International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 3, March-2015, pp: (199-207), Impact Factor: 1.252, Available online at: www.erpublications.com

IDS in Cloud Computing to Secure Virtual Environment

Muhammad Adil[1], Imran Ijaz[2]
[1]SZABIST Islamabad, Pakistan
[2]FJWU Rawalpindi, SZABIST Islamabad, Pakistan

Abstract: Cloud computing is an modern blockbuster of the past few years which offers many smart services as per demand in term of cost efficient and reliability. The clients of cloud increasing very rapidly as they assure their data are placed in safe location, many question arises on security of the cloud. As security becomes critical issue as with the quick increase of size of networks. Authentication is one of the key issue in security, many techniques implemented to get secure authentication and working is in progress on some techniques to modify according to the situation. The motivation behind this independent study is to outline the security techniques utilized in cloud computing.

INTRODUCTION

Cloud computing is the most emerging technology on internet. Cloud computing is the entire infrastructure (etc: servers, softwares) that is not local to your organization but instead all infrastructure is in the remote location in internet and they can access through web base interface. Cloud is internet from where we can access resources like application, data storage or CPU utilization using web browser. It includes the terms: grid computing, utility computing, virtualization, clustering, etc. Hardware and software are being used as resources for cloud computing to deliver services over internet.
Example:

Email: mail.gmail.com (exchange server of gmail is using to send and receive mail)
Document: MS workspace / google doc → one online document and all people edit that document in real time.

The most growing technology in this day and ages cloud computing and numerous association and separate clients are moving online on the grounds that they don't need to convey any sort of software or hardware anyplace. Clients feel free on using cost on the hardware and to keep legitimate look out for frameworks. We need to consider each and every solicitation created by the client for the availability of diverse or particular resources which are accessible in pool. In this nature, the alternatives have been few: delay advancement that energizes the business or permit business clients to get administrations without IT oversight that guarantees dependability, security, agreeability and influence norms are met for the business. This is especially genuine in today's amazingly aggressive commercial center and much all the more so with the approach of substitute and focused access devices in the commercial center.

As cloud computing and the up and coming era of information promptly accessible on the web and could be gotten to from anyplace and all over the place. Information openness answers for distinctive gathering of clients are an altogether different in prerequisite. It is the up and coming era of engineering which brings together everything into one. In it the customer can get to numerous cloud benefits at the same time. This new helpful perfect model for enrolling is a captivating, gigantic, far reaching scale theory that consolidates any participation based or pay-for each usage organization over the Internet. The Cloud computing model allows close clients to lease computing infrastructure as required, rather than obliging them to purchase their resources. In addition, customers can increase or decrease the span of their Cloud resources in a straightforward and auspicious manner, contingent upon their computing requirements. Purchasers utilize these administrations taking after a pay-as-you-go model, paying for the particular amount of time or level of administration used. This categorization is based on the many-sided quality of the administration, from raw process resources, for example, storage or transforming power, to refined software administrations, for example, databases or other applications.

Services offered by Cloud Computing

Anything that includes conveying host benefits over the web is a piece of cloud computing. These administrations are fundamentally part into three classifications: Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Software As A Service (SaaS):

SaaS is software base service available over the Internet, that end user can access any time on demand. Hence, it's also known as "software on demand". There are many advantages of SaaS like the accessibility of cloud from anywhere in the internet.

Infrastructure As A Service (IaaS):

IaaS delivers computer infrastructure based services. Network equipment, data-center space, software and servers are included in this service. Those organizations which can't afford the infrastructure of such expensive hardware and software but have the expertise to manage them, generally uses the IaaS services.

Platform As A Service (PaaS):

PaaS are on-service demand which include several development platforms and solution stacks. This service provides an environmental platform for software developments to built new applications or enhance the old ones without baring the load of purchasing and managing the required software and hardware and there hosting abilities.

