I.J. Computer Network and Information Security, **2014, 8, 34-40**
Published Online July 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.08.05

Security, Privacy and Trust Challenges in Cloud Computing and Solutions

Seyyed Yasser hashemi
Department of Computer Engineering, miyandoab Branch, Islamic Azad University, miyandoab, Iran
Email: hashemi.uni@gmail.com

Parisa Sheykhi Hesarlo
Department of Computer Engineering, miyandoab Branch, Islamic Azad University, miyandoab, Iran
Email: Hahemi_uni@yahoo.com

Abstract—Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing recently emerged as a promising solution to information technology (IT) management. IT managers look to cloud computing as a means to maintain a flexible and scalable IT infrastructure that enables business agility. As much as the technological benefits, cloud computing also has risks involved. In this paper Cloud Computing security challenges will be discussed and proposed many new recommendations to increase security and trust also maintaining privacy.

Index Terms—Cloud Computing, Security Challenges, Security, Privacy, Trust.

I. Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. In cloud computing, the end-users need not know the details of a specific technology while hosting their application, as the service is completely managed by the cloud service provider (CSP). Users can consume services at a rate that is set by their particular needs. This on-demand service can be provided any time. CSP takes care of all the necessary complex operations on behalf of the user. It provides the complete system which allocates the required resources for execution of user applications and management of the entire system flow. [2]. There are four different broad service models for cloud computing:

Software as a Service (SaaS): The services provided by SaaS include using functional programs on the infrastructure of cloud and access through the web browser [3]. in this section the customer doesn't manage the infra-structure of cloud including the net, servers, operational systems, and saving area, except the functional software to limited degree of adjustment at the level of user [4].

Platform as a Service (PaaS): In this kind of service, the client has the option of putting the purchased functional programs on the infra-structure of cloud [3]. Here also the client dose not mange or control infrastructure of the cloud such as the net, servers, storage. He just has control over the functional program installed or Settled by him [4]. In fact the PaaS is similar to SaaS the difference is that PaaS includes exclusive program environment and computing platform, developing and solution strategies.

PaaS allows for the secure storage and processing of users' confidential data by leveraging the tamper-proof capabilities of cryptographic co-processors. Using tamper-proof facilities provides a secure execution domain in the computing cloud that is physically and logically protected from un-authorized access. PaaS central design goal is to maximize users' control in managing the various aspects related to the privacy of sensitive data. This is achieved by implementing user-configurable software protection and data privacy mechanisms. Moreover, PaaS provides a privacy feedback process, which informs users of the different privacy operations applied on their data and makes them aware of any potential risks that may jeopardize the confidentiality of their sensitive information[5].

Infrastructure as a Service (IaaS): This kind of service providing includes process potential, saving space. Nets and other basic computing re-sources and even operational system and application programs [4]. The client dose not manage or control in infra-structure but has control over the operational system, saving area, and the established programs. In this service an artificial server is completely available for the client [3]. IaaS itself is comprised of the following components[6]:

Servers (both physical and virtual).
Storage systems by means of network attached storage (NAS) and storage area network (SAN).
Network segmentation using different network blocks and virtual local area networks.
Communication network (including routers, switches, firewalls, load balancer, etc.).

High speed internet connectivity (often on OC 192 backbones).
Platform virtualization environment.
Service-level agreements.
Utility computing billing.
Security by means of hardware or virtual machine (VM) based firewall and intrusion detection & prevention system.
Hardware load balancer.
Domain name service (DNS), Dynamic host configuration protocol (DHCP) and other management and support services.
Power, cooling and disaster recovery system.

Hardware as a Service (HaaS): where the cloud provides access to dedicated firmware via the Internet.

Cloud computing offerings also differ by scope. In private clouds, services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organization's data centre delivers cloud computing services to clients who may or may not be in the premises. Public clouds are the opposite: services are offered to individuals and organizations who want to retain elasticity and accountability without absorbing the full costs of in-house infrastructures. Public cloud users are by default treated as untrustworthy. There are also hybrid clouds combining both private and public cloud service offerings [1].

