FRAMEWORK FOR SECURE CLOUD COMPUTING

Kashif Munir[1] and Prof Dr. Sellapan Palaniappan[2]

[1]School of Science and Engineering, Malaysia University of Science and Technology, Selangor, Malaysia
kashifbwp@hotmail.com
[2]School of Science and Engineering, Malaysia University of Science and Technology, Selangor, Malaysia
sell@must.edu.my

ABSTRACT:

Cloud computing has changed the entire process that distributed computing used to present e.g. Grid computing, server client computing. Cloud computing describes recent developments in many existing IT technologies and separates application and information resources from the underlying infrastructure. Cloud computing security is an important aspect of quality of service from cloud service providers. Security concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. In violation of security in any component in the cloud can be disaster for the organization (the customer) as well as for the provider. In this paper, we propose a cloud security model and security framework that identifies security challenges in cloud computing.

KEYWORDS:

Cloud Computing; Security Challenges; Security Threats; Security Framework.

1. INTRODUCTION

Cloud computing is emerged as the modern technology which developed in last few years, and considered as the next big thing, in the years to come. Cloud computing technology requires new security issues and need to face new challenges as well [1]. In recent years it has grown up from just being a concept to a major part of IT industry. Cloud computing widely accepted as the adoption of virtualization, SOA and utility computing, it generally works on three type of architecture namely SAAS, PAAS, and IAAS. There are different issue and challenges with each cloud computing technology. Security concerns and challenges are addressed in and reviewed in terms of standards such as PCI-DSS, ITIL, and ISO-27001/27002 [2], [3].

Cloud computing has three main aspects: SaaS (software as a service), PaaS (platform as a service) and IaaS (infrastructure as a service). As shown in Figure 1, SaaS provider hosts and manages a given application in their data centre and makes it available to multiple users over the Web. Oracles CRM on Demand, Salesforce.com are some of the well known SaaS examples.

DOI : 10.5121/ijccsa.2013.3202

PaaS is an application development and deployment platform which delivered over the web to developers. PaaS facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure. All of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available through Internet. This platform includes a database, middleware , development tools and infrastructure software. Well-known PaaS service providers include Google App Engine, Engine Yard. IaaS is the delivery of hardware and software as a service.

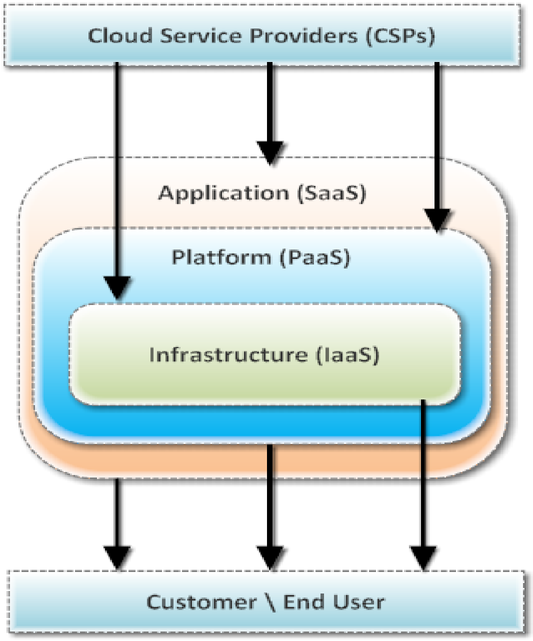

Figure 1. Cloud Computing Environment

It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Amazon Web Services Elastic Compute Cloud (EC2) and Secure Storage Service (S3) are examples of IaaS services. Cloud computing faces a lot of different challenges. Security is one of the key challenges, and has become the key of popularization cloud computing and restrictive factor. In recent years, the cloud services appear many security accidents. For example, in March 2009, Google leaked a large number of documents. Microsoft Azure platform stopped working for about 22 hours. In April 2011, Amazon’s EC2 service disruptions, influences the service of Quora, Reddit etc. When happened, these security problems caused a great loss, even devastating blow. Therefore, to make the enterprise and the organization accept cloud computing services, it is necessary to solve the security problems [4][5].

The rest of this paper is organized as follows: in section 2, we provide an extensive review for the most recent work in cloud security. In section 3, we discuss possible threats\attacks present in cloud computing environment. We provide our framework for cloud security and privacy. In section 4, we propose our security model and framework for cloud computing. Finally, in section 5 we give our concluding remarks and future work.