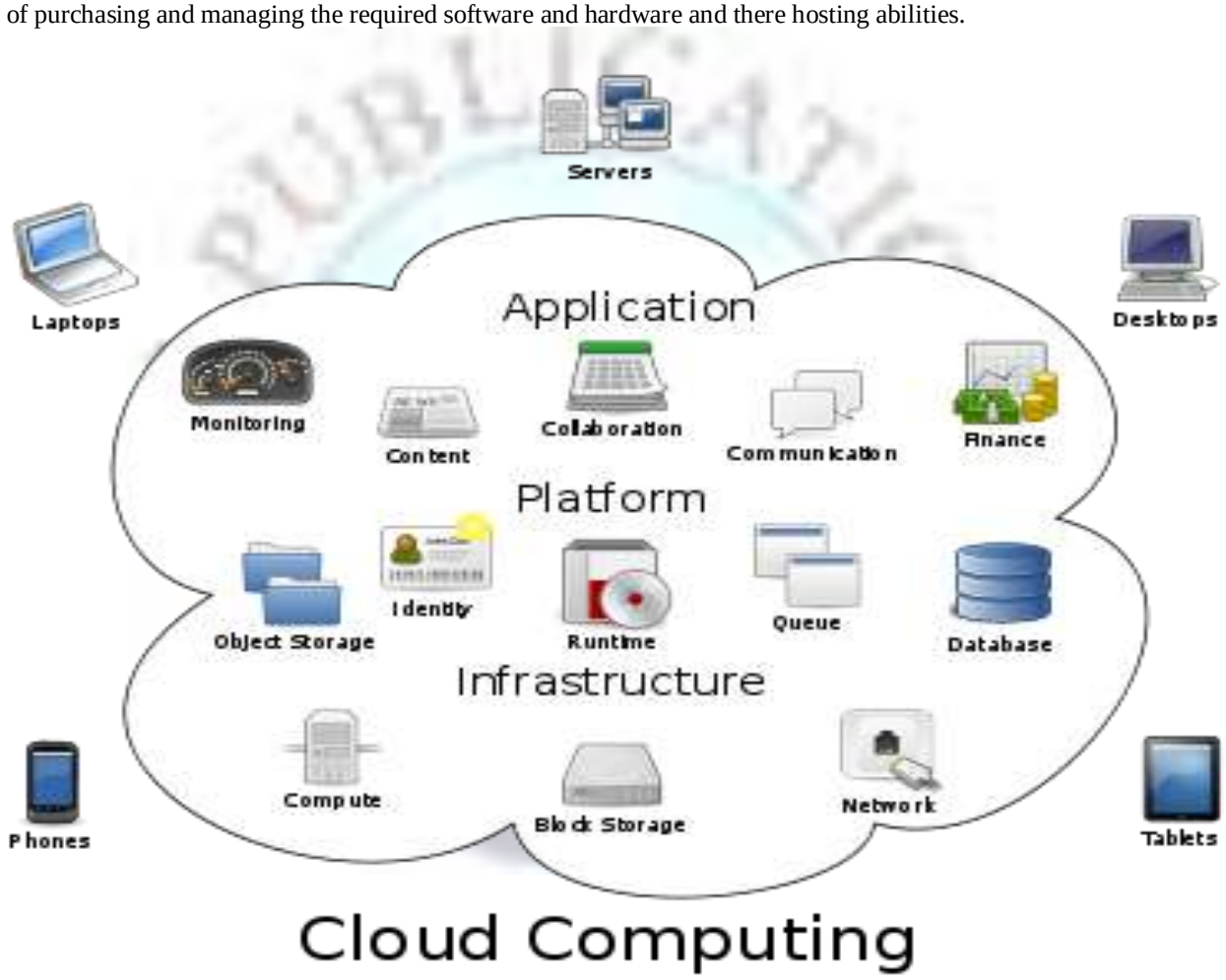


Figure 5: Example of Service Models http://www.trencom.co.za

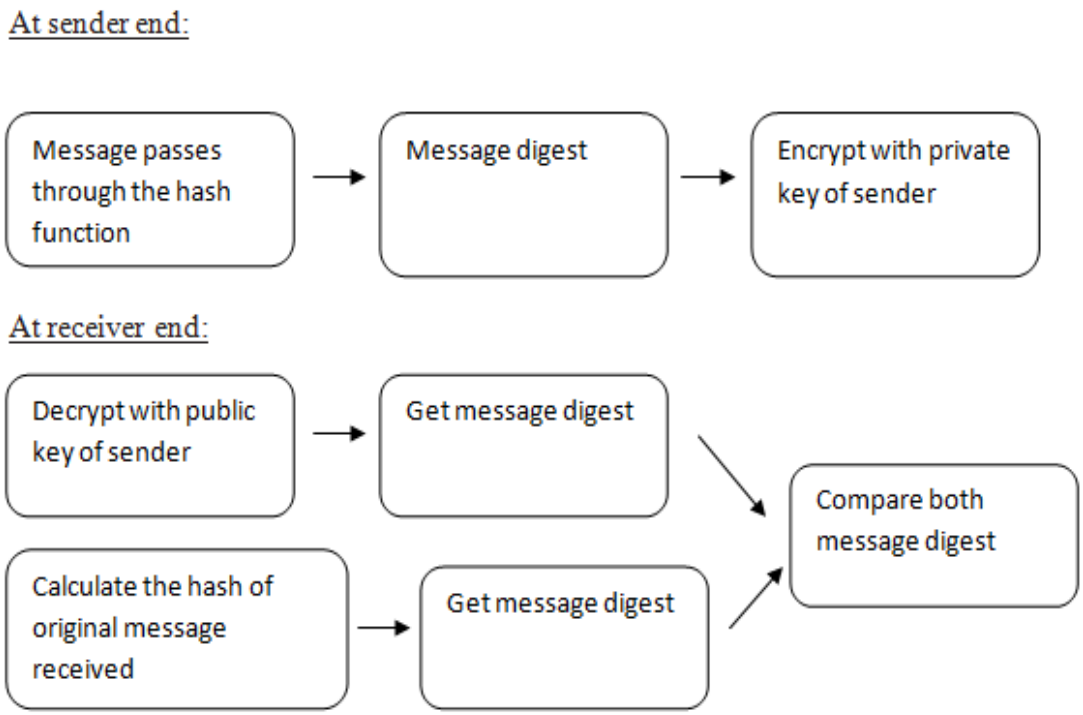
II. BACKGROUND STUDY

Although cost-effectiveness and flexibility are good reasons to switch on cloud computing but as its new emerging field still there are some issues which compromise security of cloud.

1 - Digital signatures with RSA algorithms

Here author are proposing a thought of cutting edge signature with RSA calculation, to encoding the data. In Digital Signature, programming will break down the data, record into essentially several lines by a using "hashing calculation". Programming then scrambles the message digest with his private key. By then it will handle automated imprint

.Software will unscramble the propelled signature into message digest with open key of sender's and his/her private key. We are using Digital imprints with the objective that we can pass on programming, cash related transactions, over the framework and in diverse circumstances where it is key to recognize fabrication and altering.



2 - Secure Socket Layer (SSL) and Transport Layer Security (TLS):

All through the trade, use Transport Layer Security (TLS) or SSL (secure socket layer) can move data in secured procedure. Both TLS and SSL are cryptographic protocols that offer security to correspondences over frameworks, for instance, the Internet. TLS and SSL encode the parcels of framework cooperation at the layer 7 that is Application Layer to insurance secure node-to-node go at the layer 4 that is Transport Layer. SSL is a layer 2 (Transport layer) protocol use for securing communication in client server architecture. SSL always works with TCP b/c it uses reliability feature of TCP. SSL use digital certificates for secure communication which contains identity info about the certificate owner and a public key which is consequently use for encrypting communication. SSL only implements on server / client architecture. SSL can be used to secure any type of client server application. SSL uses symmetric cryptography use for bulk data transfer b/w server and client however asymmetric cryptography use to negotiate the key.

3 - Digital signature with AES

