Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ADDRESSING SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

S.SUDHA[1], V.MADHU VISWANATHAM[2]
[1]Asstt prof (sr), School of Information Technology and Engineering
[2]Assoc. Prof., School of Computer Science and Engineering
VIT University, Vellore, India
E-mail: [1]sudha.s@vit.ac.in, [2]vmadhuviswanatham@vit.ac.in

ABSTRACT

Cloud computing offers a new way to deliver services while significantly changing the cost structure underlying those services. This new technical and pricing opportunities change in the way the business operate. It combines the features of traditional computing technology like grid, parallel and distributed computing and so on. The aim of cloud computing is to provide a high performance computing system to the customer with the low cost without relying on their own infrastructure. The cloud offers the various levels of services like Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) & Infrastructure-as-a-Service (IaaS) to the customers over the internet. Since all the services are offered over the internet, there is a great deal of uncertainty about security and privacy at various levels are arises. This extensive survey article aims to address security and privacy issues threatening the cloud computing adoption at the end user at the various levels (network, host, and application and data levels).

Keywords: *Network Level, Host level, Application level, Data level, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS)*

1. INDRODUCTION

The popularity of the internet evolved many new technologies of which the cloud computing is one of the emerging paradigm that attracts many industries. Cloud become popular due to its unique features like dynamic massive scalability, elasticity, measured service and self provisioning of resources. According to the NIST definition, cloud computing can be defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources.[1] Cloud computing provider provides services based on three fundamental service delivery models and cloud model can be deployed based on four deployment models.

An Infrastructure-as-a-Service (IaaS) model provides the capability to provision the computing and storage resources on demand by customers. The customers are able to deploy and run the software which includes operating system and other applications. The customer manages the underlying operating system, developed application, storage and some selected network component, but they don't control the cloud infrastructure. Cloud providers bill the IaaS customers based on number of resources allocated and consumed by them. Security consideration for IaaS includes the management of virtual resource allocation and addressing the virtualization vulnerabilities and risks that affect the IaaS delivery model.

The Platform-as-a-Service (PaaS) model provides the computing platform and solution stack as a service to the customers. The customers are able to develop their applications without purchasing and managing the hardware and software necessary for their application development. The complete life cycle support for delivering applications and services are provided by the PaaS model. The customer has control over the deployed applications and application hosting environment configurations, but they do not manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage. Security considerations for PaaS include access and authorization issues, working with distributed applications, storage and data security.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Software-as-a-Service (SaaS) model allow the cloud users to access the applications from cloud providers. This eliminates the cloud users to install and maintain the application that runs on their own local computer. The applications are mostly accessed by users using thin clients via the web browser. The customer has control over only their application configuration settings. The underlying cloud resources should be managed and controlled by the cloud providers. SaaS are used as common delivery model for most of the business applications like Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Human Resource Management (HRM) and so on. In effect, there should be more focus provided for access control and identities for accessing the enterprise applications in cloud. SaaS Customers are billed based on the usage in monthly or yearly basis. [2]

All these cloud services are accessed via the cloud clients such as desktop, laptop, smart phones, tablets and wireless sensor nodes which are connected to the network. Irrespective of the service models, the four deployment models offered by the cloud computing are private cloud, public cloud, hybrid cloud and community cloud. Each model has its unique features and characteristics that meet the cloud user's particular requirement.

In the private cloud deployment model, the cloud infrastructure solely operated for the specific organization needs. A private cloud customer can have a high degree of control and supervision of the physical and logical security aspects of the private cloud infrastructure—both the hypervisor and the hosted virtualized operating systems. With that high degree of control and transparency, it is easier for a customer to comply with established corporate security policies, standards, and regulatory compliance. Private Cloud players are combination of the big technology companies such as HP, IBM, Cisco, EMC and VMware.

In the Public cloud deployment model, the cloud infrastructure like various applications, storage and other resources are offered to the large industry group and it is managed by the third party vendor who is responsible for the public cloud service offering. Hence, the customer of public cloud has a low degree of control and oversight of the physical and logical security aspects of a public cloud infrastructure. Google, Amazon web services and IBM's blue cloud are examples of public cloud service provider.

In the Community cloud deployment model, the cloud computing infrastructure is shared by the multiple organizations from the specific community with common concerns like security, policy and compliance requirements. It may be managed by an organization or by a third party vendor and it may be hosted on-premise or off-premise. It offers the advantages of the private cloud, without its heavy costs.

