Protect Confidential Information in PPH Cloud Environments by Using End-End Access in Secure Way

M. Rama Raju

Asst. Professor, Department of Computer Science & Engineering, ChristuJyoti Institute of Technology & Science, Jangaon, Warangal, A. P. India.

Abstract— In Cloud computing PPH private public and hybrid respectively the cloud environments are available in now a days. Cloud computing has many benefits and security challenges in various cloud environments. But regarding some business-critical applications, the organizations, especially large enterprises, still may not move them to cloud. The market size of the cloud computing shared is still far behind the one's expectation. From the consumer's perspective, cloud computing security concerns, especially protecting critical information in various cloud environment issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides the benefits and security challenges in various cloud environment and techniques and solution for various issues of security challenges of various cloud environments. Finally, this paper describes future research work about protecting critical information in cloud by using all these techniques to overcome time process by using utilities in cloud computing by the reduce cost by performing better way.

Keywords: Cloud Computing, Security, and End – End access.

I. Introduction

Cloud computing introduced new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, like different service and deployment models, and can coexist with other technologies and software design approaches. The global cloud computing market is grow from a $40.7 billion in 2011 to $241 billion in 2020, according to Forrester Research.

On the way to all of the growth are a few notable reports.

- For starters, the infrastructure as a service market will peak a $5.9 billion in global revenue in 2014 and then commoditization, price pressure and falling margins.
- Business Process as a service will be notable, but face modest revenue.
- Virtualization will recede to the background as new technologies take over.

To determine whether the increased risks of truly worth the agility and economic benefits. Maintaining control over the critical information is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where the sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity.

As we shown in figure 1. This shift in control is the number one reason new approaches and techniques are required to ensure organizations can maintain data security. When an outside party owns, controls, and manages infrastructure and computational resources, how can you be assured that business or regulatory data remains private and secure, and that your organization is protected from damaging data breaches—

and feel you can still completely satisfy the full range of reporting, compliance, and regulatory requirements?

In this paper we describe the following:

- The benefits of cloud computing
- Cloud Computing Security Challenges
- Techniques for Protecting Data in the Cloud
- Cloud Security Solutions

The Benefits of Cloud Computing

In recent years, cloud computing has emerged as an important solution offering enterprises a potentially cost for effective model to ease their computing needs and accomplish business requirements. Considering:

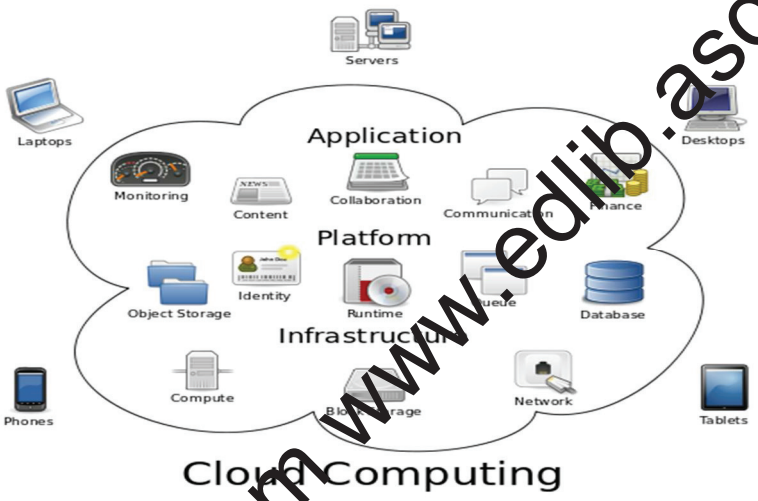

Figure 1 Cloud Environments

As shown in Figure 1

a) **Optimized server utilization** – In most of enterprises typically underutilize their server computing resources, cloud computing will manage the server utilization to an optimum level.
b) **Cost saving** – IT infrastructure costs are almost always minimal and are treated as a capital expense (CAPEX). However if the IT infrastructure usually becomes an operating expense (OPEX). In some countries, this results in a tax advantage regarding income taxes. Also, cloud computing cost saving can be realized via resource pooling.
c) **Dynamic scalability** - many enterprises include a reasonably large buffer from their average computing requirement, just to ensure that capacity in a place to satisfy peak demand. Cloud computing provides an extra processing buffer as needed when a low cost and without the capital investment or contingency fees to the users.

II. Security Reasons in Cloud Area

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic to manage the cloud infrastructure, but are often uneasy about granting them visibility into sensitive data, to use the cloud due to cost savings and new agile business models. But when it comes to cloud security, it's important to understand the various threat landscape that comes into play. There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data

Such issues give rise to tremendous anxiety about security risks in the cloud. Enterprises worry whether they can trust their employees or need to implement additional internal controls in the private cloud, and whether third-party providers can provide adequate protection in multitenant environments that may also store competitor data.

Specific security challenges pertain to each of the three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Techniques for Protecting Data in the Cloud

In Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks.

