Industrial Science
ISSN : 2347-5420
Volume-1 | Issue-7 | Oct-2014

A SURVEY TO PROVIDE DATA SECURITY IN CLOUD COMPUTING

Archana Wagh[1] and Sunny Bagga[2]

[1] MTECH Scholar, Computer Science Department, SIA, Indore, India,
[2]Asst. Professor, Computer Science Department, SIA, Indore, India,

Abstract:-Cloud computing takes advantage of virtualization technologies with self-service capabilities to offer cost-effective access to computing resources via the internet. This paper identifies the security and integrity concerns involved in cloud computing when data moves from one location to another. Security is one of the most difficult job to execute in cloud computing. Different types of attacks occur in the application and in the hardware components. To provide security different cryptographic algorithms are been used. The main aim of this paper is to collect information (survey) on secure environment for storage of data in cloud.

Keywords:cloud computing,Saas,Paas,Laas, Private cloud, Public Cloud,Hybrid Cloud,Community Cloud.

INTRODUCTION

A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers. Cloud computing is a model that enables suitable, on-demand network access to a common pool of configurable computing assets such as networks, servers, storage, applications that can be quickly provisioned and free with least management attempt or service provider's communication[1]. In common cloud providers propose three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

1.1 Cloud Computing Environment

•Features
•It makes use of internet-based services to maintain business procedure
•It lease IT-services on a utility-like basis

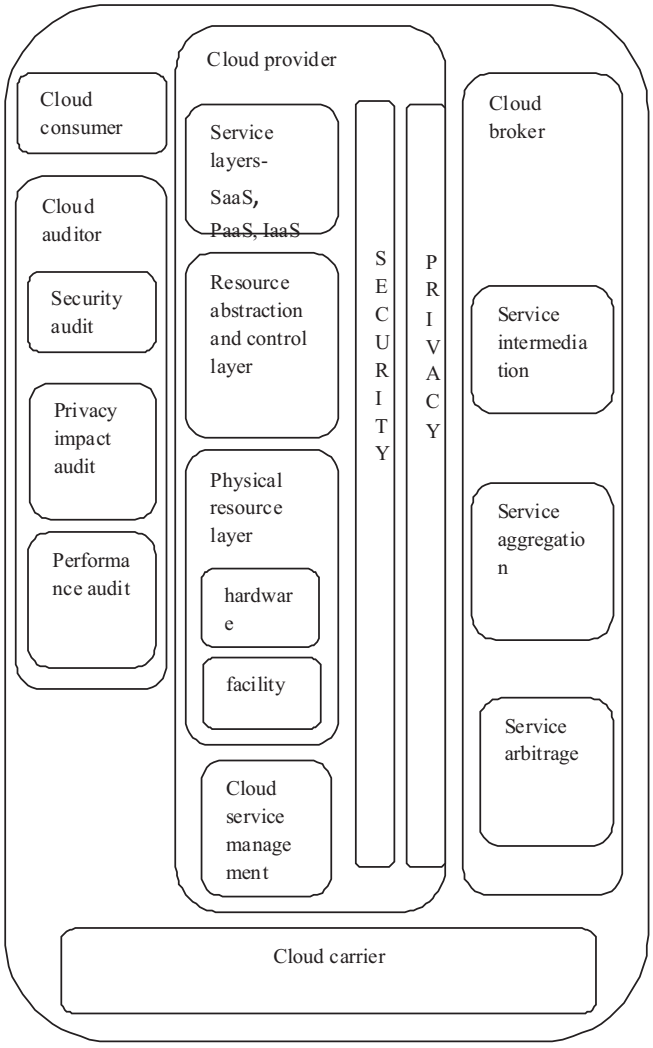

Fig- 1: Cloud Computing Environment

•Attributes
–Deployment is very rapid.
–Startup costs is very low with very less capital investments
–The overall cost is based on usage or subscription
–Multi-tenant sharing of services and resources is done.

•Essential characteristics
–It provides on demand self-service
–omnipresent network access
–Resource pooling is independent of location.
–Rapid elasticity
–Measured service

"Cloud computing is a collection of accessible techniques and technologies, packaged

inside a new infrastructure paradigm that provides enhanced scalability, elasticity, business alertness, quicker startup time, compact management costs, and just-in-time accessibility of resources" [2].

Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software. From one perception, cloud computing is not anything new because it uses approaches, concepts, and top practices that have previously been well-known. From another point of view, everything is original because cloud computing changes how we create, build up, set up, level, update, sustain, and pay for applications and the infrastructure on which they run. It is a technology that uses the internet and remote servers to manage and retain data and applications. It allows businesses and consumers to make use of applications without installation and right to use their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing memory, storage, bandwidth and processing [10].

