ISSN 2310-4090

International Journal of Scientific Footprints

Open Access

A Review on Security Issues in Cloud Computing

Saimunur Rahman[1] and Minhajur Rahman[2]

[1]Department of Business Administration, International Islamic University Chittagong, Bangladesh
[2]Software Engineering and UI Design Lab, FS Systems Limited, Bangladesh

Keywords:
Cloud Computing; Pervasive Computing; Security; Trust; Cloud Solutions.

Correspondence:
Saimunur Rahman. Department of Business Administration, International Islamic University Chittagong, Bangladesh
E-mail: saimun1992@gmail.com

Funding Information:
No funding information provided.

Received:
September 2014; Accepted: October 2014

International Journal of Scientific Footprints 2014; 2(5): 9–21

Abstract

Cloud computing is a hot topic in current computing world. Cloud computing is comes with various features which makes new possibilities for different organizations. Among a lot of challenges faced by cloud users and providers security concerns is one of the major issue. The growth of cloud computing is challenged by the security issues. In this paper we have analyzed several issues in cloud computing environment. Several solutions were proposed to minimize the existing issues in cloud computing. This paper introduces some analysis of existing solutions which can be a motivation for development of trusted solutions in cloud environment.

1. Introduction

Cloud Computing is a type of computing infrastructure that consists of a collection of inter-connected computing nodes, servers, and other hardware as well as software services and applications that are dynamically provisioned among competing users. Services are delivered over the Internet or private networks, or their combination. The cloud services are accessed over these networks based on their availability, performance, capability, and Quality of Service (QoS) requirements. The focus is to deliver reliable, secure, fault-tolerant, sustainable and scalable services, platforms and infrastructures to the end-users. These systems have goals of providing virtually unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. Thus cloud computing is a new way of delivering services.

Depending on the type of service provided, there are three types of cloud services also termed as delivery models; Infrastructure as a service, (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

- IaaS deals with providing computing facility, storage or any other hardware resource. Amazon is one of the cloud providers offering IaaS, where these services are EC2 and S3.
- PaaS provides platforms in terms of operating system and other system software that can be used to build custom applications by the users. User can configure and develop their application on the specific platform. Microsoft Azure is an example of PaaS.
- SaaS deals with using any application or service via cloud. Google Apps is one of the examples that provide collaboration on various applications, like event management, project management etc. via internet.

1.1 Features and Obstacles

Cloud computing started its base in the mid of 2007 and is growing rapidly till date. It has various features that make users want to switch to the cloud computing environment. Some of these features are discussed below:

1. **Elasticity and Scalability:** The cloud resources can be provisioned or de-provisioned as per the increase or decrease in the user demand. The computing power, memory and other facility can be scaled up or down as per the user requirement.
2. **Ease of use:** There is no need to own and maintain hardware, software and other resources by the cloud user. The cloud services are directly accessed using a web browser. No extra resources are needed to run and execute cloud services. A simple desktop with normal internet connectivity is sufficient.
3. **Device and Location Independent:** Since the cloud services can be accessed through web browser, it can be accessed from geographically anywhere and from any device that supports web interface. A cloud service can be accessed like any web service.
4. **Provision for custom application development using PaaS:** Software development using PaaS is easier compared to in-house application development, which requires hardware and software support as well as necessary development tools to be owned, installed and managed. Where-in cloud computing environment development tools and software are available in the form of service which makes development easy and faster.
5. **Reduced cost:** For making an entry in to a business, cost required for infrastructure is reduced by moving to the cloud. As computing power, storage and other resources are used from cloud; cost to purchase as well as manage them is greatly affected. It is advantageous for the organizations if the resources are needed by them only for small duration. So instead of owning them cloud is a better option.
6. **Multi-Tenancy:** A single data server, computing and other resources are shared among multiple users by using virtualization and isolation. This feature termed as Multi-tenancy, allows efficient utilization of resources.
7. **Reliability:** Multiple resources are available like computing power, Storage etc. for providing services to the users. Also the data may be stored at multiple locations by provider. This

redundancy in terms of data storage and other resource enables provision for disaster recovery and achieves reliability and availability of data as well as services.

