Legacy and Privacy Issues in Cloud Computing

Anurag Chandna, ²Yashveer Singh², Sagar Choudhary³

[1,2,3]*Assistant Professor, Department of Computer Science and Engineering, Roorkee College of Engineering, Roorkee, Uttarakhand, India*

---***---

Abstract - *Clouding Computing is popular nowadays. It is like the on-demand availability of computer system resources like data storage and computing program or application, information or multimedia content, or elements for multimedia information sharing. All these data or information is available to different user with the help of internet. The cloud computing architecture in which third party users, virtual machine and cloud service provider are involved for data uploading and downloading with the help of internet. Legacy and privacy of the cloud is very important concerns of nowadays as more and more clients using the cloud for storing their data and information. As now mobile and computer is increasing in numbers, result the numbers of attackers is also increasing. The main concern of legacy is to provide the legal data to the client and privacy should be maintain on this data is also very important.*

***Key Words*:** **Cloud Computing, Legacy, Privacy, DoS, Security, User, ID, Server Authentication**

1. INTRODUCTION

Cloud computing is the on-demand delivery of IT resources like data or information, over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers for personal or business use, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider with a very high speed data rate.[1] Cloud computing has two meanings. The most common approach to running workloads remotely and with the help very high-speed data communication over the internet in a commercial provider's data center, also known as the "public cloud" model. Popular public cloud offerings—such as Amazon Web Services (AWS), Google Cloud, Salesforce's CRM system, and Microsoft Azure—all exemplify this familiar notion of cloud computing. Today, most businesses take a multi-cloud approach, which simply means they use more than one public cloud service.[2]

The second meaning of cloud computing describes how it works: a virtualized pool of resources, from raw compute power to application functionality, available on demand by the cloud service provider like Google, Amazon, Microsoft etc. When customers or clients procure cloud services, the cloud service provider fulfills those requests using advanced automation rather than manual provisioning. The key advantage is agility: the ability to apply abstracted compute, storage, and network resources to workloads as needed and tap into an abundance of prebuilt services. [2]

But, probably, the most widespread today is the one given by Mell and Grance in [3]; Cloud computing is "*a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction*". The Gartner's special report by Smith in [4] says in its very opening statement: "*cloud computing is maturing, but it continues to be the latest, most hyped concept in IT*".

Infrastructure as a Service (IaaS)

IaaS contains the basic building blocks for cloud Information Technology and data sharing with the authenticate customer. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives you the highest level of flexibility of cloud data and information and management control over your IT resources like data and information shared with each other or access this information for further manipulation. It is most like the existing IT resources with which many IT departments and developers are familiar. [1]

Platform as a Service (PaaS)

PaaS removes the need for you to manage underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about the software, website designing or coding, resource procurement, capacity planning, software maintenance, patching, or any of the other software requirement or undifferentiated heavy lifting involved in running your application for cloud computing. [1]

Software as a Service (SaaS)

SaaS provides you with a complete product that is run and managed by the service provider. In most cases, people referring to SaaS are referring to end-user applications (such as web-based email). [1]

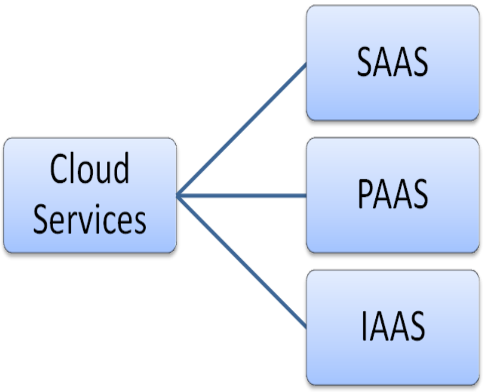

Figure 1: Service Model of Cloud Computing

2. DEPLOYMENT MODELS

Cloud Computing architecture consists of four deployment models, and, on top of the deployment models, rest the three main service delivery models, as illustrated in Figure 2. Each of these models brings about different security, legacy and privacy challenges that need to be taken into consideration when planning to move business processes, data and information to the cloud, for the betterment of the cloud and business:

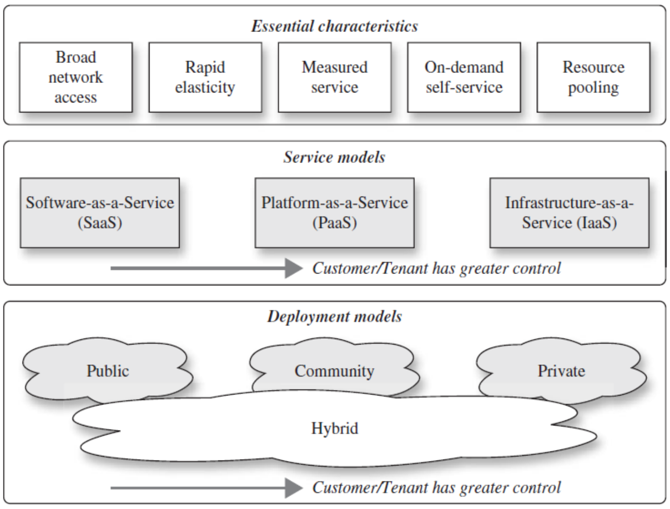
Essential characteristics
Broad network access
Rapid elasticity
Measured service
On-demand self-service
Resource pooling
Service models
Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)
Customer/Tenant has greater control
Deployment models
Public
Community
Private
Hybrid
Customer/Tenant has greater control

Figure 2: NIST Cloud Computing Model [6]

Organizations planning to adopt Cloud Computing services can choose from four main deployment models. First thing that we need to take care, there is the private cloud also known as internal cloud; the infrastructure is operated solely for an organization. It is managed by the organization or a third party and may be some of internal online or offline support. Usually, big organizations with multiple sites implement this model to service their office locations that might be scattered across the globe. At the other extreme, there is the public cloud also known as external cloud model, It is available to the general public or a large industry group and is owned by an large or medium level organization offering cloud services for a fee or free, as per the cloud service provider policy. A public cloud is hosted, operated and managed by a third-party vendor from one or more data centers [7]. The community cloud model is shared by multiple organizations that have a common objective and supports a specific community that has shared concerns such as mission, security requirements, policy and compliance considerations. It may be managed by the organization or by an assigned third party. The hybrid cloud model is a composition of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability [8].

Cloud Computing services are generally delivered through three main delivery models to the end-user, as illustrated in Figure 2. SaaS is a software distribution model in which applications are hosted by a vendor or service provider, and made available to customers over a network, typically the internet. SaaS has emerged as the dominant delivery model and an underlying technology that supports web services and service-oriented architecture (SOA). The SaaS model is associated with the pay-as-you-go subscription licensing model. North Bridge [9] identifies SaaS as the leading model, with a 63% share of the market, while according to the Yankee Survey (2010) [10], PaaS and IaaS are taking longer to develop. Some of the major players in this area are IBM Lotus Live, Google Apps, Oracle, Facebook, Netsuite and Salesforce.com. PaaS provides the development environment and it rests on top of Infrastructure-as-a-Service (IaaS). PaaS delivers operating systems and associated services over the internet, without the need to download or install applications on end-user computers. It provides an operating environment for delivering a variety of applications and is essentially an outgrowth of the SaaS application delivery model. Sub-types of PaaS include Desktop-as-a-Service (DTaaS) and Testing-as-a-Service (TaaS). Vendors in this area include Amazon Web Services, Google App Engine, Windows Azure Platform, Force.com and Caspio.

IaaS provides the entire infrastructure stack that delivers the computer infrastructure, and it leverages significant technology, services, and data centre investments, to deliver IT as a service to customers. IaaS differs from SaaS in that, instead of software, IaaS delivers hardware such as servers, memory, CPUs, disk space and network connectivity. Service providers in this model include Flexiscale, Rightscale, Gogrid, Amazon Web Services and Cisco Unified Service Delivery. IaaS is the fastest growing model and is expected to give way to PaaS in five years' time.

Cloud Computing Inhibitors

There several barriers to Cloud Computing adoption [6] identify the following: security, privacy, connectivity and open access, reliability, interoperability, independence from cloud service providers (CSP), economic value, IT governance, changes in the IT organisation, and political issues due to global boundaries. Other Cloud Computing adoption problems in developing economies for SMBs are the following: poor basic infrastructure, access to ICT devices, poor internet coverage and geographical location of cloud data.

3. PRIVACY OF CLOUD COMPUTING

Privacy of cloud is very important factor for cloud infrastructure. There are many laws and regulations for maintaining the privacy of data and information.

