SECURITY ISSUES IN CLOUD COMPUTING

Ashutosh Kumar

Assistant Professor
Department of Computer Science & Engineering
Institute of Technology,Gopeshwar

ABSTRACT

Cloud computing is engineering for giving computing service through the web on interest and pay per uses access to a pool of shared assets in particular networks, storage, servers, services and applications, without physically securing them. So it spares managing cost and time for associations. generally information was put away in Relational Databases on at least one servers located inside the association and the customers expected to require information from these server machines. This paper presents point by point analysis of IAAS and its parts. We present how security at IAAS layer should be deal with carefully as conveyance models-Platform as a Service and Software as a Service are based upon IAAS layer. We focus how IAAS security issues-information declaration and use scrutiny, start to finish classification and informative, basis solidify and start to finish encryption should be established.

Keywords: Cloud Computing, Customer relationship management(CRM), Application Service Provider (ASP)

1. INTRODUCTION:

Cloud is referred as great collection that holds easily accessible and utilizable virtualized resources. To manage variable load and optimum usage, these assets are reconfigured dynamically. Cloud Computing is a distributed architecture that centralizes server assets on a scalable stage so as to provide on demand computing resources and services. Cloud service providers offer cloud platforms for their user to use and create their web services, much like internet service providers (ISP) offer cone reservation, Cloud Computing has provided many exciting services and features like flexibility, reliability, unlimited storage, portability and the fast processing power but cloud security is still a big issue. Security issues including require of expectation, the risk of malicious insiders, and the failing of cloud services have been discussed. High speed broad band to access the internet.

2. CLOUD COMPUTING SERVICES:

2.1. Infrastructure as a service(IaaS)

In IAAS model, Cloud Service Provider outsources storage, servers, hardware, networking mechanism, etc. to the user. CSP owns the equipment and responsible for cover, running and maintaining it. In this model,user pays on per-use basis.

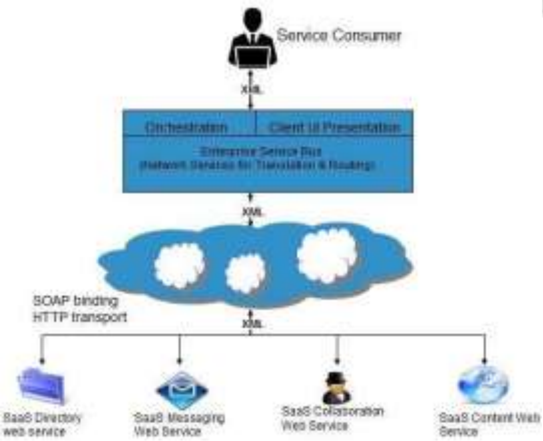

Figure 1.Infrastructure as a services(IAAS)

Characteristics and segment of IAAS include: strategy based services

- Dynamic scaling
- Automation of administrative tasks
- Utility computing service and billing model.
- Internet connective
- Desktop virtualization

2.2. BACK GROUND WORK:

Being the most trending technology of the age, the research is being done generally on Cloud (CSA) was formed with the aim to provide confident security within cloud computing environment.CSA launched “Security Guidance for Critical Areas of Focusin Cloud Computing” as their initial product to help users get better insight about clouds and the security parameters. The Cloud computing interoperability Group and the Multi-Agency Cloud Computing Forum have made lot of efforts to deliver efficient and effective controls to provide information security in Cloud situation.

Different models of cloud computing

Cloud services can be divided into three categories:
Software as a Service (SAAS)
Platform as a Service (PAAS)
Infrastructure as a Service (IAAS)

Software-as-a-Service (SAAS)

SAAS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the user to get rid of installing and operating the application on own computer and also eliminate the incredible load of software maintenance; continuing operation, protection and support. SAAS vendor advertently takes responsibility for deploying and managing the IT communications (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (communications patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SAAS features a complete application offered as a service on demand.

