SECURITY AND PRIVACY SOLUTIONS IN CLOUD COMPUTING AT OPENSTACK TO SUSTAIN USERS' CONFIDENCE

AsmaaAlzahrani

Webster University, Missouri, USA

ABSTRACT

Cloud computing is an emerging model of service provision that has the advantage of minimizing costs through sharing and storage of resources combined with a demand provisioning mechanism relying on pay-per-use business model. Cloud computing features direct impact on information technology (IT) budgeting but pose detrimental impacts on privacy and security mechanisms especially where sensitive data is to be held offshore by third parties. Even though cloud computing environment promises new benefits to organizations, it also presents its fair share of potential risks. It is considered as a double edge sword considering the privacy and security standpoints. However, despite its potential to offer a low cost security, customer organizations may increase the risks by storing their sensitive information in the cloud. Therefore, this study focuses on privacy and security issues that pose a challenge in maintaining a level of assurance that is sufficient enough to sustain confidence in potential users.

In this study, survey questions were sent to different non-profit and government organizations, which assisted in collecting fundamental information. The data was acquired by conducting surveys in OpenStack Company to identify the critical vulnerabilities in the cloud computing platform in order to provide the recommended solutions.

So, analysis will be made on how the cloud's characteristics such as the nature of the architecture, attractiveness, as well as, vulnerability are tightly related to privacy and security issues. Privacy and security are complex issues for which there is no standard and the relationship between them is necessarily complicated. The study also highlight on the inherent challenge to data privacy because it typically results in data to be presented in an encryption from the data owner. Thus, the study aimed at obtaining a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments, and identify and describe the most representative of the security and privacy attributes and present a relationship among them.

Finally, in order to ensure that the standard measure of validity is achieved, validity test was conducted in order to ensure that the study is free from errors. Various recommendations were provided. The study also explored various areas that require future directions for each attribute, which comprise of multi-domain policy integration and a secure service composition to design a comprehensive policy-based management framework in the cloud environments.

Lastly, the recommendations will provide the potential for security and privacy approaches that can be implemented to improve the cloud computing environment to ensure that a level of trust is achieved.

KEYWORDS

Cloud Computing, Security, Privacy, Information Technology

1. INTRODUCTION

Cloud computing is a new concept with tremendous momentum; however its unique aspects contribute to security and privacy challenges. Cloud computing is not a very new concept in Information Technology and it is a more advanced version of data processing services.
However, the best-known firms in the Information and Technology field offer cloud computing services to many users from different types of organizations. The concept of cloud computing can be described in very simple terms as providing IT services that are hosted on the web and the most common known platforms is Platform as a Service (PaaS), Infrastructure as a Service (IaaS) , and Software as a Service (SaaS) (Ko, Ahn&Shehab, 2009).

The technology is in the market as an efficient and cheap solution that will, in the near future, replaces the client-server concept. This transition will lead to the loss of control over information as well as new security and privacy concerns. As a result, it is advisable to deploy and utilize cloud computing in organizations. On the other hand, with cloud computing becoming common, it is fundamental to highlight on the resulting risks. For this reason, privacy and security issues are the most important and should be addressed before cloud computing establishes a market share. In addition, several studies have been conducted and most IT agencies have been made aware of the risks that are associated with cloud computing and have produced reports and analyses to document the risks (Leavitt, 2009).

In both academia and IT industry, cloud computing has generated a lot of interest.Essentially, the main aim of cloud computing is to consolidate the economic utility model coupled with the evolutionary development of the existing approaches and computing technologies comprising of distributed services, applications and information infrastructures comprising of pools of computers, networks, as well as, storage resources.There is a lot of confusion on how cloud differs from the existing models and how these variations affect its adoption. Some users consider cloud computing as a novel approach while others see it as a natural evolution of technology, culture, and economy. However, cloud technology is a fundamental concept with a potential to minimize the costs through optimization and increased operating coupled with economic efficiencies.