In the hybrid cloud deployment model, the cloud infrastructures are combination of private, public and community cloud. This model presents the opportunity to store sensitive information in a private cloud and non-sensitive information in a public cloud. It helps to provide varying levels of security, control and scalability.

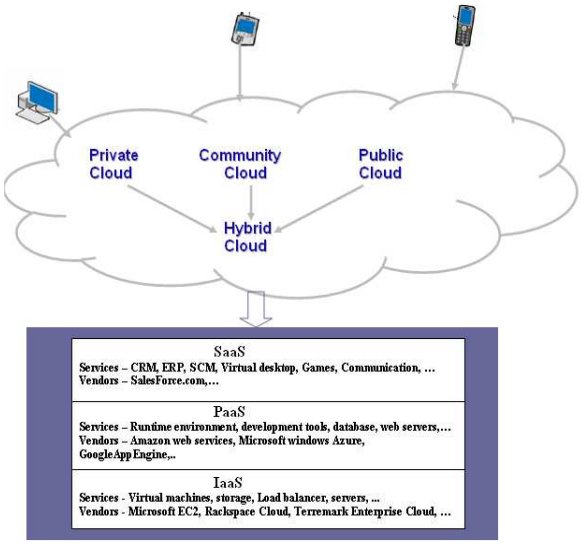

Figure1: A Cloud Model Represents Three Cloud Services and Four Deployment Models.

Services provided through the various cloud models are still evolving and barriers are being overcome and enablers are being developed. A major concern in the cloud models is to trust the cloud customer's information is both secure and private. Establishing this trust is a major milestone in the adoption of the full range of cloud computing.

t.org E-ISSN: 1817-3195

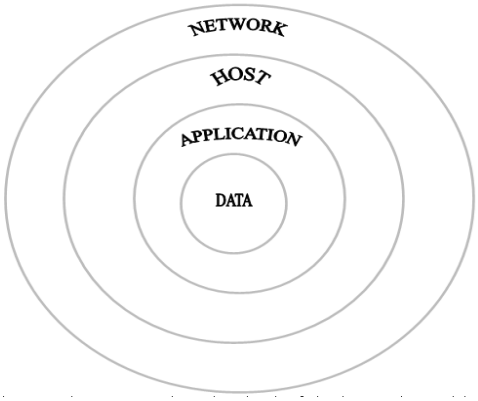

Figure2: Security Concern at the Various Levels of Cloud Computing Model

Figure2 denotes the security in depth at the various levels of cloud computing [6].This layered architecture helps to increase the survivability of a cloud environment in the event of an attack. This paper aimed to provide the detailed discussion on the security threats, challenges and guidance associated at the various levels based on the layered architecture. The paper is organized as follows. Section 2 discusses the security threats and challenges at the network, host, application and data level. Section 3 discusses the privacy concern related to cloud adaptation. Section 4 discusses the Identity and Access Management model in cloud. Section 5 discusses some of the current security solutions used in cloud. Section 6 presents the conclusion arrived from this survey.

2. SECURITY THREATS AND CHALLENGES IN CLOUD

2.1 Network Level

When discussing on the network level security, it is important to differentiate between public and private clouds. Since private cloud infrastructure lies within the organization boundaries, the customer has more control over the cloud infrastructure. This implies that there are no new attacks or vulnerabilities are possible in private cloud. However, in the public cloud environment ensuring proper access control, ensuring confidentiality and integrity of the customer's data in transit, ensuring availability of internet resources are the major risk factor needs to be considered to ensure the network level security. The network-level risks exist irrespective of what types of cloud computing services are being used. [4]

2.1.1 Ensuring proper access control:

The following security loopholes that may affect the access control restrictions of cloud resources.

Issue with reused IP addresses: With respect to cloud provider the IP address is the billable entity. It will be reassigned and reused by new user when the existing users no more using that IP address. From the customer perspective it can pose the security risk to their resource access by some other user due to the time delay between the change of an IP address in DNS and clearing that address in DNS cache. The similar time delay may occur for changing physical address in ARP tables and clearing that address from an ARP cache. With the impact of this issue, the Amazon web services a leading cloud provider has announced the elastic IP address, by which the customers are assigned with a set of routable IP address and they have control over that IP address until they release it. [7] However, the issue can persist in non-routable IP addresses where the customers can reach the provider's network via the private address. [8]

Limited auditing capability: An organization using a public cloud irrespective of any type of service models face the significant risk in their data. They have limited ability to access the network-level logs and audit the cloud provider operations. [4]

