DATA STREAM CONTROL AS A SERVICE FOR CLOUD SECURITY

[1]Priyanka N, [2]Ranjitha V, [3]Manikanta K B
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
Computer Science and Engineering Department,
GITAM School of Technology, Bengaluru,
INDIA

Abstract: As the web technologies and Service-oriented architecture (SOA) are improving, services of web have turn out to be serious mechanism of SaaS (Software as a Service) applications inside cloud system environment. To maintain and process information with high alertness, the majority of such applications influence multi-tenant information to be stored as a back end. Though there is a benefit with these technologies, they place SaaS applications at danger in contradiction to novel plus predominant assault vectors. This security threat is more exaggerated through the failure of manage along with deficit of safety enforcement on delicate information influenced by these SaaS appliance. An efficient explanation abide required to achieve numerous necessities instigating in the changing and circuitous environment of alike appliances. Motivated through the increase of Security as a Service (SecaaS) model, "Information Flow Control as a Service (IFCaaS)" is presented. IFCaaS gibe the groundwork of cloud-delivered IFC-based safety examination and scrutinizing actions. In case of the implementation of the IFCaaS, a novel structure that concentrate on the recognition of information flow vulnerabilities in SaaS applications. Basic analyses demonstrate that this structure is a feasible way to defend adjacent to data integrity and confidentiality violation that leads to loss of information.

IndexTerms - vulnerability detection; static analysis; information flow control; cloud applications; Saas

I. INTRODUCTION

Cloud Computing provides us a way through which we access applications, by making use of the internet. Construction, organization and if any modification of applications can be done online. Cloud is a network or internets. Storage of information and services can also be done online. Cloud which is located at remote location and services can be provided over the network that is public or private networks. E-mail and web conferencing is an example of applications that run in a cloud. Platform dependency issues in cloud computing can be overcome by installing a fragment of software on local PC. This is the reason why Cloud Computing in business application is mobile and collaborative.

1.1 OVERVIEW

To make Cloud Computing viable as well as easy to get to end users many services and models are running behind the scene. There are two models as follows:

- Deployment Models
- Service Models

One type of accessing the cloud is by making use of the deployment models, which consists of four categories as shown in the figure.

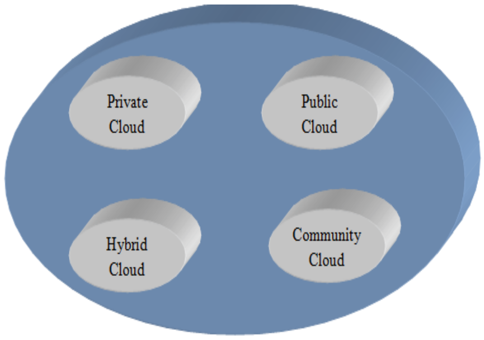

Fig 1: Types of cloud

Public Cloud: This makes the services to be accesses without difficulty. Because of its openness it is less secure, for example electronic mail.

Private Cloud: Here the structure and services are accessed inside the organization. Since it has a private nature it is secured.

Community Cloud: Here structure and services are accessed via collection of organizations.
Hybrid Cloud: Is a combination of public along with private cloud. Private cloud is used for the critical activities where as public cloud is used for non-critical activities.

Service Models: Reference models are the basis of cloud computing and these models are also called as service models. There are three categories:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Infrastructure as a service (IaaS) is the primary level of the service models. Underlying service representation is utilized by each service models that is it take over the protection and supervision mechanism from the basic model, which is exposed in the subsequent figure.

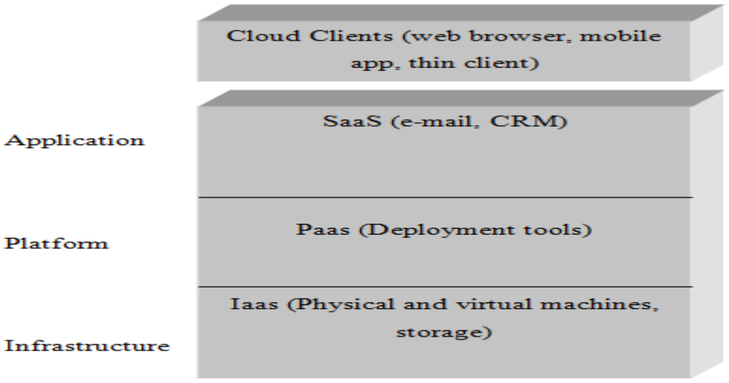
Cloud Clients (web browser, mobile app, thin client)
Application
SaaS (e-mail, CRM)
Platform
Paas (Deployment tools)
Infrastructure
Iaas (Physical and virtual machines, storage)

