of Advanced Science and Technology, Volume 35, 2011, pp. 1-10.

[19] Ramakrishnan Raghu, Gehrke Johannes, "Database Management Systems", McGraw-Hill Higher Education, 3rd Edition (en), 2003, pp. 282.

[20] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur, "Security Issues in Cloud Computing", High Performance Architecture and Grid Computing Communications in Computer and Information Science, Volume 169, 2011, pp 36-45.

[21] Ramgovind S, Eloff MM and Smith E, "The Management of Security in Cloud Computing", Proceedings of IEEE International Conference Information Security for South Africa, 2010, pp. 1-7.

[22] William Stallings, "Cryptography and Network Security: Principles & Practices", 4th edition, Prentice Hall, ISBN: 978-0-13-187316-2, 2005.

[23] Yau SS, An HG., "Confidentiality Protection in Cloud Computing Systems", International Journal of Software Informatics, Volume 4, Issue 4, 2010, pp. 351-365.

[24] Arijit Ukil, Debasish Jana and Ajanta De Sarkar, "A Security Framework in Cloud Computing Infrastructure", International Journal of Network Security & Its Applications, Volume 5, Issue 5, 2013, pp. 11-24.

[25] Dr. L. Arockiam, S. Monikandan," Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 8, ISSN : 2278-1021, August 2013, pp. 3064-3070.

BIOGRAPHY

Dr. S. S. Manikandasaran is working as Dean in Christhuraj Institute of Computer Application, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India. He has 8 years of experience in teaching and 5 years of experience in research. He is completed his MCA and M.Tech in Bharathidasan University, Tiruchirappalli in 2007 and 2009 respectively and also completed his Ph.D degree in Manonmaniam Sundaranar University, Tirunelveli in 2015. He has attended many International and National Conferences, Seminars and Workshops. He has published more than 30 research articles in the International / National Conferences and Journals. He has delivered more than 15 lecturers in various National Level seminars, symposium and conferences. His research interest is Cloud computing, Network Security, Cloud Security, IoT and Web Technology.

DOI 10.17148/IJARCCE.2016.5123