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing. For example, at the end of 2010, the National Conference of State Legislatures reported that forty-six states have enacted legislation governing disclosure of security breaches of personal information, and that at least twenty-nine states have enacted laws governing the disposal of personal data held by businesses and/or government.

3.1 Law and Regulations

For U.S. Federal agencies, the major security and privacy compliance concerns include the Clinger-Cohen Act of 1996, the Office of Management and Budget (OMB) Circular No. A-130, particularly Appendix III, the Privacy Act of

1974, the E-Government Act of 2002 and its accompanying OMB guidance, and the Federal Information Security Management Act (FISMA) of 2002.11 Also of importance are National Archives and Records Administration (NARA) statutes, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (Title 36 of the Code of Federal Regulations, Chapter XII, Subchapter B).

The Privacy Act governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies and can be retrieved by a personal identifier (e.g., name). It requires each agency to publish notice of its systems of records (i.e., a system of records notice (SORN)) in the Federal Register and to allow individuals to request access to and correction of their records and information. The E-Government Act of 2002, among other things, requires federal agencies to complete a Privacy Impact Assessment (PIA) on all new or substantially changed technology that collects, maintains, or disseminates PII, and to make the results publicly available. M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, provides direction to agencies on conducting PIAs. A PIA is a structured review of an information system to identify and mitigate privacy risks, including risks to confidentiality, at every stage of the system lifecycle. It can also serve as a tool for individuals working on a program or accessing a system to understand how to best integrate privacy protections when working with PII.

3.2 Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively. Privacy has the following elements.

(i) When: a subject may be more concerned about the current or future information being revealed than information from the past.

(ii) How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii) Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

In commerce, consumer's context and privacy need to be protected and used appropriately. In organizations, privacy entails the application of laws, mechanisms, standards, and processes by which personally identifiable information is managed.

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behavior by the user's visit model (not direct data leakage). Researchers have focused on Oblivious RAM (ORAM) technology. ORAM technology visits several copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology. Stefanov et al. proposed that a path ORAM algorithm is state-of-the-art implementation.

The privacy issues differ according to different cloud scenarios and can be divided into four subcategories as follows:

(i) how to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale,

(ii) how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is a usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication,

(iii) which party is responsible for ensuring legal requirements for personal information?

(iv) to what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained.

4. LEGACY

Legacy systems are software solutions found in a company for a long period of time [7]. The systems have probably survived in a company because of the software maintenance (corrective, preventive, and evolutionary), internal resistance to technology changes, or they may run critical processes. Usually, these kinds of systems work in isolation and with an exclusive data repository (i.e. data files, databases, etc.). Therefore, the communication between the legacy systems to other newer application is a hard task and it requires the definition of complex communication interfaces and data conversion components. Additionally, the companies with old legacy systems need to invest money to integrate theirs tools, to adapt functionality to new technologies, and to make flexible their business processes. Most of the companies firstly transform the traditional applications to software based on SOA before adopting the Cloud paradigm, because SOA is flexible to services composition and it encapsulates the business logic through web services (WSs). Those WSs can communicate each other by standard protocols and methods of message exchanging, which facilitate the services composition. The SOA applications consist basically of three layers: (a) Presentation Layer: where is the user interface; (b) Business Layer: where are the business logic and its functionality implemented by algorithms, software components or WSs; and (c) Data Layer: where is the schema and application data. The applications can be migrated by layers. A conceptual model of system migration to Cloud Computing is presented in Fig. 1). It is considered in the migration model the following techniques:

• Application Replacement: it entails replacing the whole application or part of it for one or more standard components available in the market. As a result, some configurations and adaptation task must be conducted as part of the system migration. This replacement can generate the loss of information control, the need of creating new interfaces with other components or applications, the change of the normal workflow in the organization, and the lack of information about the internal structure of the acquired components.

• Application Conversion: it consists in transforming the whole application in a Cloud Computing solution. The transformation can be conducted automatically using a conversion engine that also maps the converted data, but it is necessary that the legacy system works normalized and without failures. — Software Conversion: it is the transformation of algorithms and software applications, keeping their functionality and their structures, but changing some programming aspects. — Data Conversion: it is the transformation of data according to a specific target schema or format. — Schema Conversion: it is the transformation of the data structure to a new equivalent structure of database.