Along with such advantages for using cloud computing applications and service, there are some obstacles that act as a barrier in its growth. They include:

1. **Lock-in:** It is nothing but the problem of portability and Inter-operability. Lock-in issue could be for data and vendor.
   a. Data Lock-in: Data stored at one cloud site cannot be easily taken back, if a user wishes to change a cloud provider. It may be due to lack of standardized API. This results in a problem of data lock-in.
   b. Vendor Lock-in: A cloud provider gives services in terms of APIs. API made for one provider of cloud is not useful for another providers cloud. If change of provider is required then APIs also has to be changed. This issue is termed as vendor lock-in.
2. **Service Availability:** For a cloud user, service should be available at all time. Whenever a user requests for a cloud service, provider and user has to sign SLA (Service Level Agreement). This defines the terms and conditions and specifications for cloud service. It also includes percentage of time service is available. A cloud user expects a high available service with no or minimal downtime. A cloud provider and its corresponding service are selected based on service availability and business needs.
3. **Bottleneck:** Data transfer bottleneck and service disruption are some of the issues caused due to bandwidth limitation.
4. **Data privacy:** For various organizations, concerns about security, privacy, compliance and control about their data are an obstacle in moving towards the cloud. Specific concerns include:
   a. Loss of governance: A cloud provider site is located in one country and the cloud user may be using the service from another country. User data which is stored from one country is owned and is under the control of cloud provider country. The data is outside organization's direct control, its misuse may have a significant impact on privacy, security and intellectual property claims.
   b. Regulatory compliance: Regulated data may reside in the cloud, the obligation for regulatory compliance may still falls with the organization that owns the data.
   c. Lack of transparency: Cloud vendors do not always disclose the details of how their services work, which third party partners they use, and exactly where data is located. The information about the user data, security measures etc. are generally not known to user.

For global businesses with offices and users in different countries, the issues are even more complex, as legal requirements vary between countries.

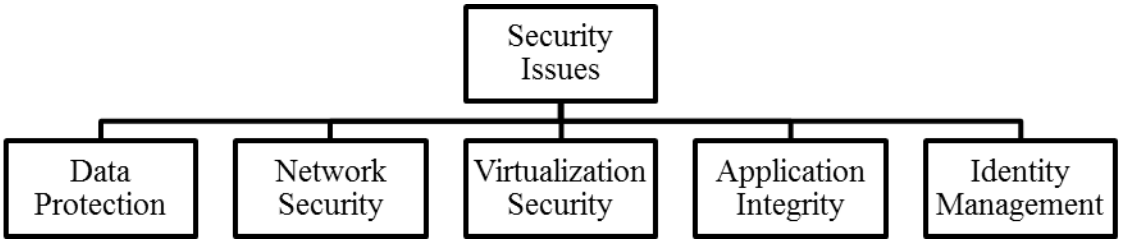
Such obstacles as discussed above acts as a barrier in the growth of cloud computing. Among them security and privacy of data and

applications are the major rising concerns. This paper is organized as follows: section 2 deals with detailed survey about the trust and its evaluation. Trust based solution and its importance is discussed in 3. The actual parameters and the overall model discussed in section 4. Finally section 5 concludes the paper.

2. Security in Cloud Environment

In cloud computing paradigm, a cloud provider creates, deploys and manages the resources, application and services. Multi tenancy and virtualization are the key features to make efficient utilization of the existing resources and application. A single server, computing facility, data center and operating system hosts many users, using virtualization. A large number of users are getting served by a cloud provider by this concept of resources sharing. Data protection, communication, resource management for isolation, virtualization etc. are some of the security issues arises due to multi-tenancy and virtualization in the cloud environment. Major types of security threats in the context of cloud application are briefly described below.

Figure 1: Classification of Security issues



2.1 Data Protection

The cloud computing infrastructure is shared among multiple users at any point of time. User data is stored and processed in the shared environment in a cloud that is under provider's control. User data may be tampered by other malicious entity in the cloud. Lack of transparency about the data storage location in the cloud environment, regulatory issue due to cross border storage etc. makes the requirement of data privacy and protection in cloud environment more prominent.