2. RELATED WORK

In [6] the authors proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. They designed the framework to detect and stop a large number of attacks defined through an expressive policy description language and to be easily interfaced with various data management systems. They showed that they can efficiently protect a data storage system by evaluating their security framework on top of the BlobSeer data management platform. The benefits of preventing a DoS attack targeted towards BlobSeer were evaluated through experiments performed on the Grid5000 test bed.

The work in [7] investigated the problem of assuring the customer of the integrity (i.e. correctness) of his data in the cloud. The cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised since the data is physically not accessible to the user. The authors provided a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud provider and the customer and can be incorporated in the service level agreement. The authors suggested that this scheme ensures that the storage at the client side is minimal which will be beneficial for thin clients.

In [8] the author discussed some security and privacy issues in cloud computing and suggested four methods for cloud security and privacy including: 1) access control method which is an application of Role-Based Access Control (RBAC) [9] on cloud computing to produce one algorithm called cloud-based RBAC. The author defined the basic component in this method as: Cloud User, Access Permission, Role and Session. He stated that at the beginning of each session, Cloud Users can request to acquire some of the roles (permissions). If the Role is enabled, some sensitive requests are granted. In this way, the malicious attacks on user data can be prevented as for such activity a user cannot acquire the access permission, 2) policy integration method which is a dynamic policy control mechanism that handles the multi-policy problem and dynamically determines the dominant policy during certain data processing, 3) identity management method which is used to prevent the unauthorized secondary usage of data. In this method the author added the Cloud Privacy Label (CPL) to the user centric identity management [10] to get a mechanism to protect the cloud users' privacy, 4) user control method which is a method to solve the problem that the cloud users will lose control of their data as a result of virtualization. To address this problem the author introduced the Third Party Auditor (TPA) [11] to balance the power between cloud service providers and cloud users. The author concluded that his methods can only deal with one or two aspects of cloud security problems so some more methods have to be proposed in the future in order to provide a more secure cloud.

In [12] the authors discussed the security issues in a cloud computing environment. They focused on technical security issues arising from the usage of cloud services. They discussed security threats presented in the cloud such as VM-Level attacks, isolation failure, management interface compromise and compliance risks and their mitigation. They also presented cloud security architecture, using which; organizations can protect themselves against threats and attacks. According to the authors the key points for this architecture are: single-sign on, increased availability, defense in depth approach, single management console and Virtual Machine (VM) protection.

In [13] the authors analyzed vulnerabilities and security risks specific to cloud computing systems. They defined four indicators for cloud-specific vulnerability including: 1) it is intrinsic to or prevalent in core technology of cloud computing, 2) it has its root in one of NIST's essential cloud characteristics, 3) it is caused by cloud innovations making security controls hard to implement, 4) it is prevalent in established state-of-the- art cloud offerings. The authors were certain that additional cloud-specific vulnerabilities will be identified; others will become less of an issue as the field of cloud computing matures. However, they believe that using a precise definition of what constitutes vulnerability and the four indicators they identified will provide a level of precision and clarity that the current discourse about cloud computing security often lacks.

In [14] the author discussed some vital issues to ensure a secure cloud environment. This included a basic view of security policies (e.g., inside threats, access control and system portability), software security (e.g., virtualization technology, host operating system, guest operating system and data encryption) and hardware security (e.g., backup, server location and firewall). The author concluded that an important issue for the future of cloud security is the use of open standards to avoid problems such as vendor lock-in and incompatibility. Furthermore, the author believes that although there are no security standards specific to cloud computing, conventional security concepts can be usefully applied.

La'Quata Sumter et al. [15] says: The rise in the scope of cloud computing has brought fear about the Internet security and the threat of security in cloud computing is continuously increasing. Consumers of the cloud computing services have serious concerns about the availability of their data when required. Users have server concern about the security and access mechanism in cloud computing environment. To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment. They have claimed that there proposed security model for cloud computing is a practical model cloud computing. The advantage of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments.

Meiko Jensen et al. [16] have shown that to improve cloud computing security, the security capabilities of both web browsers and web service frameworks, should be strengthened. This can best be done by integrating the latter into the former.

M. Jensen et al. [17] focus on special type of Denial of Service attacks on network based service that relies on message flooding techniques, overloading the victims with invalid requests. They describe some well known and some rather new attacks and discuss commonalities and approaches for countermeasures.

Armbust M Fox et al. [18] discuss that resources should be virtualized to hide the implementation of how they are multiplexed and shared.

