International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.2, June 2012, pp. 53~58
ISSN: 2089-3337

World of Cloud Computing & Security

Ashish Kumar
Departement of Computer Science & Engineering, Bharatividyapeeth college of Engineering

Article Info

Article history:

Received Apr 27th, 2012
Revised May 10th, 2012
Accepted June 3th, 2012

Keyword:

Cloud computing
Security
Identity based Encryption

ABSTRACT

Cloud computing promises to increase the velocity with which application are deployed, increase innovation and lower costs, all while increasing business agility and hence envisioned as the next generation architecture of IT Enterprise. Nature of cloud computing builds an established trend for driving cost out of the delivery of services while increasing the speed and agility with which services are deployed. Cloud Computing incorporates virtualization, on demand deployment, Internet delivery of services and open source software .From another perspective, everything is new because cloud computing changes how we invent, develop, deploy, scale, update, maintain and pay for application and the infrastructure on which they run. Because of these benefits of Cloud Computing, it requires an effective and flexible dynamic security scheme to ensure the correctness of users' data in the cloud. Quality of service is an important aspect and hence, extensive cloud data security and performance is required.

Corresponding Author:

Ashish Kumar
Departement of Computer Science & Engineering,
Bharatividyapeeth college of Engineering,
A-4 Paschim vihar, Delhi-110063, India.
Email: ashish.kumar@bharatividyapeeth.edu

1. INTRODUCTION

The emerging Cloud computing field offers so many advantages to the web connected devices. To handle the massive amount of data present in cloud and the popularity that gains cloud computing over the past few years, security becomes a major concern for all who are using it and also those who want to utilize it but would not able to do so because no one can assure them in terms of security of their data on the cloud. A layered framework is required to secure the data in cloud. The storage security and the data security is must to store, manage, share, analyze and utilize the substantial amount of data. Data residing on the cloud should be secure, authenticated and encrypted so that three level securities can be provided. Cloud computing has eminent IT [1] to newer altitude by offering the market environment data storage and capacity with flexible scalable computing processing power to match the demand and supply, diminishing down the cost capital within the secure environment. The cloud system should (a) support the efficient and encrypted storage of sensitive data (b) supervise, query and save the enormous amount of data (c) support strong reliability and authentication (d) sturdily maintain integrity and confidentiality of the secret data. There are many cloud computing systems in the real world which are not suffered from security and privacy problems but based on the analysis we find that cloud systems do have security problems because the concerns provided by the companies are inadequate and accordingly causes a big barrier for the users to acclimatize themselves to the world of cloud computing. Whenever the matter of cloud computing comes up there are two facts that seem to govern the conversation. The first is that enterprises and small business would desperately like to make greater use of the explosion in new cloud services and offerings. Concerns over the security of information in cloud infrastructures, especially public cloud infrastructures, continues to stifle adoption of cloud services

and restraints many organizations to traditional approaches to providing business IT services. Fundamentally, the concerns over cloud security fall into various category: concerns over security, privacy, availability, confidentiality and integrity. And it's not hard to see why businesses are afraid to plunge into the cloud. Moreover, many security and privacy incidents are also observed in today's Cloud Computing systems. A few latest cloud security concerns are listed as:

- In March 2011 a prolonged period of interruption to Amazon's Elastic Block Storage (part of the AWS offering) caused a large number of websites to go suddenly, and painfully, dark.
- In June 2011, cloud storage provider Dropbox suffered from an administrative error. For a period of four hours *everything* was available. Access to Dropbox storage accounts suddenly and unfortunately, no longer required the correct password.
- Google Docs found a flaw that inadvertently shares users' docs in March 2009 [2].
- Epic.com lodged a formal complaint to the FTC against Google for its privacy practices in March 2009. EPIC was successful in an action against Microsoft Passport.

2. CLOUD COMPUTING DEPLOYMENT

Making better use of existing storage and controlling growth various cloud computing models are deployed. In providing a secure Cloud computing solution, a major decision is to decide on the type of cloud to be implemented. There are four cloud deployment models are offered, specifically, a public, private, hybrid and virtual private cloud. Depending on the usage, metering and accounting, the organizations can have an agreement with the cloud providers to consume their cloud facilities for private or personal user. Each model includes slightly different parameters and features which may fascinate to some but not to others. Cloud providers are the entities or the companies which are specialized in providing the cloud capabilities to the user with their security implications on the cloud. Cloud computing is classified based on the location of the cloud and type of services a cloud offers.