2. SITUATIONAL ANALYSIS

In order to understand the importance of cloud computing together with its adoption, it is vital to decipher its fundamental characteristics, delivery, as well as, deployment models and who the users of these services are and how to offer protection to them (Shin & Ahn, 2005). All the fundamental characteristics are geared towards using the cloud concept rather seamlessly and transparently. For instance, rapid elasticity enables users to scale up and down their resources. Measures services are primarily derive from business model properties and demonstrate that cloud based computing services control and optimize the use of computing resources and through the automated resource allocation, load balancing and metering tools, as well. It has been observed that all applications that are developed and run for cloud computing platforms exhibit various security and privacy challenges based on the underlying delivery and deployment models (Leavitt,
2009).

As stated before, the key delivery models are SaaS, PaaS and IaaS. In IaaS, the provider offers a set of virtualized infrastructural components such as the virtual machines (VMs) and storage on which users can create and run the cloud based applications. These applications will eventually reside on the Virtual Machines and the virtual storage system. Thus, in IaaS, there are various

concerns such as trusting the virtual machine image, securing inter-host communication, and hardening hosts, which are very critical areas. On the other hand, PaaS enables programming environments to access and use additional application building blocks. However, these programming environments have a visible impact on the application architecture, such as constraints where the service applications can make requests from the OS. Finally, in SaaS, the providers of the cloud platform enable and offer application software as an on-demand service. Due to the fact that users acquire and use the software components from various providers, there are several issues, such as securely composing them and ascertaining that data is handled well and protected.

Cloud deployment models comprise of public, private, community, as well as, hybrid clouds. Public clouds are primarily external or publicly available to users in the cloud environments and can be accessed by multiple tenants. On the other hand, private clouds are basically tailored environments with dedicated virtualized resources in the cloud environment for specific organizations. Similarly, community clouds are primarily tailored for a specific group of users.

3. STATEMENT OF THE PROBLEM

There is no area of ICT that is not affected by cloud computing since it is equated to the industrial revolution and it is transformational in nature but is associated with significant security risks and privacy risks. These comprise of loss of control data and dependence on the cloud computing provider. In particular, concerns regarding data privacy and security have been considered as a barrier to the uptake of cloud computing services and the identified issues could contribute to a number of legal and security concerns that are related to infrastructure, identity management, integrity control, and the provider dependent risks. Therefore, data privacy and security are regarded as key risk factors for all cloud computing environments, especially where data to be disseminated to a service provider that is sensitive and supposed to be held offshore.

3.1. Premise

Cloud computing platforms offer access to information, but the challenge is to ensure that only authorized parties are allowed to gain access to it. When cloud environments are used, clients depend on third parties to arrive at decisions concerning the data and platforms in various ways that have been experienced in computing. Thus, it is critical to have appropriate mechanisms to prohibit cloud providers from using the clients' information in a manner, which is not tentatively agreed upon (Leavitt, 2009). Therefore, before making any steps with any cloud computing arrangement, it is vital to determine and assess whether it is appropriate for the data to be transferred into the cloud environment, because for certain types of data, customers may arrive at decisions that the potential benefits of cloud computing do not outweigh the heightened security and privacy issues especially where data may be transferred offshore.

3.2. Definition

Cloud computing: refers to a model that enables a convenient on demand network access to a shared pool of configurable computing resources which can be rapidly provisioned and released with minimal effort or service provider interaction (Zhang & Joshi, 2009).

3.3. Limitations

Cloud computing could potentially enhance collaboration, agility, and scale; therefore, it can enable a truly global computing model over the Internet infrastructure. However, without adequate security and privacy solutions, which are specifically designed for cloud computing, the potentially revolutionizing computing concept could experience a huge failure. Several studies of potential cloud adopters cite that security and privacy concerns pose a challenge to its adoption. In addition, when those network resources
are built on systems, various platforms and applications shared with others introduce another set of threats.

