



## Enhancing Security for a Secure Cloud Computing Environment

Divya Chaudhary\*

Department of Computer Science & Applications  
M.D. University, India

**Abstract**—Cloud computing is a major advancement in field of distributed computing. It is one of the latest developments in the IT industry also known as on-demand computing. It is the new and upcoming paradigm that offers huge benefits including such as reduced time to market, unlimited computing power and flexible computing capabilities. This paper elaborates the cloud computing confidentiality framework (CCCF) and trusted system framework for the security. It presents various confidentiality and security threats on the system. This is a step-wise process based on the sensitivity of the data which specifies security controls in computing environment. Trusted computing platform (TCP) model attempts to enhance cloud computing security without increasing complexity.

**Keywords**— Cloud Computing Confidentiality Framework (CCCF), Trusted computing platform (TCP), Cloud Computing, Confidentiality

### I. INTRODUCTION

Cloud Computing is one of the most talked about technology in the recent times and has gained lot of attention from the analyst as well as media because of wide range of opportunities. The term Cloud Computing is used to describe both a type of an application and a platform. Cloud Computing describes the applications that are accessible through internet and for this purpose large data servers are used to host web applications and web services. On the other hand as a platform, it supplies, configures and reconfigures the servers. The cloud is a metaphor of Internet. It is a subscription based service where one can obtain computer resources and networked storage space. It is also said as a internet based On-Demand computing in which the shared resources, information and software are provided to the computers and other devices on-demand, as in electric grids. The clouds are like virtualized data centres [1]. Cloud computing platforms are dynamically built using virtualized hardware, software, data sets and networks. Thus, Cloud computing is a new computing paradigm, involving data and/or computation outsourcing, with:-

- Infinite and elastic resource scalability
- On demand “just-in-time” provisioning
- No upfront cost ... pay-as-you-go (pay as you use)

It provides virtualization and dynamic scalability of the system. The definition of cloud computing as provided by NIST states that:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

#### A. Characteristics of Clouds

- a) Rapid elasticity: The cloud computing resources can rapidly match with the increasing cloud capabilities if the demand increases.
- b) Measured service: It enables the measuring [2] of used resources similar to the utility computing.
- c) Resource pooling: This resource pool helps in enabling the use of physical and virtual resources by multiple users.
- d) Broad network access: Cloud services are available on any kind of network.
- e) On Demand Self-service: Cloud Computing resources can be obtained and disposed of by the consumer without human intervention among cloud service providers.

#### B. Cloud Service and Deployment Models

- a) Software-as-a-Service (SaaS): The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer.
- b) Platform-as-a-Service (PaaS): The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud-based infrastructure. “
- c) Infrastructure-as-a-Service (IaaS): The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity.

#### C. Cloud Deployment Models

- a) Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

- b) Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.
- c) Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
- d) Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

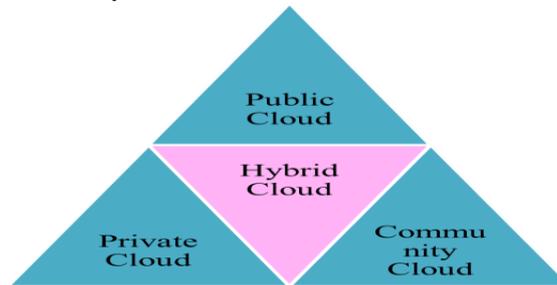


Figure1: Deployment Models

The rest of this paper is organized as follows. The security aspects of the cloud computing are discussed in Section II. It also depicts the various harms or threats pertaining to the clouds. The emerging trends for making a secure cloud are presented in Section III. It highlights the CCCF (Cloud Computing Confidentiality Framework) as well as the Trusted Computing Platform along with a number of security solutions. Finally, the conclusions and the future works are discussed in Section IV.

## II. SECURITY ASPECTS IN CLOUD COMPUTING

In cloud computing the security plays a major role in the development of the system. More than user authentication with passwords or digital certificates and confidentiality is needed for providing security in distributed systems. Intruders find a great target in cloud computing environments as, [3] intruders are willing to explore possible vulnerabilities by impersonating legitimate users with the inappropriate use of resources.