2.2 Application Security

Application software running on or being developed for cloud computing platforms presents different security challenges. It is depending on the delivery model of that particular platform. Flexibility, openness and public availability of cloud infrastructure are threats for application security. The existing vulnerabilities like Presence of trap doors, overflow problems, poor quality code etc. are treats for various attacks. Multi-tenant environment of cloud platforms, the lack of direct control over the environment, and access to data by the cloud platform vendor; are the key issues for using a cloud application. Preserving integrity of applications being executed in remote machines is an open problem.

2.3 Network Security

A cloud computing can be of type public or private depending on the accessibility of services. Service and applications are accessed from remote locations in a cloud environment. Continuous availability of cloud service without any disruption, denial of service, and other attacks are network security issues. Also Distributed Denial of Service, Signature wrapping attack etc. creates data transmission risks in the cloud network. The virtualization technology has severe impact on network security. Invisible network created by virtual servers makes it difficult to monitor network traffic and performance. Standard network security controls are not sufficient to control VM traffic and their job monitoring. Lack of robust sniffer, tracking and firewalling tools for virtualized network makes it difficult to achieve a secure network.

2.4 Virtualization Security

Virtualization technology introduces new attacks with the hypervisor and other management components. Multi-tenancy in cloud infrastructures for sharing physical resources between VMs (Virtual Machine), can give rise to man in the middle attack at the time of authorization for any service. VMs are created and revert back as and when needed in the cloud environment. Because VMs can quickly be reverted to previous instances, and easily moved between physical servers, it is difficult to achieve and maintain consistent security.

2.5 Identity Management

Identities are generated to access a cloud service by the cloud service provider. Each user uses his identity for accessing a cloud service. Unauthorized access to cloud resources and applications is a major issue. A malicious entity can impersonate a legitimate user and access a cloud service. Many such malicious entities acquire the cloud resources leading to unavailability of a service for actual user. Also it may happen that the user crosses his boundary at the time of service usage in the cloud environment. This could be in terms of access to protected area in memory or performing any other operation that are not maintained in Access control List for a specific resource and application. Thus Identity Management system for providing authentication and authorization is an issue for both provider as well as user in a cloud computing environment. Security concerns are an active area of research and experimentation. Lots of research is going on to address the issues like network security, data protection, virtualization and isolation of resources.

Addressing these issues requires getting confidence from user for cloud applications and services. Obtaining user confidence can be achieved by creating trust for cloud resource and applications, which is a crucial issue in cloud computing. Trust management is attracting much attention. Providing secure access to cloud by trusted cloud computing and by using service level agreements, made between the cloud provider and user; requires lots of trust and reputation management. We will be focusing on the analysis of solution in the cloud computing environment. Also lots of our survey based in the field of trust and trust management.

3. Related Work to Achieve Solutions in Cloud Computing

We conducted extensive literature survey and found that several attempts have been made to address many of the issues mentioned in the earlier section. We have classified the survey based on the type of solutions provided in various collaborative environments. Some of the related works may be consolidated as under for cloud computing:

3.1 General Cloud Security

This section provides the research for general security issues in the cloud computing environment. General cloud computing security considerations at various levels are identified by author [4]. Data security at various protocol stacks, host security, network security and virtualization is discussed with issues and solutions. Various security challenges are identified and addressed in the area of cloud computing by David [5]. Security requirement are considered with risk assessment. Privileged user access, regulatory compliance, data security and long term viability are some of the risk raised by Gartner [6]. Cloud computing security challenges can be handled practically by performing security assessment [7]. An architecture ontology approach for secure cloud computing is defined by Kelvin Jackson [9]. The architecture of cloud includes various security components like Access Management, Security API, Network Security and Storage Security. These components embedded in the cloud architecture to provide secure cloud computing.