2.1 Public cloud

Cloud infrastructure is hosted at vendor's premises. Public cloud is that model of cloud which allows the user to access the cloud facilities using the interim layer as web browser. Thus, all the services and infrastructure of cloud provider is available through internet. It also reduces the capital expenses as the cost is distributed and shared across a very large group of individuals and businesses.

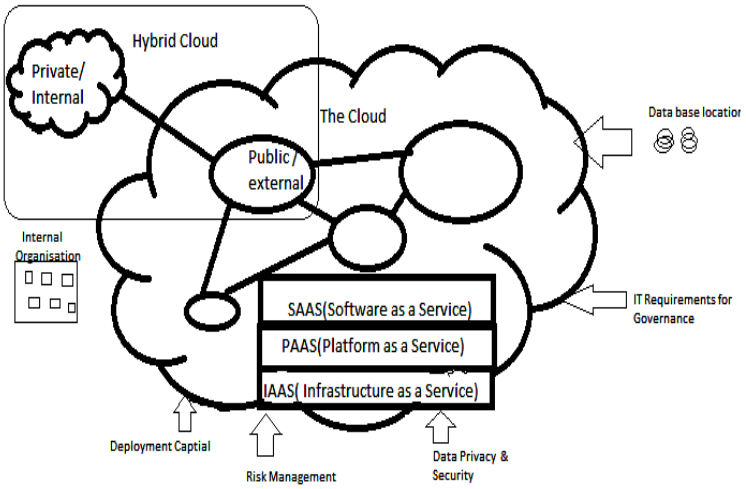

Figure 1. Cloud Deployment Architecture

2.2 Private cloud

Private Cloud is that model whose infrastructure is dedicated to a particular organization and is setup within an organization's internal datacenter. Private clouds are of two types: On-premise private clouds and

externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise [3] private clouds. The private cloud is ideal in situations when a company has a unique product or service that needs to be kept under strict control. In situations when there is a frequent need to fiddle with the infrastructure, a private cloud is the best choice.

A Virtual Private Cloud (VPC) is a private cloud existing within a shared or public cloud (i.e. the Intercloud). Amazon Web Services launched Amazon Virtual Private Cloud on 2009-08-26, which allows the Amazon Elastic Compute Cloud service to be connected to legacy infrastructure over an IPsec virtual private network connection [4].

The various clouds are also classified based on the architecture they are using and they are given as follows:

Table1: Description of Clouds Layers/Platforms

Service based Architecture	**Advantages**	**Features**	**Examples(Service Providers)**
Software as a service (SaaS)	Offers Application as a service on Internet	Easy to collaborate or access data, Pay per use.	Google Apps ,Microsoft 365, Salesforce.com, Rackspace
Platform as a Service(PaaS)	Used by developers for developing new applications.	Allow for launching new application, requires minimal expenses	Google App Engine, Microsoft Azure, SalesForce.com
Infrastructure as a Sevice(IaaS)	Providers Provide the features on demand Utility.	Small portion of cloud is provided free.	Amazon Elastic Compute Cloud, Rackspace, Terremark(owned by Verizon) ,AT&T Synaptic Compute & Storage.
Desktop as a service(DaaS)	Virtual Desktop Infrastructure where third part can host desktop services.	Data storage, security and backup managed by service provider.	Citrix

2.3 Hybrid cloud

Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. It combines the advantages of private and public cloud in a very striking manner. The hybrid cloud is becoming an increasingly attractive option. It offers the benefits of the public cloud (chiefly affordability) and the advantages of the private cloud. The hybrid cloud is the ideal way to effectively meet the needs of various parts of a business. Many modern businesses have a wide range of concerns. With the hybrid cloud, exceptionally sensitive information can be placed in the private cloud and less sensitive data in the public cloud. Many businesses are now looking to cloud computing to reduce or even replace their internal IT infrastructure [5].