1.2 Advantages of Cloud Computing

•It is less expensive as compared to buying a software or a hardware
•It can be used from any location with the computer or device , just we need is an Internet connection
•It does not require a large internal storage system.
•It is compatible with many computers and operating systems
•Its updates happen across the service

1.3 Disadvantages of Cloud Computing

•Security Issues
•Terms of Service
•Privacy Policies

Cloud computing represents significant opportunity for service providers and enterprises. Offering flexibility and choice, mobility and scalability, all coupled with potential cost saving. However, the area is causing organizations to hesitate most when it comes to moving business workloads into public cloud is security [3].

2. LITERATURE SURVEY

2.1 Related Work

Cong Wang et al in the paper propose that publicly auditable cloud data storage is able to help this nascent cloud economy. With expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data. This provides a transparent yet cost-effective method for data owners to gain trust in the cloud. They describe approaches and system requirements that should be brought into concern, and summarize challenges that need to be determined for such a publicly auditable secure cloud storage service to become a reality. [4]

John Harauz et al in 2009 printed a writing in step with their article, within the Nineties, the globe was introduced to the net, and that we began to ascertain distributed computing's power complete on an outsized scale. Today, we've got the flexibility to utilize ascendible, distributed computing environments inside the confines of the net, referred to as cloud computing. This setting strives to be dynamic, reliable, and customizable with a secured quality of service. inside this technique, user shave a myriad of virtual resources for his or her computing desires, and that they don't want an entire understanding of the infrastructure. [5]

Balachandra et al in 2009 provides an study about the security in cloud environment, according the given architecture, the world of computation has changed from centralized (client-server not web-based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing). In cloud computing the examination and data maintenance is done by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. When we look at the security of data, the cloud vendor has to provide some assertion in service level agreements (SLA) to convince the customer on security issues. [6]

KawserWazedNafietal have planned new security design for cloud.AES primarily based

file encoding system and asynchronous key system for exchanging data or knowledge is enclosed during this model. This structure is simply applied with main cloud computing options: e.g. PaaS, IaaS and SaaS. These models additionally embody generally positive identification system for user authentication method. The given work primarily deals with the protection system of the full cloud computing platform [7].

Cloud computing has been considered as one of the promising solutions to our increasing demand for accessing and using resources provisioned over the web. It offers powerful process and storage resources as on-demand services with reduce scale back price, and increase potency and performance. The target of this survey is to explore potential security issues related to securing cloud computing for critical infrastructure suppliers. It highlights security challenges in cloud computing and investigates the security requirements for various critical infrastructure providers. [8]

Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PC to giant information centers. It refers to applications delivered as services over the Internet as well as to the actual cloud infrastructure—namely, the hardware and program in information centers that give these services. In this paper Madhu Chauhan et al presents different aspects of security issues related with cloud computing, and its possible solution. [9]

Cloud computing, an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.[10].

"Cloud" computing – a relatively recent term, builds on decades of research in distributed computing, virtualization, utility computing web, networking and software services. It gives service oriented architecture with reduced overhead for the end-user, provide on demand services and reduced the total cost of ownership. This paper emphasize on some of the issues of "cloud" computing which tries to address, related research topics, and a "cloud" implementation available today[11].

Cloud computing is current buzzword in the market. It is paradigm in which the resources can be leveraged on per use basis thus reducing the cost and complexity. It reduces the total expenditure let IT departments focus on strategic projects. It is a construct that allows user to access applications that actually reside at location other than user's own computer or other Internet-connected devices. There are numerous benefits of it. This implies that they handle cost of servers, they manage software updates and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, privacy and authenticity [12].

Cloud computing is a promising technology to facilitate development of large-scale, on-demand, flexible computing infrastructures. But without security embedded into innovative technology that supports cloud computing, businesses are setting themselves up for a fall. The trend of frequently adopting this technology by the organizations automatically introduced new risk on top of existing risk. Obviously putting everything into a single box i.e. into the cloud will only make it easier for hacker. This paper presents an overview and the study of the cloud computing. Also include the several security and challenging issues, emerging application and the future trends of cloud computing.[12]

3. DIFFERENT MODELS OF CLOUD COMPUTING

Generally cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

3.1 Software-as-a-Service (SaaS): SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. Thus customer does not require the installation and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support . SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure which is essential to run and control the solution. It features an application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