Some of the threats of cloud computing:

### A. Abuse and Nefarious Use of Cloud Computing

Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

### B. Insecure Interfaces and APIs

Provisioning, management, orchestration, and monitoring are all performed using these interfaces. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

### C. Malicious Insiders

This kind of situation clearly creates an attractive opportunity for an adversary ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

### D. Shared Technology Issues

IaaS vendors deliver their services in a scalable way by sharing infrastructure. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources.

### E. Data Loss or Leakage

Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Unauthorized parties must be prevented from gaining access to sensitive data.

### F. Account or Service Hijacking

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.

### G. Unknown Risk Profile

Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Security by obscurity may be low effort, but it can result in unknown exposures.

## III. EMERGING TRENDS IN SECURE CLOUD COMPUTING

Confidentiality plays a prima facie in the concept of secure cloud computing. [4] It is basically defined as:

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information”.

The potential impacts are:

- LOW: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

- MODERATE: The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- HIGH: The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A. CCCF(Cloud Computing Confidentiality Framework)

The task of this framework is to elaborate the differences between the security in [5] cloud computing environment and the security in the present day information security practices.

The CCCF specifies the 3 dimension:-

- System tasks:  
Specifies whether the data is to be stored, processed and transferred
- Protection Mechanisms:  
Refers to the controls that are protecting the information system
- Data Location:  
The Amount of control on data by the data owner

The framework described as:

First the identification of business goals and objectives those need to be followed. They are the vital ingredients of the framework. They are considered to be specified in the scope of the research for both cloud computing environments and traditional environments. [6] The impact analysis of the particular process is the identification of the system and processes in the organization. The creation of the logistic plan for a particular computation is done.

The data and system classifications are matched with the particular practices of the todays.it specifies what data needs to be secured and how valuable the data and information systems are. [7] The main emphasis is the security of the system. On the basis of providing the security to the particular system we select the security control selection of the system along with the data protection.

Limitations are defined in the system keeping in mind the various trust, policy, system task and data protection dimensions. Then we specify the cloud security solutions respectively.

