CLOUD COMPUTING SECURITY ANALYSIS

Ms. Kavitha D.[1], Rohit Kumar Pathak[2], Saket Bharti[3], Pratyush Kaushal[4], Ajay Kumar Pal[5]
[1]Asst. Prof, [1,2,3,4]Electronics & Communication Engineering,
[5]EEE, MVJ College of Engineering, Bangalore

Abstract
Cloud Computing is the science of architecture for supplying computing services through the internet on request and pay per use access to a pool of sodality instruments. It also goes without saying that this perspective of computing excerpts its personel defiances the major part reverberate being security. Safety concerns herein, birthed by the unveiling of the cloud to various risks, continues to convey hesitance on probable consumers and it is exclusive advisable that such concerns are addressed. Consumers who hand over their data and documents to the cloud want their documents to be protected and secured with the powerful terms and conditions. To build the Cloud Computing extra protected, secured and reliable few steps has to be contracted against the menace of Cloud Computing prototype. This document procures a extensive security and protection expications of Mobile Cloud Computing (M2C) and all the blusters concerned to Cloud Computing is compared along with their believable rectifications.
Keywords: Cloud Computing Security; Cloud Threats; Challenges in Cloud, Authentication

I.INTRODUCTION

Cloud Computing is the process of utilization of computational instruments which includes hardware and software that are conferred as a service over a network. Scilicet, Cloud Computing can be further described as a modern form of computing wherein dynamically gaugeable and often virtualized instruments that are supplied as a services through Internet. Mobile Cloud Computing (M2C) has received rising zest with various defiances striking its negative evolution, principally concerning security, protection and privacy of clients as well as consumers.

[1]. Cloud Computing (CC) is a network of parallel and dispensed by virtualized tools presented as a unit to provide clients with different IT services. Cloud Computing is classified in two different methods one is with deployment of prototype and the another is service delivery prototype

Deployment prototype of the clouds are:
Private Cloud: Private Clouds are given by an institution or their referred service providers and offers them a dedicated operating environment with all the advantages and functionality of flexibility and the availability prototype of Cloud.
Public Cloud: Public Clouds are given by an reffered service provider and may proposed either a dedicated or shared operating environment with all the advantages and working capacity of flexibility and the utility prototype of Cloud.
Community Cloud: It is an associative exertion in which infrastructure is divided amid organisations organisations from distinct community with considerations (cyber security, jurisdiction , etc.) whether managed from outside or inside.
Hybrid Cloud: It is a computing environment that utilizes a blend of other enclosures, private cloud and third-party, public cloud services with orchestration between the two platforms. Service distribution prototype of the cloud are:
Software as a Service: It is a software dispensation prototype in which a third gang granter hosts utility and creates them attainable to consumers over the internet. It is also expressed as SaaS. It is one of the three main classes of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).

Platform as a Service: It is a grade of cloud computing services that confers stage permitting consumers to evolve, execute and manage applications in absentia the complicacy of creating and laying the infrastructure. (e.g., java, python, .Net).

Infrastructure as a Service : The capability provided to the consumer is to rent processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

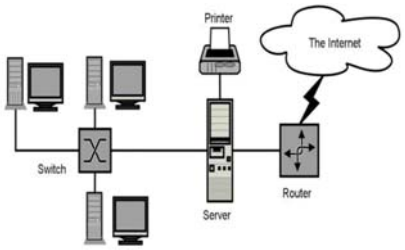

Fig1. An Overview of the Cloud Computing

II.USE CASE SCENARIOS

The SW shop company which manufactures the software for online platform developer and provide services to their customers via online front storerooms to link with them. It has two different ways of operations: backend operations, which comprise the growth and verification of SW and frontend operation, which represents by sale of products manufactured by SW company. 2C-Shop scenario discovers the application of two CSPs co-operating to show SWShop. 2C-Shop will assist us to notice the collaborative interactions between amid CSPs.

A. IC-Shop

In a single Cloud Solution backend and frontend rectifications are confered from single CSP. Amazon Cloud service procured each and every outlay of services. First of all register for AWS services is preparative steps. Security set-up comprises the building of SWShop groups, deciding traffic laws, and building and Amazon Directory with specific Developers. It also permits for the composition of One-Time Passwords (OTP) for company account or their developers.