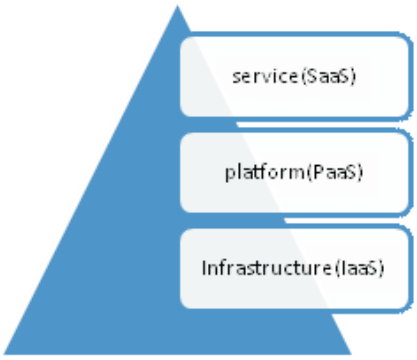

Fig- 2: Cloud Computing Models

3.2 Platform as a Service (PaaS):

"PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for end-users, developers or IT managers. To implement and test cloud applications, it provides an infrastructure with a high level of integration. The user controls the applications deployed and their configuration but does not manage the infrastructure which includes the servers, network, operating systems and storage. Examples of PaaS includes: Google App Engine, Force.com and Microsoft Azure.

3.3 Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) uses the virtualization technology for the sharing of hardware resources for executing services. Its main purpose is to make servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the storage, operating systems and deployed applications. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

4. CLOUD DEPLOYMENT MODELS

There are also four different cloud deployment models. Details about the models are given below.

4.1 Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on- premises or off-premises. It is more expensive and secure as compared to public cloud. In this cloud there is no need of legal requirements, additional security regulations or

bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized power of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems [13].

4.2 Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of management, installation, provisioning and maintenance. Customers pay the charges for the resources they use, so under-utilization is eliminated. Since consumers have little control over the processes requiring powerful security, infrastructure and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine.

4.3 Hybrid Cloud: A hybrid cloud comprised of two or more different cloud models which are connected in such a way that information transfers takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the cloud provider and the enterprise. A company can sketch out the goals and needs of services [14]. A well-constructed hybrid cloud can be useful for providing secure services such as employee payroll processing for receiving customer payments, as well as those that are secondary to the business,. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. The services from different vendors can be acquired in such as if they were originated from a single location, and interactions between public and private components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

4.4 Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook which is showing in figure 1.

5. CONCLUSION

Nowadays cloud computing has become a potential weapon in day to day life. It provides software services, computational ability, data storage and other important applications distantly. Several different cryptographic algorithms are used for providing the security. The major drawback for using the given algorithm is it consumes a large amount of time for execution. The proposed work provide security for storage of data with client server mutual authentication scheme. This is an efficient and effective technique which is required for data preservation.

6. REFERENCES

1.Rabi Prasad Padhy,ManasRanjanPatra,Suresh Chandra Satapathy, “Cloud Computing: Security Issues and Research Challenges”,IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS),Vol. 1, No. 2, December 2011.
2.https://www.cs.purdue.edu/homes/bb/cloud/cloud-complete.ppt
3.Amar Gondaliya,” Security in Cloud Computing”, Cloud 20/20 Version 3.0, Unisys Confidential contest Technical Paper Contest 2011
4.Cong Wang and KuiRen, Wenjing Lou ,JinLi, Toward Publicly Auditable Secure Cloud Data Storage Services, IEEE Network • July/August 2010,0890-8044/10/$25.00 © 2010 IEEE

5.John Harauz, Lori M. Kaufman, Bruce Potter, Data Security in the World of Cloud Computing, JULY/AUGUST 2009■ 15407993/09/$26.00 © 2009 IEEE■ COPUBLISHED BYTHEIEEE COMPUTERANDRELIABILITYSOCIETIES
6.Balachandra Reddy Kandukuri, Ramakrishna PaturiV, Dr.AtanuRakshit, Cloud Security Issues,2009 IEEE International Conference on Services Computing, 978-0-7695-3811-2/09 $26.00 © 2009 IEEE, DOI 10.1109/SCC.2009.84, 517, 2
7.KawserWazedNafi, TonnyShekhaKar, SayedAnisulHoque, 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
8.YounisA.Younis,MadjidMerabtiandKashifKifayat, Secure Cloud Computing for Critical Infrastructure :A Survey, ISBN: 978-1-902560-27-4 © 2013 PGNet
9.MAdhu Chauhan, Riidhei Malhotra, MukulPathakandUdayPratap Singh, DIFFERENT ASPECTS OF CLOUD SECURITY, Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com, Vol. 2, Issue 2, Mar-Apr 2012, pp.864-869
10.Pankaj Arora,Rubal Chaudhry Wadhawan,Er. Satinder Pal Ahuja,"Cloud Computing Security Issues in Infrastructure as a Service",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 1, January 2012.
11.Mladen A. Vouk," Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246.
12.Rajesh Piplode,Umesh Kumar Singh, "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 2, Issue 9, September 2012.
13.B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.
14.Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

Archana Wagh
MTECH Scholar, Computer Science Department, SIA, Indore, India,