3.2 Data Security

A secure cloud also means providing data protection in the cloud. Some techniques to provide data security are discussed as follows. Pearson [1] discusses policies and assessment procedures for privacy enhancement methods and tools. Privacy in terms of legal compliance and user trust, data leakage for sensitive data are provided. Ji Hu Klein [10] gave a benchmark to secure data-in-transit in the cloud. Protecting data during migration is discussed via benchmark for encryption overhead and security. More encryption is desirable for strong security but it requires more computation. So a benchmark gives balance forthe security and encryption overhead. Large scale search system for the purpose of Information exchange between internet communities leads to formation of covert Channels [11]. An agent based security model to control data from covert channel is presented. It may solve the problem of data leakage in the cloud environment. Descher et al [12] discuss the privacy issue by retaining data control to user to increase confidence. Cloud computing attacks are discussed and some provisions and means to overcome from the same are proposed.

3.3 Network protection

Network infrastructure security levels can be enhanced by DNSSEC- Domain Name System Security implementation, developing Denial of Service prevention and router security tactics. [8].

3.4 Protection from attacks at various levels

Jensen et al [2] give the foundations of technical Security issues which consist of web service security using XML and SOAP messages, and Transport Layer security using SSL. Various attacks are considered like XML signature wrapping, browser based, cloud malware injection, metadata spoofing and flooding. Arshad et al [3] propose a

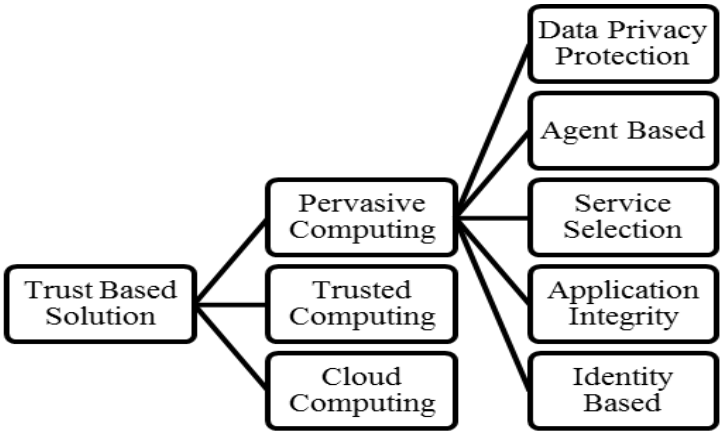
method to assure quality of service for compute intensive workloads in term of security attack, encryption algorithm and authentication. Effective intrusion prevention and detection at the time of resource acquisition is provided. An open source resource manager Haizea is used to perform experimentations and giving an estimation to achieve security. VM specific attack, backdoor protection, guest operating system integrity, etc., are considered as security requirements.

4. Related Research in Trust

Trust is an important aspect of decision making for Internet applications and particularly influences the specification of security policy. It implies depth and assurance of confidence based on some evidence. The trust ability of entity can be defined in a particular regard like security, reliability, availability or any property. The importance of trust can be used for achieving security. Security is an important aspect for trusting an entity in any collaborative environment.

Trust addresses security issues in various collaborative environments. We have identified techniques and methods of incorporating trust in various collaborative environments. Trust evaluation in such environments is discussed in this section.

Figure 2: Classification of Trust Based Solutions



4.1 Pervasive Computing

Lots of research for trust in pervasive environment is going on. Various sub sections are identified depending on the way of obtaining trust in such environments as below:

4.1.1 Data privacy

A trust based approach has also applied to control privacy exposure in ubiquitous computing [25]. Trust values are used to provide fine-grained control over the exposure of personal information. A probabilistic trust management in pervasive computing environment is proposed [22]. Trust decisions in terms of trust metrics are used to provide security and privacy of data. A global trust

management scheme for pervasive computing environment is given [23] to control the data transfer.

4.1.2 Agent based trust evaluation

An automated Agent based trust negotiation scheme for dynamic trust establishment is proposed in [16]. Agent centric approach for intelligent environment is proposed in [17]. Multi stage protocol architecture to maintain and negotiate trust before performing the actual operation among entities, used to evaluate the expected behavior of the device. A dynamic trust model based on agent is presented [21]. Automated trust negotiation using X.509 certificate is used to achieve security. Agent based solution for calculating trust metric in complex environment is achieved by checking user behavior and actions [26].