3.4. Delimitations

If information is kept in the cloud use of standardized interfaces in the cloud-environment, it could ease security management; whereas, the scale of a provider that is hosting many users can be used to generate more information that can enhance better threat monitoring. Furthermore, centralized security management and monitoring can be more effective than the local efforts used by IT professionals with limited security experience. In addition, moving critical systems and information to a network-accessible framework introduces new classes of vulnerabilities through the creation of new interfaces to be exploited.

4. DATA ANALYSIS

In this research, there were survey questions, which assisted in collecting fundamental information used in the study. The data was obtained by conducting surveys in OpenStack Company to identify the critical vulnerabilities in the cloud computing platform. The survey questions were sent to different nonprofit and government organizations to identify security vulnerabilities in order to provide the recommended solutions.

4.1. Security Threats in the Cloud Environment

These can vary based on the cloud delivery models that are used by the cloud users. There are various types of cloud security threats, which make the cloud computing environment to be vulnerable. An overview of cloud security threats is categorized according to confidentiality, integrity, as well as availability of the security model and their relevance to each of the cloud delivery models.

Table 1. Cloudsecurity threats

Securitythreat	Description
Confidentiality	
Internaluser threats i. Maliciouscloudcomputing provider user ii. Maliciouscloudcomputing client user iii. Maliciouscloudcomputingthird party user that supports either the cloud computing provider or customerorganizations	These are the cloud threats of the insiders that accesscustomerinformationthatisheldwithin the cloud environment. It is the greatest threat on each of the cloud delivery models and leads to the introduction of the need of multiple internal users SaaS- is the customer and provider administrators PaaS- Application of the cloud platform developers and test environment manages IaaS- refers to third party cloud computing platform consultants
External cloud environment attacker threats i. Attack of the cloud computing infrastructure remote software ii. Attack of the applications of the remote software iii. Attack of the hardware against the cloud iv. Attack of the hardware and software against the cloud user organizations endpoint software and hardware v. Social engineering of the cloud customer and provider users	External threat attacks are perceived to apply several to public Internet that cloud platform faces; however, all forms of cloud delivery models are affected by the external attackers especially in the private clouds where the target is mainly the user endpoint. Ideally, cloud providers with large data stores who have credit card details, personal data and sensitive government or intellectual property will be prone to attacks from groups with significant resources with some intention to retrieve information. These comprise of threats of hardware attacks, social engineering, aswell as, supply chain attacks by attackers who are dedicated.
Leakage of information: i. Lack of security access rights across various domains ii. Lack of physical and electronic Transport systems for cloud data backups	These are threats that originate from wide spread data leakage among various competitor organizations, which utilizes similar cloud provider that could contribute to human error of faulty hardware that may eventually contribute to data compromise

Integrity	
Information segregation i. Security parameters, which are wrongly defined ii. Virtual machines (VMs) and hypervisors, which are wrongly configured	The integrity of information within a complex cloud computing platform hosting SaaS and are configured to share cloud resources could be a threat to security if the system resources are effectively segregated
Access of users: i. Identity and access management and identity procedures done in a poor manner	This comprises of the implementation of poor access control methods that lead to various threat possibilities such as disgruntle dex-staff members of the cloud provider firms maintain remote access to administer customer cloud services and can contribute to intentional damage to the information sources.
Quality of information: i. Introduction of poor quality applications or cloud infrastructure components	The threat of implication of poor information quality, which increased as cloud provider users host several customer data. Thus, the introduction of misconfigured or faulty component by other cloud users could cause detrimental effects to other cloud users who share the same cloud infrastructure.
Availability	
Management of change: i. Testing of customer penetration, which affects other users ii. Changes in infrastructure upon cloud provider, customer and third party systems that affect cloud customers Service threat denial: i. Denial of service of the network bandwidth distributed ii. Denial of service of network DNS i. Denial of service of application and data	As a result of the increasing workload of the cloud provider for change management within all models of cloud delivery, there is possibility of threat, which could lead to negative effects. These could occur due to changes in hardware or software to the existing cloud services This is a threat of denial of service against available cloud-based platform computing resource. Generally it is regarded as an external threat against public cloud services. However, this threat can affect service models as an external and internal threat agents who could introduce applications or hardware components that can lead to denial of service