In the proposed model, they used three protection schemes. Initially the key is created for key exchange, and for this purpose Diffie-Hellman algorithm is used, then for authentication digital signature is utilized, after that for encryption and decryption of information files of client Advanced Encryption Standard (AES) is used. All these security schemes are used to attain trusted and reliable cloud computing environment and to avoid data alteration at the cloud service provider's end. To get such security two individual servers are maintained, one performs encryption of data known as (trusted) computing platform and another for storing client's data files known as storage server. When a client need to upload a file to the server on cloud, first Diffie-Hellman is used for key are exchange, then the client is authenticated using digital signature and then AES is used to encrypt client's data file and only then it can be uploaded to another cloud Storage server. Whenever user needs that same file which he uploaded, following steps will be taken place after the user login: Firstly encryption keys exchange take place between both systems, then user select file to be downloaded, then digital signature are use for authentication process, and at last for decryption AES is used and after decryption user can access the required file.

Execution Steps:
1. User Login
2. Key Exchange took place using Diffie-Hellman
3. Digital Signature use for authentication
4. Data Encryption by using AES

5. Data upload / download from cloud Storage server
6. User Logout.

4 - File Assured Deletion (FADE)

File Assured Deletion (FADE) is a cloud storage system, which gives access control guaranteed cancellation to document. We then present approach based document guaranteed erasure, in which records are definitely erased and made unrecoverable by anybody. In FADE information first scramble with information key gave by the clients then with the control key gave by the outsider. An asset stored in cloud server has set of access consents which are, no doubt situated by the information holder while transferring to the server by means of cloud. A document is erased (or for all time blocked off) on the off chance that its associated policies are renounced and get out of date. That is, regardless of the possibility that a record duplicate that is connected with renounced policies, it stays scrambled and we can't recover the relating cryptographic keys to recoup the document. Consequently, the document duplicate gets unrecoverable by anybody (counting the holder of the record).