Cloud computing has revolutionized the architecture of computer systems. Enterprises can lower costs, save energy, and automatically upgrade their systems by replacing traditional computer systems and facilities with cloud computing services. Because of its increasing popularity, cloud computing is surely the future of information technology. Eventually, cloud computing will provide the basic levels of computing services that are considered essential to meet the everyday needs of the general community, similar to water, gas, telephone, and electrical utilities [7].

Cloud computing has many advantages. But one of the most fundamental challenges facing cloud computing is "security". In this paper we Investigate "security", "privacy" and "trust" as the basic issues in cloud computing security.

This paper is organized as follows: In Section II, the related works in this field is presented, In Section III, the security, privacy and trust is described in detail. In Section IV, Critical Security Challenges in Cloud computing is investigated. Recommendations for cloud computing security challenges are presented in Section V. Finally the paper is concluded in section VI.

II. RELATED WORKS

Tsaiw et al. in [8] introduced a four-tier framework to improve based on web. It was interesting but had a remark on just one facet of the process. Isolating resources for the security of data during processing is done by isolating processor caches in virtual machines and isolating those virtual caches from hypervisor caches [9]. The problems of privacy and control can't be solved unless just to trust to service-level agreements (SLAs) or by keeping the cloud itself private [10]. According to the platform computing assessment 8 out of 10 firms choose internal clouds and want to keep in-house cloud initiatives. Milne [11] suggests a simple way which is widely employed among UK corporations. This is why they employ private clouds in-house. Of course, private cloud has limited function and more cost for firm, so provided the increased security. Other models of cloud will be better and functional for corporations. Nurmi et al. in [12] provided a preview with one of existing home-grown clouds (Eucalyptus) to show their open-source cloud computing. They conclude using their previous experiments that, EUCALYPTUS is helping to supply the research community with a much needed, open-source software framework around which a user-base of cloud-computing researchers can be developed Also, Khalifehlou and Gharehchopogh [13] are presented new directions in cloud computing environments. They are described the various methods for more security in cloud environments. In reference [10], a security framework is provided dynamically different methods which one its component refers to security maintenance by archiving and accessing by meta data in order to restore when the war's data fail or damage. Each segment of this framework is provided to the applications as one or multi layers in the format of security as a service to meet necessary functions [10]. The study introduces the concept of security of cloud according the real worlds security systems in which the amount of security depends on the property and organization of person. Maybe this is a good suggestion but it should be clear whether security is provided to gather with the service or not. Here the provider should pay some part of his attention to security problems. It may undermine and reduce the improvement of service-providing [10, 14]. Jamil et al. [15] study four security problems an including XML signature element wrapping, browser security, cloud malware injection attack and flooding attacks and their reactions. They believe that these security systems need deep and comprehensive analysis because of attacks may use different vulnerable points which can cause unauthorized access to data by hackers or the invaders may put a damaging service on the cloud system for special purpose and this can amount to loss for users or even the system itself [15]. Che et al. [16], studied security models and cloud computing strategies. They want to show the status of existing security in cloud computing and introduce some works to improve the level of security in this computing security also the studied the most favorite security models in cloud computing security for example multiple tenancy model, accumulation model cube model and a summary of the risks obtained from different organizations. Finally, they offered some security strategies according their structure, operation and security of response the event for solving the common security problems of cloud computing [16]. D. Zissis et al. [17] pointed to security problems in their paper and divided

their aim into two parts. First they studied the security of cloud using exclusive security needs and in the second part they tried to offer a solid solution to remove the potential treats. In the paper, they offer trust as a special security feature on cloud sphere. The suggested solution of encoding based on public key related to SSO and LDAP which is wholesomeness and confidentiality of the respected data and communications (to ensure identification) [16]. A combination of PKI, SSO and LDAP can show many of treats related to coherence, confidentiality, accuracy and accessibility of data. Also, Monsef et al. [18] devoted their attempts to the concerns about private area and trust in cloud. This study is done following some concerns on privacy and trust as a main function in cooperation of cloud. These factors have important roles in decreasing complete support of corporations from business and work field of cloud. Different ideas and structures have been discussed in this paper in order to avoid the mentioned problems like three foiled structure of protecting data to meet users various needs. So, the industry's dealing with this subject will be clear. Firdhous et al. [19] discussed the matter from different angles and various definitions of sciences from trust. Then they studied trust in cloud computing and categorized the latest developments in the area. Takati et al. [20] worked on security and privacy challenges in the cloud computing which we can mention identification check and identification management (IDM) access control, trust, coherence management, privacy and protecting data. In this paper, cloud providers and venders should share security and privacy maintenance in cloud computing share. But hinted the degree of sharing is different depend on different models which is essential in developing cloud [20].