4.1.3 Trust for service selection

A model called TMSS- Trust Management and Service Selection was presented by the authors Shangyuan Guan et al [19]. A trust space in terms of vector form stores the attribute value of the particular service. These vector values are calculated and updated to measure trust. Dynamic Trust Evaluation Algorithm is presented by authors Liang He et al [20]. It includes systematic and adjusted subjective logic evaluation as well as evolutionary based approach for composite and individual service. A novel Cloud based trust model was presented [15] for entities and their communication by associating uncertainty.

4.1.4 Identity based solution

Identity management solution using trust is achieved by measuring authentication and access control. Trust based solution by developing a security policy, assigning credentials to entities, delegating trust to third party, and reasoning about user access rights [13]. Roles are assigned and can be delegated for controlling user access based on security policy. Access control based on level of trust is given by the trust based security architecture [14]. Trust calculation, updation, reputation evaluation are carried based on experience and recommendations. A Generalized Role Based Access Control is used to propose the architectural framework to calculate trust and reputation of the users and shared facilities [17]. A trust based access control mechanism is proposed for accessing a service in a pervasive computing environment [30]. Access control in the internet is provided by analyzing user behavior trust [31]. A trust based solution comprising of trusted computing also provides access control [28]. Multilevel trust management scheme is proposed by Zhong Dong et al [24]. The multilevel discrete trust metric is used to evaluate reputation for trusted authentication. In virtual computing environments (VCE), resources such as storage, memory, and processors are aggregated together and cooperate with each other to provide services for upper layer applications [27]. In the face of heterogeneous and complex resources, applications must select appropriate and trustworthy resources to achieve robust and reliable performance. A decentralized management of trust for authentication and authorization is given [18].

4.1.5 Application security

Application running in collaborative environments has threats for integrity. Integrity requires that application code is not

tampered with, prior to or during execution, by a rogue user or a malicious software agent. Application oriented trust is proposed by the authors Riccardo Scandariato et al [27]. The integrity of the application that is executed by the remote machine will be maintained by the continuous replacement during run time. The integrity check is done using tag generated by the respective machine to prove its authenticity. This cryptographic method of entrusting required checking the licensing and originality of software that is executed.

4.2 Trust by Trusted computing

A trust model based on trusted computing proposed by Yin Zhixi in [28] for peer to peer systems. For communication between the various peers Identity is more important aspect for security concerns. The identity verification process is implemented by trusted platform module (TPM) of computer hardware where it performs cryptographic authentication that can be used for attestation of the system. Nuno Santos et al [32] proposed the idea of secure cloud computing through trusted computing, named as Trusted Cloud Computing Platform (TCCP). It ensures confidentiality and integrity of computations that are outsources to IaaS.

4.3 Trust based solutions for cloud computing

Incorporation of trust in a cloud environment is an active area of research. Trust based solution for reliability, data protection, user behavior and recommendations etc. are given by various researchers. Hyukho K. et al [33] presents a trust model for efficient reconfiguration and allocation of computing resources depending upon the user request. Trust calculations are made to achieve reliability. A collaborative trust model of firewallthrough based on Cloud Environment is proposed by Zhimin Yang et al [34]. This model uses the trust model based on trust domains and divides the trust relationships among members into within-domain and inter-domain trust relationships according to the domain members, while adding the risk value table. A protocol to establish trust and confidentiality while accessing data is proposed by Mahbub Ahmad et al [35]. User behavior trust evaluation based on time, abnormal degree of behavior and access times is discussed by Tian L. et al [36].

5. Analysis

A security issue in cloud environment is an active area of research and experimentations. We have analyzed the various issues and classified them on the basis of achieving solution by multiple means based on the type of solution provided; i.e. without incorporating trust and with trust. The following section gives the classification of both the types.

5.1 Security issues in cloud computing

Various issues discussed with respect to cloud security are analyzed and categorized based on their type. Many solutions are given in the literature. Solutions mapping to various identified problems are summarized as below:

Table1: Security issues and mapping in cloud

Problems / Solutions	Data protection	Application Security	Network Security	Identity Management	Virtualization
Data leakage / Privacy protection	√	–	–	–	–
Network protection	–	–	√	–	–
Attack prevention	√	√	√	√	√
General cloud Security	√	√	√	√	√

5.2 Analysis of trust based solution

Trust based solutions are also identified in a various computing environment. Some of the security issues in pervasive and ubiquitous computing are identified in terms of accessing data and service. The solutions are categorized based on method of achieving trust for these issues.