A separate segment of the AWS cloud was made for SWShop to strike EC2 illustrations with intrinsical trace in the stipulated limit nay than randomly prescribed public IP addresses [6].

As for payment, AWS supplies customers with a choice of pay-as-yougo for the provisioned services. The interfacing authorities in the under mentioned resolutions are:

1) The client, SWShop, represented by an **Admin**, User **Uj** referring to developers in the batch, and User acceding a changeable introduction **TUi**, similar as the role of an online dealer.

2) CSP tools includes AWS management console (**MC-AWS**), personal AWS services (**AWS-Sx**)

B. 2C-Shop

The 2C-Shops utilizes two CSP's: AWS for the backend manipulations and various different CSP X for the frontend manipulations. The interfacing entities to this rectifications are:

1) SWShop described by **Admin**, Developers **Uj**, **TUi**, which qoutes the streaky consumers speculating an absolutely defined preface such as the contribution of a website visitor.

2) AWS instruments comprising **MC-AWS**, and **AWS-Sx**, which refer to individual AWS services.

Fig2. General Architecture of 2C-Shop Solution

The generic architecture for 2C-Shop is shown in Fig.-2 depicts SWShop using the services of AWS and CSP X to show their frontend and backend operation.

As with 1C-Shop scenario, the requirement of **Admin** is to register for both CSP AWS and CSP X services.

III. GENERIC MODEL MC-MODEL

According to the previous sections we introduce a generic model for the M2C. It collaborates with

the multiple CSP‟s and perform tasks for a single client. The interacting entities are following:

1. Client **C**, described by:

Admin which refers to the administrator

Uj, which is an employee of C

TUi, which is a temporal user assuming a pre-defined role such as the role of a storefront shopper

2. For **n** CSPs, each CSP is described by:

MCSPx refers to each CSP X Management Console, where x is between **1** and **n**

3. Financial Third Party, F.

The credentials design for MC-Model is as follows [8]:

C1: Individual user accounts credentials, PWDu, are for login by an individual user.

C2: OTP‟s are provided by an MFA Hardware or software generator.

C3: Username and password (PWDroot) are the login credentials for the root account.

C4: Certified Public/Private key pair (X509-PUK/PRK). The user signs SOAP-protocol requests to service interfaces with his X509-PRK.

For M2C Model, the execution workflow goes as follows:

(1) The **admin** registers for CSPs and creates credentials C1-C7 described above.

(2)**Admin** or individual users **Uj** use credentials from (1) to login to CSPs.

(3)**Admin** or individual users **Uj** request needed CSP services through MCSP.

SSL protects communicated messages secrecy and authentication for steps (1-3).

The interaction is classified into three types:

1. **User to Service (U-to-S)**: A sample of this conversation is when a consumers urge to a service S from a CSP. For this method of interactions, authentication probably confered via Public/Private key pair, X509 certificates, or Secret Keys depending on the service S type.

2. **Cloud Service to another Cloud Service**: There are two seperate methods of this interaction:

Service-to-Service provided by the same CSP (Sto- S): This method of interplay happens when one cloud service S1 urges other service S2 prepared by the same CSP.

Service Sa on CSP X to another Service Sb on CSP AWS (Sa-CSPx-to-Sb-CSPy): This method of interplay happens when one cloud service S1 provided by CSP X demands other service S2 provided by another CSP Y.

3. **User to Management console of CSP (U-to-MCSP):** Security set-up, Registration and the user demanding services from CSP‟s are illustrations of this method of interaction.

IV. SECURITY ATTRIBUTE FOR CLOUD SERVICES

The prototype of cloud computing has altered the manner we utilizes the IT instruments. Cloud computing has cumulatively modified business and government, and framed recent security and safety defiances. The CSA (Cloud Security Alliance) [2] has acknowledged the top nine cloud computing danger for 2013. These dangers are the most fundamental dangers that can be plausible in the recent cloud environment. These are as follows:

1. Data Breaches

The idea of data breach is that any malicious person or unauthorized person enters into a corporate network and stolen the sentient or confidential data.

