International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 1 347 - 350

Access to Encrypted Data in Cloud Database

Sakshi Sanjay Deshmukh
Department of Computer Science & Engg.,
P.R.M.I.T. &R., Badnera. India.
ssdeshmukh18@gmail.com

Dr.G.R.Bamnote
Head, Computer Science & Engg. Department,
P.R.M.I.T. &R., Badnera. India.
grbamnote@rediffmail.com;www.hod_comp@mitra.ac.in

Abstract— Today internet is considered as one of the basic need for human being and to make it more interactive various technologies have been developed and cloud computing is one of them. Cloud computing is a well-known technology which has become today's important research area due to its ability to reduce the costs associated with computing. It is one of the enticing technology which provides various services to its user as per demand over the internet. Social media channels, corporate structures and individual consumers all are switching towards the magnificent world of cloud computing. This technology is having security issues of data confidentiality, data integrity and data availability. Cloud is a mere collection of tangible super computers spread across the world so authentication and authorization for data access is more than a necessity. Proposed work attempts to overcome security threats related to data in data bases over cloud. The proposed methodology suggests the encryption of the data uploaded on the cloud using various algorithms available for cloud encryption and also tries to provide an efficient access to encrypted data in database over cloud.

Keywords-*Cloud, Encryption, Encrypted database, Virtual cloud.*

*****

I. INTRODUCTION

Cloud computing has been conceived as the next generation pioneer for IT Enterprise. In modern era of networking system, Cloud computing is one the most precious and developing concept for both the developers and the users. Cloud computing is a preferable platform for those people who are mostly interrelated with the networking environment. It offers dynamically scalable resources provisioned as a service over network. Cloud computing refers to manipulate, configure, and access various applications online. It can be defined as "A set of network delegate services providing extensible, inexpensive computing platforms on demand; which could be accessed simply and ubiquitously" [20].Provisions of Economic benefits are the main motivators for the use of Cloud services, since it promises the reduction of capital expenditure and operational expenditure. Reduced hardware and maintenance cost, attainable throughout the world, flexibility, platform independency are some advantages of Cloud computing. Multi-tenancy and elasticity are the key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance among different and multiple tenants. Elasticity allows scaling up and down resources as per the demands of clients. Both characteristics focus on improving resource utilization, cost and service availability. From past few years the world of computation has changed from centralized (client-server) system to distributed systems. Generally in Cloud computing services data maintenance provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. Logically, the client has no control over it. Internet is the communication media for Cloud computing. In the Cloud computing environment, applications, resources and information are shared among all of the servers and clients. As a result files or data stored in the cloud many times accessible to all [6]. Therefore, there is possibility that all other users of the cloud can handle that data or files of an individual. Thus the data or files become more prone to attack. So it is very easy for an intruder to disturb the original form of information [19]. Another difficulty with the Cloud computing system is that it has to face is that an individual may not have control over the place where the data needed to be stored. Resource allocation and scheduling policies which are provided by the cloud service provider used by clients over cloud. Thus, it is important to protect the data or files in the midst of unsecured processing. Although Cloud computing has achieved a great success in various industries like a software industry, a Government Sectors or a Medicare sector. From the security viewpoint, various risks and issues are identified in the area of Cloud computing. There are various threats associated with the security but one of the major issues is the security of data being stored on the provider's cloud and privacy while the data is being transmitted [18]. So to make Cloud computing technology more secure, concurrent access to data on cloud and independent access of data; a framework is proposed to encrypt the data over cloud using various encryption algorithms.

II. PRELIMINARY CONCEPTS OF CLOUD COMPUTING:

Cloud computing services:

According to National Institute of Standards and Technology (NIST); Cloud computing services can be available by three ways are: SaaS, PaaS and IaaS which are as shown in Figure1 [20].

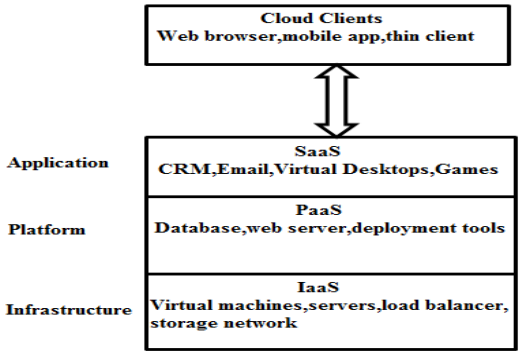

Figure 1: Cloud service delivery models

❖ **Software as a Service(SaaS):-**

SaaS provides software application as a service for clients. Customer Relationship Management (CRM) applications, Help Desk Applications, Human Resource (HR) Solutions are some applications provided by SaaS.