5 - Simplified File Assured Deletion (SFADE)

To address this issue, we came up with an approach called **SFADE (Simplified File Assured Deletion)** which is such a system that guarantees assured deletion and data security to the users, at the same time it is ease to implement and use. Since the proposed system involved the elimination of the key manager system the users and the cloud servers are indirect communication with each other. The significance of SFADE as the name suggest, (i) it is simple and easy to implement with less complexity relative to FADE, (ii) it is user friendly and does not involve the hassle of key manager system or any other third party agents, and (iii) it guarantees assured deletion.

A. Uploading a file

Suppose a user wants to upload a file to the cloud storage. For that purpose (i) at first, the user needs to enter a secret phrase (Phrase1), for example, 'my cloud password', or, 'my storage password', etc., which can be easily recalled. (ii) then, SFADE generates a random key (Key2). The length of the key, could be 64 or 128 bits, will depend on the encryption standard that is used to encrypt the data (iii) Key2 is used to encrypt the data which has been explained shortly (iv) using Phrase1another key (Key1) is be generated which is used to encryptKey2 using a stronger encryption technique. We generate Key1from Phrase1 using secure hash algorithm (SHA2) (iv) finally, the encrypted files and the encrypted Key2 are uploaded to the cloud. The whole procedure has been depicted in 2.

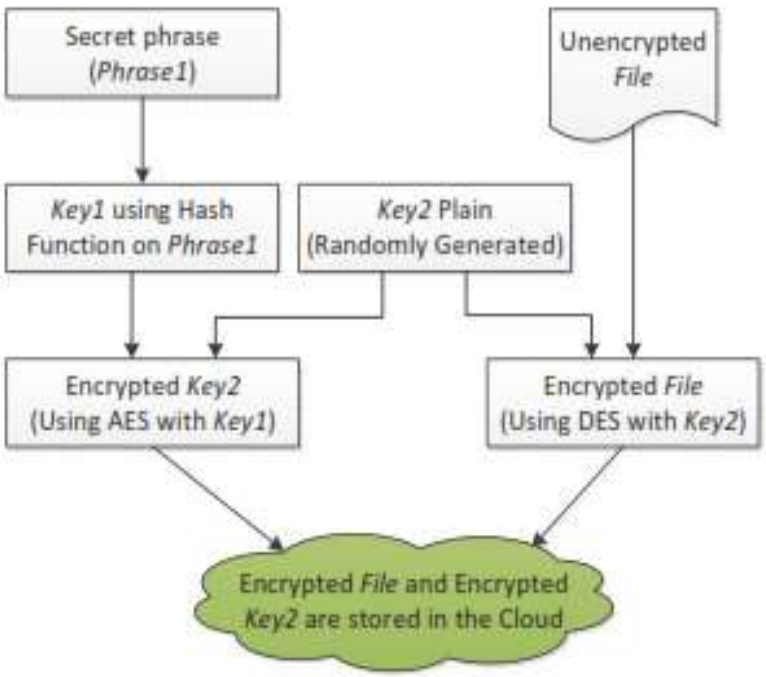


Fig. 2. Flow chart depicting encription procedure for SFADE.

B. Downloading a file

Now, suppose the user wants to download an uploaded file from the cloud storage. For that purpose (i) the Phrase1 must be entered and the Key1 should be generated, (ii) this Key is used to decrypt the encrypted Key2, (iii) the Key2 is used to decrypt the files. Thus the files will be downloaded. The whole procedure has been shown in 3.

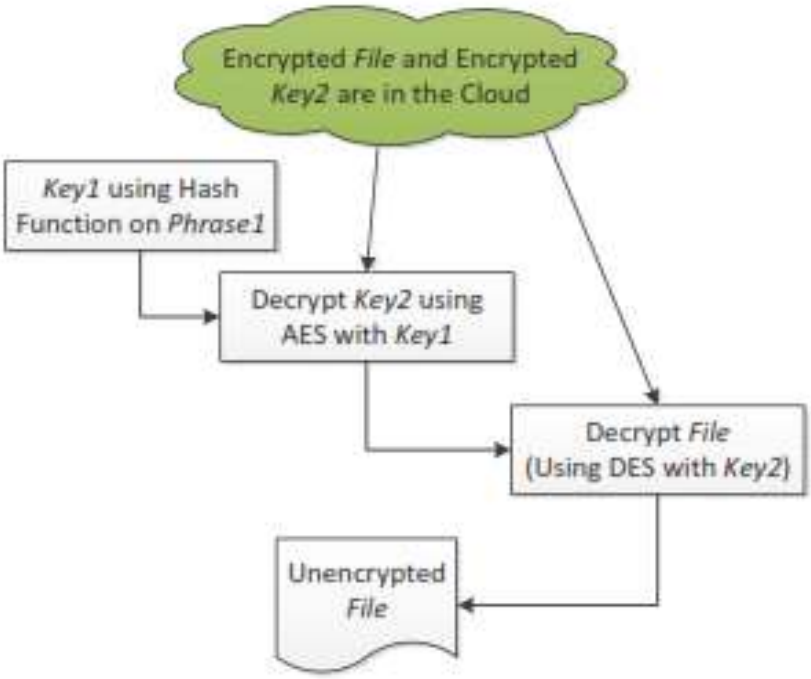


Fig. 3. Flow chart depicting decryption procedure for SFADE.