Table 2: Trust based solutions

Problems / Trust based Solutions	Data protection	Application /Service
Data Privacy	√	–
Data protection	√	–
Agent based	–	√
Service selection	√	√
Application integrity	–	√
Identity based	√	√

The security goals like Authentication, Authorization, Confidentiality and Integrity can be achieved by having trust between entities. An entity is secure means it is trustable.

6. Conclusion and Future Work

The cloud security issues are attracting great attention since its beginning. Many solutions exist and many are evolving. Issues like information security, data protection, virtualization and isolation are active research area for academics and Industry.

The analysis of security issues in the area of cloud computing is done and various categories identified based on the type of security. Various trust based solution are also categorized based on the way of providing trust in a collaborative environment. Trust based solution also exists for cloud but not

directly addressing all security issues discussed. In future we are trying to look in to the trust based solution for a cloud computing environment.

7. References

[1] Pearson, S. "Taking account of privacy when designing cloud computing services" Software Engineering Challenges of Cloud Computing, 2009, pages, 44 –52, Vancouver, BC.

[2] Jensen, M. Schwenk, J. Gruschka, N. Iacono, "On technical security issues in Cloud" IEEE International Conference on Cloud Computing, 2009, pages 109-16, Germany.

[3] Arshad, J. Townend, P. Jie Xu , "Quantification of Security for compute Intensive Workloads in Clouds", 15th International Conference on Parallel and Distributed Systems, School of Computation, pages 478-486, Dec. 2009, UK.

[4] Saurabh, "Security issues in cloud Computing", http://serl.iiit.ac.in/cs6600/saurabh.ppt, 2009.

[5] David Sherry," Cloud Computing: Security Risks and Compliance Implications", http://media.techtarget.com/searchFinancialSecurity/downloads/FISD09_Breakout_Session5_CloudComputing_Sherry.pdf, June 2009, Brown University.

[6] Gartner "Seven Cloud Computing Security Risks", http://www.infoworld.com/d/security-central/gartnerseven-cloud-computing-security-risks-853?page=0,1, July 2008.

[7] Carl Almond, "A Practical Guide to Cloud Computing Security", http://www.avanade.com/Documents/Research%20anad%20Insights/practicalguidetocloudcomputingsecurity574834.pdf, August 2009.

[8] Diana Kelley," Cloud computing security model overview: Network infrastructure issues", http://searchcloudsecurity.techtarget.com/tip/, 2009.

[9] Kevin Jackson, "Secure Cloud Computing: An Architecture Ontology Approach" http://sunset.usc.edu/gsaw/gsaw2009/s12b/jackson.pdf, DataLine, 2009.

[10] Ji Hu Klein, "A Benchmark of transparent data encryption for migration of web application in cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pages 735 – 740, Chengdu.

[11] Tetsuya, M. Kazuhiro, S. Hirotsugu, K. "A system for search, access restrictions and agents in the Clouds", Ninth Annual International Symposium on Applications and the Internet Cloud, 2009. Pages 201-204, Japan.

[12] Descher, M. Masser, P. Feilhauer, T. Tjoa, A.M. Huemer, D., "Retaining data control to the Client in Infrastructure Cloud", International Conference on Availability, Reliability and Security, 2009, pages 9-16, Dornbirn.

[13] Lalana Kagal, Tim Finin, and Anupam Joshi, "Trust-Based Security in Pervasive Computing Environments", Computing and Processing 2001, pages 154-157, Baltimore, MD.

[14] Naima Iltaf, Mahmud U, Kamran F "Security &Trust Enforcement in Pervasive

Computing Environment", HONET 2006, pages 1-5, NUST Pakistan.

[15] Rui He; Jianwei Niu; Man Yuan; Jianping Hu; "A novel cloud-based trust model for pervasive computing", The Fourth International Conference on Computer and Information Technology,2004, pages 693 – 700, China.