❖ **Platform as a Service(PaaS):-**

PaaS offers the runtime environment for many applications. Development & deployment tools, required to develop application can be provided. It has a feature of point-and-click tools that allow non-developers to create web applications. Google Apps and Microsoft Windows Azure are generally known PaaS providers.

❖ **Infrastructure as a Service(IaaS):-**

In IaaS cloud vendors deliver computation resources, storage and network as internet-based services. IaaS also provides access to fundamental resources such as physical machines, virtual machines, virtual storage. Amazon's EC2 is most IaaS provider.

Cloud classification:

Accessibility of cloud services depends on how it is located. Various types of accessibility or deployment modes are as shown in Figure2 [7][19].

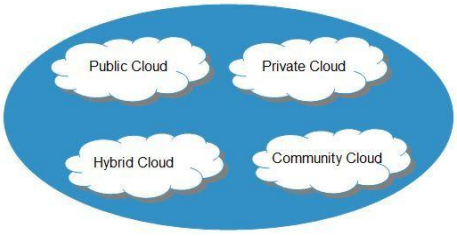

Figure 2: Cloud Deployment Models

a) Public Cloud:

It allows many services and applications to be easily accessible by all people; e-mail service is best example. A cloud infrastructure is provided to many customers and is managed by a third party. At the same time, multiple enterprises are able to work on the provided infrastructure.

b) Private Cloud:

It allows many services and applications to be accessible within an organization. Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider. This uses the concept of virtualization of machines, and is a proprietary network.

c) Community cloud: It allows many services and applications to be accessible by a particular group within an organization.

d) Hybrid Cloud: It is a concatenation of two or more cloud deployment models, generally Public cloud and Private cloud.

Cloud computing architecture:

The architecture is mainly consisting of two parts Front End and Back End as shown in Figure 3 [20].

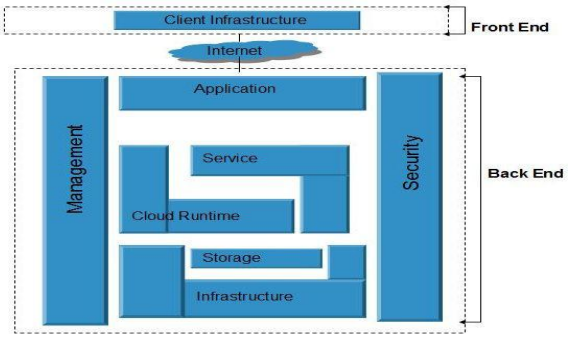

Figure 3: Cloud computing Architecture

- **Front End:** Front End includes client infrastructure. It provides interfaces and applications that are necessary to access cloud computing platforms. Example is web browser.
- **Back End:** Back End includes cloud components. Various applications provided by it, services, storage strategies, infrastructures are included by this.

III. RELATED WORK:

Cloud computing includes logical entities like data, software which are accessible via internet. Historically, some software such as phrase processor or paint brush required a license to be installed on client's machine. The client-server model came in to existence, which provided with large storing capabilities allowing users to host applications with data for workgroup. The client machine would demand a browser to get into these server functionalities, and would use client CPU and memory for processing. On Cloud computing technology different security models and algorithms were applied. But, many times these models failed to solve all most all the security threats. Many researchers done useful work on cloud computing and also proposed some security techniques. **Luca Ferretti, Michele Colajanni, and Mirco Marchetti** proposed a novel architecture for describing possibility of executing concurrent

operations on encrypted data and integrates cloud database services with data confidentiality [1].**Sushmita Ruj, Milos Stojmenovi and Amiya Nayak** proposed a new decentralized access control scheme .In that cloud verifies the authenticity of unknown user before storing data [2]. **Julisch K. & Hall. M.** proposed importance of Virtualization, Web Service, Service Oriented Architecture and Application Programming Interfaces for cloud computing [14]**.Gellman** discussed standards for collection, maintenance and disclosure of personal information over cloud. **Jarabek and Hyde** described possible attacks on cloud data [12][15].**Guo Yubin et al.** had done work on storage solution for No SQL database using homomorphic encryption algorithms. Data querying Protocol described in this work and algorithms for data manipulation are given also[5].**Ming Li et al.** proposed a novel framework of secure sharing of personal health records over clouds. Considering partially trustworthy cloud servers, patients will be able to maintain their own privacy through encrypting their PHR files to allow fine-grained access [6].**Omer K. Jasim et al.** discussed the various encryption symmetric key algorithms and asymmetric key algorithms. They also discussed the performance of encryption algorithms on a cloud environment for input blocks of different sizes and how the change in the size of the files after encryption is complete [7].**T. Sivasakthi and Dr. N Prabakaran** proposed use of digital signature for authentication purpose in cloud computing. The propose work assured to secure the information in cloud server[3].**SanjoliSingla, Jasmeet Singh** proposed a design that can help to encrypt and decrypt the file at the user side that provide security to data at rest as well as while moving. For this Rijndael encryption algorithm along with EAP-CHAP used [4].**Kuyoro S. O.**described key security considerations and challenges which are currently faced in the Cloud computing [8].**J. Bethencourtet al,** discussed Attribute Based Scheme (ABE). For this, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs that are In key-policy and Cipher text-policy [17]. **ENISA**(European Network Information and Security Agency)investigated the different security risks related to adopting cloud computing along with the affected areas, various risks, impacts, and vulnerabilities in the cloud computing may lead to such risks[18]. **Balachandra** et al, discussed the security SLA's specification and objectives related to data locations, segregation and data recovery[16].**Kresimir** et al, discussed high level security concerns in the cloud computing model[14]. **Bernd** et al, discussed the how security weaknesses existing in the cloud platform and how they affect the client data. [20]. **Cloud Security Alliance (CSA)** had given TOP threats to cloud computing [19].**Service Level Agreements (SLA)** also defined many times for data on the cloud [20].