6 - Provable Data Possession (PDP)

A **Provable Data Possession (PDP)** plan checks that a document, which comprises of a gathering of n pieces is held by a remote cloud server . The information holder forms the data record to create some metadata to store it mainly. The record will be then sent to the server, and the holder erase the local duplicate of the document. The manager confirms the ownership of document in utilizing test reaction convention. This method is utilized by customers to check the integrity of the information and to occasionally check their information that is put away on the cloud server. So this procedure guarantees server security to the customer. PDP plan helps dynamic extension.

7 - Cooperative Provable Data Possession (CPDP)

Let's consider multi-cloud storage service to deal with this type of issue, as explained in the next figure. In this construction modeling, an information stockpiling service includes three separate elements. Customer who has a lot of information to be put away in multiple mists and have the consents to get to and control put away information. Cloud service providers (CSP) who cooperate to give information storage services. Trusted Third Party (TTP) is the trusted party who stores some confirmation parameters or data validation information and perform checks for data integrity any time.

In this design multiple CSPs are presence to store and the customer's information. In addition, Cooperative Provable Data Possession (CPDP) is utilized to confirm the integrity and availability of client's data placed in all CSPs.

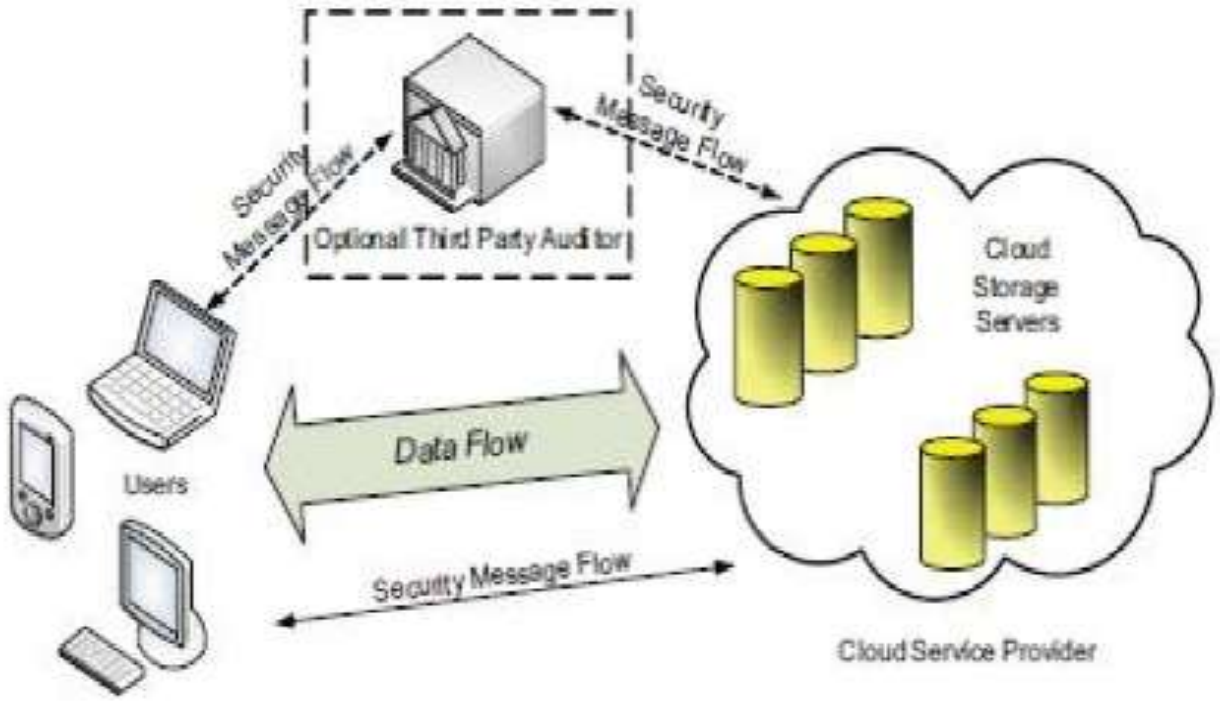


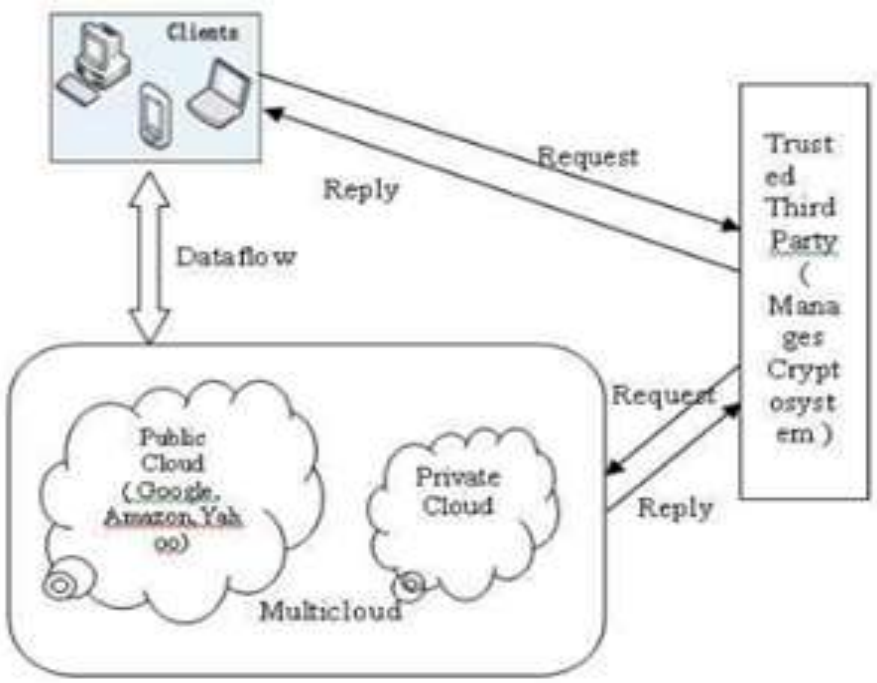
Fig. 1: Cloud data storage architecture

The confirmation system is portrayed as takes after:

Firstly, a customer (information holder) utilizes the secret key to professional process a document which comprises of a gathering of n pieces, produces a set of open check data that is put away in Trusted Third Party (TTP), transmit the record and some confirmation labels to CSPs and may erase its nearby duplicate; Then, by utilizing a confirmation convention, the customers can issue a test for one CSP to verify the integrity and availability of information stored on outsourced servers.

8 - RSA with CPDP

Existing CPDP schemes are not able to fulfill the characteristic prerequisites to store and recover information from multiple clouds as far as correspondence and processing expenses. They offer openly open remote interface to check integrity and oversee gigantic measure of information. To address this issue, we consider a multi-cloud stockpiling administration. In multi-cloud construction modeling, an information storage administration includes three separate elements: Customers who have a lot of information to be put away in multiple clouds and have the consents to get to and control put away information. Cloud Service Providers (CSPs) who cooperate and have noteworthy stockpiles and calculation assets to deal with customer's information and give stockpiling administration to them and Trusted Third Party (TTP) who is trusted to store confirmation parameters and offer open question administrations for these parameters. We consider the presence of multiple CSPs to cooperatively store and keep up the customers' information. Additionally, a cooperative PDP is utilized to confirm the integrity and accessibility of their put away information in all CSPs. A customer (information owner) has information or records which comprise of n pieces to be store in cloud. Customer pre-processes a document and produces a set of open confirmation data that is put away in TTP. Customer then transmits the document and some check labels to CSPs, and may erase its neighborhood duplicate; then, by utilizing a confirmation convention, the customers can issue a test for one of the CSP to check the integrity and accessibility of outsourced information concerning open data put away in TTP.