3. SECURITY IN CLOUD

Within the cloud computing systems environment, the virtual environment lets users access computing power that exceeds that contained within their own physical worlds. Fundamentally , abundant security issues arises as it comprises many technologies including networks, virtualization [6], operating systems, resource scheduling, transaction management(when user query about some secure data), load balancing(preventing the cloud from crashing when the user demand increases),concurrency control(many users simultaneously requesting or accessing the same data on the cloud) and memory management. Data security doesn't only engross encrypting the data but also comprises on implementing and enforcing the appropriate policies for data sharing and as well as authenticating the user who required to access the data on cloud. It also

encompasses scheduling data backup and safe storage of the backup media. Security is implicit within these capabilities, but moreover elementary concerns exists that need attention. To beat these concerns, a security model must be developed which ensures CIA (confidentiality, integrity, and availability) [7]. With the competence provided by the cloud systems, as the number of users enhances, the probability of cybercrime increases. Cloud computing is becoming a tempting target for cybercrime. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cybercriminals. As cloud systems are inherited architecture so a single cyber attack offers opportunity to the attacker to influence a large number of sites through a single malicious activity. The cloud computing concerns are listed as [8]:

- Authorized access: Who will decide who will be the administrator and has the privileged access to the data?
- Authenticated access: On which policies, the user who is accessing the cloud should be authenticated? And who will authenticate these users?
- Data Security: Does the vendor allow the user to know the exact location of the data storage and what are those various levels on which data should be encrypted? And which encryption scheme should be used so that it secures the data from malicious attack?
- Data Recovery: If some disaster occurs, what will happen to the lost data (how we can recover the misplaced data)? And how long that process take?
- Research support: how does vendor would work to halt an inappropriate and malicious activity so as to provide a secure support to it s user.

Cloud computing guidelines and policies should be clearly placed in an effort to protect the cloud from unauthorized and illegal access. A cloud computing system has capability in providing redundancy to enhance the high availability of the systems in nature.

4. BUILDING SECURE CLOUD

The cloud security and privacy is a big concern now a day. Security, privacy and secure storage of data [9] are two barriers which are preventing the organizations and users from adopting the cloud computing. Emphasis must be given on security, privacy and stability on the cloud based technologies and computing to make them admirable among the corporate multitenant environment. Malicious and Abusive attacks are proliferating cloud security. The data leakage and security attacks can be caused by Insufficient authentication, authorization, and audit (AAA) controls [1], inconsistent use of encryption and software keys, operational failures, persistence and remanence challenges: disposal challenges, risk of association, jurisdiction and political issues, data center reliability, and disaster recovery. Some of the risks in cloud computing are well known in traditional computing models[11].