III. Defining Security, Privacy and Trust

First of all, we define the basic concepts [1]:

Security: Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation.

Privacy: Privacy concerns the expression of or adherence to various legal and nonlegal norms regarding the right to private life. In the European context this is often understood as compliance with European data protection regulations. Although it would be highly complex to map cloud issues onto the full panoply of privacy and personal data protection regulatory architectures, the globally accepted privacy principles give a useful frame: consent, purpose restriction, legitimacy, transparency, data security and data subject participation.

Trust: Trust revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine (eg, handshake protocols negotiated within certain protocols), human to machine (eg, when a consumer reviews a digital signature advisory notice on a website) or machine to human (eg, when a system relies on user input and instructions without extensive verification). At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives.

IV. Critical Security Challenges in Cloud Computing

A. Technical challenges

1) Virtualization

The main enabling technology for cloud computing is virtualization. Virtualization generalizes the physical infrastructure, which is the most rigid component, and makes it available as a soft component that is easy to use and manage. By doing so, virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. On the other hand, autonomic computing automates the process through which the user can provision resources on demand. By minimizing user involvement, automation speeds up the process and reduces the possibility of human errors. Virtualization challenges are:

Security: Integrity

Privacy: Segregation of personal data on shared infrastructure

Trust: Compromised virtual machines/hypervisors permit loss of trust.

2) Grid technology

Form of distributed and parallel computing, whereby a super and virtual computer is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks. Grid technology challenges are:

Security: Availability (resource available)

Trust: Interoperability.

3) Service-oriented architectures

Service-oriented architecture (SOA) is a software design and software architecture design pattern based on discrete pieces of software providing application functionality as services to other applications. This is known as Service-orientation. It is independent of any vendor, product or technology. A service is a self contained unit of functionality, such as retrieving an online bank statement. Services can be combined by other software applications to provide the complete functionality of a large software application. SOA makes it easy for computers connected over a network to cooperate. Every computer can run an arbitrary number of services, and each service is built in a way that ensures that the service can exchange information with any other service in the network without human interaction and without the need to make changes to the underlying program itself. Service-oriented architectures challenges are:

Security: Integrity, managing services metadata, lack of testing in SOA.

Trust: The reliance of distributed systems on different security credentials.

4) Web application frameworks

The main challenges about Web application frameworks are:

Security: Integrity and availability

Trust: Trust across distributed environments

5) Encryption in the cloud context

The main challenges about Encryption in the cloud context are:

Security: Confidentiality

Privacy: Security and confidentiality

6) Electronic communication in the cloud

The main challenges about Electronic communication in the cloud are:

Privacy: Safeguarding communications secrecy

Trust: Protection against Eavesdropping (surveillance by public and private parties)

7) Scope and quality of services (SLAs)

The underlying benefit of cloud computing is shared resources, which is supported by the underlying nature of a shared infrastructure environment. Thus, service level agreements span across the cloud and are offered by service providers as a service based agreement rather than a customer based agreement. Measuring, monitoring and reporting on cloud performance is based upon an end user experience or the end users ability to consume resources. The downside of cloud computing, relative to SLAs, is the difficultly in determining root cause for service interruptions due to the complex nature of the environment. As applications are moved from dedicated hardware into the cloud these applications need to achieve the same or even more demanding levels of service as classical installations. SLAs for cloud services focus on characteristics of the data center and more recently include characteristics of the network to support end-to-end SLAs. Any SLA management strategy considers two well-differentiated phases: the negotiation of the contract and the monitoring of its fulfillment in real-time. Thus, SLA Management encompasses the SLA contract definition: basic schema with the QoS (quality of service) parameters; SLA negotiation; SLA monitoring; and SLA enforcement according to defined policies. The main point is to build a new layer upon the grid, cloud, or SOA middleware able to create a negotiation mechanism between providers and consumers of services. Scope and quality of services challenges are:

Security: Transparency and security metrics are needed to ensure that security targets are met.