Wayne [19]: In this paper benefits of cloud computing are highlighted along with the basic security issues that are still associated with cloud services. Shaping the security of critical systems is very important. Addressing the security issues faced by end users is extremely mandatory, Researchers and professionals must work on the security issues associated with cloud computing. Strong security policies must be designed to ensure data is safe and prevented from unauthorized access, in both corporate data centers and in the cloud servers. This research brings primary problems in terms of cloud security, which are alleged to cloud computing security and privacy issues. Further the study gazes primary security and privacy Problems. It mainly focuses public clouds that needs significant consideration and presents required facts and figures to make organizations data security decisions. Key security issues identified and addressed in this paper are end user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, Server-Side Protection, Access Control and Identity management.

The strengths of their work is identification and discussion on cloud computing security issues which educates end users about security and private risks associated with cloud services. The weakness is that they haven‘t proposed any tool or framework to address identifies issues.
M. Okuhara et al. [20] explain how customers, despite their deep-seated concerns and uneasiness about cloud computing, can enjoy the benefits of the cloud without worry if cloud services providers use appropriate architectures for implementing security measures. They also describe the security problems that surround cloud computing and outline Fujitsu’s security architecture for solving them.

[21] takes a detailed look at cloud computing security risks and conclude that, as computing takes a step forward to cloud computing, security should not move backward. Users should not accept moving backward in terms of security, and computing technology and security both, must advance together.

[22] shows that some of the cutting edge technologies for cloud security are: self-protecting data, trusted monitors, and searchable encryption. With the integration of these technologies into their solutions, customers will have even more trust in their cloud provider.
[23] discusses the fundamental trusted computing technologies on which latest approaches to cloud security are based.

[24] argues that, with continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a business-intelligence stand point, over the isolated alternative that is more common now a days.

[25] describes Amazon Web Services’ (AWS) physical and operational security processes for network and infrastructure under Amazon Web Services (AWS) management. It also gives service specific security implementations for Amazon Web Services (AWS).

3. THREATS TO CLOUD COMPUTING

In this section, we discuss threats relevant to the security architecture of Cloud services. We discuss here some potential threats relevant to Cloud and their remedies based on our experience of implementing the cloud.[26].

Changes to business model

Cloud computing changes the way in which IT services are delivered. As servers, storage and applications are provided by off-site external service providers, organizations need to evaluate the risks associated with the loss of control over the infrastructure. This is one of the major threats which hinder the usage of Cloud computing services.

Mitigation: A reliable end-to-end encryption and appropriate trust management scheme can simplify such a threat to some extent.

Abusive use of Cloud computing

Cloud computing provides several utilities including bandwidth and storage capacities. Some vendors also give a predefined trial period to use their services. However, they do not have sufficient control over the attackers, malicious users or spammers that can take advantages of the trials. These can often allow an intruder to plant a malicious attack and prove to be a platform for serious attacks. Areas of concern include password and key cracking, etc. Such threats affect the IaaS and PaaS service models.

Mitigation: To remediate this, initial registration should be through proper validation/verification and through stronger authentication. In addition to this, the user's network traffic should be monitored comprehensively.

Insecure interfaces and API

Cloud providers often publish a set of APIs to allow their customers to design an interface for interacting with Cloud services. These interfaces often add a layer on top of the framework, which in turn would increase the complexity of Cloud. Such inter- faces allow vulnerabilities (in the existing API) to move to the Cloud environment. Improper use of such interfaces would often pose threats such as clear-text authentication, transmission of content, improper authorizations, etc. Such type of threat may affect the IaaS, PaaS, and SaaS service models.

Mitigation: This can be avoided by using a proper security model for Cloud provider's interface and ensuring strong authentication and access control mechanism with encrypted transmission.

Malicious insiders

Most of the organizations hide their policies regarding the level of access to employees and their recruitment procedure for employees. However, using a higher level of access, an employee can gain access to confidential data and services. Due to lack of transparency in Cloud provider's process and procedure, insiders often have the privilege. Insider activities are often bypassed by a firewall or Intrusion Detection system (IDS) assuming it to be a legal activity. However, a trusted insider may turn into an adversary. In such a situation, insiders can cause a considerable effect on Cloud service offerings, for example, malicious insiders can access confidential data and gain control over the Cloud services with no risk of detection. This type of threat may be relevant to SaaS, PaaS, and IaaS.

Mitigation: To avoid this risk, more transparency is required in security and management process including compliance reporting and breach notification.

Shared technology issues/multi-tenancy nature

In multi-tenant architecture, virtualization is used to offer shared on-demand services. The same application is shared among different users having access to the virtual machine. However, as highlighted earlier, vulnerabilities in a hypervisor allow a malicious user to gain access and control of the legitimate users' virtual machine. IaaS services are delivered using shared resources, which may not be designed to provide strong isolation for multi-tenant architectures. This may affect the overall architecture of Cloud by allowing one tenant to interfere in the other, and hence affecting its normal operation. This type of threat affects IaaS.