Therefore based on the information on the table above, it is clear that data privacy and security issues are regarded as key risk factors for all cloud computing environments with regards to confidentiality, integrity, availability, accountability, as well as, privacy issues are concerned, especially where sensitive data is supposed to be held offshore.

4.2. Quality standards: Reliability and validity

In order to reduce the possibility of getting wrong answer, attention was paid to reliability and validity, as quality standards. Reliability is the extent to which measurements are free from error; therefore it yields constant result. The standard approach for the evaluation is where the path loadings extracted from constructs, measure what they are supposed to measure and are expected to be strong, approximately 0.7% or higher this value. Therefore, measures of reliability were assessed using internal consistency scores, using internal consistencies. The internal consistencies for all the variables are considered acceptable because they exceeded 0.7% and this demonstrated a very tolerable reliability.

Table 2: Composite reliability

construct	*Composite reliability*
confidentiality	*0.87*
integrity	*0.84*
availability	*0.82*
accountability	*0.85*
privacy	*0.94*

5. SUMMARY FINDINGS AND RECOMMENDATIONS

5.1. Summary

Cloud environments are multi-domain where each domain can use different security and privacy needs. In addition, they can potentially employ different mechanisms, interfaces, as well as, semantics. In addition, the domains could represent individually enabled services or other infrastructural or application components. Thus, service oriented architecture is considered to be naturally relevant technology that is primarily used to facilitate the formation of the multi-domain through service composition. Thus, it is fundamental to leverage the existing study on multi-domain policy integration as well as a secure service composition to design a comprehensive policy-based management framework in the cloud environments.

5.2. Authentication and Identity Management

When cloud services are used, it enables users to easily have access to their personal data and make it available for other users across the Internet. Therefore, through an adoption of an identity management mechanism, it can assist users to authenticate their services based on their characteristics and credentials. However, a fundamental issue concerning identity management in the cloud computing environment is the interoperability challenges that could result from using different identity negotiation protocols. Thus, password-based authentication has an inherent limitation and this contributes to potential risks (Leavitt, 2009).

Implementation of IDM systems should be able to protect private and sensitive information related to users and processes. However, further studies should be conducted to understand how cloud environments affect the privacy of identity information. In addition, there is also a possibility of multijurisdiction concerns, which can complicate the protection measures. Thus, as a result of the interaction of users with a front-end service that might need to ensure that their identity is secure and is protected from other services with which it interacts. Therefore, in a multi- tenant cloud environment, providers should segregate customer identity and the

authentication. The components of IDM and authentication should also be easily integrated with other security components (Shin & Ahn, 2005).

5.3. Access Control and Accounting

A diversity of services, heterogeneity and the domains' diverse access requirements in cloud computing environments demand a fine-grained access control policies. Practically, access control services should be flexible enough to capture a dynamic context or attribute. This means that credential based access needs should enforce the principle of 'least privilege'. Therefore, access control services should beintegrated with the privacy protection needs and should be expressed through the complex rules and standards. The access control system that is implemented in the cloud environments easily managed and the associated privilege distribution is administered in an efficient manner. Therefore, it is vital to ensure that cloud delivery models offer generic access control interfaces to enhance a proper interoperability. This will call for a policy-neutral access control specification and enforcement framework, which can be used to address cross-domain access issues.

