International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 08 | August - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Survey on Novel Approach of Securities in Cloud Computing

Mrs. Rekha S. Kotwal
Information Technology Department
JSPM's Bhivarabai Sawant Institute of Technology & Research
Pune, India

***Abstract*—Now a days Cloud computing is the rapidly growing technology in the computer world these days—maybe too big of a buzz. Cloud computing is on-demand access, over the internet, to computing the resources like applications, servers data storage, development tools, networking capabilities, and more—hosted at a remote data center managed by a cloud services provider. Cloud computing means different things to different people Cloud computing is a innovation that is introduced recently. Research firm IDC thinks that cloud computing will reach $42 billion in 2012. Cloud computing separated the application from the operating system and hardware via middleware. You can do everything on cloud from running applications to storing data off-site. You can run entire operating systems on the cloud. This paper is for anyone who may have recently heard the term "cloud computing" for the first time and needs to know what it is and how it helps them.**

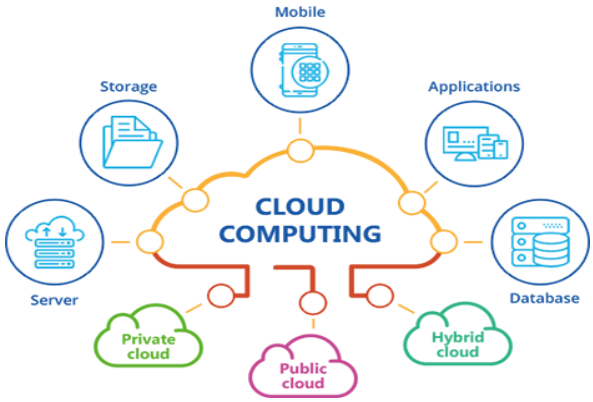
Keywords-Cloud Computing; Data Center; cloud security;

I. INTRODUCTION

Cloud computing is almost used in every field. We can assume any tech magazine or visit almost any IT website or blog and we'll be sure to see talk about cloud computing. The only problem is that not everyone agrees on what it is. Ask ten different professionals what cloud computing is, and you'll get ten different answers. And is cloud computing even worth all the hype? Some people don't think so. There are three types of clouds in the cloud delivery model. It includes private (local) public, and hybrid clouds. The public cloud corresponds to the Internet according to the standard cloud computing model. The service provider uses the Internet to provide all services to the user. Services can be free or paid. An organization has private or local clouds. It offers all the advantages of the public cloud, such as flexibility, automation, monitoring, and administrative support. It offers more security in the cloud, since it is implemented in the firewall. The public and private hybrid is a hybrid cloud. Both are mixed to use both and create more value. Cloud Computing includes to both the hardware and systems software in the datacenters that provide those services and applications delivered as services over the Internet.The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. In Public cloud syatem cloud or resourses are made available in a pay-as-you-go manner the service being sold is Utility Computing.

The term Cloud Computing has been defined in many ways by analyst firms, academics, industry practitioners, and IT companies. Table I shows how selected analyst firms define or describe Cloud Computing. Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization.

Whereas in private cloud system private data centers of enterprise are not made available publically. In short the private cloud access is limited to that particular organization only. Therefore we can say that cloud computing is the combination of hardware or platform services, software services, and infrastructure on demand services[4].



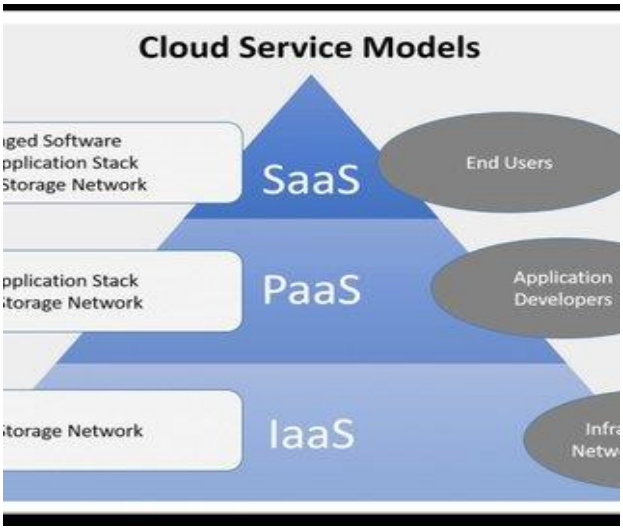
Fig(1). Cloud Computing System

II. RELATED WORK AND COMPONENTS OF CLOUDS

The National Institute of Standards and Technology (NIST) has defmed cloud computing as an Information Technology (IT) model for enabling the convenient, on-demand network access to a shared collection of configurable resources that can be put for provisioning any time and it can be released with minimal management effort or service provider interaction [2]. At a back end of the cloud system a data center and redundant network connection connect to the system, through which a person can build a cloud system with limited number of resources. Hence a system build in this way presents many real and superficial security concerns that have become some of the problems why cloud has not been adopted by many companies and organizations