Mitigation: Implementation of SLA for patching, strong authentication, and access control to administrative tasks are some of the solutions to address this issue.

Data loss and leakage:

Data may be compromised in many ways. This may include data compromise, deletion, or modification. Due to the dynamic and shared nature of the Cloud, such threat could prove to be a major issue leading to data theft. Examples of such threats are lack of authentication, authorization and audit control, weak encryption algorithms, weak keys, risk of association, unreliable data center, and lack of disaster recovery. This threat can applicable to SaaS, PaaS, and IaaS.

Mitigation: Solutions include security of API, data integrity, secure storage for used keys, data backup, and retention policies.

Service hijacking

Service hijacking may redirect the client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. Phishing attack, fraud, exploitation of software vulnerabilities, reused credentials, and passwords may pose service or account hijacking. This threat can affect IaaS, PaaS, and SaaS.

Mitigation: Some of the mitigation strategies to address this threat include security policies, strong authentication, and activity monitoring.

Risk profiling

Cloud offerings make organizations less involved with ownership and maintenance of hardware and software. This offers significant advantages. However, these makes them unaware of internal security procedures, security compliance, hardening, patching, auditing, and logging process and expose the organization to greater risk.

Mitigation: To avoid this Cloud provider should disclose partial infrastructure details, logs, and data. In addition to this, there should also be a monitoring and alerting system.

Identity theft

Identity theft is a form of fraud in which someone pretends to be someone else, to access resources or obtain credit and other benefits. The victim (of identity theft) can suffer adverse consequences and losses and held accountable for the perpetrator’s actions. Relevant security risks include weak password recovery workflows, phishing attacks, key loggers, etc. This affects SaaS, PaaS, and IaaS.

Mitigation: The solution is to use strong authentication mechanisms.

4. ATTACKS ON CLOUD COMPUTING

By exploiting vulnerabilities in Cloud, an adversary can launch the following attacks.

Zombie attack

Through the Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. These types of hosts are called *zombies*. In the Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood the large number of requests via *zombies*. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services. The Cloud may be overloaded to serve a number of requests, and hence exhausted, which can cause DoS (Denial of Service) or DDoS (distributed denial of service) to the servers. Cloud in the presence of attacker’s flooded requests cannot serve valid user’s requests.

Mitigation: However, better authentication and authorization and IDS/IPS can provide protection against such an attack.

Service injection attack

Cloud system is responsible for determining and eventually instantiating a free-to- use instance of the requested service. The address for accessing that new instance is to be communicated back to the requesting user. An adversary tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. Cloud malware affects the Cloud services by changing (or blocking) Cloud functionalities. Consider a case wherein an adversary creates his/her malicious services like SaaS, PaaS, or IaaS and adds it to the Cloud system. If an adversary succeeds to do this, then valid requests are redirected to the malicious services automatically.

Mitigation: To defend against this type of attack, service integrity checking module should be implemented. Strong isolation between VMs may disable the attacker from injecting malicious code in the neighbor’s VM.

Attacks on virtualization

There are mainly two types of attacks performed over virtualization: VM Escape and Rootkit in hypervisor.

VM Escape

In this type of attack, an attacker's program running in a VM breaks the isolation layer in order to run with the hypervisor's root privileges instead with the VM privileges. This allows an attacker to interact directly with the hypervisor. Therefore, VM Escape from the isolation is provided by the virtual layer. By VM Escape, an attacker gets access to the host OS and the other VMs running on the physical machine.

Rootkit in Hypervisor

VM-based rootkits initiate a hypervisor compromising the existing host OS to a VM. The new guest OS assumes that it is running as the host OS with the corresponding control over the resources, however, in reality this host does not exist. Hypervisor also creates a covert channel to execute unauthorized code into the system. This allows an attacker to control over any VM running on the host machine and to manipulate the activities on the system.

Mitigation: The threat arising due to VM-Level vulnerabilities can be mitigated by monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewall.

Man-in-the Middle attack

If secure socket layer (SSL) is not properly configured, then any attacker is able to access the data exchange between two parties. In Cloud, an attacker is able to access the data communication among data centers.

Mitigation: Proper SSL configuration and data communication tests between authorized parties can be useful to reduce the risk of Man-in-the-Middle attack.

Metadata spoofing attack

In this type of attack, an adversary modifies or changes the service's Web Services Description Language (WSDL) file where descriptions about service instances are stored. If the adversary succeeds to interrupt service invocation code from WSDL file at delivering time, then this attack can be possible.