It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility. An effective cloud security solution should incorporate three key capabilities:

- Data lockdown
- Access policies
- Security intelligence

First, make sure that data is not readable and that the solution offers strong key management. Second, implement access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root users cannot view sensitive information. Third, incorporate security intelligence that generates log information, which can be used for behavioral analysis to provide alerts that trigger when users are performing actions outside of the norm.

Cloud Security Solutions

Secure access to cloud resources with intelligent authentication tokens—

Ensuring that only authorized users gain access to cloud-based resources is critical for cloud providers and enterprises. Providers need to ensure proper access controls for users at client sites, and for administrators within the service provider's organization.

Secure cryptographic key storage—

Any cryptographic system and trust in the protected data is only as strong as the underlying protection of the keys used to encrypt data. A centralized, hardened security appliance manages cryptographic keys, access control, and other security policies. In addition, a virtualized instance of this appliance is deployed in the cloud to replicate policies and security enforcement on the data.

Secure storage in the cloud across file, application, and database systems—

Driven by a need to use the cloud's elastic storage, enterprises can securely store data in the cloud, effectively using the cloud for the backup, disaster recovery, and archival of data. Protection of stored data

through a hardened appliance that centralizes encryption processing, keys, logging, auditing, and policy administration across file, application, and database systems.

III. Implemented Methodologies in Infrastructure within Public and Hybrid Clouds-

Clouds are a target rich environment for cyber-attacks on the interconnected critical fabric that weaves together the elastic computing, storage and connectivity in the back-end of the cloud data centers.it provides strong Layer 3 and Layer 2 link encryption solutions to harden this critical network infrastructure while maintaining low-latency -- high throughput data exchanges to keep the cloud operating at peak efficiency. Together, these solutions deliver the critical capabilities required for a robust, cost-effective and secure cloud security implementation.

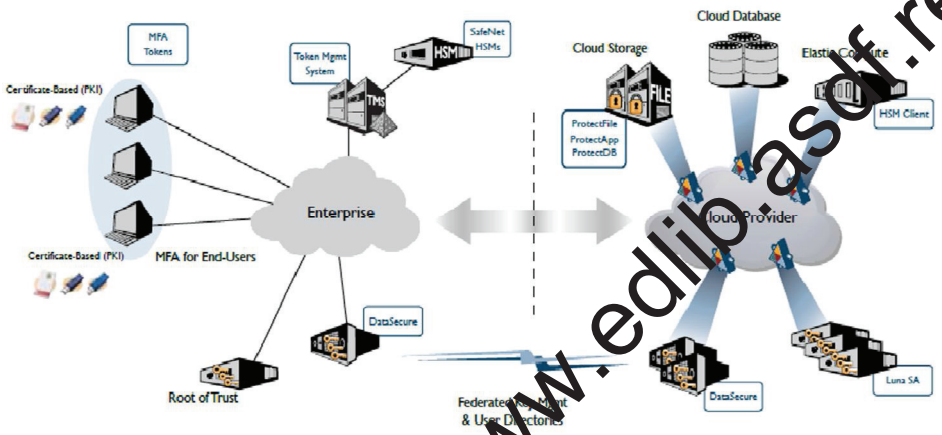

Figure 3. Cloud data providers interaction

SaaS Architectural Maturity Level 4-Scalable: At this fourth SaaS maturity level, scalability is added by using a multitier architecture. This architecture is capable of supporting a load-balanced farm of identical application instances running on a variable number of servers, sometimes in the hundreds or even thousands. System capacity can be dynamically increased or decreased to match load demand by adding or removing servers, with no need for further alteration of application software architecture.

1. Coming to the Key Characteristics of SaaS

a. A Network-based management and access to commercially available software from central locations rather than at each end use customer's site, enabling end user customers to access applications remotely via the Internet.
b. Application delivery from a one-to-many model (single-instance, multitenant architecture), as opposed to a traditional one-to-one model. Centralized enhancement and patch updating that obviates any need for downloading and installing by a user. SaaS is often used in conjunction with a larger network of communications and collaboration software, sometimes as a plug-in to a PaaS architecture.

2. Coming to the Benefits of the SaaS Model

Application deployment cycles inside companies can take years, consume massive resources, and yield unsatisfactory results

i. Streamlined administration
ii. Automated update and patch management services

iii. Data compatibility across the enterprise (all users have the same version of software)
iv. Facilitated, enterprise-wide collaboration
v. Global accessibility

As we have pointed out previously, server virtualization can be used in SaaS architectures, either in place of or in addition to multi tenancy. A major benefit of platform virtualization is that it can increase a system's capacity without any need for additional programming. Conversely, a huge amount of programming may be required in order to construct more efficient, multitenant applications. The effect of combining multi tenancy and platform virtualization into a SaaS solution provides greater flexibility and performance to the end user.

b).End use access in Location of Encryption Devices only

With end-to-end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The data, in encrypted form, are then transmitted unaltered across the network to the destination terminal or host. The destination shares a key with the source and so is able to decrypt the data. This approach would seem to secure the transmission against attacks on the network links or switches. There is, however, still a weak spot.