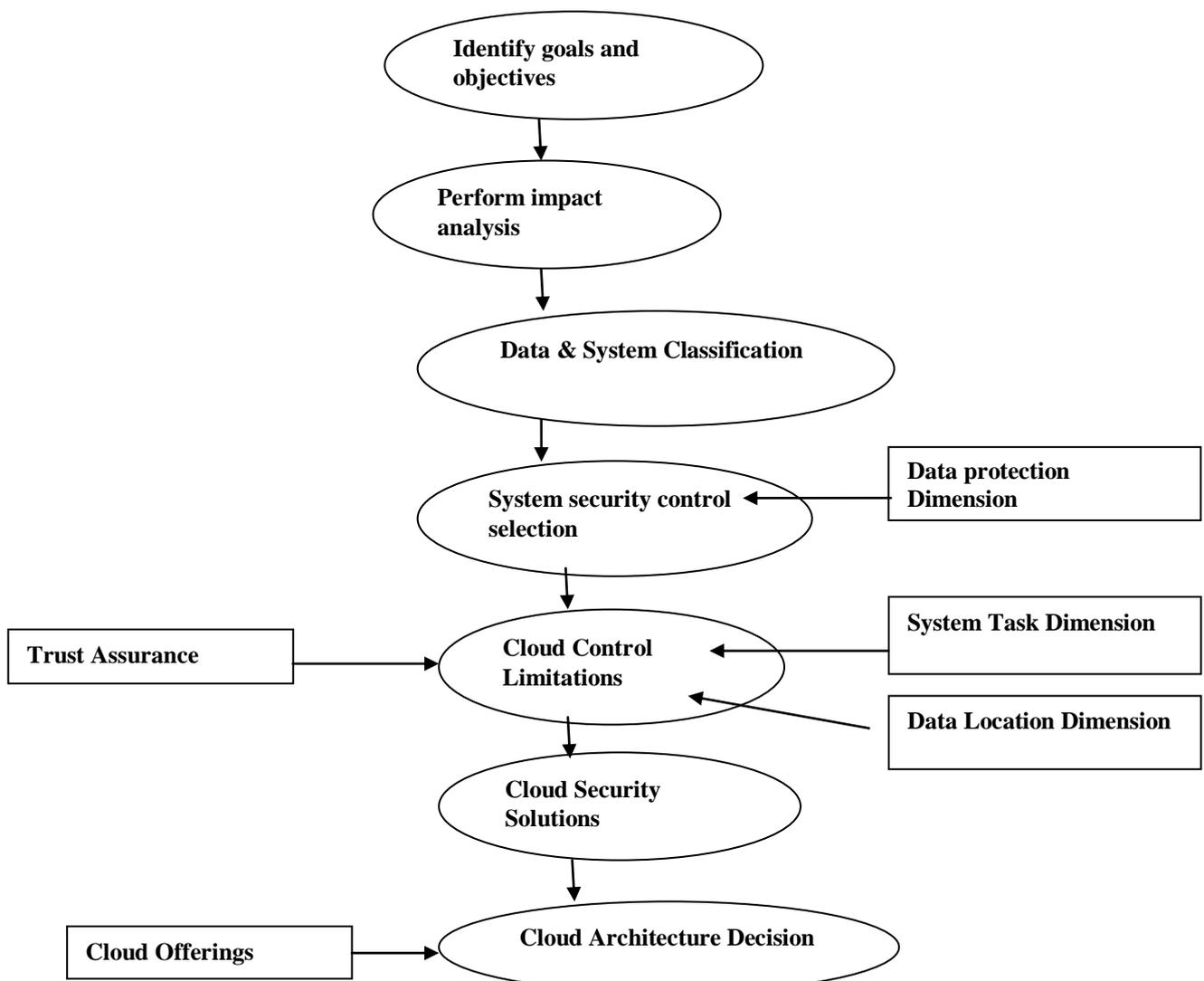


Figure2: Cloud Computing Confidentiality Framework (CCCF)

**B. The Cloud Security Solutions:**

**a) System Solution**

They are based on the information systems physical layer. To achieve the security requirements it directly manipulates the hardware and the software. They provide the security at the lower levels of the technology stack. The solution such as encryption i.e., cryptography act as a base for the behavioural solutions. Another system solution techniques IDS (Intrusion Detection system), [8] detects the security breaches by monitoring the data transfers and execution of functionality.

**b) Behavioral solutions**

These act on the higher level of abstraction. They focus on the behaviour of the users in the information system. It is formed on the basis of the trust based solutions i.e., information to only trusted and the policy based solutions i.e., limit the users access to the information resources.

**c) Hybrid solutions**

It comprises a combination of the system and behavioural solutions indicating both authentication and authorization.

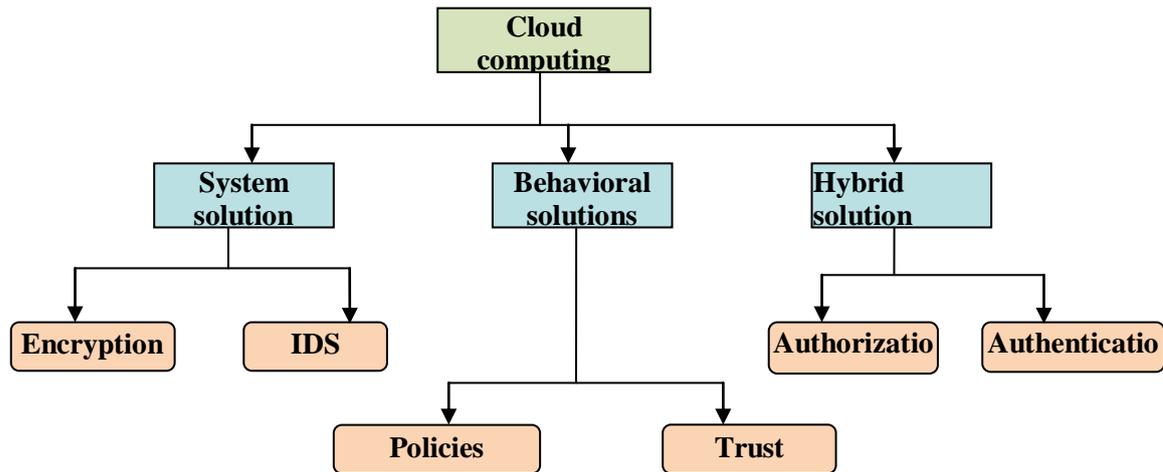


Figure3: Cloud Security Solutions

**C. Trusted Computing Platform:**

The Trusted Computing Platform will be used in authentication, confidentiality and integrity in cloud computing environment. [9] The Trusted Platform Module is an international standard, hardware security component built into many computers and computer-based goods. The TPM includes capabilities such as machine authentication, hardware encryption and secure key storage.