2.1.2 Ensuring confidentiality and integrity of customer data

Each customer data in the public cloud environment are exposed to internet, create the significant risk in ensuring the confidentiality and integrity of their data. According to the Amazon web services security vulnerability report, the AWS signature version 1 proven as insecure and the customers are requested to switch to AWS signature version 2 or switch to HTTPS would mitigate the integrity risk. [9]

Attack against SSL\TLS: Secure Socket Layer and Transport Layer security is the protocol used to create an encrypted channel to provide communication over the public cloud. Many cloud providers support this protocol to provide secure communication. The researchers Juliano Rizzo and Thai Duong presented a new attack by which the hackers are able to break the SSL encryption in million of websites. This attack named as BEAST (Browser Exploit Against SSL\TLS). It is like a Trojan horse attack where attacker inserts a bit of java script code into the web browser and java script combine with network sniffer to destroy the HTTPS connection. [10] This implies that even HTTPS cookies are no longer safe.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1.3 Ensuring availability of internet facing resources

Reliance on network level security has increased because most of the customer data is stored in cloud provider premises. There are many factors which affect the availability of public cloud resources that are being assigned to your organization.

DNS attacks: Several forms of DNS attacks may increase an organizational risk at the network level in cloud computing because of increased number of external querying. DNS cache poisoning attack make the name server to return the wrong IP address by which it divert the traffic to other computer. It is recommended to use the IP address for the cloud computing services that requires highest security. But using an IP address is not always feasible. DNSSEC (DNS security extension) is used as a security measure to protect cloud computing services from cache poisoning attack. It allows the DNS server to provide support for digitally signed messages. However, DNSSEC does not help to protect DNS server from DOS and DDOS attacks.[11]

IP spoofing Attack: It replaces the source IP address in the IP packet header with the fake IP address by which it hide the identity of real source entity and make destination feel that the packet has arrived from different computer. It is used for sending spam mails and to launch DOS attacks. Non-Blind, blind spoofing, Man-in-the middle are the variations of IP spoofing attacks. [12]

Attackers and target machine are resides on the same subnet in Non-Blind spoofing. The attacker sniffs the existing transmission in order to understand the sequence\acknowledge cycle between target machine and other host. Once the sequence number known, the attacker can hijack the session and easily bypass the authentication mechanism. The attacker resides outside the target machine in blind spoofing attack and sends the multiple packets to the target in order to understand sequence number order.

The Man-in-the-middle attack intercepts a legitimate communication between two hosts. Then, the attacker controls the data flow and alters the information being exchanged between two hosts without the knowledge of either the original source or the destination.

Halton and Basta (2007) suggested one method to prevent IP spoofing by means of encrypted protocols wherever possible. [13] Jonathan Hassell suggested top five ways to prevent the IP spoofing in his article [14].

BGP prefix Hijacking, a misbehavior in which a malicious or misconfigured BGP router originates an IP prefix that announces the false network layer reachability information. This attack is become an increasingly serious security problem that affect the availability of cloud computing resources. Zheng Zhang, Ying Zhang, et al proposed a mechanism for automatic reactive *mitigation* mechanism in response to detected attacks.[15]

ARP cache poisoning attack: This attack broadcast forged ARP replies on a local network by which it fool the network nodes. This can be done because lack of authentication feature in ARP, thus blindly accepting any request and reply that is received or sent. To protect a hosts ARP cache from being poisoned it is possible to make it static. One way to prevent an ARP cache poisoning is to make static MAC cache, it will not process any ARP Replies received unlike a dynamic ARP cache. But this is not possible for large networks as the correct IP address to MAC address association of each and every host should be present in the cache of every host before it is made static. It is possible to detect ARP cache poisoning attack using an Intrusion Detection System. Arpwatch is a tool that will monitor any change in a MAC address to IP address association in a network. [16]

2.2 Host Level

Host level security issues are those which affect the host infrastructure when it is affiliating itself to the cloud computing environment. Security challenges at host level can be considered in the context of different service delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid).[4]

Threats that are specific to cloud computing at the host level are directly related to virtualization vulnerabilities like VM escape, threats to hypervisor due to weak access control caused in public cloud environment.