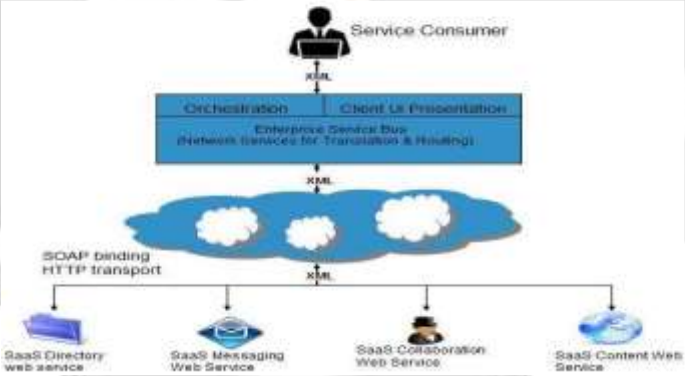

Figure 2.Software as a Service (SAAS)

Platform as a Service (PAAS):
PAAS is the delivery of a computing platform and solution heap as a service without software downloads or installation for developers, IT managers or end-users. It provides an communications with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PAAS includes: Force.com, Google App Engine and Microsoft Azure.

2.3. Platform as a service:

Platform as a Service (PAAS) is a way to rent hardware, operating systems, storage and network capacity over an Internet. PAAS is an outgrowth of SAAS that allows hosted software applications to be made available to user over an Internet. Developer gets many advantages from PAAS. With PAAS, OS can be changed and upgraded as many times as needed. PAAS allows geographically distributed teams to work together on software development projects. CSP have crossed international boundaries for providing on-going and demanded services to consumers.

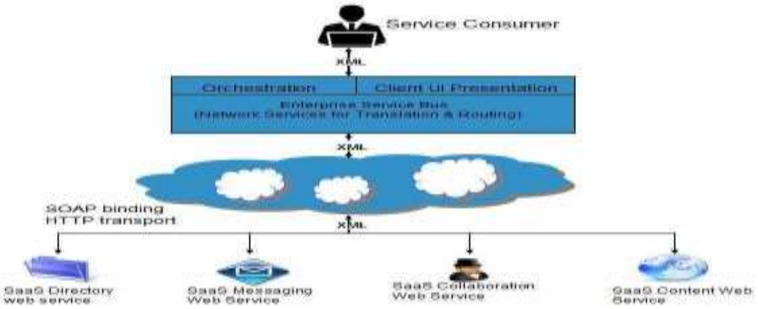

Figure 3. Platform as a Service (PAAS)

3. SECURITY ISSUES AND SOLUTION:

This section discusses the problems related to cloud computing and their proposed solutions.

3.1 Trust

Trust between user and service providers is the main issue faced by cloud computing now days. User is never sure whether the Service is trustworthy or not, and whether his data is secure from the intruders or not. The user and Service provider are bound by Service Level Agreement (SLA) document. This is a type of an agreement between the user and the service provider; it contains the duties of service provider and his future plans. But unfortunately there are no standards for SLA.

3.2 Confidentiality:

Confidentiality means to prevent the disclosure of private and important information. Since all the information is stored on geographically dispersed locations, confidentiality becomes a big issue. Many methods are used to preserve confidentiality from which, encryption is the widely used method. But it is relatively an expensive method.

3.3 Authenticity

Integrity is also a main issue faced by cloud computing. It refers to the improper modification of information. As the data resides in different places in a cloud so the access control mechanism should be very secure and each user must be verified as an authentic user. Authentication problem can be solved by using the digital signatures but even after having access to digital signatures a user can’t get access and verify the subsets of data.

3.4 Encryption

Encryption is the most widely used data securing method in cloud computing. It has many drawbacks. It needs high computational power. The encrypted data need to be decrypted every time when a query is run so it reduces the overall database performance. Many methods are presented to ensure better encryption in terms of better security or the operations. A method proposed by suggests that by using several cryptographic methods instead of only one can increase the overall throughput. Data is encrypted using these methods in each cell of a table in cloud. Whenever a user wants to make a query, the query parameters are evaluated against the data stored. The query results are also decrypted by the user not the cloud itself so it increases the overall performance.