Trust: Assurance and commitments between two parties.

8) Flexibility

The main challenges about Flexibility are:

Security: Availability and scalability

Trust: Resources must be available when needed, in accordance with agreement between parties

9) Validity and consent

The main challenges about Validity and consent are:

Security: Transparency and accountability

Privacy: Transparency must be ensured. Consent from consumers must be free, specific and informed

Trust: Assurance and commitments between two parties must be clear and enforceable.

B. Operational challenges

10) Localization

Data or services may be (or become) hosted from another country, possibly without the end user's knowledge. Localization challenges are:

Security: Challenges in data transmission

Trust: greater complexity in ensuring compliance with data protection regulations. Also Auditing of the service provider's infrastructure to ensure appropriate security may become very problematic.

11) Infrastructure Sharing

Infrastructure may be shared with other customers. Infrastructure sharing challenges are:

Security: Guarantee confidentiality

Privacy: properly protecting from personal data against accidental leaks

Trust: data segregation, securing intellectual property

12) Incidents

Incidents may cause service interruptions without it being evident where the problem lies, and thus how it may be addressed. Incidents challenges are:

Security: The loss of information or data.

Trust: Operation failure, service provider responsibility and accountability.

13) Data withdrawal

Data withdrawal might be difficult, in the sense that it can be hard for a cloud user to determine whether deleted data has actually been removed from the provider's systems, or whether it has merely been made inaccessible. Data withdrawal challenges are:

Security: Unauthorized access to information

Privacy: Leak Personal Data, Unauthorized use of information

14) Auditing and investigations

Auditing and investigations may be more challenging, due to the complexity of the system. Auditing and investigations challenges are:

Security: users of cloud service providers are expected to ensure security and reliability of the service provider, in some cases by performing local audits of the data processing infrastructure. From a practical perspective,

this is virtually impossible with cloud service providers, whose infrastructure can be spread geographically almost without limitation.

C. Legal Challenges

15) Applicable law for data storage location and service location

The main challenges about localization are:

Privacy: Existence and effectiveness of privacy protection laws/principles.

Trust: Existence of a clear legal framework as a basis for the service.

16) Dispute resolution

The main challenges about Dispute resolution are:

Privacy: Accountability: can disputes in the cloud be resolved?

Trust: Accountability: is the cloud stable enough to inspire trust

17) Data protection and privacy

The main challenges about Data protection and privacy are:

Security: Obligation to implement secure data processing approaches.

Privacy: Compliance with privacy principles.

Trust: Confidence in data protection practices.

18) Protection of Intellectual property rights

The main challenges about Protection of Intellectual property rights are:

Security: Confidentiality and availability (data portability).

Trust: Confidence in the security/confidentiality of data entrusted to the cloud.

19) Security obligations and cybercrime

The main challenges about Security obligations and cybercrime are:

Security: Confidentiality, availability and integrity; effective law enforcement.

Privacy: Safeguards against unlawful intrusions in the personal sphere.

Trust: Balancing privacy safeguards with the need for security.

20) Accountability and liability

The main challenges about Accountability and liability are:

Security: Accountability for security breaches and incidents.

Privacy: Accountability for data leaks: can incidents be identified and sanctioned?

Trust: Trust that instruments for restitution and sanction will work.

21) Harmful and illegal content

The main challenges about Harmful and illegal content are:

Security: Availability: can the cloud identify and respond to such content?

Trust: Trust in jurisdictions to apply transparent standard or approach to illegal content (in line with cloud user expectations and applicable laws)

22) Consumer protection

The main challenges about Consumer protection are:

Security: Obligation to implement secure data processing approaches..

Privacy: Data subject participation; restitution

Trust: Consumer protection rules must be effective (ie, applied and enforced in practice).