2.2.1 IaaS Host level security:

The IaaS customers are the primary responsible for securing the host provisioned in cloud. The following are the host level security issues related to IaaS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Hypervisor security threats: Hypervisor is the software that enables the virtualization. Ensuring the integrity and availability of the hypervisor throughout its entire life cycle are important in public cloud environment. It is possible for "zero-day vulnerability" in VM if the attacker controls the hypervisor. Therefore it is important to check that the hypervisor software is up-to-date and locked-down as per the best practice. [17]

Perimeter security issue: In a cloud computing model, providing perimeter security like firewalls in a virtual environment is little more complex than in a normal network because some of the virtual servers may present outside a firewall. This will be the responsibility of the service provider. Even if the cloud host is included within the perimeter the attacker inside the perimeter may hack the system. This perimeter security issue may not be too hard to solve because virtual resource spaces can be isolated. However, this approach creates a constraint on how provisioning is carried out.

Virtual machine security: IaaS customers have complete access to the virtualized guest VMs which are hosted and isolated by hypervisor software. Therefore the IaaS customers are accountable for security management of the guest VM. Cloud service provider recommends the customer to use SSH to manage the VM instances. The attacker may steals the SSH private keys that are used to access and manage virtual instances. This can be eliminated by storing the private keys on system in an encrypted form. [4] Other host security threats related to virtual machine security is attacking the vulnerable services like FTP and NetBIOS. It is recommended to run only the necessary services and turn off the unused services that are not required. Some more security threats like capture user accounts that are not properly protected with strong password, attack the systems that are not properly protected by host firewalls and deploy trojans embedded in the VM software component or within the VM image itself.[4] Cloud service provider must ensure that the strong operational security procedures are followed to secure the virtual machine from these threats.

2.2.2 PaaS and SaaS host level security

Cloud service providers do not share their host platform and the host operating system with their PaaS and SaaS customers. Hence, host security responsibility is transferred to the cloud service provider. PaaS and SaaS customers should get the appropriate level of assurance from the cloud service provider about their host security. [4]

2.3 Application Level

Many of the industry and academia people are eager to host their applications ranging from computationally intensive to light weight application on a cloud model to save money and to increase efficiency and reliability of their applications. However, due to the lack of access control over the networking infrastructures including servers, access to audit logs, patch management make the cloud applications are more vulnerable to the various security threats. Web application developed and deployed in private cloud must be protected from the external hackers by providing appropriate access control at the network and host-level. Web application built in a public cloud must be designed to use secure software development life cycle and need to guarantee that API's have been thoroughly tested for security. [5] The following security risks are identified in web application by the Open Web Application Security Project (OWASP). [18]

- Injection
- Cross-Site Scripting(XSS)
- Broken Authentication and session management
- Insecure Direct Object References
- Cross-Site Request Forgery
- Security Misconfiguration
- Insecure Cryptographic storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

2.3.1 OWASP Top-10 security threats:

Injection: Injection Flaws like SQL, OS and LDAP injection can occur when web application sends an untrusted data to the interpreter as a command or query. This often occurs in SQL and LDAP queries and OS commands. Injection can create a huge data loss and lack of accountability. Injection can be prevented by using secure API's

Cross-Site Scripting (XSS): XSS flaw occur when a web application sends the untrusted data to the web browser without proper validation and escaping. Hackers can hijack the user session and redirect the users to malicious sites and spoil the website appearance by executing the scripts in the user's web browser.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Broken Authentication and session management: The weakness in the authentication and session management in web application can allow the hackers to exploit the information such as compromising the password, keys and session tokens.

Insecure Direct Object References: Authorized user modifies the parameter value that directly refers to a system object to other object for which the user not authorized for. The attackers try to modify the portion of the URI and examine the result. This attack can be prevented by properly verifying whether the user is authorized to access the target object.

Cross-Site Request Forgery: It is type of malicious use of a website whereby unauthorized HTTP requests are sent from a user that the website trusts. The attack includes a link or script in a page that accesses a website in which the user is authenticated.

Security Misconfiguration: This attack happen when database administrator or developer leaves a security hole in the system configuration. Attacker access default password, unused patches, files and directories and try gain the knowledge of the system. It is recommended to change the default password when the OS or server tool is installed in the system. Deleting unused files, turnoff unused services and keeping up-to-date patches will help to prevent this attack.

Insecure Cryptographic storage: This attack happen when the application not securely encrypted its sensitive data stored in database. Even the encrypted content can be accessed due to the weak key generation, non rotational keys and weak encryption algorithm.

Failure to Restrict URL Access: A most common risk in web application is failing to restrict URL access which typically occurs when a web page doesn't contain appropriate access control policy in place. This vulnerability exposes privileged functionality into unauthorized users. The attackers are able to find even hidden pages using forced browsing technique. It is suggested to employ role-based authentication and authorization in appropriate place and implement security at both client and server side.