Mitigation: To overcome such an attack, information about services and applications should be kept in encrypted form. Strong authentication (and authorization) should be enforced for accessing such critical in- formation.

Phishing attack

Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. In Cloud, it may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the Cloud.

Backdoor channel attack

It is a passive attack, which allows hackers to gain remote access to the compromised system. Using backdoor channels, hackers can be able to control victim's resources and can make it a *zombie* for attempting a DDoS attack. It can also be used to disclose the confidential data of the victim.

Mitigation: Better authentication and isolation between VMs can provide protection against such attacks.

5. PROPOSDED SECURITY MODEL

In this subsection we describe security model for cloud computing against threats mentioned in previous section, which focus on scalability and security. The model is shown in Figure 2 and it consists following security units.

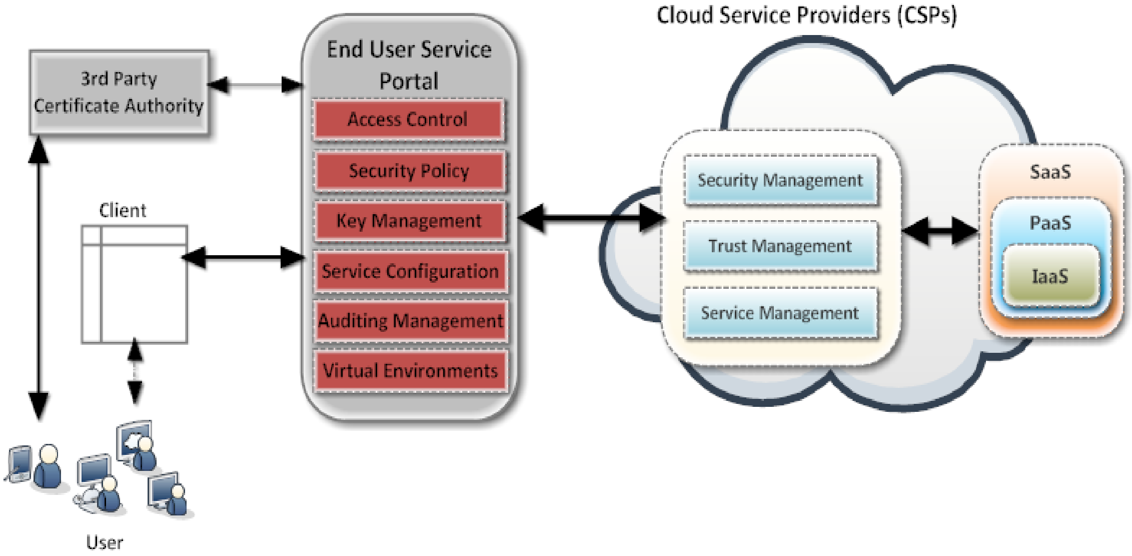

Figure 2: Security Model for Cloud Computing

User can be certificated by the 3rd party certificate authority, then can be issued token for service by End User Service Portal. After joining service portal, user can purchase and use cloud services which are provided by single service provider. End User Service Portal which is composed access control, security policy, Key management, service configuration, auditing management, and virtual environments provides secure access control using Virtual Private Network (VPN) and cloud service managing and configuration.

6. FRAMEWORK FOR SECURE CLOUD COMPUTING

The framework for secure cloud computing as shown in Figure 3 is based on the security model that will describe the details of each component and apply the needed security technologies for implementation between components in the Cloud Computing. Access control process for providing flexible service on each component is as follows:

- **Client**: users could access the client side (i.e.: web browser or host installed application) via diverse devices like PDA, laptop, or mobile phone with Multi-factors authentication provided by End-User Service Portal. The client side is the portal where users get their personal cloud. Multi-factors authentication based on certification issued by 3rd party Certification Authority.
- **End-User Service Portal:** When clearance is granted, a Single Sign-on Access Token (SSAT) could be issued using certification of user. Then the access control component share the user information related with security policy and verification with other components in end-user service portal and cloud service providers by using XACML [28] and KIMP [29]. User could use services without limitation of service providers.
- **Single Sign-on (SSO) :** Currently, Users are having multiple accounts in various Service Providers with different usernames accompanied by different password. Therefore the vast majority of network users tend to use the same password wherever possible, posing inherent security risks. The inconvenience of multiple authentications not only causes users to lose productivity, but also imposes more administrative overhead. Enterprises today are seriously considering the use of Single Sign On (SSO) technology [30] to address the password explosion because they promise to cut down multiple network and application passwords to one. To overcome this problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single Sign- On for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login, thus enabling strong authentication at the user level.
- **Service Configuration:** the service enabler makes provision for personalized cloud service using user's profile. This user's profile is provided to the service management in cloud service provider for the integration and interoperation of service provisioning requests from user. The SPML [31] can be used to share user's profile. The asset manager requests user's personalized resources with {user's profile} SPML to cloud service provider and configure service via VPN connection.
- **Service Gateway, Service Broker:** a service gateway manages network resources and VPN on the information lifecycle of service broker.
- **Security Control:** the security control component provides significant protection for access control, security policy and key management against security threats. Access Control Module is responsible for supporting providers' access control needs. Based on the requirements, various access control models can be used. Role Based Access Control (RBAC) has been widely accepted as the most promising access control model because of its simplicity, flexibility in capturing dynamic requirements, and support for the principle of least privilege and efficient privilege management [9], [32]. Furthermore, RBAC is policy neutral, can capture a wide variety of policy requirements, and is best suited for policy integration needs discussed earlier. RBAC can also be used for usage control purpose which generalizes access control to integrate obligations and conditions into authorizations. Obligations are defined as requirements that the subjects have to fulfill for access requests. Conditions are environmental requirements independent from subject and object that have to be satisfied for the access request. Due to the highly dynamic nature of the cloud, obligations and conditions are crucial decision factors for richer and finer controls on usage of resources provided by the cloud.

