International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

Study and Analysis of Data Secure Storage in Cloud Computing

[1]J.Surya, [2]S.Sathiya, [3]Mrs.M.Dukitha

Abstract- Cloud computing is architecture for providing computing service via the internet on demand and pay per user 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. A set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing architectures. Threats are 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. To the best of our knowledge, PasS (Privacy as a Service) is the first practical cloud computing privacy solution that utilizes previous research on cryptographic coprocessors to solve the problem of securely processing sensitive data in cloud computing infrastructures. By using cryptographic encryption algorithms Cloud service providers (CSP) can provide a level of privacy and security to the cloud users. By following query any user can access the data from the cloud servers through decryption.

Keywords: -SLA, privacy & Security, PasS, CSP, Security Protocols, Servers and Networks**.**

1 INTRODUCTION

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services [1]. Customers should be aware through a secure privacy auditing process of all the operations carried out to secure the storage and processing of their sensitive information. In this paper we present PasS; a set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing architectures. PasS allows for the secure storage, processing, and auditing of users' confidential data byAlthough cloud computing service providers touted the security and reliability of their services, actual deployment of cloud computing services is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents [4]. Cloud refers to any form of Network (public or private) which is present at remote location. Almost all types of applications (Email, Video Conferencing, game etc.) execute in the cloud. Cloud Computing provides us facility to access any kind of information at any time. The cloud computing provides different services to their clients called front end and the cloud itself refer as back end that provides such services to the clients [7]. Cloud computing plays an important role in improving the quality of education to achieve required performance by offering many benefits for education such as providing low-cost infrastructure, flexibility, scalability, collaboration, and ease-of-use [8].Cloud computing refers to the use of networked infrastructure software and capacity to provide resources to users on-demand. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, Laptops, mobiles and other devices computing devices. With Design perspective, Cloud computing is flexible, scalable and elastic offering IT services a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure and license software [9]. To offload storage to the cloud, there are many existing storage services for mobile devices, such as Drop box, Box, cloud, Google Drive, and Skydive We are integrating the Mobile computing and Cloud computing, surely there will be some security issues [10].

This allows developers to concentrate on the business value rather on the starting budget. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs [1]. Cloud computing has very quickly become one of the hottest topics if not the hottest one for practicing engineers and academics in domains related to engineering, science, and art for building large-scale networks and Internet applications. Nowadays, everyone's talking about clouds [2].

2 RELATED WORKS

This paper presents a protocol or set of instructions that uses the services of a third party auditor or checker not only to verify and authenticate the integrity of data stored at remote servers but also in retrieving and getting the data back as soon

- [1]*J. Surya, Second Year Master of Computer Applications in Er.Perumal Manimekalai College of Engineering, Hosur, PH-9500654651. E-mail: Lakshmisurya13297@gmail.com*
- [2]*S.Sathya, Second Year Master of Computer Applications in Er.Perumal Manimekalai College of Engineering, Hosur, PH-8883086431. E-mail: sathiyashankar888@gmail.com*
- [3]*Mrs.M.Dukitha, Assistant Professor, Master of Computer Application in Er.Perumal Manimekalai College of Engineering - Hosur, PH-, E-mail: dukitha.m@yahoo.co.in.*

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

as possible in intact form. The main advantage of this scheme is the use of digital signature to assure the integrity of local data. However, the overall process is quite problematic and complex as the keys and data are also encrypted and decrypted respectively [2]. The authors deal with the problem of security of data during data transmission. The main thing to fear about this paper is the encryption of data so that confidentiality and privacy can be easily achieved [2].

3 Models of Cloud Computing

Generally cloud services can be divided into three categories:

- ✓ Software as a Service (SaaS),
- ✓ Platform as a Service (PaaS),
- ✓ Infrastructure as a Service (IaaS) [6].

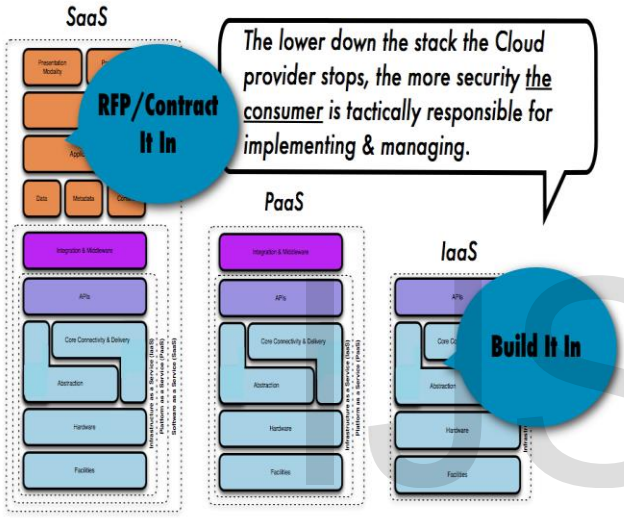


Fig 1: How Security Gets Integrated

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. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support.

