International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-2, Issue-1, March 2012

An Approach for Secure Data Transmission in Private Cloud

Anurag Porwal, Rohit Maheshwari, B.L.Pal, Gaurav Kakhani

Abstract— In the cloud, the data is transferred among the server and client. Cloud security is the current discussion in the IT world. This research paper helps in securing the data without affecting the network layers and protecting the data from unauthorized entries into the server, the data is secured in server based on users' choice of security method so that data is given high secure priority.

Index Terms— Cloud, Private Cloud, Security, Secure data Transmission.

I. INTRODUCTION

Cloud computing is a recent trending in IT that where computing and data storage is done in data centers rather than personal portable PC's. It refers to applications delivered as services over the internet as well as to the cloud infrastructure – namely the hardware and system software in data centers that provide this service. The sharing of resources reduces the cost to individuals. The best definition for Cloud is defined in [9] as large pool of easily accessible and virtualized resources which can be dynamically reconfigured to adjust a variable load, allowing also for optimum scale utilization. The key driving forces behind cloud computing is the ubiquity of broadband and wireless networking, falling storage costs, and progressive improvements in Internet computing software. The main technical supporting of cloud computing infrastructures and services include virtualization, service-oriented software, grid computing technologies, management of large facilities, and power efficiency. The key features of the cloud are agility, cost, device and location independence, multi tenancy, reliability, scalability, maintenance etc.

Manuscript received Feb. 15, 2012.

Anurag Porwal, Department of Computer Science, Mewar University, Chittorgarh (Rajasthan), India, +919660484344,(e-mail: anuragporwal04@gamil.com).
Rohit Maheshwari, Department of Computer Science, Mewar University, Chittorgarh (Rajasthan), India, +919828081953, (e-mail: rohit.maheshwari27@gmail.com).
B.L.Pal, Department of Computer Science, Mewar University, Chittorgarh (Rajasthan), India, +919887164480, (e-mail: contact2bl@rediffmail.com).
Gaurav Kakhani, Department of Computer Science, Mewar University, Chittorgarh (Rajasthan), India, +918107599292, (e-mail: gauravkakhani@gmail.com).

II. DEPLOYMENT MODELS OF CLOUD

The cloud can be deployed in three models. The Fig: 2.1 explain its structure [12]. They are described in different ways. In generalized it is described as below:

A. Public Cloud:

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who bills on a fine-grained utility computing basis. This is a general cloud available to public over Internet.

B. Private Cloud:

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings.

C. Hybrid Cloud:

A hybrid cloud environment consisting of multiple internal and/or external providers "will be typical for most enterprises". By integrating multiple cloud services users may be able to ease the transition to public cloud services while avoiding issues such as PCI compliance.

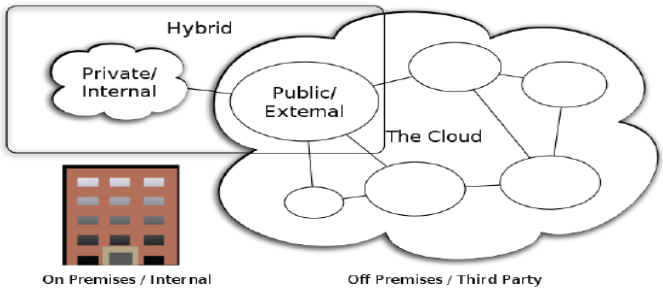

Fig 2.1: Cloud Computing Types

III. SERVICES PROVIDED BY CLOUD:

The different types of services provided by cloud are IaaS, PaaS and SaaS.

A. Infrastructure as a Service (IaaS):

IP's manage a larger set of computing resources such as storing and processing capacity. Through virtualization, they are able to split, assign and dynamically resize the resources to build ad-hoc systems as demanded by the customers, the Service providers. They deploy the software stacks that run their services. This is infrastructure as a service.

B. Platform as a Service (PaaS):

Cloud systems can offer an additional abstraction levels instead of supplying a virtualized infrastructure. They can provide the software platform where systems run on. The sizing of hardware resources is made in a transparent manner.

C. Software as a Service (SaaS):

There are services of potential interest to a wide variety of users hosted in a cloud system. This is an alternate to locally running application. An example of this is online alternative of typical office applications such as word processor.