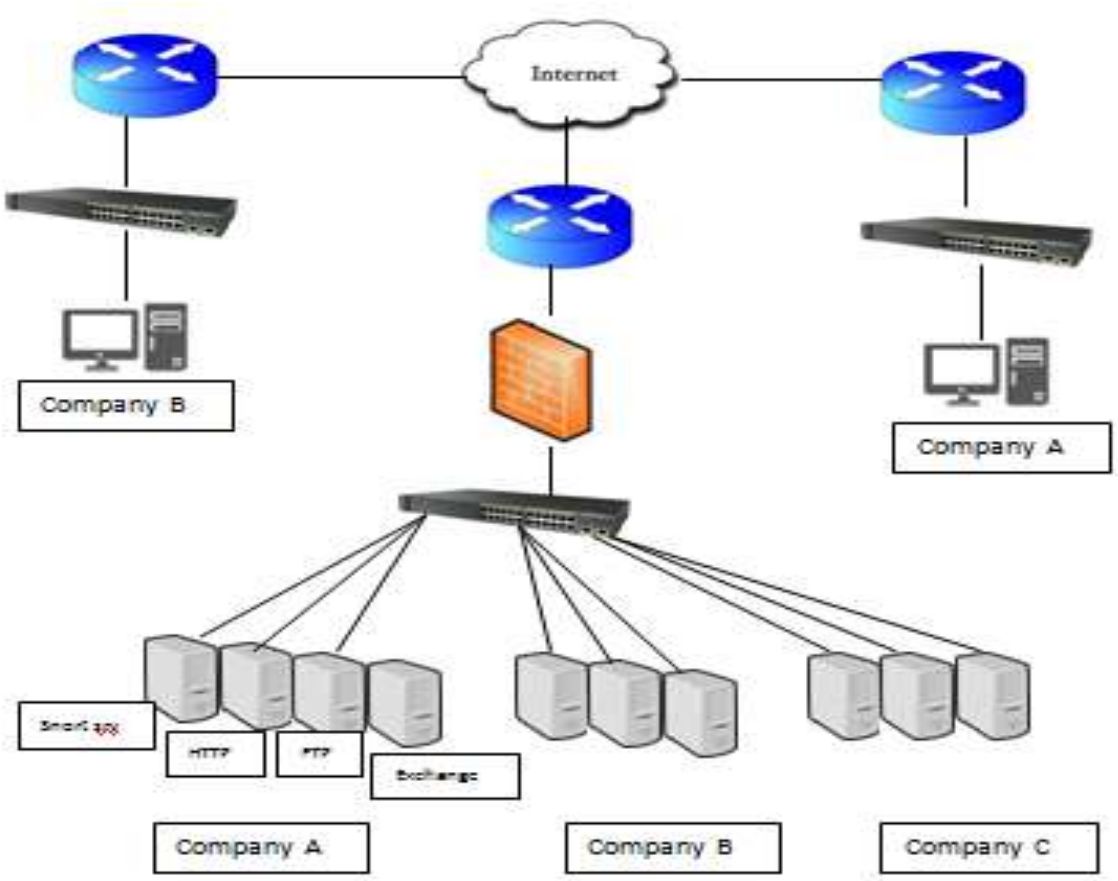
9 - Firewall and IDS:

The most important concern about cloud computing is security because all cloud customer's stores confidential data on cloud servers and for security two main components are firewalls and intrusion detection systems. Firewall is basically placed among two networks and all traffic passes through it. The authorized traffic defined by the security policy is filtered through firewall. Debar says that to detect insecure state and usage of system is monitored by intrusion detection system. Data integrity and application accessibility have to be assure by cloud security and it the end worms spreading, huge coordinated attacks and DDoS in prevented by Intrusion detection system and firewalls. There are three basic parts of security management prevention, detection and prevention. But IDS mainly concern with detection part. The most common techniques used for detection is anomaly based detection and pattern matching. Pattern matching is signature based, for known patterns all information are scanned. But the weakness is this method is that a regular update is needed for its database. Anomaly base detection allows all normal traffic it is simple approach, an alarm is raised when deviation from normality is detected. But there is a chance to raise a false alarm. In some cases an attacker can behave like a normal user so then a logarithmic logic is used for detection of intruders. The security solutions are **Snort** and commercial firewall an experiment has been done by a commercial and non-commercial solutions. **Snort** is an open source IDS, network traffic is analyzed in real time. It is based on signature which can identify known attacks. Is this experiment it can only target known port scan. The other solution is Commercial firewall it design shows that it can work as an IDS and also a network firewall. This device is a commercialized product so we do not know that the manufacturer used what mechanism to detect the intrusion and attacks. But we have got an idea that how this product work.

PROBLEM STATEMENT

From the literature review we know that the cloud environment is unsecure because cloud is hosted on internet and always available. Always availability on internet makes the cloud infrastructure an attractive target for attackers. Different companies use different techniques and mechanisms securing there servers from external attacks. Some companies use Firewall to block external attack and some use ACLs on gateway router for blocking the attack. The problem arise is that the policies which are applied on gateway are applicable for whole cloud, but in reality multiple companies are taking services from single cloud host simultaneously. Each company required security policies according to their requirement so a network security system is required for every company individually which will secure them according to their requirements. In view of the above we come to the concussion that an implement and Intrusion detection system on cloud.