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 developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications.

3.3 Infrastructure as a Service (IaaS)

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems.

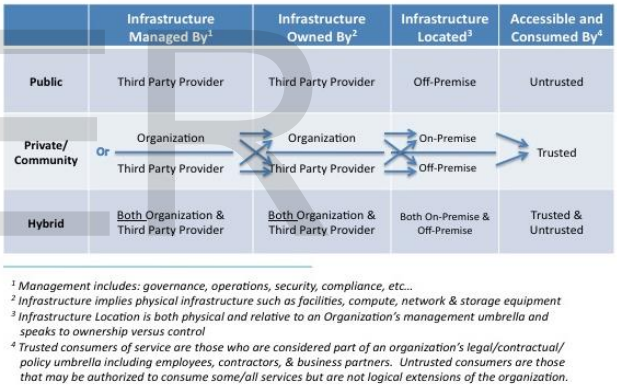
4 Cloud Security Reference Model

The cloud security reference model addresses the relationships of these classes and places them in context with their relevant security controls and concerns. For organizations and individuals grappling with cloud computing for the first time, it is important to note the following to avoid potential pitfalls and confusion [1].

The notion of how cloud services are deployed is often used interchangeably with where they are provided, which can lead to confusion. For example, public or private clouds may be described as external or internal clouds, which may or may not be accurate in all situations.

This is not to suggest that the on- or off-premise location of an asset, a resource, or information does not affect the security and risk posture of an organization because they do — but to underscore that risk also depends upon [1].

- ✓ The types of assets, resources, and information being managed.
- ✓ Who manages them and how.
- ✓ Which controls are selected and how they are integrated.
- ✓ Compliance issues.



	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or: Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] Management includes: governance, operations, security, compliance, etc...
[2] Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment
[3] Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control
[4] Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Fig 2: Cloud Computing Deployment Model

For example a LAMP stack deployed on Amazon's AWS EC2 would be classified as a public, off-premise, third-party managed-IaaS solution, even if the instances and applications/datacontained within them were managed by the consumer or a third party. A custom application stack serving multiple business units, deployed on Eucalyptus under a corporation's control, management, and ownership, could be described as a private, on-premise, self-managed SaaS solution. Both examples utilize the elastic scaling and self-service capabilities of cloud.

First one classifies a cloud service against the cloud architecture model. Then it is possible to map its security architecture as well as business, regulatory, and other compliance requirements against it as a gap-analysis exercise. The result determines the general "security" posture of a service and how it relates to an asset's assurance and protection requirements [5].

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

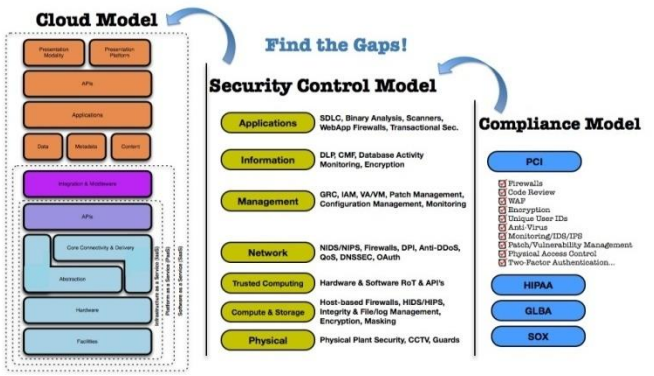


Fig 3: Mapping the Cloud Model to the Security Control & Compliance Model

5 Cloud Computing Security Issues

5.1 Security Issues Associated with the Cloud

There are many security issues associated with cloud computing and they can be grouped into any number of dimensions. According to Gartner, before making a choice of cloud vendors, users should ask the vendors for seven specific safeties Issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability [4].