Client
Application (SaaS)
Platform (PaaS)
Infrastructure (IaaS)
Server

Fig 3.1: Layers of cloud

IV. Motivation

Security in Information Technology is the main buzz word discussed in the current times. The hackers or attackers are increased in number and waiting to attack the important data over the new advanced technologies also. Among them cloud computing is one, this is the technology being adopted by every corporate company for reducing their expenditures and increasing their business profits. They are mainly worried for security of data. This leads me to this research area as my interest in security can be used in the advanced technology giving certain best solution to secure data over the cloud.

A. Security Issues and challenges

Subhashini [2] have described all security related issues present in the cloud computing. The various deployments of the cloud and all the issues present in each deployment are been defined in the paper. They have defined in respect to the service delivery where in each type of SaaS, PaaS, and IaaS. They in particular defined all the security problems in the software as a service of cloud computing. In Issues of SaaS, there are categories based on data, network, web applications and virtualization vulnerabilities.

Kresimer Popovic [7] have discussed different security concerns present in the cloud model which is losing confidentiality and integrity of the data while transfer, storage and retrieval. They also discussed on the things that is to be consider where the threats are present in cloud computing like from user to type of services. With the above issues they concluded that we need to take security and privacy in providing cloud services.

Balachandra reddy [4] have discussed about service level agreements that are been issued by user to provider before getting into cloud. This is the only trust a provider will see from user, but it not enough to provide security as it does not answers the problems to the losses of the user, there should be certain changes according to the type of service a user is working and need to be standardized with privileged user access, data segregation, location of data etc.

Steve Mansfield [12] has discussed regarding the advantages of having the cloud at the same time the issues present in cloud. When we use in our perimeter area we use many security sides like firewalls DMZ'z etc., where as in cloud all are on a remote system without any security. Author mainly points out that we need to have a great deal of trust in the design of system with good authentication and authorization capabilities.

Sameera Abdulrahman Almulla [11] have discussed about services in cloud computing, the challenges regarding the information security concerns in respect to confidentiality, Integrity and availability. They discussed security challenges of cloud computing in respect to identity and access management.

Patrick Mc. Daniel and Sean W. Smith [10] described about challenges of security and improvements that are to be made over cloud for secure data over cloud. They concentrated mainly on security issues over cloud instances. The instances over cloud will be running on some base system which may compromise and causes a security issue. There are also external adversaries over cloud which may lack protection of instances from third parties. They discussed certain opportunities which are to the great challenges for researchers.

The cloud computing security concerns were discussed in detail in [13] the main issues discussed were privacy concerns due to third party users. As the security due to hackers increase over internet and the cloud computing is totally on internet, there are different issues like attacks are discussed on it. In this it also discussed in detail about all the security issues over network, data leakage etc. as shown in below Fig:4.1, According to the IDC finding's, the users of cloud say that security is the main issue in cloud computing.

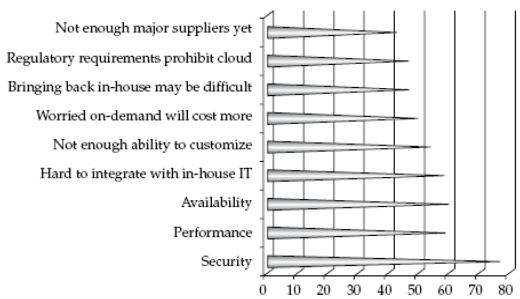

Fig 4.1: Security as a main issue

B. *Security Architectures*

The above discussion is on certain review literature by many research people on different aspects of security. The aspects went on describing the problems and threats in related to security in cloud. The literature in detail explains about the issues like security for data, virtualization security and prescribed format of SLA etc. There are many research people have keen interest in designing certain security architectures help for secure cloud computing. The following are described below:

Gary Anthes [6] has described the various security research works in cloud are discussed. He brought forward the research works done in popular companies like IBM, HP, and Microsoft. **T**here are many security risks involved in cloud computing, and also some good solutions are also been designed by the researchers which are pointed below.

1) Researchers at HP laboratories are prototyping cells as a service to automate security management in cloud. A cell is single administrative domain using security policies containing virtual machines, storage volumes across physical machines
2) IBM research people doing virtual machine introspection which puts security inside protected VM running on same machine. This employs number of protective methods listing the kernel functions. It can make reduce of running virus scanners on system.
3) Microsoft research described about cryptographic cloud storage where the data is secured by user by encrypting format such that the provider cannot get what the data is present.

