ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Special Issue , August 2019

International Conference on Recent Advances in Science, Engineering, Technology and Management at Sree Vahini Institute of Science and Technology-Tiruvuru, Krishna Dist, A.P

Cloud Computing- A Security Framework

K.Mounika , M.Manjusha

Assistant Professors, Department of Computer Science, Sree Vahini Institute of Science and Technology, Tiruvuru, India.

ABSTRACT: Nowadays, information is transfer much effective than early days. The developments of Internet have changed the world. People were starting sharing information, saving data and computing online. By doing it this way, people can save a lot of money, energy and devices. Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased.

I. INTRODUCTION

Cloud computing is emerged as a modern technology which developed in last few years and considered as next big thing in years to come. In recent years it has grown up from just being a concept to major part of IT industry. Cloud computing provides a distributed computing environment comprises of heterogeneous components like hardware, software, firmware, networking as well as services. It changed the entire process that distributed computing used to present e.g Grid computing, server-client computing. Cloud computing describes recent developments in many existing IT technologies and separates application and information resources from underlying infrastructure.

Cloud computing generally works on three type architecture namely

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

There are different issues and concerns with each of the cloud computing technology

SaaS (Software as a Service):

- Hosts and manages a given application in their data Centre and makes it available to multiple users over the web.
- Examples of SaaS are Oracle CRM on Demand and salesforce.com.

PaaS (Platform as a Service):

- Application development and deployment platform which delivere over the web to developers.
- Facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure.
- All of the facilities required to support the complete lifecycle of building and delivering web applications and services entirely available through internet.
- Includes database, middleware, development tools and infrastructure software.
- Paas service providers include Google App engine and Engine Yard.

IaaS (Infrastructure as a Service):

- Delivery of software and hardware as a service.
- It is a traditional hosting that does not require any log term commitment and allows users to provision resources on demand.
- Amazon web services elastic compute cloud (EC2) and secure storage service (S3) are examples.

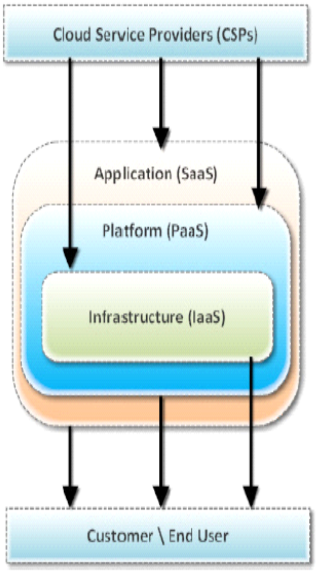

Fig 1: Cloud Computing Architecture

Cloud computing faces a lot of different challenges. Security is one of the key challenges. Security problems can cause great loss, even devastating blow. Therefore to make the enterprise and the organization accept cloud computing services, it is necessary to solve security problems.

II. RECENT WORKS

Various authors proposed different frameworks to detect and stop large number of attacks which are discussed below

- Authors proposed a generic management framework which allows the providers to enforce complex security policies. They designed a expressive policy description language to be easily interfaced with various data management systems. They efficiently protected a data storage system by evaluating their security framework on top of BlobSeer data management platform.
- Other work investigated the problem of assuring customer integrity. In order to provide a way for the user to check his integrity the authors provided a scheme. This proof can be agreed up on by both the cloud provider and customer and can be in corporated in the service level agreement.
- Authors suggested four methods for cloud security and privacy which are
  - Access control method which is an application of Role Based Access Control (RBAC).
  - Policy integration method which is a dynamic policy control mechanism.
  - Identity management method which prevents the un authorizes secondary usage of data.
  - User control method which solves the problem of cloud users losing control of their data.
- Authors focused on technical security issues such as VM-Level attacks, isolation failure, management interface, compromise and compliance risks. They proposed a cloud security architecture using which organizations can protect themselves against threats and attacks. The key points for architecture are single-sign on, increased availability, single management console and virtual machine protection.

Threats to cloud computing:

There are some potential threats to cloud computing and their remedies are discussed below

- **Changes to business model**
  Mitigation: A reliable end-to-end encryption and appropriate trust management scheme can simplify such threat to some extent.

- **Abusive use of cloud computing**
  Mitigation: Initial registration should be through proper validation and through stronger authentication. In addition to this, the user's network traffic should be monitored.
- **Insecure interfaces and API**
  Mitigation: Can be avoided by using proper security model for cloud provider's interface and ensuring strong authentication and access control mechanism with encrypted transmission.
- **Malicious insiders**
  Mitigation: To avoid this risk more transparency is required in security and management process including compliance reporting and breach notification.
- **Shared technology issues/multi-tenancy nature**
  Mitigation: Implementation of SLA for patching, strong authentication, and access control to administrative tasks are some of the solutions.
- **Data loss and leakage**
  Mitigation: Security of API, data integrity, secure storage for used keys, data back up and retention policies.
- **Service hijacking**
  Mitigation: Security policies, strong authentication and activity monitoring
- **Risk profiling**
  Mitigation: Cloud provider should disclose partial infrastructure details, logs, and data. In addition to this, there should be a monitoring and alerting system.
- **Identity theft**
  Mitigation: Using strong authentication mechanisms.