Fig 2: Categories of service model

Infrastructure As A Service (Iaas): There are some primary resources which can be accessed by IaaS. Some of the resources are physical and virtual machines and also the short-term storage.
Platform As A Service (Paas): This is used for providing a runtime environment meant for application expansion and operation.
Software As A Service (Saas): It permit end users to exploit software applications same as service.
Cloud computing comprise of many advantages as shown in the figure.

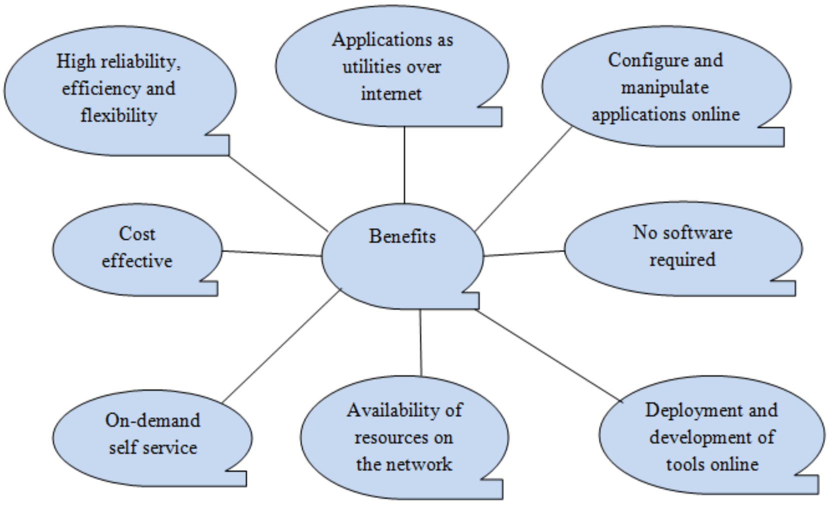
High reliability, efficiency and flexibility
Applications as utilities over internet
Configure and manipulate applications online
Cost effective
Benefits
No software required
On-demand self service
Availability of resources on the network
Deployment and development of tools online

Fig 3: cloud computing advantages

Risks: The downsides of cloud are:

- Safety.
- Lock-in.
- Isolate crash.
- Management boundary cooperation.
- Unconfident or unfinished information removal.

Characteristics:

- On-demand self capability.
- Broad system access.
- Resource pool.
- Fast elasticity.
- Calculated service.

To make cloud flexible, reliable and usable, the technologies which are working behind the cloud computing platforms are Virtualized, (Service-oriented architecture) SOA, grid and utility computing.

II. SCOPE OF THE PAPER

The aim of this project is to detect the vulnerabilities that are ranging from SQL injection, No SQL injection, cross-site scripting and information leakage in SaaS application, which is done using trusted parties. It provides cloud-delivered support safety study and examines services. It can be organized and modified in present cloud environments with no modification of the application's rules, the original platform, or VMM. The result shows that the information flow vulnerabilities are detected with high accuracy.

III. EXISTING SYSTEM

Even though there is multi-tenant information that is stored as a reverse end to process the information with more agility and offer the extraordinary benefits, it leaves the SaaS applications in risk in opposition to novel and prevalent attack vectors. So an efficient solution is essential to overcome the disadvantages such as:

Disadvantages

- To process the data with high agility multi-tenant documents is stored as a back end.

Loss of manage and lack of enforcement above important data

IV. PROPOSED SYSTEM

It establishes a faith of cloud customers within the protection of their information, which can be done by utilizing trusted party which is used to confirm the safety of cloud SaaS application. The main intention is to identify the information flood vulnerabilities is SaaS application plus resolving the risk in the development stage. The requirements are as follows

- Ease of employment to make easy its adoption in cloud environment.
- The data which is not secure should be detected including explicit and implicit paths.
- Lifecycle of cloud application should be accurately detected.