Flavio Lombardi and Roberto Di Pietro has discussed [1] about a secure virtualization technique for ensuring security at hypervisor level. In a general system at base OS level, there is a problem like a user at one guest OS may interact with other Guest OS, which may lead to data loss if they are any attackers. So the new proposal ACPS (Advanced Cloud Protection System) was introduced. This will maintain security by preventing unnecessary logins into the other guest OS by weak passwords or weak SSH.

Cong Wang [5] has proposed their work on Data Storage security with respect to Quality of service. They have proposed approach which checks whether their data has been attacked or any integrity loss is done or not over the cloud. They will generate a homomorphism token which will ensure that the data is not lost. It is like a simple hash function which will be enabled to fast recover and storage errors.

These works help in securing the cloud systems, Virtualization, Data confidentiality and data storage security, there are still issues need to be discussed in secure data transmission between cloud Provider, service provider and cloud User. The secure data transmission is anyhow achieved by protocols like IPSec, SSL over web and the data over are also through web applications these current methods can be used for secure data transmission.

The secure data transmission works designed for storage networks are discussed by Kikuko Kamiasaka [8] who discussed in his paper for secure data transmission over IP Networks by developing Middleware works below application layer and selects suitable security approach based on the cluster of data items available in Application. This was proved that will help in securing the data as well as this works well than IPSec.

Sudha M [3] has proposed an idea for secure data transmission in cloud computing using transport layer techniques, the idea proposed in that is used is socket programming for secure data transmission over the client and server. This paper has compared the general secure data transmission by applying socket programming, a key exchange and secure data over cloud. The comparison is done response time and processing time.

IV. PROBLEM DOMAIN

1) The main problem is establishing trust in remote execution because a user program runs on a remote host in a data center, which a customer must make sure that his program is executed in its base system instance providing integrity and secrecy.
2) The cloud systems are shared resources, so there must be protection provided in the execution of a cloud instance from others. There must be isolation provided between two instances.
3) There are issues from hackers or attackers where they might get access to the base system by a communication channel and loss of data may happen. There might be chances of releasing a Trojan horse or virus to get the information leaked to his system.
4) The secure data transmission is anyhow achieved by protocols like IPSec, SSL over web and the data over are also through web applications these current methods can be used for secure data transmission but certain issues like Throughput and complexity in coding comes into issue.

A. *Service level agreements [SLA]:*

In service level transfer between a service user and provider a SLA is been issued. A SLA [service level agreement] is a document which defines the relationship between two parties: the provider and the recipient. This is clearly an extremely important item of documentation for both parties [4].If used properly it should:

- Identify and define the customer's needs
- Provide a framework for understanding
- Simplify complex issues
- Reduce areas of conflict
- Encourage dialog in the event of disputes
- Eliminate unrealistic expectations

Specifically it should explain a wide range of issues. Amongst these are usually the following:

1) Services to be delivered performance, Tracking and reporting problem management legal compliance and resolution of disputes customer duties and responsibilities security IPR and confidential information termination. The SLA is the Legal agreement between provider and client. The provider can gain the trust on his client is only through SLA.
2) These SLA are been used to fulfill the issues of the service user based upon the rules present in it but they would not go for any legal action if the not met that present in agreement, they don't really help the customers fulfilling their losses. The SLA is fully not a good security consideration.

Security at Transport layer is designed using port numbers where we get end-to-end security on an IP network. As the security is at transport layer, the data is secured at port level but Security at Network layer will use approaches like IPSec protocol, here the IP Packets will be secured before transmission. The different techniques in IPSec Protocol take different time structures based on the steps that should perform. Here we have two problems with this method. First, to encrypt an IP packet we need to change the code of the IP protocol. Second are again the problems of delay and throughput. Here each packet to be encrypted with any one of the different types of implementations of IPSec protocol. When large data is transferred the packets take a long time to get encrypted and loss in throughput.