The Three Layers of Cloud Computing As the delivery of IT resources or capabilities as a service is an important characteristic of Cloud Computing, the three architectural layers of Cloud Computing are (see fig. 2):

1) Infrastructure as a Service (IaaS) : IaaS offerings are computing resources such as processing or storage which can be obtained as a service. Examples are Amazon Web Services with its Elastic Compute Cloud (EC2) for processing and Simple Storage Service (S3) for storage and Joyent who provide a highly scalable on-demand infrastructure for running Web sites and rich Web applications[3]. PaaS and SaaS providers can draw upon IaaS offerings based on standardized interfaces. Instead of selling raw hardware infrastructure, IaaS providers typically offer virtualised infrastructure as a service. Foster et al. denote the level of raw hardware resources, such as compute, storage and network resources, as the fabric layer[4]. Typically by virtualization, hardware level resources are abstracted and encapsulated and can thus be exposed to upper layer and end users through a standardized interface as unified resources[4] in the form of IaaS



Fig(2)-Three layer model of cloud computing

2) Platform as a Service (PaaS): Platforms are an abstraction layer between the software applications (SaaS) and the virtualized infrastructure (IaaS). PaaS offerings are targeted at software developers. Developers can write their applications according to the specifications of a particular platform without needing to worry about the underlying hardware infrastructure (IaaS). Developers upload their application code to a platform, which then typically manages the automatic upscaling when the usage of the application grows [5]. PaaS offerings can cover all phases of software development or may be specialized around a specific area like content management [3]. Examples are the Google App Engine, which allows applications to be run on Google's infrastructure, and Salesforce's Force.com platform. The PaaS layer of a Cloud relies on the standardized interface of the IaaS layer that virtualizes the access to the available resources and it provides standardized interfaces and a development platform for the SaaS layer.

[ll]. Many cloud architectures do not bring the flamed aspects of on-demand access and self-service in cloud services paradigm [12]. The reason of this is inefficiencies in design and operations that are not up to the time domain requirements in cloud computing. Hence cloud architectures must be built with an eye on security. By addressing cloud security concerns, the same can be incorporated into the design of secure cloud architecture, by way of validating them or countering them with compensating controls.

Some of the primary concerns for cloud computing are:

Loss of physical control: there are a range of concerns related to loss of physical

Cloud provider viability: New cloud providers should be assessed for provider viability and commitment.

Network Availability: Value of cloud computing is realized only when network connectivity and bandwidth meet the minimum needs.

Disaster recovery and business continuity: Appropriate disaster recovery strategies in the event of catastrophic failures

Transparency: Build trust to cloud provider's security claims without exposing details of security policy.

3) *Software as a Service (SaaS)*: SaaS is software that is owned, delivered and managed remotely by one or more providers and that is offered in a pay-per-use manner [6]. SaaS is the most visible layer of Cloud Computing for end-users, because it is about the actual software applications that are accessed and used. From the perspective of the user, obtaining software as a service is mainly motivated by cost advantages due to the utility-based payment model, i.e. no up-front infrastructure investment. Well known examples for SaaS offerings are Salesforce.com and Google Apps such as Google Mail and Google Docs and Spreadsheets. The typical user of a SaaS offering usually has neither knowledge nor control about the underlying infrastructure [7], be it the software platform which the SaaS offering is based on (PaaS) or the actual hardware infrastructure (IaaS). However, these layers are very relevant for the SaaS provider because they are necessary and can be outsourced. For example, a SaaS application can be developed on an existing platform and run on infrastructure of a third party. Obtaining platforms as well as infrastructure as a service is attractive for SaaS providers as it can alleviate them from heavy license or infrastructure investment costs and keeps them flexible. It also allows them to focus on their core competencies. This is similar to the benefits that motivate SaaS users to obtain software as a service. According to market analysts, the growing openness of companies for SaaS and the high pressure to reduce IT costs are major drivers for a high demand and growth of SaaS.

also for Cloud Computing, in the next years. In August 2007, analyst firm Gartner forecasted an average annual growth rate of worldwide SaaS revenue for enterprise application software of 22.1% through 2011, reaching a According to market analysts, the growing openness of companies for SaaS and the high pressure to reduce IT costs are major drivers for a high demand and growth of SaaS, and by that also for Cloud Computing, in the next years. In August 2007, analyst firm Gartner forecasted an average annual growth rate of worldwide SaaS revenue for enterprise application software of 22.1% through 2011, reaching a $14.5 billion [8].

III. CLOUD COMPUTING SECURITY ISSUES

There are many issue related to privacy, security in cloud computing. The security issues are concerned in cloud computing because in cloud at any time the data can outbreak the service provider and the information is deleted deliberately. The cloud is expected to offer features such as encryption strategies to ensure a secure data storage environment, rigorous access control, secure and stable backup of user data. However, the cloud allows users to reach computing power that exceeds their physical domain. This leads to many security problems. The main security concerns are: Identification and Authentication: Multiple access to the cloud allows access to one instance of the software for more than one user [3]. This will create an identification and authentication problem because different users use different tokens and protocols, which can cause interpretation problems. Access control: illegal access to confidential data can be obtained due to moderate access control. If the appropriate security mechanisms are not used, there may be unauthorized access. Since data has been in the cloud for a long time, the risk of illegal access is greater.