[16] Zhaoyu Liu and Daoxi Xiu, "Agent-based Automated Trust Negotiation for Pervasive Computing", Second International Conference on Embedded Software and Systems, 2005, pages,1-8, USA.

[17] J Basu and V Callaghan, "Towards A trust based Approach to Security and User Confidence in pervasive computing Systems", The IEE International Workshop on Intelligent Environments, 2005, pages 223 – 229, UK.

[18] Tao Sun, Mieso K. Denko, "Distributed Trust Management Scheme in the Pervasive Computing Environment", Canadian Conference on Electrical and Computer Engineering 2007, pages 1219-22,Guelph.

[19] Shangyuan Guan, Xiaoshe Dong, Weiguo Wu, Yiduo Mei, Shihua Liao," Trust Management and Service Selection in Pervasive Computing Environments", International Conference on Computational Intelligence and SecurityWorkshops 2007, China.

[20] Yan Yang, Liang He, Xueming Cai, "A Dynamic Trust Evaluation Algorithm based on Subjective Logic in pervasive computing Environment", 10th International Conference on Automation, Robotics and Vision Hanoi, December 2008,pages 1078-83, Shanghai.

[21] Jing Wang, Zhimin Yang, Yunlei Chen, Weili Kou, Zengguang Zhang, "A Trust Model in Pervasive Computing", Third International Conference on Pervasive Computing and Applications, 2008, pages 370-74, China.

[22] Mieso K. Denko and Tao Sun," Probabilistic Trust Management in Pervasive Computing", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008,page 610-15, Canada.

[23] J. Valarmathi ,Dr.V Rhymend Uthariaraj, G. Arjun Kumar, Praveen Subramanian, R Karthick, "A Novel Trust Management Scheme In Pervasive Computing", The 2nd IEEE International Conference on Information Management and Engineering, 2010, pages 141-45, Chennai, India.

[24] Zhong Dong, Zhu Yian, Lei Wanbao, Gu Jianhua, Wang Yunlan, "Multilevel Trust Management Framework for Pervasive Computing", Third International Conference on Knowledge Discovery and Data Mining, 2010, pages 159-62, China.

[25] Pho Duc Giang, Le Xuan Hung, Riaz Ahmed Shaikh, Yonil Zhung, Sungyoung Lee, Young-Koo Lee and Heejo Lee, "A Trust-Based Approach to Control Privacy Exposure in Ubiquitous Computing Environments", IEEE International Conference on Pervasive Services, July 2007, pages 149 –152, Korea.

[26] Huafei Zhu, Feng Bao, "Computing Trust in a Complex Environment", 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. Pages 1-5, Singapore.

[27] Gup Riccardo Scandariato, "Application-oriented trust in distributed computing", 3rd International Conference on Availability, Reliability and Security, 2008, pages 434-439, Leuven.

[28] Yin Zhixi, "A Secure Trust Model Based on Trusted Computing", International Conference on E-Business and Information System Security, 2009, pages 1 – 7, Taiyuan.

[29] Yunzhao Wei,Yanxiang He, Liming Hao," An identity privacy enhanced trust model in fully distributed virtual computing environments", International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pages 704-708, China.

[30] M Younas Javeed, Sidra Nawaz, Distributed Trust Based Access Control Architecture for Pervasive Computing", The 4th International Conference on Ubiquitous Information Technologies & Applications, 2009, pages 1-6, Pakistan.

[31] Li Wen, Ping Lingdi, Lu Kuijun, Chen Xiaoping, "Trust Model of User behavior in Trustworthy Internet", International Conference on Information Engineering, 2009, pages 403-406, China.

[32] Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues, "Towards Trusted Cloud Computing", Conference on Hot Topics in Cloud Computing 2009, pages 1-5, USA.

[33] Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems", International Journal of Grid and Distributed Computing, March, 2010.

[34] Zhimin Yang at el, "A Collaborative Trust Model of Firewall-through based on Cloud Computing", 14th International Conference on Computer Supported Cooperative Work in Design, 2010, China.

[35] Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, Australia.

[36] Tian Li at el, "Evaluation of User Behavior Trust in Cloud Computing", International Conference on Computer Application and System Modeling -ICCASM 2010, China