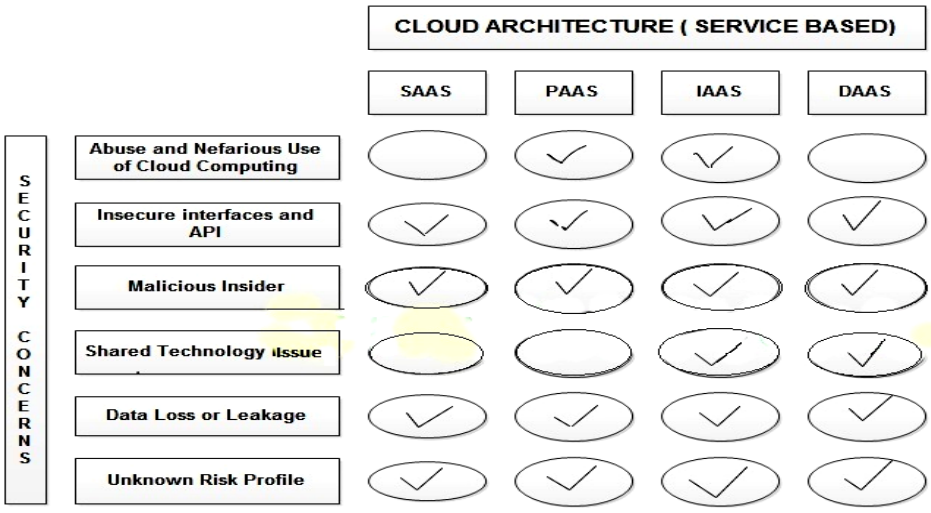

Figure 2. Security concerns in Various Clouds Architecture

These risks include, for example, malicious insiders, insecure user authentication (such as usage of weak passwords), malicious code running on the cloud, vulnerabilities of the shared resources leading to information leakage, or account hijacking by phishing methods, unknown risk profile[12], data loss(no stability in data storage on cloud). Many of these risks can be handled using conventional security practices. The top security concerns in various models are compared as [10] follows:

5. Encrypting the Cloud

The cloud has sufficient advantages and if the cloud is encrypted [13] then the cloud is widely and well accepted and adopted by the users. Two encryption algorithms for encrypting the cloud are proposed. They are Homomorphic encryption and identity based encryption. The privacy concerns can be satisfactorily addressed if users encrypt the data they send to the cloud. If the encryption scheme is homomorphic, the cloud can still perform meaningful computations on the data, even though it is encrypted. The fully homomorphic encryption algorithms has been improved but the efficiency of the algorithm is not very appreciable when the algorithm actually practically implemented. The identity based algorithm is a non interactive authentication framework. This is certificate free cryptography. In this process, which can be initiated by the sender, a unique identifier of the recipient (such as his e-mail address) is used to calculate a public key. Identity-based cryptographic is a kind of public-key based approach that can be used for two parties to exchange messages and effectively verify each other's signatures. With identity-based cryptography user's identity that can uniquely identify that user is used as the public key for encryption and signature verification.

Identity based cryptography can ease the key management complexity as public keys are not required to be distributed securely to others. Another advantage of identity-based encryption (IBE) is that encryption and decryption can be conducted offline without the key generation center. A trusted third party server known as public key generator (PKG) is required for this cryptography and the requirement of key generator is the main barrier which causes the implementation of IBE complicated. It requires centralized server. IBE centralized approach implies that some keys must be created and held in escrow and are therefore at greater risk of disclosure. It also requires a secure channel between sender or recipient and the IBE server for transmitting the private key. Identity based signature can be represented as:

Consider two entities of cloud computing E_1 and E_2. To sign a message m, Entity (E1) of the cloud computing [14] can be represented as:

1. Compute $P_m = H_1(DN_0 \| DN_1 \| DN_2 \| m)$;
2. Compute $\delta = S_{E1} + {}_{\varrho 1} P_m$ where $\varrho 1$ is the secret point of entry E_1 .
3. Output the signature $= < \delta, P_m , Q_{ID\ E1\ 11} , Q_{ID\ E2\ 12} >$.

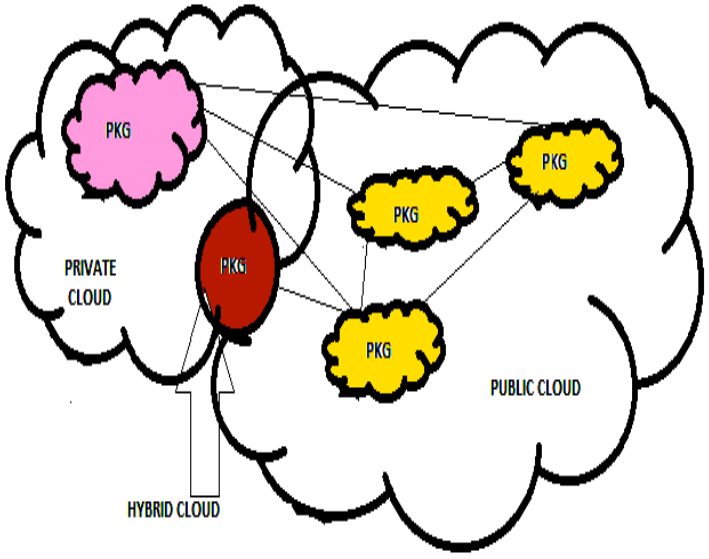

Figure 3. PKG in various cloud environments [15]