IV. PROPOSED WORK:

To allow independent access to the data over cloud database, to share that data concurrently on many clouds and to handle all data transactions of data present on cloud data base proposed work will be useful. Proposed work will try to achieve following objectives:

- Creation of secured distributed, concurrent and independent encrypted data over cloud.
- Creation of Multiple virtual clouds in which every cloud will itself act as an owner of particular data and encryption can be performed over it.
- Secure cloud data in databases via encryption techniques and by using symmetric keys and asymmetric keys.
- Confidentiality and Security of Public cloud access would be maintained.

V. CONCLUSION:

Cloud computing is a very vast research area today. Cloud computing is like a coin having two ends. One end focuses on fastest technology, a huge array of applications to use, seemingly unlimited storage space. On the other end lie various security threats which emerge with shared spaces such as breach of confidentiality, hampering of data integrity and non- availability of data. Business and government is continuously trying to improve Cloud environment so that an effort to reduce costs, improve efficiencies and reduce administrative overhead. Here propose a framework; which encrypts data before it is uploaded on to the cloud and it also create secured, concurrent and independent access to encrypted data over cloud. Thus, if used securely, cloud computing provides a user with amazing benefits and overcomes its only disadvantage of security threat.

REFERENCES

[1] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud databases", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 25, no. 2, pp.437-445, FEBRUARY 2014.

[2] Sushmita Raj, Milos Stojmenovic, Amiya Nayak," Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 25,no. 2, pp.332-345,February 2014.

[3] T. Sivasakthi and Dr. N Prabakaran, "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" , *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 2,pp.12-18, February 2014.

[4] Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", *International*

Journal of Advanced Research in Computer Engineering & Technology ,vol. 2, no. 7,pp.2232-2235, July 2013

[5] Guo Yubina, Zhang Liankuanb, Lin Fengrena, Li Ximinga,"A Solution for Privacy-Preserving Data Manipulation and Query on NoSQLDatabase", JOURNAL OF COMPUTERS, VOL. 8, NO. 6, 1427-1432, JUNE 2013.

[6] Ming Li, Member, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 24, no. 1, 131-143, JANUARY 2013.

[7] Omer K. Jasim, Safia Abbas, Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Efficiency of Modern Encryption Algorithms in Cloud Computing", *International Journal of Emerging Trends & Technology in Computer Science*,vol.2,no.6,pp.270-274,December 2013.

[8] Kuyoro S. O., Ibikunle F., AwodeleO. ,"Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol. 3, no.5, 247-255, 2011.

[9] Gartner," From Secure Virtualization to Secure Private Clouds", *http://www.vmware.com/files/pdf/analysts/Gartner-From-Secure-Virtualization-to- Secure-Private-Clouds.pdf*, October 2010.

[10] "Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud", *https://www.cloudsecurityalliance.org,December,2009.*

[11] Jericho Forum," Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration", April, 2009.

[12] C. Jarabek,"*A Review of Cloud Computing Security: Virtualization, Side-Channel Attacks, and Management"*, Department of Computer Science, University of Calgary, 2010.

[13] Julisch, K., & Hall, M., "Security and control in the cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.

[14] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349,2010.

[15] D.Hyde,"A Survey on the Security of Virtual Machines", *http://www1.cse.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf*, April 2009.

[16] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, pp. 517-520, 2009.

[17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[18] *http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing- risk-assessment*

[19] *https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.*

[20] *http://en.wikipedia.org/wiki/Cloud_computing.*