ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

A Study on Effective Methods for Ensuring Privacy in Cloud Computing Environment

Mahendran D, Jothi Prakash V, S.Manikandan, K. Karthiban

Assistant Professor, Karpagam College of Engineering, Coimbatore, India.

ABSTRACT: Cloud computing has grown as a network based service oriented computing model. Cloud computing allows users to access computers and software applications hosted by remote servers. While providing access to such data we must keep in mind the privacy of the data stored in such remote machines or servers. Thus there arises a need for protecting the privacy of the data. There arises a serious concern in privacy when the data is stored and shared over the distributed databases. Relinquishing the control over data and application poses challenges of security, performance, availability and privacy. The critical factors to consider for the wide utilization of cloud computing environment are confidentiality, authentication, integrity and non-repudiation. A major concern is that the user may download a malware or a virus that steals user data and spreads across the entire cloud network. If such attacks are possible then it the integrity and confidentiality of the data will be lost. In this paper we provide a study on the various privacy issues related to cloud computing.

KEYWORDS*:* Cloud computing, privacy, data sharing, data security.

I. INTRODUCTION

Cloud computing is a new computing standard that allows the use of a computing structure as an on-demand service made available over the internet or other networks. It is sold on demand, typically by the minute or the hour. The user can use the service based in the time limit or the validity period and can also expand the service by paying the amount. Due to its flexibility and availability at lower cost, cloud computing is a topic that has been receiving a great deal of attention.

Cloud Computing can be classified into 4 types on the basis of location where the cloud is hosted [2]:

A. *Public Cloud*: A public cloud is one in which the infrastructure and other resources that it comprises are made available to the public over the Internet. It is owned by a cloud service provider external to an organization.

B. *Private Cloud*: A private cloud a proprietary network or a data center that supplies hosted services to a limited number of people. It may be managed either by a third party or an organization, and hosted within the organization's data center or outside of it.

C. *Community Cloud*: A community cloud is similar to a private cloud, but the infrastructure and resources are shared by numerous organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization.

D. *Hybrid Cloud:* A hybrid cloud is a mixture of two or more clouds that remain unique entities but are bounded together by proprietary technology that enables interoperability.

As cloud computing is becoming more popular, some concerns are being stated about the possible security issues introduced through the adoption of it. According to a Gartner survey [6] on cloud computing revenues, the cloud market worth USD 58.6B in 2009, is expected to be USD 68B in 2010 and will reach USD 148B by 2014. These figures imply that cloud computing is a promising platform. Moreover, it increases the attackers' interest in finding existing vulnerabilities. In this paper we attempt to clarify the unique privacy issues introduced in a cloud environment. Along with that, we propose a method that will prevent unauthorized access to the system.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

II. CLOUD SERVICE MODEL

There are three well-known and frequently-used services [1] provided by cloud computing:-

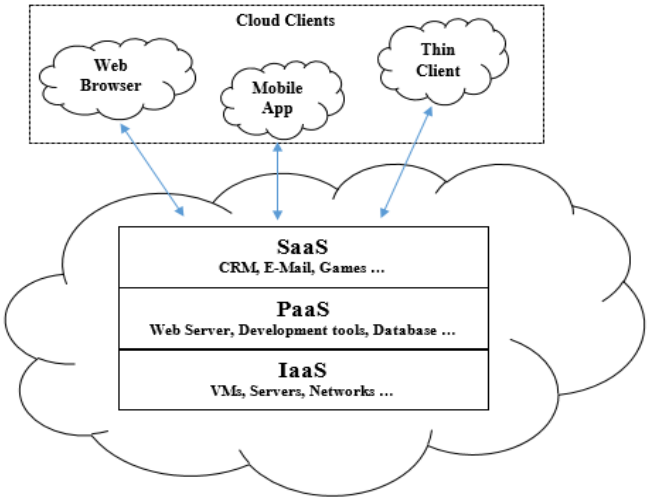

Figure 1. SaaS Component Stack and Scope of Control

1) Software-as-a-Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network. Also known as "on demand" software, it is the most mature type of Cloud Computing because of its high flexibility, proven support services, enhanced scalability, reduced customer maintenance, and reduced cost due to their multi-tenet architectures As shown in figure 1, it is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

2*) Platform-as-a-Service* **(**PaaS) provides infrastructure on which software developers can build new applications or extend existing applications without requiring the need to **(**purchase development, QA, or production server infrastructure. As shown in figure 2, it is a model of software deployment where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

.

