International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue:1 January 2017 p-ISSN: 2394-8280

IMPACT OF SECURITY ISSUES IN CLOUD COMPUTING ENVIRONMENT: A SURVEY

Mansi Verma[1], Prof Nishant Sinha[2]
Research Scholar-ME-IT, Medi-caps Institute of Technology and Management,
mansiverma14@gmail.com
Professor-Department of computer science Medi-caps Institute of Technology and Management,
nishant.sinha.k@gmail.com

ABSTRACT

The Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, where end-users consume power without needing to understand the component devices or infrastructure required to provide the service.

The project work will implement a RADIUS system with access control. Proposed system will carried a RSA algorithm for cryptography and mobile device to introduce third party authentication service. Later on it will also develop an access control table at service server end to ensure the user to "Who Can Access what."

Keywords: Cloud computing, Access Control, Mobile Verification

1. INTRODUCTION

A **cloud,** of course, is a visible mass of droplets or frozen crystals floating in the atmosphere above the surface of the Earth or another planetary body. A cloud is also a visible mass attracted by gravity. Lately, cloud computing has been exerting a strong gravitational pull its own— entire one that has been attracting a mass of money. The big players in cloud computing are Google, Amazon, and, of late, Microsoft and IBM. Maybe Oracle/Sun, maybe HP will join them. Rack space, GoGrid, and AT&T want in too.

Google has built the world's largest cloud computing infrastructure. Amazon has not only built the world's largest marketplace, but also is prime mover in the cloud computing revolution, hosting a myriad of other businesses on its Cloud Services infrastructure. With the recently gone-live Microsoft Azure, Microsoft has entered the cloud-computing business as well, simplifying migration for all Windows applications. Salesforce, VMware, Oracle (Sun), IBM, Adobe, and RackSpace among others, have all tied their futures to cloud computing. (Rackspace and Oracle are mostly into "private clouds").Specialized vendors such as Intuit (maker of Quickbooks) and "command and control" vendors such as CA Technologies (formerly Computer Associates) also have cloud-based offerings. As cloud computing matures, it is being embraced not only by small start-ups, but also by major enterprises (albeit more slowly); they appreciate the scalability and reliability that cloud computing can provide.

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, where end-users consume power without needing to understand the component devices or infrastructure required to provide the service.

There are five essential characteristics of the cloud model:

1. Rapid elasticity
2. Service on demand
3. Broad network access
4. Resource pooling
5. Location independence
6. Measuring service

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services

The Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This frequently takes the form of web-based tools or applications that users can access and use through a web browser as if they were programs installed locally on their own computers. Typical cloud computing providers deliver common business applications online that are accessed from another Web service or software like a Web browser, while the software and data are stored on servers. Most cloud computing infrastructures consist of services delivered through common centers and built on servers. Clouds often appear as single points of access for consumers computing needs. Commercial offerings are generally expected to meet quality of service (QoS) requirements of customers, and typically include service level agreements (SLAs).

At its simplest, cloud computing is the dynamic delivery of information technology resources and capabilities as a service over the Internet. Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. It generally incorporates infrastructure as a service (IaaS), platform as a service (PaaS),and software as a service (SaaS).According to Gartner Group the attributes of cloud computing are:

1. Service-based
2. Scalable and elastic
3. Shared
4. Metered by use
5. Use of Internet technologies

The most frequently cited benefits of cloud computing are:

1. It is agile, with ease and speed of deployment
2. Its cost is use-based, and will likely be reduced
3. In-house IT costs are reduced
4. Capital investment is reduced
5. The latest technology is always delivered
6. The use of standard technology is encouraged and facilitated.

2. LITERATURE REVIEW

The **cloud computing service** can support the both computer hardware or software resources to user conveniently. Cloud services have three types of service.

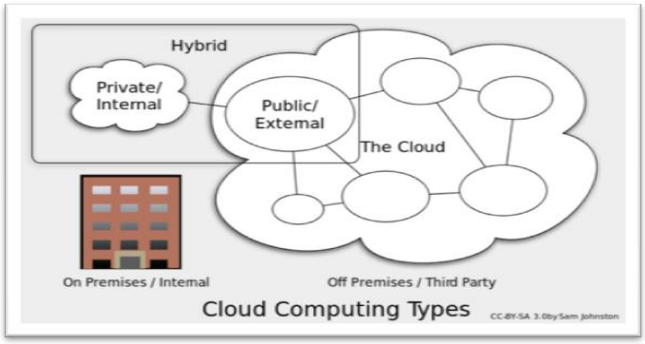

Figure 1: Deployment models in Cloud

2.1 Public Cloud Model: -

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free or offered on a pay-per-usage model. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure Express Route" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider. Public cloud users are lower about 22%.