Data interception: the company providing the services may violate the law. There is a risk of data interception by foreign government institutions. Encryption/ Decryption: There is an issue of the Encryption/ Decryption key that are provided. The keys must be provided by the customer itself. Policy Integration: different servers in the cloud can use different tools to ensure the security of customer data. That is why integration policy is one of the main security problems. Accessibility: accessibility is the main problem in cloud computing. During virtualization of customer data, customers have no control over physical data [3]. If the data or service is not available in the cloud, it is difficult to obtain the data. Secure Data Management: because data is an important element of cloud computing in aspects of the secure cloud. In particular, security concerns, ranging from how to effectively store data on foreign computers, to queries about encrypted data, because a large part of the data in the cloud can be encrypted, is a key challenge in the implementation of security schemes in Cloud Computing

IV CLOUD SECURITY REQUIRMENTS

After the creation of a security policy for the cloud, the security architecture of the cloud is built on these guidelines. The security policy should guide in the creation of architecture for cloud security. Based on the security requirements given below the same are applied to this cloud architecture [10]:

• Network Time Protocol helps in the correct working of systems and gives dependable system logs records by synchronizing with the same time source. Clock drifts between devices and computer in a cloud infrastructure are subject to errors that are may be difficult to diagnose.

• Identity management needed to authenticate cloud personnel, cloud tenants and users. Identity of users must be verified according to policy and legal requirements at the registration time. Historical information of the users have to be maintained so that future legal investigations when system is provisioned can be done.

Fig(3)- Cloud Security Requirement

Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cyber security threats. Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data and applications in the cloud secure from current and emerging cyber security threats.

Identity information is used by access control processes to enable and to limit the access to a cloud infrastructure. Cloud personnel should be given restricted access to customer data. Multiple authentications are required for privileged operations. Cloud audits are generated in different zones hence, security related events must be put on the records with the necessary information to analyze the event. All audit events in the record and the logs should be collected and made sure that their integrity is maintained. This should be regularly monitored in a timely manner. Critical alerts should be delivered on time. Security personnel should be enabled to investigate and prosecute by reviewing logs to identify the different security related incidents. Intrusion detection system and anomaly detection system should be installed in the entire cloud service and the same should be given as a service for all the tenants and users.

V. CONCLUSION

Cloud computing is a new emerging technology widely studied in recent years. Now there are many cloud platforms both in businesses and in academic field. How to understand and use these platforms is a big issue. In this paper, we described the definition, styles, characters of cloud computing and cloud computing services. Though each cloud computing platform has its own strength, one

thing should be noticed is that no matter what kind of platform there is lots unsolved issues. For example, continuously high availability, Performance, Data Confidentiality and Auditability, Synchronization in different clusters in cloud platform, interoperation and standardization, the security of cloud platform. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has a bright future. This paper discussed about the basic features of the cloud computing, security issues also paper identifies the concerns for cloud security and key security requirements for the cloud computing architecture. Based on security requirements and policies and architectural elements theoretical cloud architecture is proposed in the paper

REFERENCES

[1] Vic Winkler, "Securing the Cloud: Cloud Computer security techniques and tactics," 2011, Syngress, 89-123.

[2] Hongwei Li Rongxing Lu Jelena Misic Mohamed Mahmoud Security and privacy of connected vehicular cloud computing-IEEE Network/May/June 2018

[3] Amazon Web Services. http://findarticles.com/p/articles/mi_ mOETN/is _ 2002 _J uly _16/ai_ 890757 79/ . [accessed 11.11.2012]

[4] Mell P. Grance T. The NIST Definition of Cloud Computing version 15; 2009, National Institutes of Standards and Technology, Information Technology Laboratory.

[5] Brunette G, Mogull R., "Security Guidance for Critical Areas of focus in cloud computing ", Cloud Security Alliance, Version 3, p. 35, 2011.

[6] Catteddu, D., Hogben, G., "Cloud Computing Benefits, Risks and Recommendations for Information Security", European Network and Information Security Agency (ENISA), www.enisa.europa.eu/; 2009.

[7] NlST Special Publication 800-53 Revision 3, "Recommended

[8]Miller M (2008) Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online. Que Publishing, Indianapolis

[9] Reese G (2009) Cloud Application Architectures. O'Reilly Media, Sebastopol, CA

[10] Sun (2009a) A Guide to Getting Started with Cloud Computing Sun white paper. https://www.sun.com/offers/docs/cloud_computing _primer.pdf. Accessed: 10 June 2009

[11] Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud Computing and Grid Computing 360-Degree Compared
.
[12] Eymann T (2008) Cloud computing. Enzyklopädie der Wirtschaftsinformatik. Accessed: 10 June 2009