Thus, with end-to-end encryption, the user data are secure. However, the traffic pattern is not, because packet headers are transmitted in the clear. To achieve greater security, both link and end-to-end encryption are needed, as is shown in

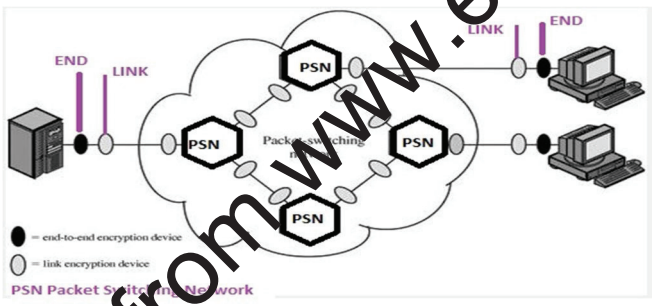

Figure 4 Encryption across a Packet-Switching Network

To summarize, when both forms are employed, the host encrypts the user data portion of a packet using an end-to-end encryption key. The entire packet is then encrypted using a link encryption key. As the packet traverses the network, each switch decrypts the packet using a link encryption key to read the header and then encrypts the entire packet again for sending it out on the next link. Now the entire packet is secure except for the time that the packet is actually in the memory of a packet switch, at which time the packet header is in the clear.

VI. Result

Using all the mentioned techniques in cloud the data is protected by using the end to end connection establishment with encryption and decryption. Validation does not identify the server to the end user. For true identification, the end user must verify the identification information contained in the server's certificate (and, indeed, its whole issuing CA chain). This is the only way for the end user to know the "identity" of the server, and this is the only way identity can be securely established, verifying that the URL, name, or address that is being used is specified in the server's certificate. More important, an understanding of why they have evolved. Standards are important, to be sure, but most of these standards evolved from individuals taking a chance on a new innovation in end user access in best way.

V. Conclusion

By Using all these techniques cloud will provide more securities services for various areas to utilize various contributions from cloud. This paper provided an overview of end-user access to cloud computing. We first talked about key trends we believe will drive collaboration further into the cloud environment. We chose five significant entities to present you with an overview of the types and levels of capability available in the cloud today-things you can use now. YouTube, an online video repository, has an amazing hold on the global audience. Collaboration suites such as Zoho both enhance mobility and allow you to maintain a virtual office in the cloud. Social networking with Facebook has become very popular, especially in academic settings. Zoho is a SaaS vendor to watch. Backed by Google, Zoho offers something for everyone.

Finally by using the Cloud Computing we can Increase the Processing capabilities can be used in a secure manner whenever we using the more effective algorithms. Than End user access quickly. In Cloud Computing SaaS can be utilize more effective manner in various sections as categories.By Using the Cloud Computing We can Smoothly using the algorithms in less burden. By Using Default IP Address to avoid unauthorized whenever IP Spoofing occurs. By Repairing those IP Address it consumes more time so avoid so those thing we can immediately use the next IP Address.

IV. Future work:

For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order to ensure no un-authorized access to organizations' cloud resources by some employees who has left the organizations.Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed.

VII. Acknowledgements

I thank my students who have implemented the extension part of this paper under my guidance Also, I would like to thank the management (Rev. Fr. Y. Papi Reddy, the director), Principal (Dr.J.B.V.Subrahmanyam) for providing this opportunity and for their constant encouragement and also to HOD A. Poorna chander reddy who motivate and suggest few concepts towards publishing the paper. I also thank CSE Staff M. Vijay Kumar and T. Prakash helping to designing the Pictures and hardware for technical support in this paper.

VIII. References

1. Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
2. M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online].Available:http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitter-documents/
3. D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [On-line]. Available: http://venturebeat.com/2010/03/24/french-hacker-who-leaked-twitter-documents-to-techcrunch-is-busted/
4. D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online].Available:http://www.zdnet.com/blog/security/french-hacker-gains-access-to-twitters-admin-panel/3292

5. P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010.[Online].Available:http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html
6. F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual ComputingEnvironments, Hong Kong, ser. DCDV '11, June 2011.
7. M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–8. [Online].Available:http://dl.acm.org/citation.cfm?id=1924931.1924934
8. *Fog Computing:* Mitigating Insider Data Theft Attacks in the Cloud. [Online].Available:http://ids.cs.columbia.edu/sites/default/files/Fog_Computing_Position_Paper_WRIT_2012.pdf
9. J. Pepitone, "Dropbox's password nightmare highlights cloud risks," June 2011.
10. ArunBiradar, Dr.RavindraC.Thool, Dr.RajappaVelur, "Voice transmission over Local Area Networkusing Bluetooth" IEEE Journal, 2009
11. James Keogh, the Complete Reference J2ME. Tata McGraw Hill Edition 2003
12. HerbertSchildt, Java2: The Complete Reference. Tata McGraw Hill , 7th edition