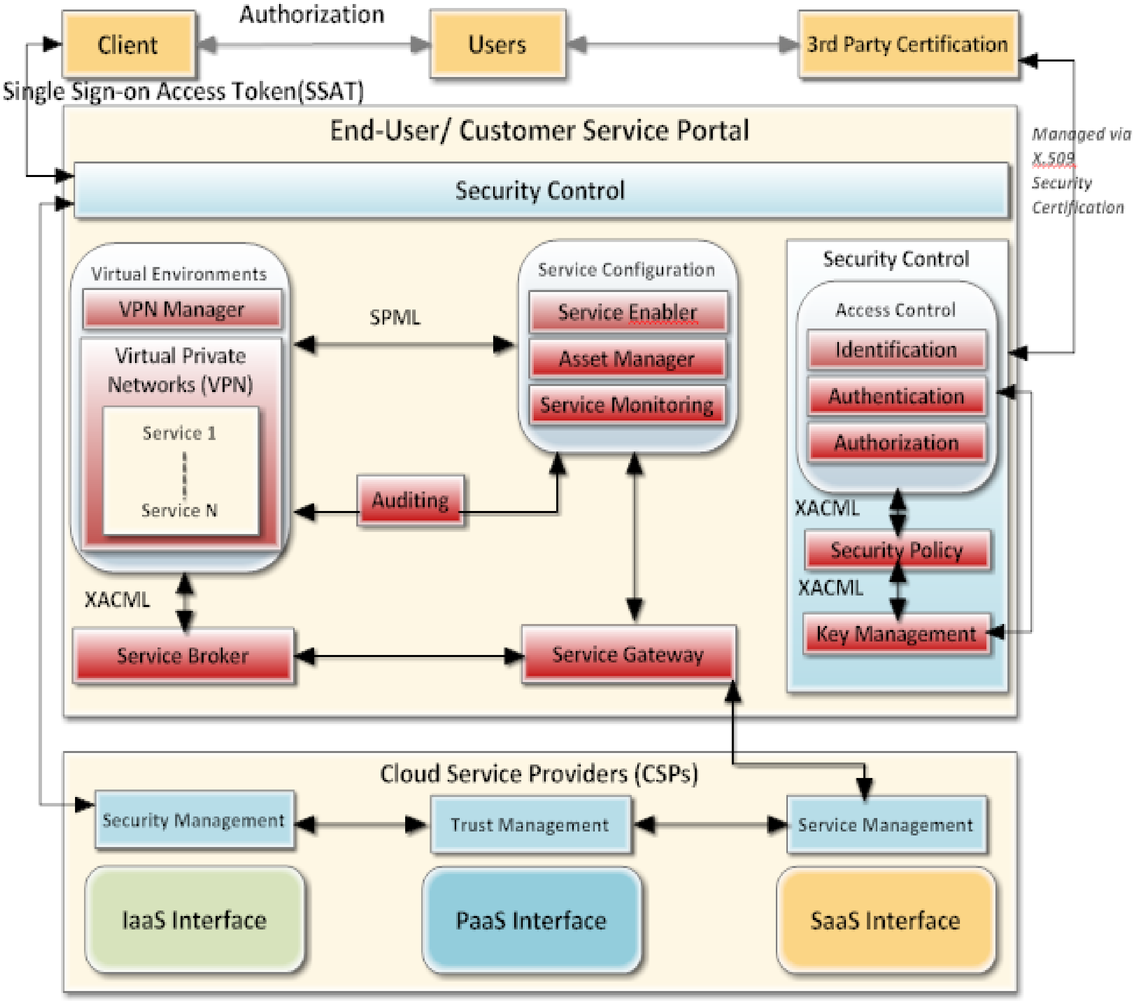

Figure 3: Framework for Secure Cloud Computing

- **Security Management:** The security management component provides the security and privacy specification and enforcement functionality. The authentication and identity management module is responsible for authenticating users and services based on credentials and characteristics.
- **Trust Management:** In the cloud, there is a challenging need of integrating requirements-driven trust negotiation techniques with fine- grained access control mechanisms. Due to the cloud's nature that is service oriented, the trust level should also be integrated with the service. The idea is that the more services a cloud service provider provides the higher trust level needs to be established. Another problem is that we need to establish bi-direction trust in the cloud. That is, the users should have some level of trust on the providers to choose their services from, and the providers also need to have some level of trust on the users to release their services to. One possible approach is to develop a trust management approach that includes a generic set of trust negotiation parameters, is integrated with service, and is bi-directional. As the service composition dynamics in the cloud are very complex, trust as well as access control frameworks should include

delegation primitives [33]. Existing work related to access control delegation, including role-based delegation, has been focused on issues related to delegation of privileges among subjects and various levels of controls with regard to privilege propagation and revocation. Efficient cryptographic mechanisms for trust delegation involve complex trust chain verification and revocation issues raising significant key management issues with regard to its efficiency [34].

- **Service Monitoring:** an automated service monitoring systems to guarantee a high level of service performance and availability.

Security framework proposed provides secure connection and convenient to the user for accessing to the cloud service. We consider cloud orchestration environments and Single Sign-On Token to provide seamless experience to user. Furthermore, we provide possible technologies for cloud collaboration.

7. CONCLUSION AND FUTURE WORK

In recent years, cloud computing is a technology of rapid development, however, the security problems have become obstacles to make the cloud computing more popular which must be solved. In this paper, we reviewed the literature for security challenges in cloud computing and proposed a security model and framework for secure cloud computing environment that identifies security requirements, attacks, threats, concerns associated to the deployment of the clouds. At the same time, cloud computing security is not just a technical problem, it also involves standardization, supervising mode, laws and regulations, and many other aspects, cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more widely. On the other hand, we suggest that future research should be directed towards the management of risks associated with cloud computing. Developing risk assessment helps organizations make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risks. However, managing risks in cloud computing is a challenging process that entails identifying and assessing risks, and taking steps to reduce it to an acceptable level. We plan to pursue research in finding methods for qualitative and quantitative risk analysis in cloud computing. These methods should enable organizations to balance the identified security risks against the expected benefits from cloud utilization.

REFERENCES

[1] On technical security issues in cloud computing , Meiko Jensen etal, 2009

[2] Cloud computing security issues and challenges, Balachandran reddy et al, 2009

[3] Cloud Computing security issues and challenges Kresimir Popovic, et al, 2010

[4] Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13 (2009)

[5] Amazon Web Services. Amazon Virtual private Cloud, http://aws.amazon.com/vpc/

[6] C. Băsescu, A. Carpen-Amarie, C.Leordeanu, A. Costan, and G. Antoniu, “Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies”, In proceeding of IEEE International Conference on Advanced Information Networking and Applications (AINA), 2011

[7] R. Sravan Kumar and A. Saxena, “Data integrity proofs in cloud storage”, Third International Conference on Communication Systems and Networks (COMSNETS), 2011.

[8] Z. Wang, “Security and Privacy Issues Within Cloud Computing” IEEE Int. conference on computational and Finformation sciences, Chengdu, China, Oct. 2011.

[9] James B.D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, “A Generalized Temporal Role-Based Access Control Model”,IEEE Computer Society, 2005.

[10] Moonam Ko, Gail-joon Ahn, Mohamed Shehab, “Privacy enhanced User-Centric Identity Management”, IEEE International Conference on Communications,2009.

[11] Cong Wang, Qian Wang, Kui Ren, Wenjing Luo, “Privacy preserving public audting for data storage security in Cloud Computing”, IEEE Communication Society, 2010.

[12] A. Tripathi and A. Mishra, “Cloud computing security considerations” IEEE Int. conference on signalprocessing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011.

[13]Vadym Mukhin, Artem Volokyta, “Security Risk Analysis for Cloud Computing Systems” The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September 2011.

