Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.528 – 534

RESEARCH ARTICLE

A Multi-Level Security Framework for Cloud Computing

Mr. Anup Date[1], Mr. Dinesh Datar[2]

[1]Department of CSE, GHRCEMA, India

[2]Department of IT, GHRCEMA, India

[1] dateap@gmail.com

[2] dinesh.datar@raisoni.net

Abstract— Cloud computing is a model of information computing, storage, delivery of services and sharing infrastructure resources provided to clients on their demand. Instead of purchasing actual physical devices servers, storage, or any networking equipment, customer used these resources from a cloud provider as an outsourced service. It defined as "a model of management of information, resources and applications as services over Internet as per requirement of clients". Cloud computing is a approach to convenient and on demand network access to a shared group of computing resources that can be provided by service provider in the form of multiple services. It introduces a new Internet-based environment for on-demand access, dynamic provision for computing resources by using various type services on cloud. These models are referred as Software as a Service, Platform as a Service and Infrastructure as a Service. Just because of that it is tough to manage the security and privacy problems in cloud caused by its sensitive data, outsourcing of infrastructure, multi-tenancy nature, and critical applications. This paper proposing a framework that identifies and summarize the security and privacy challenges in cloud services. It highlights cloud-specific attacks and risks and clearly illustrates their mitigations and countermeasures. This is also highlight a multilevel security framework for cloud computing that helps to satisfy security and privacy requirements in the clouds and protect them against intruder attacks. The purpose of this work is to demonstrate and introduced a security and privacy aspect that will take into considerations while developing and using the cloud environment either by individuals or organizations.

Keywords— Cloud Computing, Security and Privacy, Security framework, Threats

I. INTRODUCTION

Cloud computing is one of the rapidly and most acceptable growing areas of information technology. It is a new computing and processing scheme which available on Internet "Cloud'. Cloud computing is a way to delivering the convenient on demand network access to a shared band of computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction[2]. Cloud computing is categorized into two main parts: Front End and Back End. Front End is customer or client or any application (i.e. web browser etc.) which is uses the cloud services and Back End is the network of servers with a computer programs and data storage system [1].paper guidelines, please contact the

conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. CLOUD COMPUTING SERVICE MODEL

In cloud computing almost every things being delivers as a Services from access to security. The cloud is conflagration of buzzwords "as a Service" [3]. There are three types of services which are very special ongoing days.

A. *Software as a Service*

Its means to deliver the various types of software's on internet as a services. It is comes in reality around in early 2001 when it was referred as Application as a service [3]. In SaaS model, the user buys a subscription to some software product and services but these data and code available on remote server and customer can access to this services via Internet [8]. It provides the computation power in the form of software services on cloud multiple clients. Clients can use the various applications on cloud but cloud users doesn't have right to manage them. Ex. Google, salesforce, Microsoft and Zoho etc.

B. *Platform as a Service*

Its gives chance and flexibility to build, develop, test and deploy an application on service provider's machine or platform whether it's API, Storage or Infrastructure [3]. The freedom provided to the customer to create and acquire an application created using either different programming languages or tools supported by the provider [10]. Customers get access to the platform by enabling them to organize their own software and application in the cloud [4]. It reduces the cost and complexity of buying, housing and managing hardware and software components as a platform to the clients [5]. Service providers are only responsible for integrity and availability of their services where as the users responsible for confidentiality and privacy [8]. Ex. WAMP (Windows, Apache, MySql, and PHP) LAMP(Linux, Apache, MySql, and PHP)

C. *Infrastructure as a Service*

SaaS and PaaS are providing application to customers where as IaaS simply offer hardware support to customer where they can put whatever they want onto it [8]. It offers access to various fundamental resources such as available in the form of networks, servers, storage devices, computational resources and many more. The clients doesn't have authority to manage these fundamental resources over the cloud, users can just used them [4]. Ex. Amazon, GoGrid and 3tera.

III. SECURITY ISSUES WITH CLOUD COMPUTING

The security means to protect and get secure from unauthorized access, uses, disclosure, disruption, modification, perusal, inspection, recording or destruction [1]. Cloud computing has grown rapidly in various aspects including services, architecture, computing and storage due the utility of such things the security issues can be viewed as problems.