• Application Virtualization: it basically involves the generation of virtual system container, and all system components and data schema are moved into the container without changing the source code. The legacy system is considered as a black box, within which all layers are encapsulated. During the users' interaction, all the inputs/outputs are analyzed to generate a "wrapper" that is the nexus between the encapsulated legacy system and the new presentation layer deployed in Cloud Computing.

5. CONCLUSIONS

In the cloud architecture, some malicious nodes may join the network which is responsible to trigger zombie attack in the network. These zombie nodes can spoof the information of the legitimate user and communicate with virtual machine on the behalf of legitimate user. This will lead to reduction in network performance in terms of delay and bandwidth consumption. As cloud computing faces various security issues which lead to the exposure of confidential data of users. These security issues make users unstable about the efficiency, safety and reliability in cloud computing.

In this review paper, we presented NICE to protect cloud virtual networking environment from DDoS attack. NICE construct attack graph predicts the next step of the attackers and provides optimized countermeasure. NICE software switches implement the countermeasure against zombie explorative attack dynamically. To improve the detection accuracy, NICE are needed to be implement in distributed fashion. The proposed solution can reduce the risk of cloud system being misused by internal and external attack. The experimental results show less amount of CPU utilization and better success measure rate of traffic load.

6. ACKNOWLEDGEMENT

Authors would like to thank Roorkee College of Engineering, Roorkee, Dist-Haridwar, Uttarakhand, India.

7. REFERENCES

[1] https://aws.amazon.com/what-is-cloud-computing/

[2] https://www.infoworld.com/article/2683784/what-is-cloud-computing.html

[3] NIST, The NIST Definition of Cloud Computing, P. Mell and T. Grance, Editors. 2009, National Institute of Standards and Technology.

[4] Smith, D.M., Hype Cycle for Cloud Computing, in Gartner Research Report. 2011. p. 9-11.

[5] S. Choudhary, G. Pundir, Y. Singh, Detection and Isolation of Zombie Attack under Cloud Computing, in International Research Journal of Engineering and Technology (IRJET). Vol – 7, Issue-01, Jan 2020. p. 1419-1424.

[6] Winkler, V. J. R. (2011). Securing the cloud: Cloud computer security techniques and tactics. Waltham, MA: Syngress.

[7] Mather, T., Kumaraswamy, S. & Latif, S. (2009). Cloud security and privacy: An enterprise perspective on risks and compliance. Sebastopol, CA: *O'Reilly Media, Inc*.

[8] Mell, P. & Grance, T. (2011). The NIST definition of cloud computing, National Institute of Standards and Technology. *NIST Special Publication*, 800-145.

[9] North Bridge. (2013). Future of Cloud Computing Survey 2013. Retrieved November 12, 2013, from North Bridge website: http://www.northbridge.com/2013-cloud-computing-survey.

[10] Yankee Survey. (2010). The Anywhere Enterprise: 2010 U.S. Cloud Computing FastView Survey. Retrieved November 12, 2013, from Yankee Group website: http://www.yankeegroup.com/about_us/press_releases/2010-08-23.html.

[11]Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, International Journal of Distributed Sensor Networks, Volume: 10 issue: 7,July 2014, https://journals.sagepub.com/doi/pdf/10.1155/2014/190903

[12] Zalazar, Ana & Gonnet, Silvio & Leone, Horacio. (2015). Migration of Legacy Systems to Cloud Computing. Electronic Journal of SADIO. 14.

8. BIOGRAPHIES

Anurag Chandna completed his M.C.A. and Master of Technology (M.Tech). He published more than 15 International journals and attends many conferences in reputed institute and university.

Dr. Yashveer Singh completed his Master of Technology (M.Tech) in 2011 and Doctorate of philosophy (Ph.D) in 2016. He published more than 15 International journals and attends many conferences in reputed institute and university.

Sagar Choudhary graduated from Uttarakhand Technical University, Dehradun, India (B.Tech-I.T.) in 2011 and received his Master's from Uttarakhand Technical University, Dehradun, India (M.Tech-C.S.E.) in 2014. Currently he is working in Roorkee College of Engineering as Assistant Professor in the department of Computer Science and Engineering. His area of interest are wireless networks and cloud computing.