2. Data Loss

The other valued threat is the potential disability to fend the harm to our data because several of the companies recourse their data as a precious asset.

3. Account Hijacking

A malicious intruder can utilize the stolen credentials to plunder cloud computing services and they can ingress on another transaction, pour fabled data, and deflect users to pejorative web sites resulting in legal disputes for cloud service providers.

4. Insecure APIs

If the Application Programming Interfaces which are employed by the users to transfuse with the cloud services are diminutive or not sufficiently secured, accidental or malicious check up to violate them may disclose the cloud data to numerous security threats respective to rigid approach control, scalability and confined invigilate and several different issues.

5. Denial of Service (DoS)

DoS have become very deep threat when the organizations are incumbent on the services for

24/7. It temporarily negates the approach of data provided in the cloud to the authorized users by making an attack on the server by supplicant thousands of requests to it become unable to respond to the regular clients.

6. Malicious Insiders

Anybody who enters into the cloud network to damage the institutions esoteric data and assets, harms the valuable brands, punishes the pecuniary disservice, checks productivity is known as a malicious insider.

7. Abuse of Cloud Services

This threat is more of an issue for cloud service providers than cloud consumers, but it does raise a number of serious implications for those providers. It might take an attacker to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes.

V. SECURITY REQUIREMENTS

Based on the MC-Model, threat explication, and examinations we made in the previous sections, we descend a set of desirable safety needs for unbroken and influential M2C services. These are nearly affined to Authentication.

A. Entity Authentication

Entity Authentication is to secure that all interacting entity has the recognition it demands. It must be reciprocal, and it must install to all entity interactions (C-to-MCSP, C-to-S, and S-to-S) within the common domain or cross-domains.

B. Message Authentication

Message Authentication assures that information is accepted barring any alteration. It should enforce to all *REQ* and RES informations. Keyed hash significances, Message Authentication Code, or digitally initialized tokens are typical methods used to ensure messages authenticity

C. Continuous Authentication Process

Authentication should harbor through the instruments uses manipulation, which comprises Registration (Identification), introductory authentication during user login to services, and ongoing authentication: as two entities sustain to interact (all *REQ* and *RES* messages).

D. Non-Repudiation (NR)

NR should improve the scale of entrust amid entities such that all their tasks should be undeniable and traceable in series to guarantee impartial rectification of any issue.

E. Elasticity

Elasticity cited as the potence of a system to propogate as demanded in absentia harm of functionality. Elasticity is an latent nature of M2C. A dominant Cloud authentication settlement should sustenance the addition of new Clients, users within a Client, CSPs, or services provided by the CSP.

VI. EXISTING SOLUTIONS TO MANAGING CLOUD COMPUTING SECURITY

1) Mirage Image Management System

The integrity of VM images are the backbone for the entire safety and security of the cloud. In this system use of Filters reduces the threat in a versed method. We propose an image management system called Mirage that exhorts the security concerns adumbration in an effective style[8]. It offers the under-mentioned security management characteristics: A approach control structure that regulates the sharing of VM images. This decreases the publisher's threats of unauthorized access to the Images.

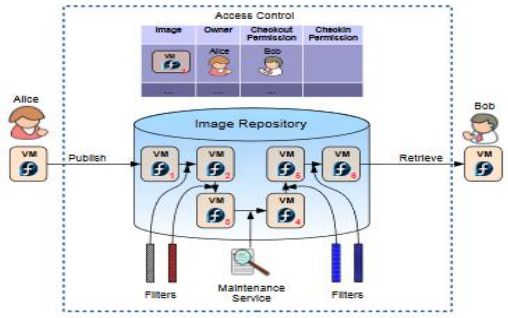

Fig3. Mirage Image Management System

2) Client-Based Privacy Manager

Privacy Manager Software on the client provides assistance to the appropriator to guard their privacy when raching cloud services. The main aspect of the Privacy Manager is that it can confer an obfuscation and de-obfuscation service, to reduce the dose of susceptive data stored within the cloud. In addition, the Privacy Manager permits the user to manifest privacy precedences about the treatment of their personal information, inclusive the intensity and type of obfuscation used. Personae – in the form of icons that correspond to sets of privacy preferences can be used to simplify this process and make it more intuitive to the user. The user personae will be defined by the cloud service interaction context.