PROPOSED MODEL



Implementing IDS on cloud:

For implementing IDS on cloud we have to create cloud first. For this purpose we took 3 servers of min core 2 duo 2.7 GHz processor, 8Mb cache, 4 GB RAM and 500GB hard disk. Install windows server 2008 R2 on all servers. Configure one server as HTTP server, second as FTP server and third as IDS server.

Validation Technique:

We had tested below mentioned 3 software to validate the working of IDS in cloud

1 - Suricata:Difficult to understand
2 - SAX2 IDS:Not free software it required activation
3 - SNORT:Snort is a freenetwork intrusion detection system (NIDS). Open source network-based intrusion detection system (NIDS) of snort is able to perform real-time traffic analysis and packet logging in a log file on Internet Protocol (IP) networks.

To understand working of snort one must understand some basic concepts about snort. There are three modes in which Snort can be configured:

1 - Sniffer mode:In this mode snort sniff the packets from the network and display all the network traffic in real time on the screen.
2 - Packet Logger mode:In this mode snort only logs the packet in a file placed in home directory under log folder.
3 - Network Intrusion Detection System (NIDS) mode:

In this mode snort performs intrusion detection and analysis on network packets.

IDS Installation and configuration:

Installing snort and configuring snort as IDS server is explained step by step below.

1 - Install snort 2.9.6.2 on server
2 - Add snort rules 2.9.6.2 in snort home directory
3 - Install winpcap 4.1.3 on server
4 - Configuring snort by configuring snort.conf file
5 - Adding rules on local_rules file
6 - Run snort in dump mode
7 - Run snort in IDS mode

Conclusion

The model is tested by launching attack on different protocols to evaluate performance of the model. Results of testing shows that as IDS is helpful in securing traditional LAN, it also provides complete solution for suggested model of cloud as well. Snort is compatible with windows as well as with Linux. Snort only required network knowledge and expertise to configure IDS accurately.

References

[1]. Somani, U., Lakhani, K., &Mundra, M. and, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing". In Parallel Distributed and Grid Computing (PDGC), 1st International Conference, 2010, October, pp. 211-216
[2]. Rewagad, P., &Pawar, Y. and,"Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", In Communication Systems and Network Technologies (CSNT), International Conference, 2013, April, pp. 437-439.
[3]. Gayatri, G., &Sowmya, B. and,"FADE: A Secure Overlay Cloud Storage System". International Journal, 2013.
[4]. Habib, A. B., Khanam, T., &Palit, R. and,"Simplified File Assured Deletion (SFADE)", In Advances in Computing, Communications and Informatics (ICACCI), International Conference, 2013, August,pp. 1640-1644.
[5]. Khalkar, M. R., &Patil, S. And, "Data Integrity Proof Techniques In Cloud Storage", International Journal, 2013.
[6]. Gadge, M. M., &Rajani, R. and, "Ensuring data integrity using Cooperative Provable DataPossession for Multi Cloud environment", In International Journal of Computer Science and Management Research (eETECME), 2013, October.
[7]. Liu, W. and, "Research on cloud computing security problem and strategy", In Consumer Electronics, Communications and Networks (CECNet),2nd International Conference, 2012, April, pp. 1216-1219.
[8]. Chalse, R., Selokar, A., &Katara, A. and, "A New Technique of Data Integrity for Analysis of the Cloud Computing Security", In Computational Intelligence and Communication Networks (CICN), 5th International Conference, 2013, September, pp. 469-473.
[9]. Sharma, S., Soni, S., &Sengar, S. and,"Security in Cloud Computing", In National Conference On Security Issues in Network Tecchnologies, NCSI, 2012, August.
[10]. Imran Ijaz, "Design and Implementation of PKI (For Multi Domain Environment)," International Journal of Computer Theory and Engineering vol. 4, no. 4, pp. 505-509, 2012.
[11]. Z. Javaid and I. Ijaz, "Secure user authentication in cloud computing " in Information & Communication Technologies (ICICT), 2013 5th International Conference, Karachi Pakistan, 2013, pp. 1 – 5.
[12]. Imran Ijaz, "Securing user Authentication through Customized X.509 in Cloud Computing", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-3, July 2014, pp. 90-94.
[13]. http://manual.snort.org.

About Authors

Mr. Imran Ijaz is a Ph.D. Scholar in SZABIST Islamabad, Pakistan. His research areas are Cloud Security, PKI and Security services through PKI under cloud infrastructure.

Supervised / Implemented a number of National level network projects. He is serving in Fatima Jinnah Women University, Rawalpindi, Pakistan.

Mr. Muhammad Adil is a MS Student in SZABIST Islamabad, Pakistan. His research area is security in Cloud infrastructure.

He is serving National University of Science and Technology (NUST), Islamabad, Pakistan.