A. *Account or Service Hijacking:*

Hijacking refers to get complete control over others account and it is not new to the today's world but the attacks like phishing, fraud and exploitation of software are need to avoid [1]. If any intruders get an access to any other account then security of account is lapsed completely and activities like deletion, updating data, and manipulation with account data create lots of burden to its account holder as well as the manger (cloud). The person who is carried out such things beings identified by the name of Intruder or Hacker. And it has been observed that mostly hacker will take an advantages of silly mistakes performed by cloud users such an not proper log off of service windows, allows additional plug ins even they are not be a part of cloud services, access illegal sites simultaneously with using on cloud services, share and distribute financial and personal information to other people etc.

B. *Unknown Risk Profile:*

Information about who is sharing infrastructure may be relevant in addition to network instruction logs, redirection attempts and other logs, but low effort of security may be it can result in unknown exposures [3]. To track the unknown profile is tedious job. So its responsibility of cloud providers to verify every users before to allow them to be a part of cloud and for that cloud providers may used telephone versification, email verification, or social network account verification and if cloud services related to financial sector then cloud providers may refer his banking or financial

information as well. It will not give guaranty to stop all fraud but at least it restricts someone. Due to this cloud contain unethical and uncontrolled account which generate misbehave on cloud.

C. *Shared Technology Issues:*

IaaS deliver the service of sharable infrastructure between multiple users. The underlying components such as CPU and Memory were not designed to offer strong isolation properties. To address this gap a virtualization hyper visor between guest operating system and the physical compute resources [3]. Strong compartmentalization must be implemented to avoid the access and control over the sharable infrastructure and the individual customers should not impact on other customers operation.

D. *Architecture of Cloud Server:*

The actual location of the infrastructure such as computing servers, Data servers, Hardware's is determined by the cloud service provider. The implementation of reliability, scalability logic and virtual machines (VM) typically to serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture [5]. A VM or hypervisor is the additional layer between Operating system and Hardware and sometimes these supports to take control over the administrative operations like migration, launching and end up the process of VM objects. If any individual get command over the other's VM object then it will create a major problem.

E. *Identity Management:*

The proper identity of customer will help to manage the uniqueness of each user and to carry out such things the different levels of user authentication and validation schemes being implemented in cloud but still the access control will create a threat. Apart from authentication the identity management should have control over the user's privileges and access to required resources [5]. Cloud should have capability to formulate and maintain user privileges about its access and task that user will performs on cloud as a part of identity management [5].

F. *Insecure Interface and API:*

The cloud providers deliver the cloud services via different interfaces and API where customers have freedom to choose interface and interact with cloud services. It's been observed that the security and availability of general cloud services is dependent on the security of interfaces and API [1]. Some time cloud users share their interface and API to access the cloud services and due to the week knowledge of security aspects, users will allow to such interfaces to store and use their personal information in the form of remember password, transaction history, scripts, cookies and additional plug inns. So its responsibility to cloud provider to invent an API and interface in such a way that interface need only meaningful information of users to provide access to cloud services and do not store user's personal information such as passwords, cookies, scripts, transaction history even user wishes to do it.

IV. FRAMEWORK FOR CLOUD COMPUTING

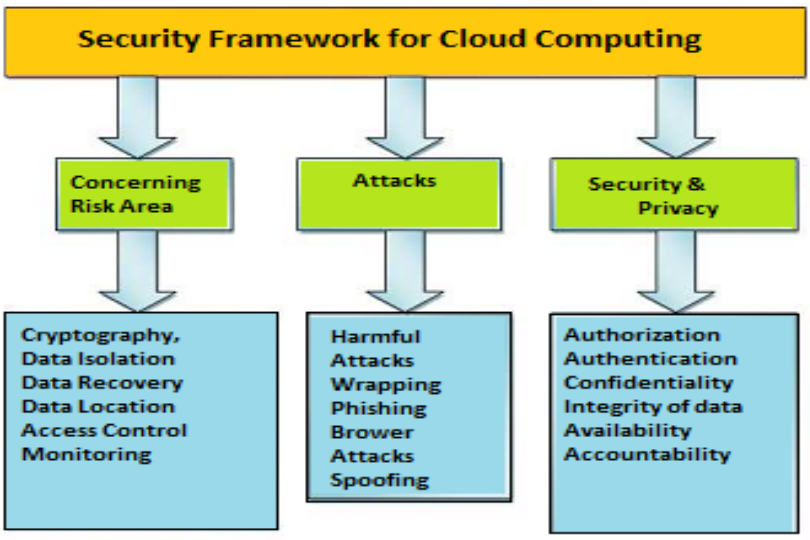

Fig 1: A framework for secure cloud computing.