The utility model also demands for a proper accounting of both user and service activities, which are vital in generating privacy issues due to the fact that customers might not want to allow a provider to maintain detailed accounting records other than for the sake of billing practices. Therefore, the outsourcing of multi-tenancy aspects of clouds could accelerate the fears that are raised by the clients concerning accounting logs. This may result into the utilization of a privacy-aware framework for access control and accounting services, which is very fundamental, and it should be easily amenable to compliance verification.

5.4. Trust Management and Policy Integration

Despite the fact that multiple service providers co-exist in the cloud environment and to work together to offer various cloud services, they might experience different security approaches, as well as, different privacy mechanisms. As a result, it is vital to address heterogeneity in the policies. Providers might require to design multiple services to allow for greater application services (Leavitt, 2009). Thus, privacy mechanisms are important to ensure that such a dynamic collaboration is managed appropriately and handled securely and that any breach of security is effectively monitored during the interoperation process. Previous studies have demonstrated that; even though individual domain policies are verified, security violations can easily occur during the integration phase. Therefore, providers should carefully manage access control policies to ensure that policy integration does not lead to any security breach.

In a cloud computing environment, the link between different service domains driven by different service needs can be dynamic, transient and very intensive. Therefore, it is also necessary to have a trust framework, which should be designed to allow for an effective and efficient capturing of a generic set of parameters needed for establishing trust and to ensure that there is an adequate management of new trust and sharing or interaction requirements. The integration task of the cloud policies should be able to address challenges, such as semantic heterogeneity and secure interoperability, as well as, policy evolution management. In addition, the behavior of customers can evolve rapidly; so it is affecting the already established trust values. This demonstrates that there is a need to design an integrated trust-based, secure interoperation framework that assists in establishing, negotiating and maintaining trust to adaptively support policy integration.

5.5. Secure Service Management

In cloud environments, service providers and those who are integrating the services create services for their clients. The responsibility of the service integrators is to offer a platform that allows independent providers orchestrate and interlock services and cooperatively offer additional services that meet the clients' protection environments. However, most providers apply on the Web Service Description Language (WSDL) (Leavitt, 2009). Thus, in cloud environments, matters such as service quality and price are very crucial in the service charge, as well as the composition. Therefore, it is significant to address these concerns in order to provide a description of the services and introduce their features. This will enable users to seek for the most appropriate interoperable options and integrate them without the provider's policies. In essence, an automatic and systematic service provisioning and composition framework that takes into account security and privacy issues is of significant impact.

5.6. Privacy and Data Protection

In the cloud environment, privacy is a core issue in all the challenges that have been identified. This includes the need to offer protection to the identity information, policy components during the integration phase, as well as, transaction histories. Most firms are not comfortable to store their information and applications on systems that are not kept within the organization and off-premise data locations. This is one of the greatest fears of customers. Thus, by migrating workloads to a shared infrastructure, the private information that the clients use face increased risk of potential unauthorized access as well as, exposure. Therefore, providers of the cloud services must ensure that their customers are assured of a high degree of transparency within their areas of operations and they must also offer privacy assurance. This means that privacy protection mechanisms must be incorporated in all security solutions.

As a matter of concern, it is important to understand who creates and modifies a piece of information and how the information is modified. This is because, provenance of information could be applied in various scenarios and for different purposes, auditing, as well as history based access control. Therefore, it is fundamental to offer a balance between data provenance and privacy, which is a significant challenge in cloud environments where physical parameters are abandoned.

6. FINDINGS AND RECOMMENDATIONS

Information security life cycle models and the existing security management models significantly change when organizations cannot adopt cloud computing. For instance, shared governance can become a significant matter of concern if it is not appropriately addressed. Thus, in spite of the potential benefits of implementing cloud computing, this may refer to less coordination among various parties of interest within the customer organizations. In addition, dependence on outside entities can also raise concerns over timely response over security incidents and in the implementation of systematic business continuity and disaster recovery plans. Similarly, there are risks and cost-benefit issues that will require involving internal parties.