VI. PROPOSED FRAMEWORK

A. Security framework for Private cloud:

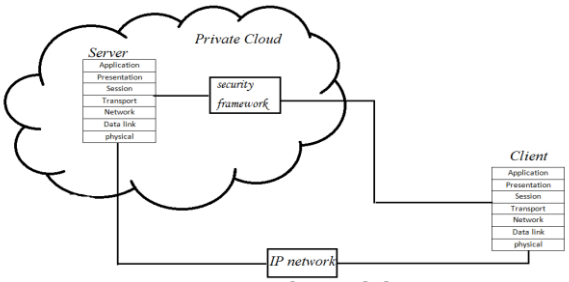

Fig: 6.1 High Level design

The Fig 6.1 is the design architecture where a new security layer is designed for private cloud. The new security framework is present in between session layer and transport layer such that it is transparent to application layer and the lower layers. So whenever a data is transferred by the client it is first secured by certain authentication protocols and saved at the server end. With this, the data will be stored in a secured way at server end. Those who want to download the data or view it should be connected or have access through same framework to view the data. This is done in application user level so that the data will be secured and transferred where there is need to disturb any lower layers of the network.

VII. DESIGN OF THE SYSTEM

A. Security Framework Model

The detailed design of the framework is in the below Architecture Fig 7.1. The nodes which are connected to server will be connected to the security layer. When an Application user wants to send data to private cloud, he needs to select a Security Algorithm based on the privacy level of the document, if he needs more security there must be a strong security algorithm to be selected. The security server will secure the document and save it in database.

Here all the systems which belong to that network are connected to the same architecture. When any other user wishes to select any document from the data center, he is required to be connected to the same security server to get the original document. This helps in security and privacy of the documents.

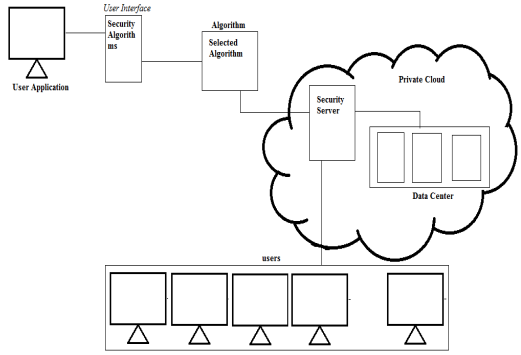

Fig 7.1: System Architecture

B. Process at sender:

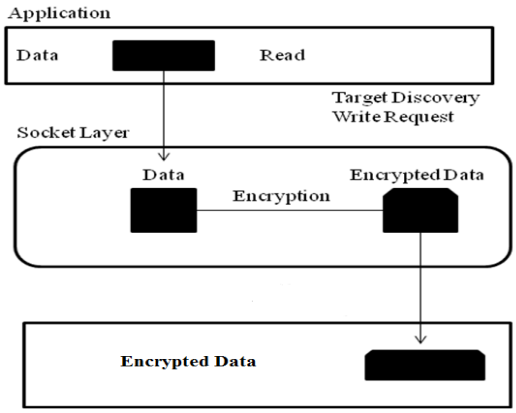

Fig 7.2: process at the sender

The data at the initiator end (client) will all set his data. He encrypts the data by selecting the appropriate approach from the interface and sends it to the server end. As shown in the above figure, at the client end the data is read, ready to send data. At socket layer, before sending it to the remote end the data will be encrypted for each byte and send encrypted data. The data is carried by the protocol to process the other commands which happens in a network. The data will be secured at the sender end by the security framework which helps in secure data transfer.

C. Process at receiver end:

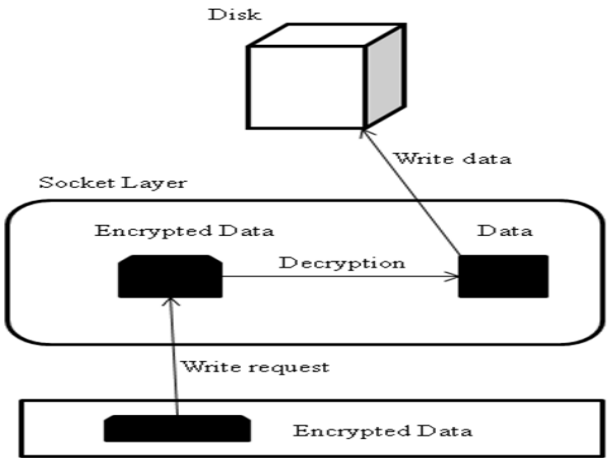

Fig 7.3: process at the receiver

At the receiver end when the data is received, the data will be decrypted and written on the disk. The data will be decrypted by the security approach used at encryption end. This is again worked above transport layer just where the packets arrive at end application. As before the write request is given by the protocols, the security framework decrypts the data and saves on to the disk.