Encryption and signing are well known techniques, but the TPM makes them stronger by storing keys in protected hardware storage space. Machine authentication is a core principle that allows clouds to authenticate to a known machine to provide this machine and user a higher level of service as the machine is known and authenticated.

TCP provides services like Authenticated boot, Encryption, Confidentiality, Integrity and Security. [10] Trusted Platform can address:

- Identity theft and impersonation through unprotected passwords and sensitive information.
- Unauthorized network access, such as to a corporate network, a wireless network, or a VPN.
- Regulatory compliance issues for strong authentication and data protection.
- Unauthorized access to unprotected files, documents, or email on client PCs or servers.

Trusted computing consists of the following components [11]:-

i. Trusted Platform Support Services:

Trusted Platform Support Services is middleware that act as an intermediate between the TCP and the users.

ii. Trusted Platform Module:

TPM is a security device that can store the cryptographic keys.

iii. Core Root of Trust for Measurement:

It is software that can be used to identify the trusted root.

The benefits of Trusted Computing technology is that it creates a safer environment in cloud computing providing Safer Remote Access through a Combination of mechanism and User Authentication. [12] Trusted computing Protects against data leakage by confirmation of platform integrity prior to encryption and decryption. The Hardware Protection for Encryption and Authentication Key is used by Data (Files) and Communications (Email, Network Access).

The Hardware Protection for individually Identifiable Information such as User Ids and Passwords. It comprises the lowest cost hardware security solution i.e., No Token to distribute or Lose, No Peripheral to buy or Plug In, No Limit to Number of Keys, Files or IDs Protected.

**IV. CONCLUSIONS AND FUTURE SCOPE**

This paper presents a detailed description of the cloud computing comprising various development and deployment models. It highlights the security threats on the clouds such as Abuse and Nefarious Use of Cloud Computing, Malicious

Insiders, Data Loss or Leakage, Service Hijacking, etc. The threats are amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain. Cloud Computing Confidentiality Framework (CCCF) and Trusted Computing Platform provides cloud computing system with some imperative security functions, which include authentication, confidentiality, integrity, communication security and data protection.

Cloud Computing Confidentiality Framework can be extended by adding the analysis of operational and management security controls. Supplemental controls act as limitations in cloud computing environments. Hybrid cloud computing is a very promising cloud deployment model that can cope with the security limitations occurring in a public cloud environment in future.

#### **REFERENCES**

- [1] [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing)
- [2] [http://www.techno-pulse.com/ Cloud Computing for Beginners](http://www.techno-pulse.com/Cloud_Computing_for_Beginners)
- [3] Security and Privacy in Cloud Computing(Lecture 1, 01/25/2010) by Ragib Hasan at Johns Hopkins Universityen.600.412
- [4] USCERT-Cloud Computing Huth Cebula
- [5] [http://en.wikipedia.org/wiki/Trusted\\_Computing](http://en.wikipedia.org/wiki/Trusted_Computing)
- [6] Cloud Security Alliance: Security Guidance Critical Areas of Focus in Cloud Computing, <http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>. April 2009.
- [7] AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING by Anthony Bisong and Syed (Shawon) M. Rahman at International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011
- [8] Cloud Security Alliance: Top Threats to Cloud Computing V1.0, March 2010
- [9] Cloud computing and Confidentiality, W. Pieters and Prof. Dr. P.H. Hartel, University of Twente.s
- [10] Management and Security for Grid, Cloud and Cognitive Networks by Carlos B. Westphall, Carla M. Westphall, Fernando L. Koch: <http://www.fsma.edu.br/si/sistemas.html>
- [11] Cloud computing and Confidentiality, W. Pieters and Prof. Dr. P.H. Hartel, University of Twente.s
- [12] Enhancing Security in Cloud computing using Public Key Cryptography with Matrices Birendra Goswami & Dr. S. N. Singh: [www.ijera.com](http://www.ijera.com) Vol. 2, Issue 4, July-August 2012
- [13] Improving the Security of Cloud Computing using Trusted Computing Technology by P. Senthil, N. Boopal & R. Vanathi : [www.ijmer.com](http://www.ijmer.com) Vol.2, Issue.1, Jan-Feb 2012