Above figure shows the essential security components such as

A. *Authentication:*

To provide authenticated access to cloud is the major issue in the cloud environment. To manage this problem there is need individually verification and validation. Authentication is one of the process that keep data away from unauthorized users and it typically identity-based, which makes authentication of the user's identity [5]. When cloud users logon to their accounts the Authentication system get activated and identify whether user if genuine user or not [2]. For authentication usernames and passwords are used to access the cloud.

B. *Authorization:*

It is a process where privileges are allocated to cloud users as per their login status and role they want to play on cloud. Sometime User authentication and chosen service on cloud will decide the privileges for customers and according to that user authorization gets a shape. As per the norms of authority the customer can do and manage the things on cloud. The Authorizations will decide what operation and task will execute by user.

C. *Confidentiality of user:*

It refers only right user get command and access over the things in cloud. It specifies that the genuine customer should get the access to the resources like computation, infrastructure, data storage and application handling.

D. *Availability of resources at location:*

It indicates that all resources whether they are logical or fundamental they should make available to respective customer wherever and whenever they needed. Only authenticated and authorized user should get access of the resources.

E. *Integrity of Data:*

It is responsibility of cloud server to maintain the accurate computing of data that comes from integration of various files and deliver it within specified time. While performing this operation the cloud should make sure that there I provision for error during computing. Also there should be some mechanism that can assure the customers that whatever data will be stored on the files servers will not hampering any other data elements [1]. Additionally it also specify to protect cloud data and applications from unauthorized deletion, modification, theft, falsehood or abused [2]. Integrity may come from the accuracy, Isolation, Atomicity, completeness, availability, Consistency, and Durability of a data.

F. *Harmful Attacks:*

An attack can happen in several ways on cloud and every attacker come to spoil the things on cloud. Someone randomly create a threat on cloud and someone do it by specific intention. These attacker either come to collect the valuable data present on cloud or to disturb the behaviour of cloud by introducing the spoiling agents like virus, malwares etc. These attacks may follow then Unethical Browsing and wrapping of data. Wrapping of data means attacker wrap the communication between two people in such a way that the individual feels that the data comes from original sources but actually it's being designed by attacker not by original source. Unethical Browsing means where bad actions being happens such as phishing, spoofing, alteration of browser certificates etc [2].

G. *Concerning Risk Area:*

It specifies the things related to access control, Monitoring of data, changing of data format (encryption and decryption), data isolation and many more. It exposes the new era of concerning risk. Data Isolation, Data recovery and data location is one of them. Data isolation means every individual will enjoy the separate copy data elements like maintain by any database. Data Recovery is ability to restore and recover the data if a disaster occurred [2]. Data location is nothing but the data should maintain and store in the same geographical regions where user belonged i.e if any user comes from India and its data should manage and store in the same territory so data will not be spread to some another one because norms and regulation may violet according to the territory.