Insufficient Transport Layer Protection: Insufficient Transport Layer Protection provides the ability to monitor the network traffic by hackers. Hence, the hackers can compromise web application and steal sensitive information. The SSL\TLS could be used only during the account authentication, but not elsewhere, expose the data and session id are able to be intercepted. The weakness in cryptography and mis configured or expired certificate vulnerabilities lead to the exposure of user information.

Invalidated Redirects and Forwards: Web applications more often redirect and forward the victim to other web pages or websites. Without the proper validation hackers can redirect the victim to malware sites or use forwards to access unauthorized web pages.

Other than Top 10 security risks pointed out in OWASP, there are some more security threats at application level are captcha breaking, application level DOS and EDOS attack and Google hacking.

2.3.2 CAPTCHA breaking:

CAPTCHA (Completely Automated Public Turing Test to tell Computers and Human Apart) is a method to perform simple challenge-response test to the user before they gain access to the specific cloud service. CAPTCHA generates the random string image that can be easily understandable by human. However, it makes very difficult for the computer or bots to understand the code and get authorized to access the cloud service. Now a day even CAPTCHA breaking is possible by using various methods like reuse of session-id of known image, optical character recognition technique and cracking MD5 hash of CAPTCHA solution. [19]

Application level DOS and EDOS attack: The denied service at the application level rather at the host level prevents the system usage and disrupts the cloud services. It takes advantage of flaws in the application code to execute the DOS and throw the victim's system into infinite loop and extremely long running of recursive subroutine in order to consume huge CPU resources, disk bandwidth and database bandwidth. It quickly overcome the cloud service budget and increases your cloud utility bill. Hence it creates a huge impact to companies economic, this attack also being classified as EDOS (Economic denial of Sustainability). [20]

Google Hacking: Google Hacking or Google scanning is the attack that makes use of the Google search engine to locate the security loop holes in the internet. It could be caused due to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

software vulnerabilities and user misconfiguration. Hackers target a specific system and try to identify the security loop hole to get access to that system. If the attacker knows the security loophole that he knows to utilize but there is no specific target, then he employs the scanner. Scanner examines the huge amount of system for a security flaw.

2.4 Data Level

Data level security is become much important in all types of service delivery models. Various aspects of data security includes data-in-transit, data-at-rest, processing of data, data lineage, data provenance and data remanence [4]

"Data-in-transit" is all being transmitting a data over the network. This data is consider to be secured only if it is properly authenticated, authorized and identified by the communicating parties by means of using strong encryption algorithm and secured transport protocol.

"Data-at-rest" is data stored on storage medium. This data can be secured by using strong encryption algorithm and protecting the key from the hackers. However, in the cloud computing model encrypting the "data-at-rest" in all cloud based applications are not possible, because encryption could thwart indexing and searching of that data.

Although the data might be encrypted during the transit and at rest in cloud provider database, it definitely needs to be decrypted before it is processed. However, the algorithm like homomorphic encryption are aimed to support computation in ciphertext, it slows down the performance of the system due to the complexity involved in algorithm execution. A scientist Craig Gentry in year 2009 has developed a fully homomorphic encryption method consider to be a huge advancement in cryptography and once it is implemented practically it will give significant positive impact to cloud services.

Data lineage is a method of tracing a data path in order to know when and where the data is located in provider premises and it is important for audit and compliance purposes. However, providing the exact data path is not really possible in a public cloud.

Data provenance is a method of proving the data integrity and ensuring the computation accuracy of the data. In a cloud computing with the usage of shared resources poses the data provenance is a critical one.

Data remanence is the residual representation of the data that stays even after the attempt made to remove that data. This residue occurs due to data left in nominal file deletion or disk reformatting would have not properly removed previously written data. This may leak the sensitive information to the unauthorized user. [21]

Considering all these aspects of data security and risk associated with it makes the customer to concern about data security mitigation. The only suitable choice for mitigation is to make sure that no sensitive information and regulated data is made available into a public cloud.

3. 3. PRIVACY CONVERN IN CLOUD

Cloud model increases the privacy concern because the service provider has access to all the user data that resides in their premises. They may deliberately or accidentally uncover it or misuse the user data. There are some consideration with respect to privacy in cloud are storage, retention, destruction, regulatory compliance, auditing and monitoring and privacy breaches.