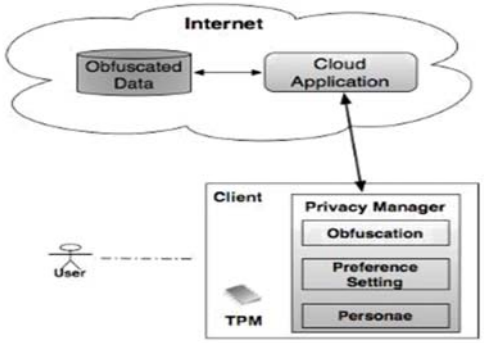

Fig4. Client Based Privacy Manager

VII. RELATED WORK

By the growth of cloud technology it builds a new safety and security challenges that gives direction to several disquisition work in field of cloud security. The CSA (Cloud Security Alliance) released The Notorious Nine [2] in 2013 and demonstrates the top nine threats of the cloud and their persumable solutions. Cloud Standard Customer Council published in 2012 Practical Guide to Cloud Service Level Agreements [3] that handles with the all dimensions of a criterion service level agreement. For the security of virtual environment and the whole virtualization a structure is created with the illustrations of Xen platform [4]. In the shared cloud infrastructure a technology page coloring based cache spliting [5] is used for abscission and resource management in virtualization. To ascertain the resonable security and isolation for diverse tenant user several techniques such as segmentation, introspection and automation are discussed. A honeypot system [7] is a deception trap, designed to entice an attacker into attempting to compromise the information systems in an organization.

VIII. CONCLUSION AND FUTURE WORK

Cloud computing is surely a method of computing pattern that will stays for a long time to come. In the near future, cloud computing can emerge in several dimensions. Though M2C supplies IT solutions to an amplifying number of enterprises and individuals, arising security issues may hinder effective utilization of such solutions. Effective and efficient security solutions should allow more clients to use M2C securely. The main problem with the cloud is about its security model, although it has various features to provide it is still not promising when it comes to security. Implementation of each and every aspect which is discussed in this paper will definitely make the cloud more promising. We can achieve a more secure and reliable cloud services with the proper planning and execution of a robust security model that must have the capability to manage all the layers of cloud.

REFERENCES

[1] N. Khan, *et al.*, "Towards secure mobile cloud computing: a survey," *Future Generation Computer Systems,* vol. 29, pp. 1278-1299, 2013.

[2] Cloud Security Alliance (CSA), The Threats Working Group- The Notorious Nine: Cloud Computing Top Threats in 2013, Available at: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pd f.

[3] Cloud Standards Customer Council- Practical Guide to Cloud Service Level Agreements- Version1.0, Available at: http://www.cloudcouncil.org/2012_Practical_Guide_to_Cloud _SLAs.pdf.

[4] Hanqian Wu, Yi Ding, Chuck Winer, Li Yao- National Natural Science Foundation of China and the Natural Science Foundation of Jiang Su Province of China- "Network Security for Virtual Machine in Cloud Computing", Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4541951&rep =rep1&type=pdf.

[5] Himanshu Raj, Ripal Nathuji, Abhishek Singh, Paul England Microsoft Corporation, "Resource Management for Isolation Enhanced Cloud Services", *CCSW'09,* November 13, 2009, Chicago, Illinois, USA, Available at: http://www.cs.jhu.edu/~sdoshi/jhuisi650/papers/spimacs/SPI MACS_CD/ccsw/p77.pdf.

[6] "Amazon Web Services: Overview of Security Processes," June 2014.

[7] The Government of the Hong Kong Special Administrative Region, "Honeypot Security", Feb-2008, Available at: http://www.infosec.gov.hk/english/technical/files/honeypots.pdf.

[8] I. Khalil, *et al.*, "Cloud Computing Security: A Survey," *Computers,* vol. 3, pp. 1-35, 2014.