V. MULTILEVEL SECURITY FRAMEWORK FOR CLOUD COMPUTING

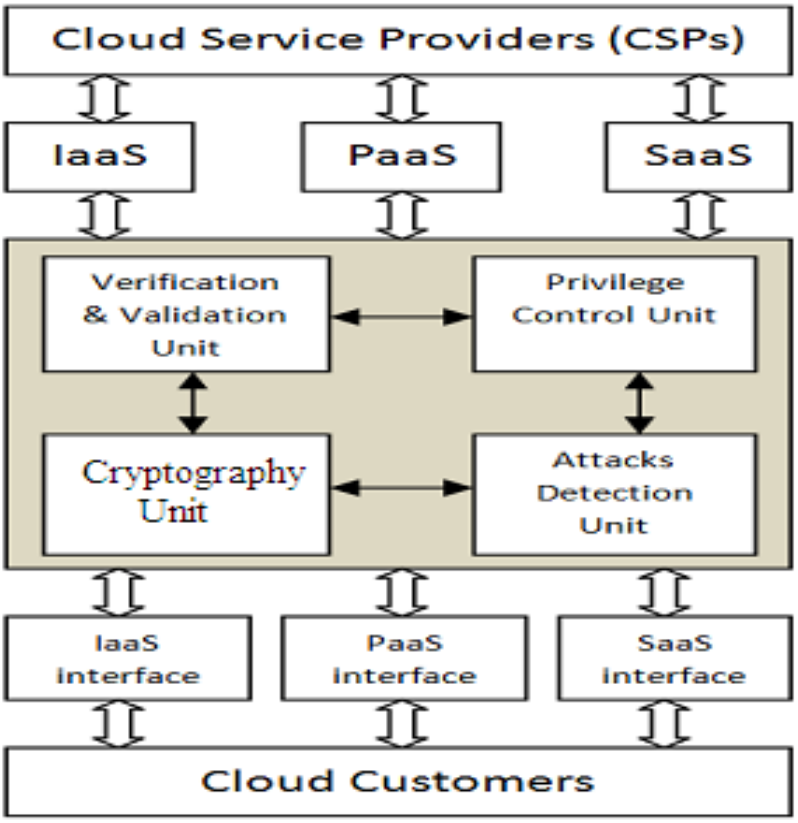

Fig 2: Cloud Computing Security Model

The above figure stated as the multilevel security model for cloud computing by introducing the security and privacy instruments in cloud to protect the cloud against external crisis.

A. *Verification and Validation Unit:*

The main task of any cloud security is to verify and authenticate the genuine user and to ensure that the correctness of data and services on the cloud [2]. Here the user authentication mechanism will identify the user and allocates privileges and authorization as per the prescribe norms. To maintain the authentication of user on cloud we can implements various techniques such as simple user name and password protection scheme, Graphical passwords protection scheme or bio information based user authentication as per the requirements of data and cloud services. Digital signature is one the era of user authentication and authorization where documents being verified on the basis of digital signature to maintain the secrecy.

1) Provide Secure Interface

During verification and validation of user most of the Interfaces and API are stored the user personal information such as remember password, transaction history, scripts, cookies and additional plug inns without concerning or with concern to users. This information some time will access by cloud service provider to track the client and maintain the web traffic records. Sometime it will reach to intruder and entire securities of user as well as service provider get leaked to the outside world. So its responsibility to cloud provider to invent an API and interface in such a way that they will need only important information of users to provide interaction with cloud services and do not store user personal information such as passwords, cookies, transaction history even user wishes to do it.

B. *Privileged Control Unit:*

On cloud there are millions and billions of users who are performing thousands of operation of same or different data element in a same or different area of computing. To manage the privacy and secrecy among these people is really a tedious job. Here privileged based separation will reduce the burden of mixing. This unit is essential because it protects users' privacy and security. It ensures that data integrity and confidentiality by applying a set of regulations and policies that govern the authorization process of cloud users [2]. Only authorized customers get access to data. Privileges set by cloud service provider as per the security norms fulfilled by services users. Privileges may verify time to time using public key encryption.

1) Policy Approach:

In this framework the cloud should make a decision about to enforce privacy protection mechanism publically or privately to the access of data stored on cloud server either concerning to user or automatically [6]. Every user should specify the private or public access to all its data. Every file, documents, or data unit should consist of these policy norms, and if any user forgets to specify security policy then automatically security norms being allocated to its all data elements on cloud server. If any other person want to access data preset on cloud but it belongs to other user then policy approach will take into consideration and as per the security approach if data is available publically then other user will get access to it otherwise access should denied to that documents or files. Important documents such as financial data or personal data may be protected by introducing the run time alert on user's mobile phone.

C. *Cryptography Unit:*

Data always stored in the encrypted format which encrypted get at the time of data uploading on the cloud either by single key or double key (public key) encryption. The cloud will maintain the unique random key generator so every user on cloud will have unique key for data encryption and decryption purpose. Standards for communication protocols and public key certificates allow data transfer to be protected using cryptography [5]. Only cryptography is not the single solution to privacy for cloud provider should invent used standards protocol for communication. Without a properly designed auditing protocol, encryption itself cannot prevent data from flowing towards external parties during the auditing process [3]. It will help to maintain the unique access to data. Whenever user want to access the data then every time this user will get his decryption key via E-mail on his registered mail id registered at the time of creation of account on cloud. Techniques for data protection such as truncation, redaction, obfuscation, and others can be used in this security component [2].