2.2 Private Cloud Model: -

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualized the business environment, and requires the organization to reevaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run data centers are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept". The enterprises of 20% degree are using a service only from domestic.

2.3 Hybrid Cloud Model: -

Hybrid cloud is a composition of two or more clouds private and public that remains distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

Gartner, Inc. defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

Hybrid cloud services are only hopeful services. This service selects strong points between the public cloud service and private cloud services. This service must agree network, database, and security services between service providers before make services. And this is a very difficult. Hybrid cloud services must understand vulnerable points of private cloud services and public cloud services and they must support to resolving the security threats. They must provide a secure authentication system for hybrid cloud services in mobile communication environments.

Hybrid cloud service must have three security services that are very important. First, user authorization is a user identification and access control service. Second service is a mobile device authentication service such as smart phone, tablet, and PC. Third, hybrid cloud service user requested data or its stored media must have authentication service for them.

3. SERVICE MODELS

Service delivery in Cloud Computing comprises three different service models. The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services.

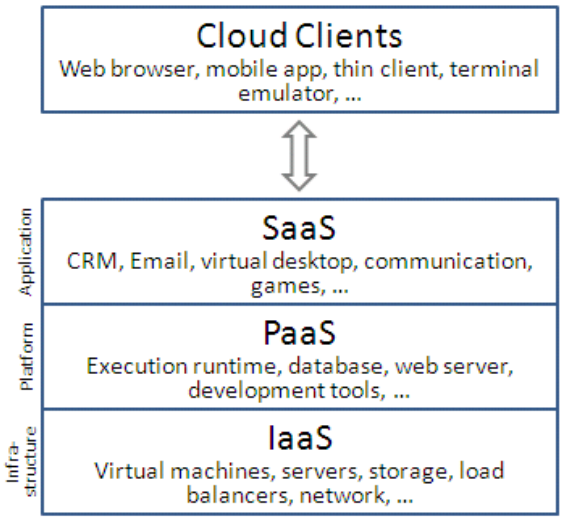

Figure 2: Service models in Cloud

3.1 Software-as-a-Service: -

Software-as-a-Service provides complete applications to a cloud's end user. It is mainly accessed through a web portal and service oriented architectures based on web service technologies. Credit card or bank account details must be provided to enable the fees for the use of the services to be billed. The services on the application layer can be seen as an extension of the ASP (application service provider) model, in which an application is run, maintained, and supported by a service vendor. The main differences between the services on the application layer and the classic ASP model are the encapsulation of the application as a service, the dynamic procurement, and billing by units of consumption (pay as you go). However, both models pursue the goal of focusing on core competencies by outsourcing applications.

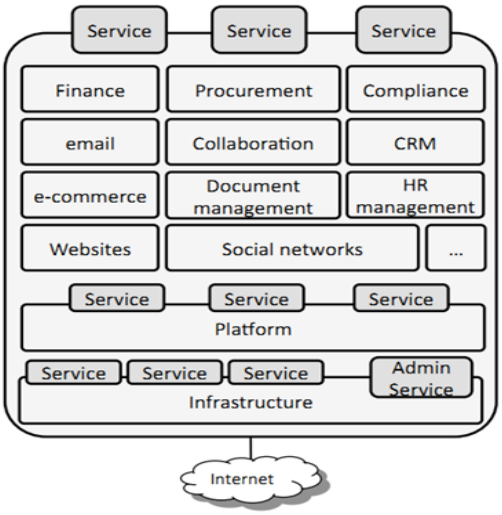

Figure 3: Software-as-a-Service (SaaS) Stack

2. Platform-as-a-Service: -

Platform-as-a-Service comprises the environment for developing and provisioning cloud applications. The principal users of this layer are developers seeking to develop and run a cloud application for a particular platform. They are supported by the platform operators with an open or proprietary language, a set of essential basic services to facilitate communication, monitoring, or service billing, and various other components, for instance to facilitate startup or ensure an application's scalability and/or elasticity. Distributing the application to the underlying infrastructure is normally the responsibility of the cloud platform operator. The services offered on a cloud platform tend to represent a compromise between complexity and flexbility that allows applications to be implemented quickly and loaded in the cloud without much configuration. Restrictions regarding the programming languages supported, the programming model, the ability to access resources, and persistency are possible downsides.