V. Recommendation

A. National and international laws

Some national and international laws and treaties has led that applicable regulatory texts exist for at least some of the key aspects to be addressed. Doubtless they will prove to be useful as general frameworks to handle some of the issues. But is necessary work towards a greater emphasis on international harmonization of relevant legal and normative frameworks via further efforts to improve consistent application of relevant legal frameworks across the Member States through the conduct of implementation, monitoring and evaluations of relevant international legislation and Continue to support broad international dialogue fostering harmonization of relevant legal frameworks (especially regarding privacy).

B. Guidelines, good practices and self- and co-regulatory approaches

As cloud computing is still a relatively young domain, not many examples of self- and co-regulatory approaches are likely to have emerged yet. But is necessary Develop suitable awareness raising mechanisms to help users to become aware of their own privacy and security risks by Draft, prepare and issue guidance for cloud users (both organizations and individual consumers) on the benefits, risks and consequences of the storage and use of personal data in the cloud and Draft, prepare and issue guidance for cloud providers on how they should inform cloud users (especially consumers) of their rights in an accessible and understandable manner.

C. Contractual frameworks and terms and conditions (T&Cs)

In most business relationships contractual agreements (including in the form of standardized T&Cs) play a dominant role in guiding such issues as conflicts of law, choice of forum, and outlining rights, responsibilities and guarantees. It is vital that this contract shall be vary

according to the conditions described above to be added to consumers' rights and the legal obligations.

D. Compensation mechanism

Appropriate compensation mechanisms towards any victims of security or privacy breaches in a cloud deployment.

E. Operational Transparency

Ensuring that the operation of a cloud deployment is sufficiently clear to all stakeholders, including service providers and users, both professional businesses and private consumers, and that its operation in practice can be assessed where necessary (including the identification of incidents).

F. General assessment model

Create a generic maturity model to independently ex-ante measure and assess cloud security provision.

G. Detection of emerging threats

Establish effective locations and types of security detection mechanisms in cloud architectures to support rapid detection of emergent threats from the cloud.

H. Secure environment

Establish secure virtualized architectures and trust domains for cloud computing environments.

I. Permit for interrogation and collation

Design a test method for middleware, software interfaces and APIs for Security Event and Incident Management (SEIM) to permit interrogation and collation of all events that might be of interest in measuring security (eg, CPU failure, hardware failure, etc.) as well as establishing alert thresholds.

J. Policies in distributed cloud environments

Explore and investigate appropriate means for interoperability of both data exchange (where possible) and enforcement of security, privacy and business policies attached to data across distributed cloud environments.

K. Policies untrustworthy cloud environments

For implementing interoperable abstraction of security, privacy and trust policies to enable data 'policy stickiness' in un trustworthy cloud environments.

L. Increasing levels of data security

Use of technical means to provide for increased levels of data security across trust domains (eg, automated data expiry mechanisms and secure movement or deletion of data).

M. Establish International organization for Cloud Crimes

In order to Address Violations in the Cloud environment and Tracking Crime and Victim Support It is essential that Establish an International organization for Cloud Crimes that accepted by all countries.

N. Vetting cloud service providers

Create the conditions accepted by all countries for vetting cloud service providers in security, privacy and trust section.

O. Personal encryption method

Preparations of highly personalized service for data encryption that even the service providers are not aware of them.

P. Permissions for data tracking

Permission granting for the tracking data to ensure of data withdrawal.

Q. Localization

Localize the physical location of data storage and service in cloud environment.

R. Personal security service (Pss)

Multi-level security services that is user-defined.

CONCLUSIONS

Addressing the security, privacy and trust challenges of cloud computing is a complex undertaking since it requires a combination of technological solutions and legal approaches that is capable of addressing operational realities and concerns. In this paper we investigated these challenges and proposed many recommendations such as Establish International organization for Cloud Crimes, Vetting cloud service providers, Personal encryption method, Permissions for data tracking, Localization, Personal security service (Pss) to increase security and trust also maintaining privacy. But it should be noted that, security and privacy can never be assured and secured 100% in these areas.