Storage: Identifying where the users data is stored and in which location data center it resides are hidden from the user. Sometimes the users sensitive information may be transferred to other country without their knowledge, place the legal issues because each country privacy laws will differ from others.

Retention: The users sensitive data once moved to cloud, the question arises that how long that resides in the cloud, what type retention policy is used to manage that data and who implement this policy in the cloud.

Destruction: After the retention period, the user personal information should be destroyed from the provider storage. In case if multiple copies are maintained to ensure the availability of the data that replicated copies should be removed from the respective server. A major concern arises when the organization need to ensure all these things are performed correctly.

Regulatory compliance: The consumer should need to know privacy compliance requirement in the cloud and who is responsible to managing this compliance and how existing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compliance requirement impacted by moving to the cloud.

Auditing and monitoring: The organization needs to monitor the cloud service provider activities in order to provide the guarantee to their stakeholder that the privacy requirement is not violated when their personal information is in cloud. Regularly the cloud provider activities should be audited to assure the user personal information is not leaked.

Data breaches: If the user data breach occurs in cloud, how they get notified about the breach and who is responsible for breach notification. In case if the cloud provider neglect to undertake that responsibility, how could be determined who is at fault.

These all the major privacy concern that the consumer can thing about it before moving to cloud. The consumer should read the terms of services and privacy policy thoroughly before they put their sensitive data to cloud and they should try to avoid placing the information that should be hidden from private litigate.

4. IDENTITY AND ACCESS MANAGEMENT

Monitoring the identity and access control for corporate applications remains the major challenges in today's IT world. It's been necessary to have proper identity and access management strategy in place to utilize the cloud services effectively by corporate users.
It is become mandatory for the cloud provider to implement the suitable IAM solutions in order to protect and secure all outsourced data and access to that data in cloud.

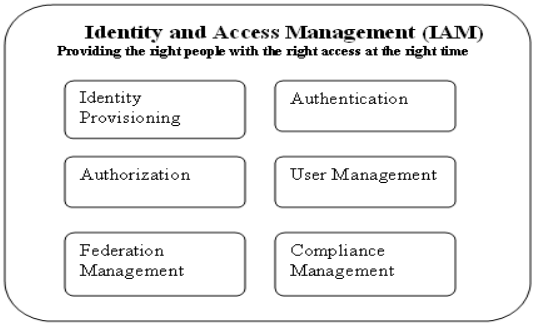

Figure3: Identity and Access Management Model

Figure 3 denotes the various functional activities supported by IAM model to ensure the successful management of identities. [32]

Identity provisioning and deprovisioning: The process of on-boarding (provisioning) of user when they join and off-boarding (deprovisioning) the user when they leave the enterprise in a timely and secure manner is a primary challenge for the enterprise adapting the cloud services. Provisioning allow the users gain access to various system resources, applications and databases based on their identity. While deprovisioning means deactivate the user access to the various resources.
Further, the cloud provider should extend their support for the exiting user management policies that are used in enterprises.

Authentication: The authentication is a process by which the user gets enough credentials to gains the access to the system or a particular service. A session is created once the authenticated users are allowed to access the system and it will be terminated once they log off or timeout occur. Authentication supports single sign-on process through which the user needs not log-on again to access other application system.

Identity Federation Management: Identity Federation management is the method of establishing the trust relationship between different enterprises. It supports an enterprise willing to exchange their users and resource information to enable the collaboration and transaction with their partners. Identity federation will support access to various cloud provider services in single sign-on process.

Authorization and user profile management: Authorization is a method that ensures whether the user has access to particular system resources or services. Authorization model support complex access control policies comprises of user roles, user groups and its attributes. Depends upon the user role as a cloud consumer or member of an enterprise, the requirement of access control policy and user profile will differ.

Compliance Management: It is a process that clearly track and monitor the access rights and privileges of the users are not violated in order to ensure the security of the cloud resources. It helps auditors to validate compliance to several on-premises access control policies and standards involve periodic auditing, reporting and separation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of duties. It should be clearly noted to the consumer about how identity management can support compliance with regularly requirements.