In the similar way when the client requests a file from server the same process as mentioned will be happened. This will make sure that data is secure over the network. We can have confidentiality and integrity checks at the receiver end.

VIII. CONCLUSIONS AND FUTURE WORK

In our proposed method, transferred data is encrypted in the upper-layer on top of the transport layer instead of using IPSec or SSL. Thus, the scheme for the performance improvement can be applied without modifying the implementation of IP layer, and efficient secure communications by pre-processing of encryption in the upper-layer are realized. We have used file uploading as service as web application, the security is applied over to the data at the background using the encryption algorithms like AES, Triple DES and DES.

Adding secure cloud storage using the proposed cryptographic solution and with a searchable encryption technique for the files to be accessed, it will work as a better approach to the user to ensure security of data. The cloud security using cryptography is already in use for secure data storage which can be enhanced for secure data transmission and storage.

In the security application we should apply some pseudo random key generation approaches based on the user prescribed key which should help the user to keep data safe and no other attackers can get the secure data easily.

REFERENCES

[1] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.
[2] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.
[3] Sudha.M, Bandaru Rama Krishna rao, M.Monica, "A Comprehensive approach to ensure secure data communication in cloud environment" International Jornal Of computer Applications, vol. 12. Issue 8, pp. 19-23.
[4] Balachander R.K, Ramakrishna P, A. Rakshit, "Cloud Security Issues, IEEE International Conference on Services Computing (2010)," pp. 517-520.
[5] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing" proceeding of International workshop on Quality of service 2009", pp.1-9.
[6] Gary Anthes, "Security in the cloud," In ACM Communications (2010), vol.53, Issue11, pp. 16-18.
[7] Kresimir Popovic, Željko Hocenski, "Cloud computing security issues and challenges," MIPRO 2010, pp. 344-349.
[8] Kikuko Kamiasaka, Saneyasu Yamaguchi, Masato Oguchi, "Implementation and Evaluation of secure and optimized IP-SAN Mechanism," Proceedings of the IEEE International Conference on Telecommunications, May 2007, pp. 272-277.
[9] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, "A Break in Clouds: Towards a cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009, pp. 50-55.
[10] Patrick McDaniel, Sean W. Smith, "Outlook: Cloudy with a chance of security challenges and improvements," IEEE Computer and reliability societies (2010), pp. 77-80.
[11] Sameera Abdulrahman Almulla, Chan Yeob Yeun, "Cloud Computing Security Management," Engineering systems management and its applications (2010), pp. 1-7.
[12] Steve Mansfield-Devine, "Danger in Clouds", Network Security (2008), 12, pp. 9-11.
[13] Anthony T. Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, Tata Mc GrawHill 2010.

Anurag Porwal is an Asst. Professor in Department of Computer Science and Information Technology at Mewar University, Chittorgarh (Rajasthan). He has completed his B.Tech.(I.T.) form Rajasthan University and M.Tech.(CSE) from Mewar University Chittorgrah **(**Raj.). His areas of interest are Ad-hoc Networks, Network Security and Cloud Computing.

Rohit Maheshwari is an Asst. Professor in Department of Computer Science and Information Technology at Mewar University, Chittorgarh (Rajasthan). He has completed his B.E. (Hons.) in I.T. form Rajasthan University (2005) and M.Tech. (CSE) from Rajasthan Technical University, Kota**.** His research interests are in the field of Network Security, Cloud Computing and Algorithms.

B.L.Pal is an Asst. Professor in Department of Computer Science and Information Technology at Mewar University, Chittorgarh (Rajasthan) .He has completed his B.Tech. (IT**)** from AAI_DU Allahabad U.P. (2002-06) and M.Tech. (SIT) from DAVV Indore. M.P. (2007-09). His research interests are in the field of GIS, Spatial Database Management System and N/W Securities.

Gaurav Khakani is an Asst. Professor in Department of Computer Science and Information Technology at Mewar University, Chittorgarh (Rajasthan). He has completed his B.Tech. (I.T.) form Rajasthan University and M.Tech. (CSE) from Mewar University, Chittorgrah. His areas of interest are Ad-hoc Networks and Computer Networks.