This means that customers need to consider newer risks, which are introduced by the parameter-less environment. This implies that such data leakage that occurs within multi-tenant clouds as well as resiliency issues such as local disasters and providers' economic stability should be taken into consideration (Shin & Ahn, 2005).

On the other hand, the possibility of internal threat may be extended when data is outsourced as well as cloud processes. This means that within a multi-tenant environment, a single tenant could be a highly victim of attack and this could significantly jeopardize the activities of other tenants. In addition, the existing life cycle models and risk analysis and management processes, penetration testing, as well as, service attestation should be reevaluated in order to ensure that the clients can enjoy the potential benefits of the clouds.

There have been significant problems in the information security area, and this calls for an establishment of appropriate security metrics to allow for consistent and realistic measurements that can assist in ameliorating risk issues. Therefore, it is important to reevaluate best practices in cloud computing and develop standards to ensure implementation of secure clouds. These are vital issues that may necessitate a properly structured cyber-insurance industry. However, the global nature of cloud computing environment makes the prospect to be very complicated one.

6.1. Security and Privacy Approaches

There are various security and privacy approaches that can be adopted to cope with security and privacy challenges. This can lead to primary solutions in the cloud environments and provide a trustworthy cloud computing environment. These security and privacy approaches can be adopted to address security and privacy requirements of the cloud service providers, service integrators and the entire cloud
environment in general.

Identity management and authentication: In the cloud environment, user centric identity management (IDM) has received much attention in the areas of handling critical identity attributes. Based on this approach, identifiers or contributors assist in the identification and definition of users. In addition, based on this approach, users are able to control their digital identities and do away with the complexity of the IDM of the enterprise; therefore, it enables them to emphasize on their own functions. In addition, since users can access the clouds from different locations, they must be in a position to export their digital identities and ensure that they are securely transferred to various computers. This means that user centric identity management ensures that the system must properly maintain the semantics of the context of users' identity information. At times, they may constrain or relax them in order to make them better to respond to users' requests under give instructions. In addition, IDM services should be able to be integrated with an organization's existing IDM framework. In some instances, it is essential to have protocols, which preserve privacy, in order to verify various identity attributes by applying a zero-knowledge proof –based approach. These are important techniques that apply pseudonyms, and this allows them to accommodate various identities, which can protect user's privacy.

In addition, this can further assist in creating a desired usercentric IDM for cloud environments. Furthermore, IDM solutions can also be extended with delegation capabilities in order to address identification, as well as, authentication issues in the composed services. Access control needs: A role-based access control method has been widely used as the most appropriate model because of its simplicity, flexibility in capturing dynamic requirements and also offering support for the privilege as well as efficient privilege management.

In addition, role based access control is a neutral policy and this means that it is neutral for policy integration needs. Due to the dynamic nature of the cloud platforms, it is necessary to have obligations and conditions, which are very vital deciding factors for finer control on usability of resources that are offered by the clouds. Recent access control needs such as those which are credential based, generalized temporal, as well as location based access control

models offer necessary modeling constructs and capabilities, which can be used to capture context based fine grained access requirements. In cloud environments, providers usually have no knowledge of their users in advance. This makes it difficult to assign roles directly to users in access control policies. This means that by applying credential or attribute based policies might be fundamental in enhancing this capability. However, more research should be conducted on how to employ access control needs ad extensions within the intensively service oriented cloud environment.

Secure interoperation: there are various studies that have focused on the multi-domain control policies as well as their integration in the cloud environment. These policies can be implemented to create a comprehensive policy management framework in the clouds. In addition, researchers have also focused on how to secure interoperation as well as secure policy engineering approaches that can be used to integrate access policies of different domains and define universal access policies (Ko, Ahn & Shehab, 2009). Thus, a centralized approach can be used to design such policies, which can be used to mediate all access and this is very appropriate for cloud applications that comprise of various needs and is more or less fixed. On the other hand, in a more dynamic environment, the application domains are transient and there may be needed to interact for a specific purpose. This means that a centralized approach is very inappropriate and this may call for a decentralized approach. Specification frameworks may also be required in order to ensure that all cross-domains accesses are appropriately specified, verified, and enforced. In addition, policy engineering mechanisms can assist in defining global policies that can accommodate all parties' needs. There is also an emerging role mining technique, which can be used to support this notion.