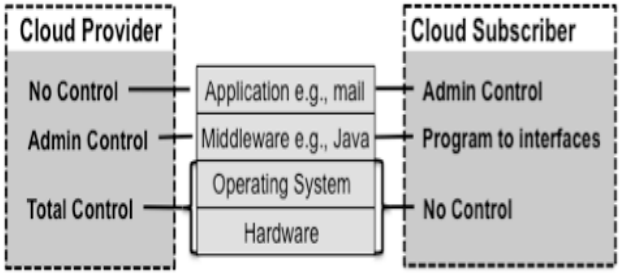

Figure 2. PaaS Component Stack and Scope of Control

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

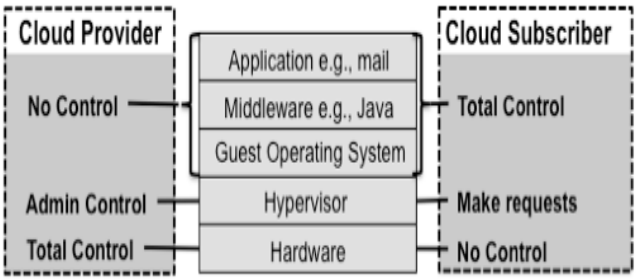

Figure 3. IaaS Component Stack and Scope of Control

3) Infrastructure-as-a-Service-(IaaS) Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. As shown in figure 3, its scope of control. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

III. CHALLENGES OF THE CLOUD COMPUTING

The IDC study has specified the key challenges facing by cloud computing as shown in Figure 4. Since advantages of cloud computing are obvious, but the security risks associated with each cloud service model hinder its widespread adoption. The externalized aspect of outsourcing makes it difficult to maintain data integrity, privacy, availability and above all compliance check of security measures taken by the service provider [13]. According to a survey in 2009, cloud security was revealed as the top most challenge/ issue of cloud computing among others like availability of services, performance, lack of interoperability standards and so on.

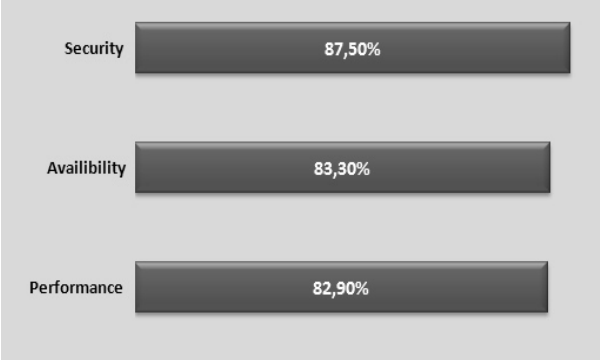

Figure 4 . Cloud users' Survey–Security at the top

IV. SECURITY AND PRIVACY ISSUES RELATED TO CLOUD COMPUTING

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability. The sections below highlight privacy and security-related issues that are believed to have long-term significance for cloud computing. There are various Cloud computing guidelines [1] [13] that should be seen as the cornerstone of the Cloud strategy with Cloud governance and transparency forming part of the security perspective.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

A. Cloud Govenance

Governance implies control and oversight over policies, procedures, and standards for application development, as well as the design, implementation, testing, and monitoring of deployed services. Cloud computing policies and procedures should be put in place in an effort to protect the cloud from potential of threats, hacks and the loss of information. As cloud computing simplifies platform acquisition, it doesn't means that it alleviate the need for governance.

B. Data Compliance and auting

Data compliance: - It means conformance with an established specification, standard, regulation, or law. There are various types of security and privacy laws and regulations that has been defined by various countries, national, state, and also at the local levels, making compliance as a complicated issue for cloud computing

- *Data Location*: Data location is one of the most common compliance issues facing by an organization As user data is stored in data centers maintained by the organization , user is unaware of where the data has been saved and security measures has been take to protect the data. In contrast to it, a characteristic of cloud computing services is that detailed information related to the location of an organization's data is unavailable or not disclosed to the service subscriber. Whenever the information crosses the borders, the governing legal, privacy, and regulatory regimes can raise a variety of concerns. The constraints on flow of sensitive data over the trans-border, have become the subject of national and regional privacy and security laws and regulations
- *Law and Regulations*: The Federal Information Security Management Act (FISMA) requires that the federal agencies have to protect their information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction. That makes it mandatory to have protecting information systems used or operated by an agency or other organization on behalf of an agency. That is, any external provider handling federal information or operating information systems on behalf of the federal government must meet the same security requirements as the source federal agency.

Auditing: - As an IT professional, you already know the headache of securing your own local network.
But when you send your data to the cloud, a whole new set of issues arise. This is largely because your data is being stored on someone else's equipment.

