IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 52-56

Overview of Cloud Architecture and Issues of Cloud Computing

Nandini.N, Dhanushya.T, Mrs.W.RoseVaruna
Department of Information Technology Bharathiar University
Assistant Professor Department of Information Technology Bharathiar University

Abstract: *Cloud computing is architecture for providing computing services through the internet on demand and pay-per-use access to a pool of shared resources namely networks, storage, servers and applications without physically acquiring them. So it saves managing cost and time for organizations. Developing an application in the cloud enables users to get their product to market quickly. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, storage space occupied etc. Cloud computing architecture comprises of many cloud components, which are loosely coupled. Cloud computing infrastructure is a collection of hardware and software elements needed to enable cloud computing. Cloud platform is the hardware and operating environment of a server in an internet-based datacenter. Security is generally perceived as huge issues for the cloud. Most of the cloud venders instead of acquiring a server, try to lease a server from other service providers because they are cost effective and flexible for operation. The customer does not know about those things, there is a high possibility that the data can be stolen from the external server by a malicious user.*

Keywords: *Cloud architecture, components and issues*

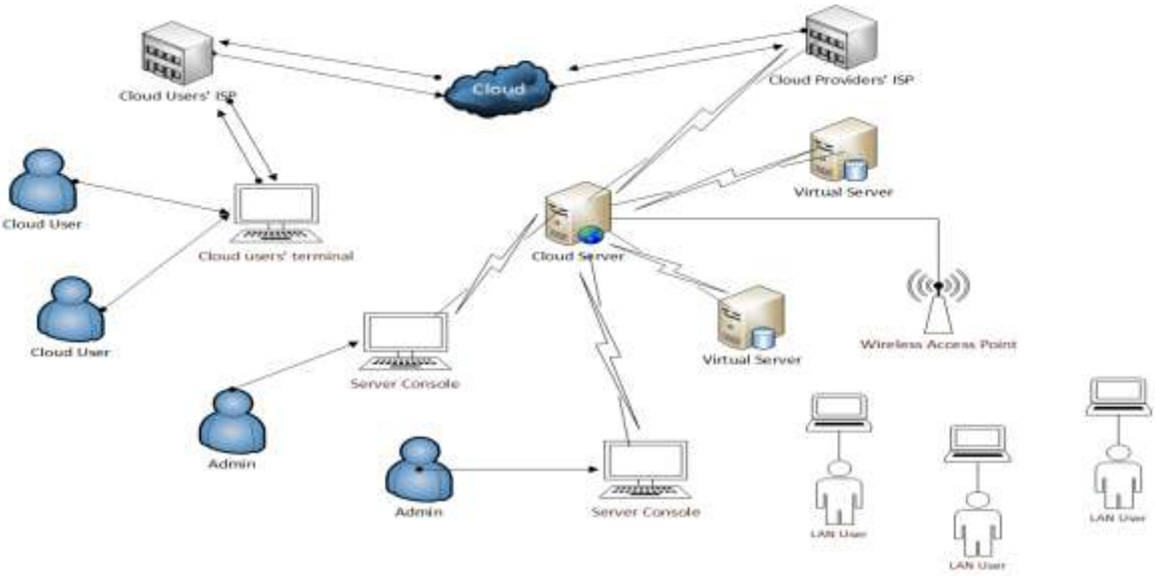
I. INTRODUCTION

Recent developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.
- All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one.

II. CLOUD COMPUTING INFRASTRUCTURE

The term cloud computing is rather a concept which is a generalized meaning evolved from distributed and grid computing. The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done by using someone else's network where ownership of hardware and soft resources are of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially in the form of distributed computing; though this is not apparent or by its definition of cloud computing, do not essentially have to be apparent to the users. In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing.