Each of these IAM functions has its own challenges with respect to the services it offers and few functions are immature in some type of service delivery model say for example user management and authorization management is not matured in PaaS and IaaS model. [4]

5. CURRENT SECURITY SOLUTION IN CLOUD

Several research works focused on providing solutions to overcome the various security issues discussed in the cloud computing context. In order to address the cloud standard issues, several cloud organizations works together to maintain a common standard that ensures interoperability of various cloud provider services. [22] The cloud standard coordination is a wikipedia includes details of several cloud standard organization. It allows the various standard organizations to post their ideas. Cloud security alliance (CSA) is a forum that encourage the series of best practices to ensure the security in cloud computing. [23] Several best practices it supports are CSA Controls Matrix, Security Guidance focus on critical areas of cloud computing, Cloud Audit, Cloud Data governance and CloudTrust Protocol.

Distributed Management Task Force (DMTF) is working group that focus on providing standards to make IaaS service model as scalable and highly flexible. It developed Open Virtualization Format (OVF) that provides the secure, efficient and portable format for packaging and distribution of software that can be run in virtual machines. [24] Open Cloud Consortium (OCC) forum provide the framework that enable the interoperability between the cloud provider. [22] Open Grid Forum is a leading open forum works in the area of distributed computing such as grid and cloud. [22].

Table 1 Comparison of Some of the Existing Security Schemes in Cloud Computing

Security Model	Proposed Approach	Strengths	Limitations
Resource management for isolation enhanced cloud storage [26]	Uses cache hierarchy aware core assignment and page coloring based cache partitioning to provide resource isolation and better resource management by which it guarantees security of data during processing.	Cache hierarchy aware approach is easy to implement than page coloring approach. However the processor resources efficiently utilized only in page coloring approach	Platform resources are under-utilized in cache hierarchy aware approach in case if VM uses fewer cores than the total number cores assigned to its group. Page coloring approach enforces the performance degradation in case VM's working set doesn't fit in cache partition.
Fuzzy keyword search over encrypted data [27]	Proposed a fuzzy keyword search over encrypted data in cloud. It uses the edit distance to measure the similarity of the strings.	When the searched keyword is not exactly matched with the files, the closest possible matches will be retrieved.	The method only supports the single keyword search. Conjunction of keyword search and sequence of keywords are yet to be developed.
Secure virtualization in cloud [28]	Propose an Advanced Cloud Protection System to enhance a security of cloud resources.	ACPS system can monitor the guest VM to identify and block the malicious	Implementing the ACPS system may degrade the system performance.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	It provides the secure virtualization in cloud by continuously monitoring the infrastructure resources and notifying the security breaches to the security management system.	activity launched by any guest VM.	
Privacy-Aware Access control system[29]	Proposed an access control mechanism that combines the feature of role based and attribute based access control in private cloud	Improve the privacy and security of the system by combining role based and attribute based access control in cloud.	The proposed model is in its early stage and it requires further implementation to verify the performance.
API access control in cloud [30]	Addresses the insecure API issue in cloud and propose an access control mechanism to secure API, based on role based access control	It supports the two stage security at the API level to ensure only the registered users access the cloud services.	The implementation of this model is required to verify the system security.
Hierarchical Attribute-Based access control in cloud [31]	Addresses the issue of inflexibility to represent the complex access control policies in existing attribute based access control method and propose a solution based on hierarchical attribute based encryption.	It supports the scalability by extending the attribute-based encryption with a hierarchical structure. HASBE supports efficient user revocation by including expiration_time attribute to each user key.	Computation complexity differs depending on the access tree and the key structure. Computation complexity of the algorithm may limit the scalability of the system.
Capability based Access control in cloud[33]	It uses the capability based access control approach along with public key encryption mechanism to allow only the valid users to access the outsourced data in cloud.	This approach is more appropriate to individual application users compare to ACL based approach. Uses the modified D-H key exchange protocol to reduce the burden of key distribution and management at cloud service provider.	Creating a capability for individual user requires the cloud service provider to allocate and manage the large storage space for each data owner.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. CONCLUSION

As discussed in this paper, security concern related to cloud computing in various levels are the real challenge that we need to look. Although several security risks described in the article would exist in traditional computing model, it creates the high impact in cloud computing model. Hence providing the suitable security module that overcomes the security risks in cloud is necessary when consumer is migrating to cloud and to alleviate the fear of adapting the cloud for their needs. There are plenty of research works related with cloud computing security issues. Several methods and monitoring tools have been suggested to eliminate the security risks in cloud. However, providing the integrated security framework intended to support various levels of security issues are under research. There are many research carried out to ensure the security of outsourced data in an untrusted cloud data center. My research work will focus on providing solutions to address the security and privacy concern on outsourced information. Hence, developing a hybrid and hierarchy framework that supports efficient, flexible and fine grained access control mechanism is the primary focus in my future research work.