Role mining applies the existing system configuration data and this is the role definition. First, it takes into account the permission from the existing users and then aggregates them into different roles. In a cloud, users acquire different roles from different domains based on the services that they need. Therefore, in order to define global policies, access control needs system configuration to be utilized from different domains in order to define global roles and policies. This means that each global role can consist of roles from different domains that have been assigned to the same group of users.

There are several new approaches, which are proposed to be used for role engineering, and these could be implemented in the cloud environments to be used for policy engineering purposes. In addition, changes to the existing role set might contribute to disruptions to the organization and bar it from functioning effectively. Consequently, role mining should consider a set of roles both to the existing as well as an optimal set of roles. StateMiner approach is one of the best approaches that introduces new mechanisms for optimality and offers a solution to find access control needs state with the smallest structural complexity, which is similar to the optimal and existing state.

Secure-service provisioning and composition: Virtualization techniques have been used by cloud providers to optimize resource allocation. These virtualization techniques are used to separate application services from the cloud infrastructure (Molnar & Schechter, 2010). Therefore, in the cloud, providers as well as service integrators should work together to offer newly created services to their customers. This is an activity that needs automatic service provisioning together with composition frameworks, which permit cloud service providers and integrators to be able to describe their services using a uniformed standard in order to introduce their operations and functionalities. Moreover, this will also enable them to discover their existing interoperable services and securely integrate them to offer their services. These are fundamental frameworks that must include a declarative a language to describe services, features, as well as, mechanisms to provision and compose appropriate services. For instance,

the Open Service Gateway Initiative is a service platform, which offers an open common architecture to be used by service providers and to compose and manage their services. However, the challenges of such partnership include dynamic access control to the resources, which are shared by agents and controlling collaborative actions that are geared towards a collaborative goal (Ko, Ahn & Shehab, 2009).

Trust management framework: This is an important framework that is used to facilitate policy integration between different domains in the cloud environments. In addition, it offers a trust- based framework that is used in the cloud environment to facilitate automated trust-based policy integration. The current trust negotiation mechanism emphasizes credential change, but it does not address the more challenging need of integrating trust that is driven by needs and negotiating techniques with fine-grained access control approaches. An important approach is to develop a comprehensive trust-based policy integration framework, which facilitates policy integration framework that also facilitates policy integration and evolution depending on inter-domain and service-access-needs. Since service composition dynamic in the cloud environment may be complex, trust and access control frameworks should comprise of delegation primitives. For instance, role based delegation focuses on issues that are related to delegation of privileges among subjects and different levels of controls with regards to privilege propagation and revocation, which results into key management issues. Therefore, these are dynamic approaches that should be incorporated in service composition frameworks in cloud environments.

Data-centric security and privacy: In the cloud environments, data usually exists within a shared environment. However, the owners of the information should have full control of their information, and they should also have the right to use the data and what they are allowed to perform with it once they gain access (Leavitt, 2009). Therefore, to offer this data control mechanism in the cloud environment, a standard-based heterogeneous data-centric security approach is a significant element that shifts data protection from various systems and applications. Thus, based on this approach, documents must be selfdescribing and defending regardless of their environments.

Various approaches, such as usage policy rules and cryptographic approaches should be considered (Molnar & Schechter, 2010). This means that when an individual wants to access information, the system should be in a position to check the policy rules and show it only if the policies are followed and satisfied. Some of these techniques can be applied to data security. However, privacy protection and outsourced computation need some attention.