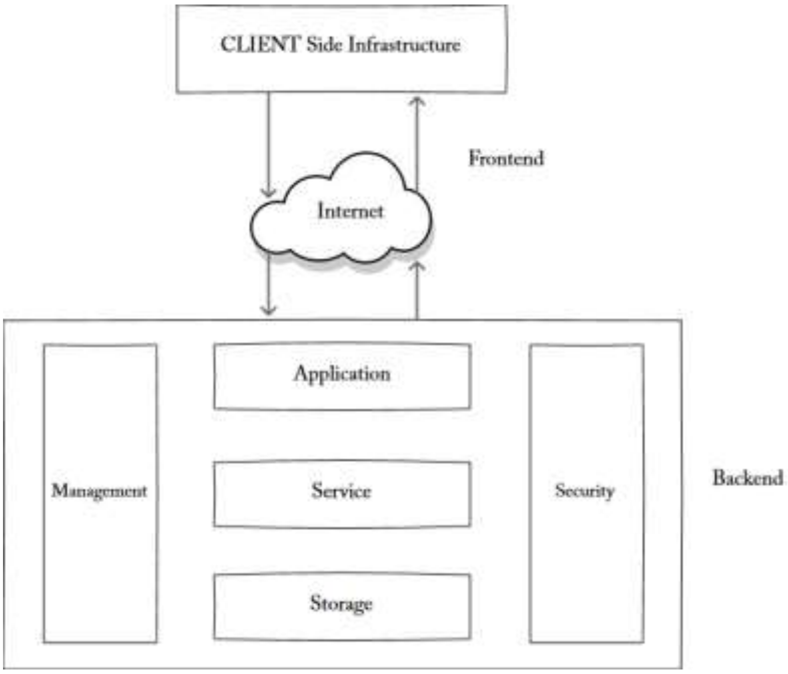
"Fig.1"

III. CLOUD ARCHITECTURE

Cloud computing architecture is divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services.

In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines.

If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of storage space. Some companies require hundreds of digital storage devices. Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients' information stored. That's because these devices, like all computers, occasionally break down. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy.



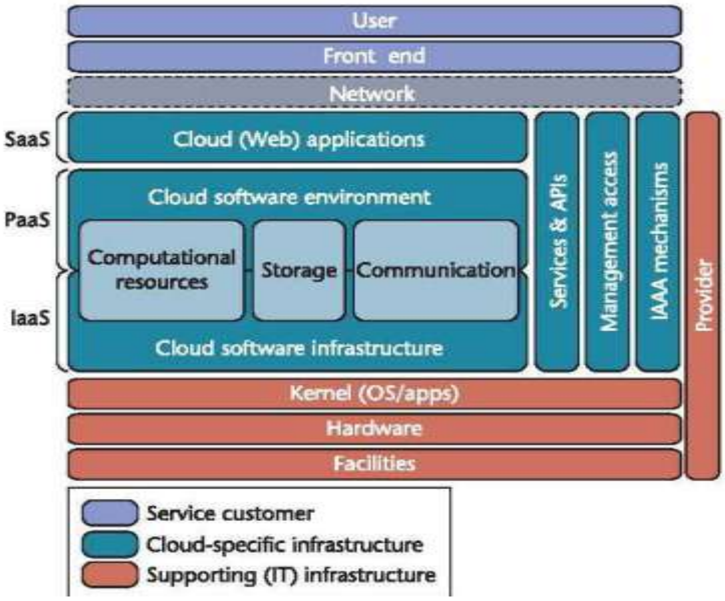
"Fig.2"

IV. ARCHITECTURAL COMPONENTS

Cloud service models are commonly divided into SaaS, PaaS, and IaaS that exhibited by a given cloud infrastructure. It's helpful to add more structure to the service model stacks. Fig.3 shows a cloud reference architecture that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

A. Software as a Service (SaaS)

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various clients (e.g. Web browser, PDA, etc.) by application users. Cloud consumers do not have control over the cloud infrastructure that often employs multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance. Examples of SaaS include SalesForce.com, Google Mail, Google Docs, and so forth.



"Fig.3"

B. Platform as a Service (PaaS)

PaaS is a development platform supporting the full “Software Lifecycle” which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Hence, the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts both completed and in-progress cloud applications. This requires PaaS, in addition to supporting application hosting environment, to possess development infrastructure including programming environment, tools, configuration management, and so forth. An example of PaaS is Google AppEngine.

C. Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2.

V. ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud; concerns are beginning to grow about just how safe an environment it is? Issues of cloud computing can summarize as follows:

A. Privacy

Cloud computing utilizes the virtual computing technology, users’ personal data may be scattered in various virtual data centers rather than stay in the same physical location, users may leak hidden information when they are accessed cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

B. Reliability

The cloud servers also experience downtimes and slowdowns as our local server.

C. Legal Issues

Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

D. Compliance

Numerous regulations pertain to the storage and use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

E. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

F. Long- Term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company.

VI. CONCLUSION

One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed infrastructure, architecture and security issues in cloud computing. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture.

REFERENCES

Books:

[1]. T. Dillon, C. Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 27-33, DOI= 20-23 April 2010.

Proceedings Papers:

[2]. http://www.ijfcc.org/papers/95-F0048.pdf

[3]. http://www.worldscientificnews.com/wp-content/uploads/2017/08/WSN-863-2017-253-264-1.pdf

[4]. https://pdfs.semanticscholar.org/ca5d/86b602c4fe2625ca80ac4da6704c18f6a279.pdf