3.5 Key Management:

While doing encryption, we need encryption/decryption keys and managing these keys itself is a big security issue in cloud environment. Storing these encryption keys on cloud is a bad option. It is easy to store single encryption key but for the real time systems it become a complex task to store these keys. This may require a separate small database to store the keys locally in a protected database. But again that’s not a good idea because the purpose for which we are shifting our data to clouds will become worthless.

3.6 Data Splitting

Data splitting may be the better alternative to encryption. It is surely very fast as compared to encryption itself. The main idea behind it is to split the data over multiple hosts that are non-communicatable. Whenever a user needs its data back, he must have access to both of the service providers to recollect his original data. No doubt it is very fast technique but it has its own security issues.

4. SOFTWARE AS A SERVICE

Software as a service now and again alluded to as "software on interest," is software that is convey over an Internet. With SAAS, a supplier licenses an application to client either as a service on interest, through a membership, in a "pay-as-you-go" model, or at no charge. This methodology is the piece of the utility computing model where the majority of the innovation is in the "cloud" got to over the Internet as a service. SAAS was at first generally sent for deals power mechanization and Customer Relationship Management (CRM). Presently it has turned out to be ordinary for some, business undertakings, including mechanized charging, invoicing, human asset the executives, financials, report the executives, service work area the board and cooperation.

In past few years, cloud computing has developed to one of the fastest growing segments of IT industry. But this growth need cloud security to be together. Below mentioned are few most important issues of cloud computing.

4.1. Privacy

Cloud computing utilizes virtual computing technology. In this, user’s personal data is reserved on various virtual data center which may cross international limitations. This is where data privacy protection may face argument of various legal systems.

4.2. Security:

Where is your information more secure, on your local hard driver or on high security servers in the cloud? Some compete that client information is ever more secure when oversee inside, while others compete that cloud suppliers have a firm moving strength to keep up trust and all things considered utilize a more significant level of security. Be that as it may, in the cloud, your information will be detached over these entity PCs paying tiny intelligence toward where your base storage area of information is at last put missing.

4.3. Reliability:

Server in the cloud have identical issues from your very own local servers. The cloud servers equally occurrence personal times and delay, what the thing that matters is that clients have a higher subject to cloud service supplier (CSP) in the model of cloud computing. There is a major distinction in the CSP's service model, when you select a specific CSP, you might be secured, in this way bring a potential business secure hazard**.**

4.4. Open Standard:

In cloud computing, open values are critical to produce. Many CSP provides well documented APIs which are unique to their implementation and thus difficult to interoperable. Towards the progress, there are many open standards are under development; OGF’s Open Cloud Computing Interface is one of them.

4.5. Long Term Viability:

It should be sure that the data you set into the cloud will never become invalid even your cloud computing provider go broke or get acquire and swallow up by a larger company. "Ask potential providers how you would get your data back and if it would be in a format that you could introduce into a replacement application.

4.5 Compliance:

Various strategy relate to the storage and utilization of information require standard informative and review trails, cloud suppliers must empower their clients to agree suitably with these guidelines. managing Compliance and Security for Cloud Computing, gives knowledge on how a top-down perspective on all IT assets inside a cloud-based area can convey a more grounded administration and authorization of compliance approaches.

5. CONCLUSION AND FEATURE WORK:

One of the greatest security stresses with the cloud computing model is the sharing of assets. Cloud service suppliers need to educate their clients on the level regarding security that they give on their cloud. In this paper, we originally examined different models of cloud computing, security issues and research difficulties in cloud computing. Information security is significant issue for Cloud Computing. There are a few other security difficulties including security parts of network and virtualization. This paper has featured every one of these issues of cloud computing. We accept that because of the unpredictability of the cloud, it will be hard to accomplish start to finish security. New security systems should be created and more seasoned security methods should have been drastically changed to have the option to work with the clouds design. As the advancement of cloud computing innovation is still at a beginning time, we trust our work will give a superior comprehension of the structure difficulties of cloud computing, and make ready for further research around there.

REFERENCES

A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment",
International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-
152, 2010. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance
Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0. R.
L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11.
http://www.interoute.com/cloud-article/what-hybrid-cloud
Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computer world. Retrieved May 02, 2014
"Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. Retrieved May 02, 2014