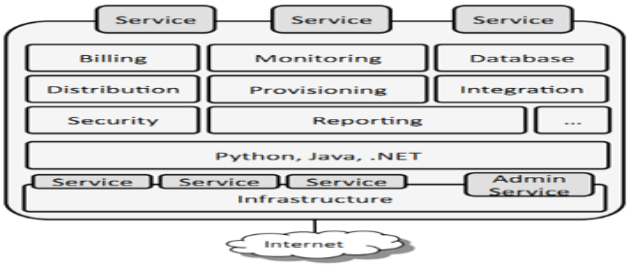

Figure 4: Platform-as-a-Service (PaaS) Stack

3. Infrastructure-as-a-Service: -

The services on the infrastructure layer are used to access essential IT resources that are combined under the heading Infrastructure-as-a-Service (IaaS). These essential IT resources include services linked to computing resources, data storage resources, and the communications channel. They enable existing applications to be provisioned on cloud resources and new services implemented on the higher layers. Physical resources are abstracted by virtualization, which means they can then be shared by several operating systems and end user environments on the virtual resources – ideally, without any mutual interference. These virtualized resources usually comprise CPU and RAM, data storage resources (elastic block store and databases).

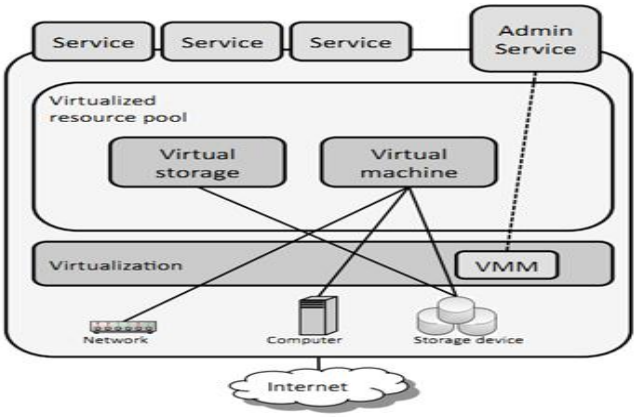

Figure 5: Infrastructure-as-a-Service (IaaS) Stack

In this base paper, they describe three related works. First, they explain character of mobile communication environments and cloud services. RADIUS authentication method is second. It is a cross-authentication method for mobile communication environment such as between smart phone and wireless access points.

4. EXISTING WORK

Characters of mobile communication environments are wired network environment using PC, terminal, and so on. Wireless network environments using smart phones or other mobile devices. Today, many users have PC, tablet, smart phone, and other devices. And they have behavior of nomadic and multiplayer ability. So, future communication environment must support mobile communication environments and ability.

4.1 RADIUS (Remote Authentication Dial-In User Service).

RADIUS is the authentication method with a token between mobile device user and wireless access pointer. The authentication server can generate a token and send it to user. Token uses device authentication by this owner and user identification. Figure 1 shows example of RADIUS architecture.

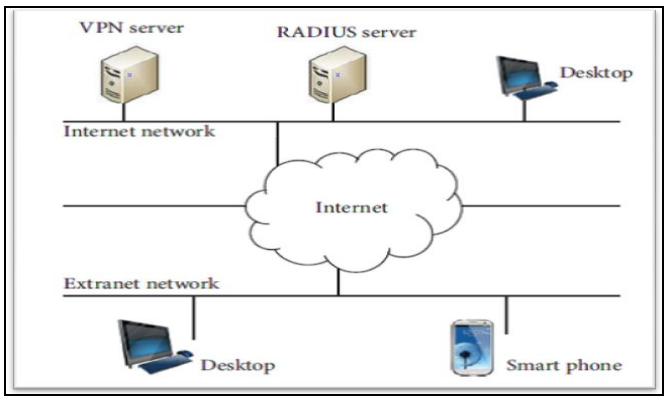

Figure 6: RADIUS

As shown in Figure 1, user of outside must request authentication way to inside RADIUS server for using computer resources such as hardware or software resource. Smart phone users in the extra network must request token for device certification to RADIUS server in the internal network using wired or wireless internet environment. Then RADIUS server checks smart phone certification by device information. And if smart phone have alright device information, RADIUS server generates the token and transmits token to smart phone users. Next time, smart phone user will Connects VPN server for user certification using token and more individual information. When smart phone user have alright user authentication, VPN server allow smart phone user wanted cloud service. And smart phone user cans use cloud service as well as SaaS (Software as a Service). RADIUS server have many complex procedures for device and user authentication. And But RADIUS server cannot provide complement security services. This is a disadvantage in RADIUS server scheme

3.3 Two-Factor Authentication Service: Generally, the authentication service is to check a user or device certification. In this time, authentication server wants to receive about user or device information such as ID, Password, Bioinformatics, and so on. And this server checks to certificates correct. Traditional authentication method confirms userID and password for certificate. However, this method is too easy, and not secure. So, a new authentication method

Propose recently that is two-factor authentication. This is very conventional method. Traditional authentication checks single identity information such as ID and password fairs. But two-factor authentication checks more two authenticate information such as ID and password fair, token, and onetime password, random number. This is more secure, convenient authentication method in mobile communication environment.