6. Conclusion

In this paper, we have discussed the various cloud computing models and their security concerns and the cryptographic algorithm which can make the world of cloud computing more secure, reliable and admirable in such a diminutive time. Security of data in cloud is still a challenge and has supreme importance as many flaws and concerns are yet to be identified. Cloud computing is becoming appreciable because of the primary benefits of cloud computing. It can reduce both capital expenditures on infrastructure, as well as operational expenditures on infrastructure maintenance and engineering. From a system security perspective it is possible to limit access to plain data by using trusted computing components in hardware and software to establish the so-called Trusted Virtual Domains: Tamper-resistant hardware embedded in computing platforms support computation that is performed by virtual machines, secure hypervisors can prevent access to virtual machines (even to system administrators) that are performing the computation on data, and attestation services can give some verifiable guarantees on the trustworthiness of the underlying hardware and software.

The excitement over the new discovery resulted however in multiple research efforts focused on constructing an efficient fully homomorphic encryption scheme. The users and servers in the cloud can generate secret session key without message exchange and authenticate each other with a simple way using identity-based cryptography. Identity based algorithm being certificate free, well adopted for providing the security to cloud world. Identity based algorithm is less vulnerable to spam and it also enables postdating of messages for future decryption. It is much efficient in terms of performance analysis. It also enables automatic expiration, rendering messages unreadable after a certain date. Ferris found that IBE required a far simpler infrastructure (meaning fewer servers and easier installation). Other findings showed that operating costs were one-fifth of those of public-key systems, and that IBE users were three times more productive than users of public-key cryptography.

REFERENCES

[1] Gens F, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges',*IDC eXchange,* from http://blogs.idc.com/ie/?p=73.
[2] E. Grosse, "Security at Scale," invited talk, ACM Cloud Security Workshop (CCSW), 2010; http://wn.com/2010_Google_Faculty_Summit_Security_at_Scale.
[3] Ramgovind S, Eloff MM, Smith E "The Management of Security in Cloud Computing" in IEEE 2010.
[4] http://en.wikipedia.org/wiki/Virtual_private_ cloud
[5] A Platform Computing Whitepaper, 'Enterprise Cloud Computing:Transforming IT', *Platform Computing,* pp6, viewed 13 March 2010.
[6] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker *Siemens "Understanding clouds vulnerabilities. In IEEE 2011.*
[7] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou "Security and Privacy in Cloud Computing: A Survey" in IEEE 2010.
[8] Farzad Sabahi , "Cloud computing threats and responses" in IEEE 2011.
[9] Jianfeng Yang & Zhibin Chen "Cloud computing Research and security issues" in IEEE 2010.
[10] Cloud Security Alliance Web site, http://www.cloudsecurityalliance.org/.
[11] L. Wang et al., 1. "Scientific Cloud Computing: Early Definition and Experience," *Proc. 10th Int'l Conf. High-Performance Computing and Communications* (HPCC 08), IEEE CS Press, 2008, pp. 825–830.
[12] "US Federal Cloud Computing Market Forecast 2010–2015," tabular analysis, publication: 05/2009.
[13] Isaac Agudo , David Nuñez , Gabriele Giammatteo , Panagiotis Rizomiliotis, Costas Lambrinoudakis " Cryptography goes to cloud"
[14] Hongwei Li, Yuanshun Dai1, Ling Tian, and Haomiao Yang "Identity-Based Authentication for Cloud Computing" in Springer-Verlag Berlin Heidelberg 2009.
[15] Liang Yan1, Chunming Rong1, and Gansen Zhao2 "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography" in IEEE 2009.

BIBLIOGRAPHY OF AUTHOR

Ashish Kumar is currently working as Assistant Professor in Computer Science Department, Bharati Vidyapeeth's College of Engineering, Paschim Vihar New Delhi (GGSIPU). He is a B. Tech from M.D. University with honours and M.Tech from GGSIP University with Distinction.He is having teaching Experience of Three Years. He is an active member of Research and Development team in Bharati Vidyapeeth and working closely in the areas of Cloud Computing. He has also authored many papers, published in International Conferences, and International Journals of computer applications.He has attended many workshops organized by Various organizations.