This service is constructed on a SaaS model and can be offered over the internet with no requirement of software setting up, hardware system, or particular training. The code of a service supplier application is analyzed by the trusted third party before it is being hosted on a cloud source platform. Service provider can analyze the results which are available in online dashboard.

Modules

- **6.2.1 Cloud Server**

Is a logical server that is fabricated, hosted and distributed through a cloud computing policy above the Internet. Cloud servers acquire and show related facilities and functionality to a distinctive server but are accessed distantly from a cloud service provider. Accessing different data centers (sets) ex.java programs, C# programs, spring programs.

- **6.2.2 Stubs:**

This is automatically created by a cloud server, to interact with cloud server. It is a section of code utilized to alter parameters during a remote procedure call, this is done because the address spaces is different for client and server. Procedures can be called by client computers remotely from a server computer by using RPC.

- **6.2.3 Alert system.**

Whenever cloud server communicating with stubs or node, the trusted centers will track all the record of stubs, they will access only for main cloud server.

- **6.2.4 Trusted Servers.**

Trusted servers are the third party as a server, the trusted server keeps all track records of all stubs that are communicating with cloud server to notify the stubs are communicating with cloud.

IV CONCLUSION & FUTURE ENHANCEMENT

The Saas applications of cloud are inclined to new-fangled assault vectors in addition to those that are existing. The vulnerabilities of stealth type together with NoSQL injection, SQL injection and data spillage challenge safety of data that is controlled by these applications. Motivated by SecaaS that is Security as a Service, an IFCaaS (Information Flow Control as a

Service) is presented to highlight cloud-convey based security examination and also observing administrations. A novel static data stream examination structure is presented for weakness identification of SaaS application. This can be done using trusted parties by offering services. The system is conveyed and adjusted in present cloud condition with no changes to the code of application, the fundamental stage, or VMM. To absolutely demonstrate the applications condition, it is applied to few systems. The model embraced by the structure assist in thinking regarding runtime data to permit the utilization of any static examination strategy. The information flow vulnerability including explicit and implicit paths can be recognized. The assessment result exhibits that the system identifies information flow vulnerabilities with high exactness.

FUTURE ENHANCEMENT

The further enhancement can be done with other technologies which give much accuracy with security.

REFERENCES

[1]CENZIC.(2014). Cloud Applications Vulnerability TrendsReports [Online]. Available: http://www.cenzic.com/downloads/Cenzic_Vulnerability_Report_2014.pdf [Accessed: February 2015]

[2] B. Sullivan. (2011, July). *Server-side JavaScript injection* [Online]. Available: https://media.blackhat.com/bh-us-11/Sullivan/BH_US_11_Sullivan_Server_Side_WP.pdf
[Accessed: April 2015]

[3] Cloud Security Alliance, “The Notorious Nine Cloud Computing Top Threats in 2013,” 2013.

[4] Cloud Security Alliance, “Expanded Top Ten Big Data Security and Privacy Challenges,” 2013.

[5] C. Hammer and G. Snelting, “Flow-sensitive, context sensitive, and object-sensitive information flow control based on program dependence graphs,” *Int. Journal of Inform. Security*, vol. 8, no. 6, pp. 399-422, 2009.

[6] D. E. Denning, “A lattice model of secure information flow,” *CACM*, vol. 19, no. 5, pp. 236–243, 1976.

[7] S. Fink and J. Dolby. *WALA–The T.J. Watson Libraries for Analysis*. Available: http://wala.sourceforge.net/.

[8] J. Graf, M. Hecker, and M. Mohr, “Using JOANA for Information Flow Control in Java Programs-A Practical Guide,” *Softw. Eng. Workshops*, pp. 123-138. 2013.

[9] V. Pappas, V. Kemerlis, A. Zavou, M. Polychronakis, and A. Keromytis, “CloudFence: Data Flow Tracking as a Cloud Service,*” Lecture Notes in Computer Science*: RAID, Springer, vol.. 8145, pp 411-431, 2013.

[10] L. Bello, and A. Russo, “Towards a taint mode for cloud computing web applications,” *Proc. 7th Workshop on Programming Languages and Anal. for Security*, ACM, 2012.