International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

Security on Cloud using High Level Encryption Techniques

Brijesh Kumar
Assistant Professor
Department of Computer Science,
Maharishi Arvind International Institute of Technology, Kota

Amrita Saraswat
Associate Professor
Department of Computer Science,
Maharishi Arvind International Institute of Technology, Kota

ABSTRACT

In today's life security of data is most important for everyone so it's very important that how secure data at the run time. With cloud computing platform it is very easy to transfer data between users and store any amount of data on cloud so it is easy to use anytime anywhere. To provide security on cloud it's very difficult because many issues are happened during provide security so with the help of this paper it's easy to provide storage security of data on cloud by physical hardware and virtual encryption process and security services on gateway to improve safe transaction of data.

Keywords: *measures Process, encryption Technique, structural design, facts security, Cloud stage, Architecture.*

1. Introduction

Cloud Computing is a scattered structural design that centralize server resources on a scalable step so as to provide on demand computing resources and services. Cloud service providers offer cloud platforms for their clients to use and construct their web services, much like internet service offer customers high rate broadband to access the internet. Computing on cloud is a way that enables smoothly, process of network access to a shared path of configurable computing resources on a different networks, servers, data, applications that can be continuous provisioned and released with lower management effort or service interaction. In general cloud providers offer

These types of services i.e. Service for Software, Platform as a facility and architecture. There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to strength for the resources on utilization time .Organizations can easily assemble the needs of swiftly changing markets to ensure that they are for all time on the foremost perimeter for their clients.

Process of gathering in-depth information to the interviewer's question from responder. Here the interviewer asks a question and expects an answer to that Different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, Objectives

- Identify existing cloud computing security challenges and their solutions from literature.
- Identify the challenges that have no mitigation strategies defined.
- Collect solutions/guidelines/practices from organizations, for a challenge with more

references but no mitigation strategies proposed (identified in literature).

There are also special types of cloud use models namely secret cloud, open cloud, mix cloud and area cloud. Details about the models are given below.
Open Cloud Network: Customers are only charged for the resources they use, sounder-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds.

Secret cloud: Secret cloud can be owned or leased and managed by the organization or a third party and exist at on- premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems.

Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities.

Mix Network : A computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Area Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in figure

II Cloud computing base

User and service provider having two types of security reason at the time of data access.

Cloud Server: in cloud server access acknowledge from the user and after that provide access of command which the users need on cloud it's a very important part by server. Service providers may also include systems parameter that build and support data centers hosting private clouds and they offer different services

III. CLOUD SECURITY ENCRYPTION

To provide security from physical layer to application layer there are Security within cloud computing at different layer by different check marks is an especially worrisome issue because of the fact that the strategy used to provide services do not be in the right place to the client themselves.

Some organizations have been focusing on security issues in the cloud computing. The Cloud Security Alliance is a non- profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Open Security Architecture (OSA) is another organizations focusing on security issues. They propose the OSA pattern, which pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis. For example, the Certification, Accreditation, and Security Assessments series increase in importance to ensure oversight and assurance given that the operations are being "outsourced" to another provider. System and Services Acquisition is crucial to ensure that acquisition of services is managed correctly. Contingency planning helps to ensure a clear understanding of how to respond in the event of interruptions to service delivery [8]. The Risk Assessment controls are important to understand the risks associated with services in a business context. National Institute of Standard and Technology (NIST), USA (http://www.nist.gov/) has initiated

activities to promote standards for cloud computing [15]. To address the challenges and to enable cloud computing, several standards groups and industry consortia are developing.