C. Architecture

The architecture of the software systems used to deliver cloud services comprises hardware and Software residing in the cloud. Virtual machines often serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture. Below in this section it specifies how security in cloud computing architecture is employed

- *Virtualization*: Virtualization allows the pooling of the computational power and storage of multiple computers, which can then be shared by multiple users. Many companies have cited security concerns as the main blocker to virtualization and private cloud adoption. Paradoxically, virtual machines can be more secure than the physical servers they replace. Because virtual machines are purpose-built, virtualization security software can offer levels of dynamic and automated security that are unequalled in the physical security realm. As organizations become more familiar with hypervisor-based security and VM Introspection, the apprehension that may have stymied virtualization of critical workloads will be appeased. We expect that terms like "hypervisor-based," "VM safe certified" and "VM Introspection" will become part of the 2011 vernacular of "must-haves" for virtual security architectures.
- *Server side protection*: The first necessary condition of cloud computing is that both of the server and database on the front end must be trusted has to be satisfied. The assurance of confidential, integrity and authentication is very important for those information transaction, data manipulation, and service provided by cloud computing on the remote side through networking. In order to monitor and process the Internet hacking, thoroughly comprehend the source, technique, and intension of networking attack and analyze their attacking behavior is a must for information protection. A honey-net has been deployed on the Intranet of a simulated enterprise for security purpose. Within the honey net, there are some honey-pots that store important data such as personal, salary, research and development project, military intelligence, or important news are installed on the server and database systems. Inside the Intranet, some folders or directories are open intended for monitoring and tracing the behavior and visiting frequency and record the tracks that have been accessed by the hackers. After analyzing and comprehending all of the hacking information, the corresponding derivation is quiet useful for enhancing the design of network-based intrusion detection and prevention systems.
- *Cloud Side protection* : This proposal has possesses more flexibility for offering the various application of cloud computing such as offering on-line storage and access data via web-based application interface (API) for all of the users of cloud computing in anytime at anywhere through wired or wireless networking devices. This service lets the user or customer to upload their data on the client side of cloud computing.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

For example, the application can be applied for very popular micro-blogging (Micro log) such as Twitter. Recently, which allow millions of the user of Microlog to store their personal information or pictures on the on-line storage that provided by the Microlog or such as the Simple Storage Service (S3) provided by the Amazon for storing the data. Data security on the cloud side is not only focused on data transmission, but it also takes care of system security and data protection for data that have been stored on the cloud side. Moreover, if there are lots of users on the client side of the cloud computing accessing the same folders or even the same files on the cloud side, then in that case service provider must pay attention to find out the possible occurred problems and it must possess the capability of perfect database and file management to avoid data hazard. So, an enterprise shall evaluate the risk of storage damage, data loss, and networking security on the cloud side.

An enterprise of the user of cloud computing should also pay attention to the data security on the storage, i.e. the protection of Data-at-rest. The rationale of adopting Data-at rest is the process of performing data encryption, authorization and authentication in the storage environment of data. An enterprise should encrypt those confidential file or sensitive data before uploading. After that, the encrypted data could be uploading to the storage designated and provided by service provider of the cloud computing through secure channel. The demonstrated operating process is shown as Figure 5.

This kind of information protection and data encryption facility is provided only by IaaS. If the data is high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication.

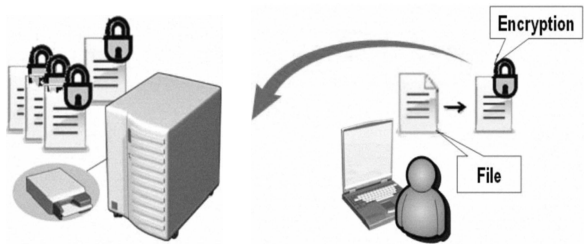

Figure 5

In addition, the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side (enterprises) to instead of the service provider [8].

D. Network Security

Regarding the utilization of cloud computing, some possible communicating scenario including wired and wireless networking which has been discussed in the following subsection.

- *Utilizing dedicated or leased line* – For a large size enterprises or business corporations, in order to assure the secure cloud computing service, the service providers of cloud computing had better construct a model that utilizing the dedicated or leased channel for communication with the enterprise. In addition to it, the encryption system and authenticating mechanism must be compulsive to maintain the information security in the process of communication.
- *Using Internet and VPN* - For medium and small size enterprises, the suitable model that has been adopted by the service providers to implement the secure application had better constructed based on Virtual Private Network (VPN). VPN solutions provide a secure means of controlling access to information and managing the risks associated with cloud computing.