Managing semantic heterogeneity: A fundamental aspect of the cloud environment is the semantic heterogeneity among other policy measures. This is a field that has received very little attention; therefore, it requires further research. This is because researchers have given little attention to automatic detection of the sematic conflicts among cloud service providers' policies. For instance, XML had been adopted as a preferred language to be used for data sharing.

However, studies have shown that it is not adequate as a method of describing information semantics. Consequently, RDF offers a facility that can be used to describe the semantics through offering support to element attributes as well as the properties description (Shin & Ahn, 2005). Even though there is a possibility that semantics can be captured using RDF, it is not easy to represent relations between different concepts, which are represented by the elements and that is vital in facilitating semantic integration of policy information within the interacting domains. This means that the use of ontology is the best approach when addressing semantic heterogeneity matters. In addition, support the development of the ontology, XML Schema and RDFS Schema can be applied to accommodate the domain specific concepts. However, an

OWL based framework is the most desirable to support semantic heterogeneity management across multiple providers within a cloud environment. Based on such framework, a system driven policy framework can be used to facilitate managing security policies in heterogeneous cloud environments, as well as, policy enforcement architecture, which is very fundamental.

7. CONCLUSION

Despite the fact that security and privacy issues in cloud computing can be managed and fine-tuned based on the available resources and skills of the experience group, which can adequately offer efficient, effective and transparent security and privacy management, the issues discussed in this study demonstrate that the current security and privacy issues should be evaluated critically with regards to their appropriateness in the cloud computing environment.

The study findings have revealed that it is essential to evaluate the appropriateness of the information that is transferred into the cloud environments because of the information may be sensitive enough; so the adoption of the cloud services should not outweigh the potential security privacy and security issues, especially where information has to be transferred offshore. There are various enhancements within the existing solutions and should be employed to ensure that cloud computing environmental benefits are fully achieved as its adoption and implementation increases in pace. However, cloud computing is a concept that is still at its infancy stage, and this means that the manner in which the security and privacy landscapes will change, it will also have a greater impact on its successful adoption by customer organizations.

REFERENCES

[1] Garfinkel, S. &Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practices. *IEEE Security and Privacy*, Vol 1, No 1, pp. 17 -27, January –February 2003.

[2] Ko, M., Ahn, G, J. &Shehab, M. (2009). Privacy-Enhanced User-Centric Identity Management. In Preceedings of IEEE International Conference on Communications, Dresded, Germany, June 2009, pp. 98-1002.

[3] Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time? IEEE Computer, Vol 42, No 1, pp. 15-22, January 2009.

[4] Molnar, D. & Schechter, S. (2010). Self-Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In Proceedings of the Workshop on the Economics of Information Security 2010, Harvard University, USA, June 2010. Retrieved on April 12, 2014 from http://weis2010.econinfosec.org/papers/session5/weis_schechter,pdf.

[5] Shin, D. &Ahn, G.J. (2005). Role-Based Privilege and Trust Management. Computer Systems Science and Engineering Joural, Vol 20, No 6, pp. 401-410, November 2005.

[6] Sinclair, S. & Smith, S, W. (2008). Preventive Directions for Insider Threat Mitigation Using Access Control. Book Chapter No 11, S. Stolfo, S.M. Bellovin, S. Hershkop, A.D Keromytis, S. Sinclair, & W. Smith eds. Insider Attack and Cyber Security: Beyond the Hacker. Springer, April 2008.

[7] Zhang, Y. & Joshi, J. (200). Acess Control and Trust Management for Emerging Multidomain Environment. Annals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyay and R.O. Rao (ed), Emerald Group Publishing, pp.421- 425,2009.

AUTHORS

Asmaa Saeed Alzahrani, work as an English teacher. I got my Master's degree in Information Technology Management from Webster University, Missouri, USA. I would like to pursue my education and get my PhD in Information Technology; so I could improve myself in this field and serve my career better, thank you for your consideration. Attached are two recommendations from my two professors at Webster University.