REFERENCES

[1] Robinson, Neil and Valeri, Lorenzo and Cave, Jonathan and Starkey, Tony and Graux, Hans and Creese, Sadie and Hopkins, Paul P., *The Cloud: Understanding the Security, Privacy and Trust Challenges* 2011.

[2] Madhan Kumar Srinivasan, K. Sarukesi, Paul Rodrigues, M. Sai Manoj, P. Revathy, "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment", *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, March, 2012, pp. 470-476.

[3] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, *Master Thesis, University of Texas, Austin*, 2011.

[4] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical *EditorBill Meine, Elsevier Publishing*, 2011.
[5] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, ―Enabling public verifiability and data dynamics for storage security in cloud computing,‖ *In: Computer Security–ESORICS (pp. 355-370). Springer Berlin Heidelberg*, 2009.
[6] Sumit Goyal, Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review, *I.J. Computer Network and Information Security*, 2014, 3, 20-29.
[7] Chiang Ku Fan, Chen-Mei Fan Chiang, Tong Liang Kao, Risk Management Strategies for the Use of Cloud Computing, *I. J. Computer Network and Information Security*, 2012, 12, 50-58.
[8] W. Tsai, Z. Jin, and X. Bai, Internetware computing: issues and perspective, Proceedings of the *first Asia-Pacific symposium on Internetware. Beijing, China*: ACM, p.1-10., 2009.
[9] H. Raj,R. Nathuji, A. Singh, and P. England ,Resource management for isolation enhanced cloud services., *Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA*,2009, p.77–84.
[10] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, *Elsevier, Network and Computer Applications*, Vol. 34, p.1-11, 2010.
[11] J. Milne, Private cloud projects dwarf public initiatives, 2010,http://www.cbronline.com/news/private_cloud_projects_dwarf_public_initiatives_281009 [accessed: 30 April 2012].
[12] D. Nurmi,R. Wolski,C. Grzegorczyk, G. Obertelli, S. Soman, L. Yousef, The Eucalyptus Open-Source Cloud-Computing System. 2009 9th *IEEEACM International Symposium on Cluster Computing and the Grid*, 2009, p.124–131.
[13] Z.A. Khalifehlou, F.S. Gharehchopogh, Security Directions in cloud Computing Environments, *5th International Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara, Turkey*, 17-19 May 2012, p.327-330.
[14] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, *Master Thesis, University of Texas, Austin*, 2011.
[15] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, *International Journal of Engineering Science and Technology*, Vol. 3 No. 4, 2011, p. 2672-2676.
[16] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, *Procedia Engineering, Vol. 23, p.586-593, Elsevier*, 2011.
[17] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, Volume 28, Issue 3, March 2012, P. 583–592.
[18] M. Monsef, N. Gidado, Trust and privacy concern in the Cloud, 2011 European Cup, IT *Security for the Next Generation*, 2011, p.1-15.
[19] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Management in Cloud Computing – A Survey, *Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/InterNetWorks*/TR2011-01, 2011.
[20] H. Takabi, J.B.D. Joshi, G.Ahn., Security and Privacy Challenges in Cloud Computing Environments, *IEEE Security Privacy Magazine*, Vol 8, IEEE Computer Society, 2010, p.24-31.

Authors' Profiles

Seyyed Yasser Hashemi was born in Miyandoab, Azarbayjane Gharbi, Iran, in 1985. He received the B.Sc. and M.Sc. degrees from Islamic Azad University of South Tehran Branch, in Computer Engineering field. He is with Computer Department of Islamic Azad University, Miyandoab Branch since 2008. He is the author or coauthor of more than ten national and international papers and also collaborated in several research projects. His current research interests include voice and image processing, pattern recognition, spam detecting, optical character recognition, cloud computing and parallel genetic algorithms.

Parisa Sheykhi Hesarlo was born in shahindezh, Azarbayjane Gharbi, Iran, in 1992. She is B.Sc. computer Engineering student at Payame Noor University.

How to cite this paper: Seyyed Yasser hashemi, Parisa Sheykhi Hesarlo,"Security, Privacy and Trust Challenges in Cloud Computing and Solutions", IJCNIS, vol.6, no.8, pp.34-40, 2014. DOI: 10.5815/ijcnis.2014.08.05