[14] Mathisen, “Security Challenges and Solutions in Cloud Computing” 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea, 31 May -3 June 2011.

[15] R. La‘Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA.

[16] Meiko Jensen ,Jorg Sehwenk et al., “On Technical Security,Issues icloud Computing ”IEEE International conference on cloud Computing, 2009.

[17] M.Jensen ,N.Gruschka et al., “The impact of flooding Attacks on network based services”Proceedings of the IEEE International conference on Availiabilty,Reliability and Security (ARES) 2008.

[18] Armbrust ,M. ,Fox, A., Griffth, R., et al “Above the clouds: A Berkeley View of Cloud Computing” , UCB/EECS-2009-28,EECS Department University of California Berkeley, 2009 http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

[19] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciesnces 2011.

[20] M. Okuhara et al., “Security Architecture for Cloud Computing”, www.fujitsu.com/downloads/MAG/vol46-4/paper09.pdf.

[21] “A Security Analysis of Cloud Computing” http://cloudcomputing.sys- con.com/node/1203943.

[22] “Cloud Security Questions? Here are some answers”http://cloudcomputing.sys-con.com/node/1330353.

[23] Cloud Computing and Security –A Natural Match, Trusted Computing Group(TCG) http://www.trustedcomputinggroup.org.

[24] “Controlling Data in the Cloud:Outsourcing Computation without outsourcing Control http://www.parc.com/content/attachments/ControllingDataInTheCloud- CCSW-09.pdf.

[25] “Amazon Web services: Overview of Security processes “ September 2008 http://aws.amazon.com.

[26] Top 7 threats to cloud computing. HELP NET SECURITY. http://www.net-security.org/secworld.php?id=8943.

[27] K. Munir & S. Palaniappan, “Security Threats\Attacks present in Cloud Environment”, International Journal of Computer Science and Network Security (IJCSNS) vol 12, No.12,December 2012, pp. 107-114, ISSN : 1738-7906. http://paper.ijcsns.org/07_book/201212/20121217.pdf

[28] OASIS, “eXtensible Access Control Markup Language(XACML)”

[29] OASIS, “Key Management Interoperability Protocol (KMIP)”

[30] Rion Dutta, ”Planning for Single SignOn”, White Paper, MIEL e- Security Pvt.

[31] OASIS, “Service Provisioning Markup Language(SPML)”

[32] James Joshi, Rafae Bhatti, Elisa Bertino, Arif Ghafoor, “Access-Control Language for Multidomain Environments,” IEEE Internet Computing, Vol. 8, No. 6, 2004.

[33] Dongwan Shin and Gail-J. Ahn, “Role-based Privilege and Trust Man- agement,” Computer Systems Science and Engineering Journal, Vol. 20, No. 6, CRL Publishing, 2005.

[34] Matt Blaze, Sampath Kannan, Insup Lee, Oleg Sokolsky, Jonathan M. Smith, Angelos D. Keromytis, and Wenke Lee, "Dynamic Trust Management," IEEE Computer, pages 44-51, 2009.

AUTHORS

Kashif Munir receives his BSc degree in Mathematics and Physics from Islamia University Bahawalpur in 1999. He received his MSc degree in Information Technology from University Sains Malaysia in 2001. He also obtained another MS degree in Software Engineering from University of Malaya, Malaysia in 2005. His research area was in the field secure network for mobile devices, Cloud and pervasive computing.

Mr. Kashif was the lecturer at Stamford College, Malaysia. Currently, he is Lecturer in the Computer Science & Engineering Unit at Hafr Al-Batin Community College\KFUPM, Saudi Arabia. He is doing his PhD at Malaysian University of Science and Technology, Malaysia.

Prof. Dr. Sellappan Palaniappan is currently the Acting Provost and the Dean of School of Science and Engineering at Malaysia University of Science and Technology (MUST). Prior to joining MUST, he was an Associate Professor at the Faculty of Computer Science and Information Technology, University of Malaya. He holds a PhD in Interdisciplinary Information Science from the University of Pittsburgh and a Master in Computer Science from the University of London.

Dr. Sellappan is a recipient of several Government research grants and has published numerous journals, conference papers and IT books. He has served as an IT Consultant for several local and international agencies such as the Asian Development Bank, the United Nations Development Programme, the World Bank and the Government of Malaysia. He has conducted workshops for companies. He is also an external examiner/assessor for several public and private universities. He was a member of IEEE (USA), Chartered Engineering Council (UK) and British Computer Society (UK), and is currently a member of the Malaysian National Computer Confederation (MNCC).