III. ATTACKS ON CLOUD COMPUTING

- **Zombie attack**
  Mitigation: Better authentication and authorization and IDS/IPS can provide protection against such attack.
- **Service injection attack**
  Mitigation: Service integrity checking module should be implemented. Strong isolation between VMs may disable the attacker from injecting malicious code in the neighbor's VM.
- **Attacks on virtualization**
  Mitigation: By monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewall.
- **Man in the middle attack**
  Mitigation: Proper SSL configuration and data communication tests between authorized parties.
- **Metadata spoofing attack**
  Mitigation: Information about services and applications should be kept in encrypted form. Strong authentication should be enforced for accessing such critical information.
- **Back door channel attack**
  Mitigation: Better isolation and authentication between VMs can provide protection against such attacks.

PROPOSED SECURITY MODEL

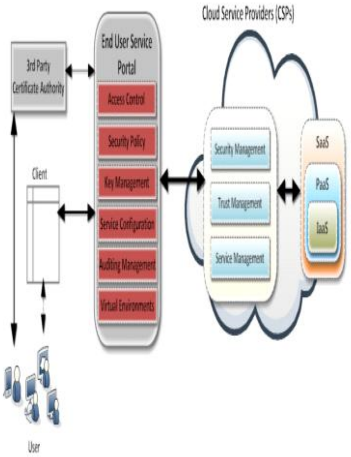

Fig 2. Block Diagram of Secure Cloud Computing

Based on all the threats described above this security model is constructed. User can be certificated by the 3rd party certificate authority, then can be issued token for service by End User Service Portal. After joining service portal, user can purchase and use cloud services which are provided by single service provider. End User Service Portal which is composed access control, security policy, key management, service configuration, auditing management, and virtual environments provides secure access control using Virtual Private Network (VPN) and cloud service managing and configuration.

IV. FRAMEWORK FOR SECURE CLOUD COMPUTING

Framework for secure cloud computing is based on the security model shown above which describes the details of each component and apply the needed security technologies for implementation between components in cloud computing. Access control process on each component is as follows:

- **Client:** users could access the client side with multi factors authentication provided by End-User Service Portal. Multi factors authentication based on certification issued by 3rd party certification authority.
- **End-User Service Portal:** when clearance is granted, a single Sign-on access token (SSAT) could be issued using certification of user. Then the access control component share the user information related with security policy and verification with each other components in end-user service portal and cloud service providers by using XACML and KIMP.

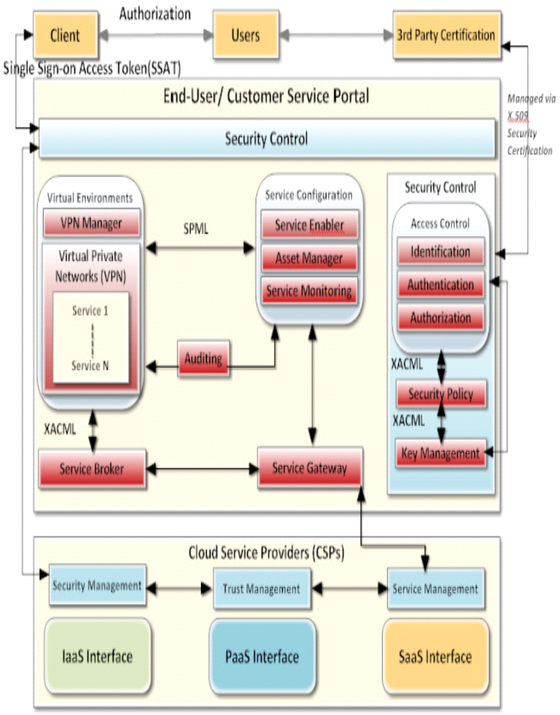

Fig 3. Framework for Secure Cloud Computing

- **Single Sign-on:** Users may have multiple accounts on different cloud services with same user name and password which poses inherent security risks. To overcome this problem, it is suggested that, to streamline security management and implement strong authentication with in the cloud.
- **Service Configuration:** The service enabler makes provision for personalized cloud service using user's profile for the integration and interoperation. The SPML can be used to share user's profile. The asset manager requests user's personalized resources with SPML to cloud service provider and configuration service via VPN connection.
- **Service Gateway, Service Broker:** Service gateway manages network resources and VPN on the information life cycle of service broker.
- **Service Control:** The security control component provides significant protection against security threats. Based on the providers access control needs various access control models can be used. Role Based Access Control (RBAC) has been widely accepted as the most promising access control model.
- **Security Management:** Provides the security and privacy specification and enforcement functionality. The authentication and identity management module is responsible for authenticating users and services based on credentials and characteristics.
- **Trust Management:** Due to the cloud's nature i.e service oriented, the trust level should also be integrated with the service. One possible approach is integrated with service, and bidirectional.
- **Service Monitoring:** An automated service monitoring systems to guarantee a high level of service performance and availability.

V. CONCLUSION

Cloud computing is a technology of rapid development, however security problems have become obstacles to make the cloud computing more popular which must be solves. This paper proposed a security model and framework for secure cloud computing environment that identifies security requirements, attacks, threats, concerns associated to deployment of the clouds. At the same time cloud computing technology is not just a technical problem, it is also involves standardization, supervising mode, laws and regulations, and many other aspects, cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more wide.

REFERENCES

1. Amazon web services. Amazon virtual private cloud, http://aws.amazon.com/vpc/
2. www.wikipedia.com
3. http://cisjournal.org/journalofcomputing/archive/vol3no3/vol3no3_13.pdf
4. http://www.academia.edu/Documents/in/Security_Framework_for_cloud_computing