E. Identity and Access Management

The key critical success factor to managing identities at cloud providers is to have a robust federated identity management architecture and strategy internal to the organization [2]. Using cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with cloud providers such as:-

- *User authentication*: For all of the enterprises, the management of user's account and its corresponding authorized access privilege is very important and must be strictly defined. A lot of enterprises usually confront the problem of user account such as the adoption of single sign on (SSO) or each employee. Each user will be dispatched

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

some different accounts to access different systems .Thus, multi-authentication for each employee might be very often to be confronted in an enterprise. Therefore, how could the administrator well manage those user's identification accounts and the corresponding passwords or achieve the state of SSO is another important issue. But by making use of Security Assertion Markup Language (SAML) standard or the OpenID standard this could be achieved. SAML provides a means to exchange information, such as assertions related to a subject or authentication information, between cooperating domains. SAML request and response messages are typically mapped over the Simple Object Access Protocol, which relies on the extensible Markup Language (XML) for its format. SOAP messages are digitally signed. For example, once a user has established a public key certificate for a public cloud, the private key can be used to sign SOAP requests.

F. Privacy

Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design [3]. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. The following tips are recommended for cloud system designers, architects, developers and Testers.

- Minimize personal information sent to and stored in the cloud.
- Protect personal information in the cloud.
- Maximize user control.
- Specify and limit the purpose of data usage.
- Provide feedback.

V. PROPOSAL BASED ON SURVEY

In cloud computing security is important as society and companies store their data in the cloud. And security is one of the main problems in which decrease the growth of cloud computing to pestilence the market. The users are the authentication in smart situation is the key issue in the security. But the increasing number of reported security vulnerabilities develops the weakness of password based verification methods loss caused to the enterprises. The password based authentication solutions are no longer an adequate protection techniques due to those vulnerabilities for enterprise applications. So easily we represent that there is increase demand of robust, dynamic one-time password based verification, secure into their IT [14].

In IT companies' unauthorized users there may be a chance to hack the passwords. To make certain security extra confidential work need to be implemented. Moreover in cloud computing high security is needed to protect the data from unauthorized users. My suggestion is that to implement dynamic password to improve security. One time password is valid only once that is dynamically generated to access our data in cloud.

a) The dynamic password is one of strong authentication technologies. It has the following features:

b)

c) One time Usage: one time password is valid only once. It won't be valid for another time. Therefore, revelation of the used dynamic passwords doesn't matter.

d) Irreproducibility: The one time passwords are similar to the tokens. Each and every time token generates different dynamic passwords.

e) Vitality: the tokens are generates different types of dynamic passwords. So that the generated dynamic passwords varies from time to time.

f) Struggle of extensive attack: The attack must be restarted when the correct dynamic passwords is not hit in a minute. Then the new dynamic passwords may hit if necessary.

g) Anti-theft: The one time passwords are generated dynamically.

h) Randomization: one time passwords are generated randomly. We can't predict it.

Dynamic one time passwords are better choice for replacing the static passwords that produce strong verification. Its good choice dynamic one time password is much better compared with static passwords. A dynamic one time password is unique password that is dynamically generated and used only once.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

VI. CONCLUSION

Cloud Computing brings new security paradigms and challenges, since physical platforms are shared by several entities. A Cloud customer may need some assurance or trust on the state and configuration of the physical platform before installing his services on it.

In this paper, various challenges that are being currently faced in the cloud computing industry & various guidelines related to securing the private data in cloud computing, has been specified. We believe that this solution will overcome the shortcoming of the cloud computing security.

REFERENCES

[1] Guidelines on Security and Privacy in Public Cloud Computing by "Wayne Jansen Timothy Grance".
[2] "Cloud computing" http://en.wikipedia.org/wiki/Cloud computing accessed on 15th sept 2011.
[3] Mohamed Al Morsy, John Grundy and Ingo Müller "An Analysis of The Cloud Computing Security Problem " proceeding of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.
[4] Dimitrios Zissis □, Dimitrios Lekkas "Addressing cloud computing security issues" Future Generation Computer Systems , 14 may, 2010.
[5] Hui Wang. Privacy-preserving data sharing in cloud computing. JOURNAL OF COMPUTER SCIENCE AND TECH- NOLOGY 25(3): 401-414 May 2010
[6] Chang-Lung Tsai Uei-Chin Lin Allen Y. Chang Chun-Jung Chen "Information Security Issue of Enterprises Adopting the Application of Cloud Computing".
[7] Gartner Incorporation, http://www.gartner.com accessed on Sep 2011.
[8] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Atanu
Rakshit, " Cloud Security Issues", proceedings of 2009 IEEE International Conference on Services Computing.
[9] "Cloud Computing", http://www.ibm.com/deveIoperswork/websp here/zones/hipods/Ii b rary.
[10] Tim Mather, "Cloud Security and Privacy", 2009.Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
[11] The Management of Security in Cloud Computing by "Ramgovind S, Eloff.
[12] MM, Smith E " Guidelines on Security and Privacy in Public Cloud Computing" by Wayne Jansen , Timothy Grance.
[13] Survey on Cloud Computing Security by "Shilpashree Srinivasamurthy David Q. Liu "
[14] "Dynamic Authentication: Need than a Choice", A.Saxena, Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference, 10 (1) (2008), 214.