REFERENCES:

[1] NIST Cloud Model: http://www.nist.gov/itl/cloud/index.cfml

[2] Chou, Timothy. "Introduction to Cloud Computing: Business & Technology". http://www.scribd.com/doc/64699897/Introduction-to-Cloud-Computing-Business-and-Technology.

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009; ISBN: 978-0596802769.http://oreilly.com/catalog/9780596802776.

[5] Subashini S, Kavitha V, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications 2010.

[6] Jon Greaves, "The Data centre of the future," www. carpathiahosting.com

[7] Announcing Elastic IP addresses and Availability Zones for Amazon EC2," http://aws.amazon.com/about-aws/whats-new/2008/03/26/announcing-elastic-ip-addresses-and-availability-zones-for-amazon-ec2/

[8]RFC1918, "Address Allocation for private Internets," http://tools.ietf.org/html/rfc1918

[9]"AWS signature version 1 is insecure," http://www.daemonology.net/blog/2008-12-18-AWS-signature-version-1-is-insecure.html

[10]"Hackers break SSL encryption used by millions of sites," http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

[11]"Threat Analysis of the Domain Name System (DNS)," http://tools.ietf.org/html/rfc3833

[12] "IP Spoofing Attack and Defenses," http://resources.infosecinstitute.com/ip-spoofing-attack

[13] Basta, A., & Halton, W. (2007). Computer Security and Penetration Testing (1st ed.). Delmar Cengage Learning.

[14] Jonathan Hassell,"The top five ways to prevent IP spoofing," http://www.computerworld.com/s/article/9001021/The_top_five_ways_to_prevent_IP_spoofing?taxonomyId=142&pageNumber=2

[15] Zheng Zhang, Ying Zhang, Y. Charlie Hu, Z. Morley Mao," Practical Defenses Against BGP Prefix Hijacking,"

[16] Harmony security Research and consultancy, "ARP Poisoning An investigation into spoofing theAddressResolutionProtocol," http://www.harmonysecurity.com

[17]Context Information Security "Assessing Cloud Node Security whitepapers@contextis.com, March 2011

[18] Open Web Application Security Project, "The Ten Most Critical Web Application Security Risks," OWASP Top 10 – 2010.

[19] "CAPTCHAs-breaking into the shadow economy," http://www.symantec.com/connect/blogs/captchas-breaking-shadow-economy

[20] Mudhakar Srivatsa, Arun Iyengar, Jian Yin, Ling Liu, **"**Mitigating application-level denial of service attacks on Web servers: A client-transparent approach," ACM Transactions on the Web, Volume 2 Issue 3, July 2008

[21] Jason Bloomberg, "Data Remanence: Cloud Computing Shell Game," May 19, 2011.http://www.zapthink.com/2011/05/19/data-remanence-cloud-computing-shell-game/.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[22]Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Fern Halper, "Cloud Computing Standards Organizations"

[23] Cloud Security Alliance. Security best practices for cloud computing, 2010 http://www.cloudsecurityalliance.org.

[24] DSP0243 Open Virtualization Format (OVF) V1.1.0 2010, http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf

[25] Open Cloud Consortium, http://opencloudconsortium.org/

[26] Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Proceedings of the 2009ACM workshop on cloud computing security, Chicago, Illinois, USA, 2009, p.77–84.

[27] Jin Li, Qian Wang,et al, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing" In: Proceedings of the IEEE INFOCOM 2010 .

[28] Flavio Lombardi, Roberto Di Pietro, "Secure virtualization for cloud computing" Journal of Network and Computer Applications 2011, p 1113–1122

[29] Ei Ei Mon, Thinn Thu Naing, "The Privacy-Aware Access control system using attribute and role-based access control in cloud" Proceedings of IEEE IC-BNMT2011

[30] Avvari Sirisha, G. Geetha Kumari, "API Access Control in Cloud Using the Role Based Access Control Model" Trendz in Information Sciences & Computing (TISC), 2010

[31] Zhiguo Wan, Jun'e Liu, and Robert H. Deng," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012.

[32] CSA Security Alliance, "Domain 12: Guidance for Identity & Access Management V2.1 (2010)," https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf.

[33] Chittaranjan Hota, Sunil Sanka, Muttukrishnan Rajarajan, Srijith K. Nair, " Capability-based Cryptographic Data Access Control in Cloud Computing" Int. J. Advanced Networking and Applications Volume: 03; Issue: 03; Pages: 1152-1161.