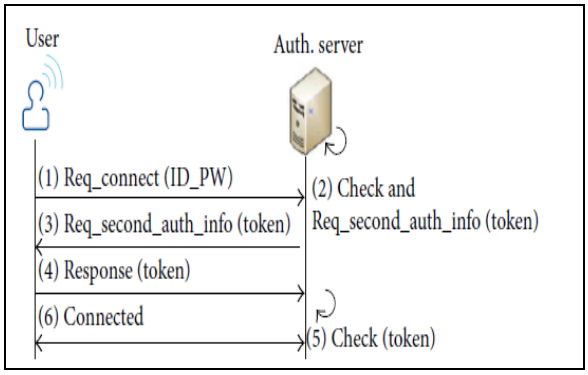

Figure 1.2: *Two-Factor Authentication Service*

Hybrid cloud service environment need two-factor authentication method for more secure certificate against of ID and password fair, SSO, PKI methods. Two-factor authentication system can support various token. So, our proposed system approach two-factor authentication method by ID and password with token. Token have user id, device information, time, date, and random number. And certificate information is USIM, MTM, and anything's. Figure 2 shows an example of a method that can provide a two-factor authentication service.

As shown in Figure 2, cloud service user sends {ID |PW} only two pairs of information in general but it is very simple. So, this scheme is very dangerous. So researcher approaches two-factor authentication system. It adds some token such as time-stamp or one-time token. And authentication server requests second authentication information user such as extended token. Next, user makes extended token and transmits server then authentication server checks extended token and allows or rejects user request. Like this, two-factor authentication server can provide general authentication token such as {ID | PW} and extend token. This way is very easy and strong authentication way for mobile communication environment using smart phone or tablet and ultra book.

5. PROBLEM DOMAIN

The security issues in cloud computing includes:

- Data security
- Identity and access control
- Key management
- Virtual machine security

Among these main security issues in the cloud, data security and integrity is believed to be the most difficult problem which could limit the use of cloud computing. In fact, access control and key management are all issues involved in data security.

Data security in the cloud refers to data confidentiality, integrity, availability and traceability (CIAT), and these requirements pose major problems for cloud computing. Data confidentiality requires that information be available or disclosed only to authorized individuals, entities or IT processes. Data integrity ensures that the data is maintained in its original state and has not been intentionally or accidentally altered or deleted. Data availability ensures continuous access to data even in the event of a natural or man-made disaster or events such as fires or power outages. Data traceability means that the data and communications are genuine in a transaction and that both parties involved are who they claim to be. Specifically, to achieve the above requirements of CIAT, the critical security challenges of data security in the cloud can be mainly outlined as follows:

1. Key management
2. Access control
3. Searchable encryption techniques
4. Remote integrity check
5. Proof of ownership

Understanding of security threats in hybrid cloud computing environment to propose authentication system suitable for hybrid cloud services is required. So we will divide and describe five kinds of threats that as follows.

1. Man-in-the-middle attack or man-in-the middle-browser attack. This threat happen between authentication server on internal network and outside user such as smart phone, tablet.
2. DoS or DDoS attack.
3. Third threat is location certification attack. On the outside, mobile devices move very frequently. But, mobile device's location information is very important for its certification.
4. Fourth threat is script attack weakness by inside attacker.
5. Outside user authentication for public cloud service.

To overcome the above problems Jin-Mook Kim and Jeong-KyungMoon proposed a RADIUS system consisting five modules to achieve secure authentication requirement. RADIUS is a good platform for hybrid cloud but still have some scope of improvement which is:

1. It uses IDEA which is 256 bit symmetric key algorithm which not only increases encryption overhead but decryption too.
2. There is no involvement of mobile phone or third party device for runtime & human authentication.
3. There is no unique algorithm for OTT generation.
4. There is no mechanism for Access Control.

6. CONCLUSION

Cloud computing comes into focus only when we think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends its existing capabilities. The proposed system will not only allow external user to get access into cloud service server but will also increase choice of security. Security customization will help user and service provider to reduce security overhead. The complete project will end with the implementation of proposed model and testing on various test cases.

REFERENCES

1. Jin-Mook Kim and Jeong-KyungMoon,"*Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments*" published in International Journal od Distributed Sensor Networks by Hindwai Publication Corporation. Volume-1, 2014.
2. Anurag Jain, Dr. Rajneesh Kumar "Confidentiality Enhanced Security Model for Cloud Environment" ICTCS '16, March 04-05, 2016, Udaipur, India
3. Nasrin Khanezaei, Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia
4. Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.
5. Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015
6. Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu "An enhanced data security and trust management enabled framework for cloud computing systems" IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China
7. Shilpi Singh, Vinod Kumar "Secured User's Authentication and Private Data Storage- Access Scheme in Cloud Computing Using Elliptic Curve Cryptography" 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development.
8. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012