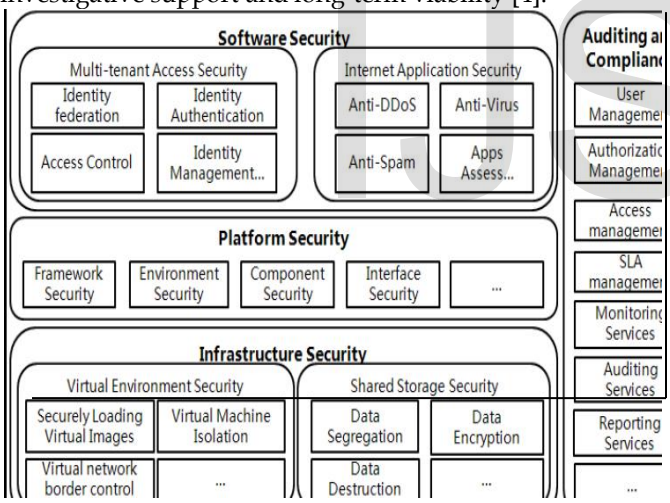


Fig 4: Cloud computing security architecture

6 Cloud Computing Securities

Cloud Computing Security as "Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing." Note that cloud computing security referred to here is not cloud-based security software products such as cloud-based anti-virus, anti-spam, anti-DDoS, and so on [4].

7 CLOUD Key Security Challenges

There are some clouds key Security challenges are [6]:

- ✓ Authentication
- ✓ Access Control
- ✓ Policy Integration
- ✓ Trust Management

7.1 Authentication

Throughout the internet data stored by cloud user is available to all unauthorized people. Henceforth the certified user and assistance cloud must have interchangeability administration entity.

7.2 Access Control

To check and promote only legalized users, cloud must have right access control policies. Such services must be adjustable, well planned, and their allocation is overseeing conveniently. The approach governor provision must be integrated on the basis of Service Level Agreement (SLA).

7.3 Policy Integration

There are many cloud providers such as Amazon, Google which are accessed by end users. Minimum number of conflicts between their policies because they user their own policies and approaches. Service Management: In this different cloud providers such as Amazon, Google, comprise together to build a new composed services to meet their customers need. At this stage there should be procuring divider to get the easiest localized services.

7.4 Trust Management

The trust management approach must be developed as cloud environment is service provider and it should include trust negotiation factor between both parties such as user and provider. For example, to release their services provider must have little bit trust on user and users have same trust on provider.

8Security Problems Faced By Cloud Computing

There is a chance where a malicious user or hacker can get into the cloud by impersonating a legitimate user, there by affecting the entire cloud thus affecting many people who are using the infected or affected cloud [8]. Some of the problem which is faced by the Cloud computing are:

- ✓ Data theft
- ✓ Integrity of data
- ✓ Privacy problems
- ✓ Loss of data
- ✓ Infected Applications
- ✓ Exact location of data
- ✓ Vendor level Security

9 Conclusion and Future Enhancement

Cloud security is an ultimate concept which will crush the drawbacks the acceptance of the cloud by the big MNCs, companies and organizations.There are a lot of

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

security algorithms which may be implemented to the cloud. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues exist in all levels in SPI service delivery models and in all stages of data life cycle. 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 various models of cloud computing, security issues and research challenges in cloud computing.

REFERENCES

1. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing Security: Issuesand Research Challenges" volume 1, issue no. 2.
2. Rishav Chatterjee, Sharmistha Roy "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud" Volume 7 issue no. 5.
3. Wassim Itani, Ayman Kayssi, Ali Chehab "Privacy as a Service:Privacy-Aware Data Storage and Processing in Cloud Computing Architectures"
4. Deyan Chen, Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" IEEE DOI 10.1109/ICCSEE.2012.193https://cloudsecurityalliance.org/wpcontent/uploads/2011/09/Do main-1.docx
5. Akshat Ajabrao Uike, Dr. M. A. Pund, Sangram S. Dandge "An Overview of Cloud Computing:Platforms, Security Issues and Applications" Volume 2, issue 5.
6. Nidhi Dahiya, Mrs. Sunita Rani "Cloud Computing Security: A Review" Volume 5, Issue 3.
7. Khalil Al-Shqeerat, Mohammad Hassan "Cloud Computing Security Challenges in Higher Educational Institutions -A Survey" DOI: 10.5120/ijca2017913217
8. Vinodray Thumar, Dr. Vipul Vekariya "A Technical Review on Mobile Cloud Computing: SecurityIssues and Research Challenges" Volume 4, issue 10.
9. Anusree Radhakrishnan Minu Lalitha Madhav "Towards Secure Data Distribution Systems in Mobile Cloud Computing: A SURVEY" Volume 4, issue 11.