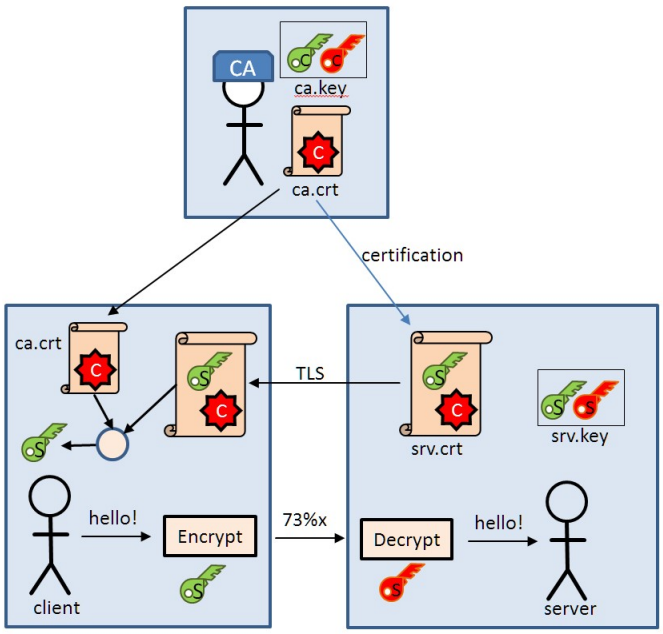

Fig.1 tls-handshaking-with-certificates-and-keys

IV. SECURITY ISSUES

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service, Utility Computing, Web Services, Platform Service , Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity

Access Applications: Server access to by user is controlled and restricted to direct or on-premise links which is not the case of cloud information centers. In cloud computing organizational access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to continue visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business Hackers have two main methods of causing problems for businesses' computer systems: they either find a way to enter the system and then change or steal in order from the inside, or they challenge to over-whelm the system with information from the outside so that it shuts down. One way a hacker might enter a small business's computer network is through an open port, or an Internet relation that remains open even when it is not being used. They might also attempt to appropriate passwords belonging to human resources or other authorized users of a computer system. each employee will be dispatched some different accounts to access different systems. Thus, multi-authentication for each employee might be very often to be confronted in an

Man-in-the-middle attacks is cryptographic show aggression is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

VM Security: essential machines are dynamic i.e it can fast be reverted to previous instances, paused and restarted, moderately easily. Ensuring that different instances running on the same physical apparatus are shared folders mechanism that grants users of a guest system read and write access to any portion of the host's file system including the system folder and other security-sensitive files. Vulnerability in Xen can be exploited by "root" users of a guest domain to execute arbitrary commands. The other issue is the

control of Server on host and guest operating systems.

Cloud Security: Networks are classify into many types like connencet and non-shared, public or private, LAN,MAN ,WAN all them having many number of threats and problem how to secure data.

Encryption at highly provide to reduce attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and in attendance are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data related to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network.

- Service Level Agreements (SLA's)
- Network Management y
- Data Encryption
- Cloud virtual machine
- Access Controls
- Energy Management

Conclusion and Feature work

Security of data is most important for everyone so it's very important that how secure data at the run time. With cloud computing platform it is very easy to transfer data between users and store any amount of data on cloud so it is easy to use anytime anywhere. To provide security on cloud it's very difficult because many issues are happened during provide security so with the help of this paper it's easy to provide storage security of data on cloud by physical hardware and virtual encryption process and security services on gateway to improve safe transaction of data.

References

[1] I. Foster and C. Kesselman (editors). The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, 1999.

2] F. Howell and R. Mcnab. SimJava: A discrete event simulation library for java. Proceedings of the first International Conference on Web-Based Modeling and Simulation, 1998.

[3] A. Legrand, L. Marchal, and H. Casanova. Scheduling distributed applications: the SimGrid simulation framework. Proceedings of the 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2003.

[4] J. E. Smith and R. Nair. Virtual Machines: Versatile platforms for systems and processes. Morgan Kauffmann, 2005.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia. Above the Clouds: A Berkeley View of Cloud computing. Technical Report No. UCB/EECS-2009-28, University of California at Berkley, USA, Feb. 10, 2009.

[6] R. Ranjan and R. Buyya. Decentralized Overlay for Federation of Enterprise Clouds. Handbook of Research on Scalable Computing Technologies, K. Li et. al. (ed), IGI Global, USA, 2009 (in press).

[7] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems, 25(6): 599-616, Elsevier Science, Amsterdam, The Netherlands, June 2009.

[8] Alok Tripathi, Abhinav Mishra, "cloud computing security consideration", 2011 IEEE International Conference on signal processing, communication and computing, 27 October2011, pp. 1-5.

[9] R. Buyya and M. Murshed. GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing. Concurrency and Computation: Practice and Experience, 14(13-15), Wiley Press, Nov.-Dec., 2002.

[10]A. Weiss. Computing in the clouds. NetWorker, 11(4):16–25, Dec. 2007.