D. *Attack Detection Unit:*

This unit is responsible to stop the unwanted operation carried out by intruder on physical or logical resources of the cloud. To stop the attacks first there is need to detect and identify the type of an attack. This unit is identify the software attack by introducing the software based solution such as log file information, history, web analytics, IP address, Mobile No, decryption key, Service provider and other things being implemented in the software security form.

VI. CONCLUSION

Cloud computing brings the application software's and databases to servers on the Internet, where the management of the data and services are not reliable. And as we moving forward to the direction of cloud computing the security and privacy issues will generate day by day in the area of computation, storage management, infrastructure handling, input/output management, resource utilization and authorized user activities. A cloud computing has its own security threat problems and such threats are completely different from threats in physical system due to this to attaining the high assurance qualities in development and implementation is an mysterious goal for computer security researchers and practitioners. So this is an important and essential factor to fulfil the security and privacy requirement while designing and implementing the cloud. In this paper it's explained that if we implement the multilevel security framework on cloud then customer can enjoy the outcome without any worry. Here we tried to identify security and privacy requirement, threats, concerns issues, risk associated to cloud and multiple security frameworks which somewhat complete cloud security requirement. Apart from this it is responsibility of cloud users and cloud provider organizations should enforce some security and privacy policies to protect cloud. There is wide scope for researcher and developers to introduce the new era knowledge in the area of security and privacy of cloud and it will bind strong and secure relation between cloud users and their vendors.

REFERENCES

[1] Harish shah, Shrikant, Sharma Shankar Anadane, "Security Issues in Cloud Computing".

[2] Ahmad Youssef, "A Framework for secure cloud computing", IJCSI international Journal of Computer Science, Issues, Vol 9, Issues4, N0 3 July 2012, ISSN(Online) 1694-0814, www.IJCSI.org

[3] Ramasami S., Umamaheshwari P., Survey on data security issues and data security model in cloud computing, International Journal of Engineering and Technology (IJEIT), Volume 1, issue 3,March 2012.

[4] Ayesha Malik, Muhammad Moshin Nazir, Security Framework for cloud computing environment : A review, Journal of engineering trends in computing and information sciences, vol. 3 No. 3 March 2012, ISSN 2079-8407.

[5] Wayne A. Jansen, NIST, Cloud hooks: Security and Privacy in cloud computing, Proceeding of the Hawaii International conferences on System Sciences-2011.

[6] Furukawa jun, Furukawa ryo, Mori Kengo, Mori Takuya, Toshiyuki, Araki Toshinor, "A Privacy-Protection Data Processing Solution Based on Cloud Computing", NEC Technical Journal, Vol. 8 No.1, Special Issue on Solving Social Issues through Business Activities

[7] Summathi M, Shravan G.S, Dinesh H.A, Implementation of Multifactor Authentication System for Accessing Cloud Service, International Journal of Scientific and Research Publication, Volume 3, Issues 6, June 2013.

[8] Sh. Ajoudanian , M.R. Ahmadi, "A Novel Data Security Model for Cloud Computing". ISCSIT International Journal of Engineering and Technology, Bol. 4, No. 3, June 2012.

[9] Masayuki Okuhara, Tetsuo Shiozaki, Takuya Suzuki, " Security architecture for Cloud Compting", FUJITSU Sci. Tech. J, Vol 46, No. 4, PP. 397-402 (October 2010).

[10] Ali Newaz Bahar, Md. ahsanHabib, Md. Manowarul Islam, "Security architecture for Mobile Cloud Computing", International Journal of Scientific and Knowledge Computing and Information Technology, 2012-13, IJSK & KAJ, July 2013, Vol. 3 No. 3.

[11] Kangchan Lee, Security Threats in Cloud Computing Environments, International Journal os security and applications, Vol. 6, No. 4, October 2012.

[12] Abdul Raouf Khan, Access Control In Cloud Computing Environment, APRN journal of Engineering and Applied Science, Vol. 7, No. 5 May 2012, ISSN 1819-6608.

[13] Amir Mohamed Talib, Security Framework of Cloud Storage Based on Multi Agent System architecture: Semantics Literature Review, Computer and Information Science, Vol. 3, No. 4, November 2010, www.ccsenet.org/cis.

[14] Peter Schoo, Volkar Fusening, Victor Souza, Marecio Melo, Paul Murry, Herve Debar, Challenges for Cloud Networking Security, 2nd International ICST Conferences on Mobile networks and Management, September 22-24, 2010, www.springerlink.com

