A Novel Trust Management System for Cloud Computing - IaaS Providers

Paul D Manuel[1], Mostafa Ibrahim Abd-El Barr[1], S. Thamarai Selvi[2]

[1]Department of Information Science, College for Women,
Kuwait University, Kuwait
[2] Department of Information Technology, Madras Institute of Technology,
Anna University, Chennai, India
p.manuel@ku.edu.kw

Abstract

Trust is one of the most important means to improve the reliability of computing resources provided in cloud environment and it plays an important role in commercial cloud environments. Trust is the estimation of capability of a cloud resource in completing a task based on reputation, identity, behavior, and availability in the context of distributed environment. It helps customer in the selection of appropriate resources in heterogeneous cloud infrastructure. The cloud computing depends on the following QoS parameters such as reliability, availability, scalability, security and past behavior of the cloud resources. This paper introduces a novel trust model to evaluate cloud resources of IaaS (Infrastructure as a Service) providers by means of Trust Resource Broker. The Trust Resource Broker selects trustworthy cloud resources based on the requirements of customer. The proposed trust model evaluates the trust value of the resources based on the identity as well as behavioral trust. The proposed model applies the QoS metrics suitable for cloud resources. The results of the experiments show that the proposed trust model selects the most reliable resources in cloud environment.

Key words: *Cloud Computing, Virtualization, Security, Trust, Trust Resource Broker.*

1. Introduction and Motivation

Cloud Computing is a paradigm that focuses on sharing data and computation over a scalable network of resources. Cloud Computing can be used as more computational-intensive domains by using scalable computational resources and it can also be used as more data-intensive domains by using scalable storage resources. The main idea is to make computing and storage infrastructure available for cloud users in spite of time and location. Cloud infrastructure supports three types of service delivery models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS model delivers specific services and clients can access and use it. PaaS model allows clients to create software as well as use it. In IaaS model, clients are able to create and use his designed software as well as create and use necessary backbone infrastructure to make the software operative. IaaS model also allows deployment of hardware resources with necessary configurations in order to run the software. This paper focuses on the trust issues of cloud resources provided by IaaS providers. The IaaS providers make use of the virtualization techniques for creating the virtual resources in the existing physical

This work was supported by Kuwait University, Research Grant No. [WI 02/08].

resources they have. Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others.

The evolution of internet based cloud computing technology requires trust and security as the major concern to resolve. The conventional business operation involves proper legal documents with signatures and known parties to trust each other. In the internet based cloud computing there is a strong need for establishing the trust between the resource providers and users. The appropriate trust management mechanism reduces the loss for both users and resource providers. The cloud computing differs from the technologies such as distributed computing, cluster computing and grid computing in large scale. Also the resources belong to different resource providers in a completely, distributed, heterogeneous, virtualized and in a scalable manner. The existing trust mechanisms such as authentication and authorization are not suitable for cloud computing.

The paper is organized as follows section 1 gives an introduction about introduction and motivation section 2 discusses the need for trust and section 3 gives an introduction to cloud middleware. The section 4 describes the background and related work, section 5 describes the proposed architecture of Trust Resource Broker for IaaS Providers, section 6 discusses the implementation details, section 7 presents the simulation experimental results and inference and the section 8 concludes the paper.

2. Need for Trust

Cloud Computing has a lot of research focus in recent years and it provides a virtual framework for sharing of resources. In such a geographically distributed environment, an entity has the privilege of using collection of resources. The idea of virtual framework such as cloud is not appealing to some entities because of the risk of being associated with the notion of sharing resources or services. Because of the sensitivity and the vitality of data or information, such entities prefer to use their own closed box resources. This is not just costly for the individual entities but also an inefficient way to utilize resources. To make cloud computing more attractive, trust must be addressed and trustworthy domains must exist where an entity can use resources or deploy services safely. In such a scenario the user/consumer and the resource provider does not have complete control over each other. The user/consumer expects good Quality of Service from a trustworthy service provider. The service provider expects the cloud resources to be protected and it allow the cloud resources to be utilized by a trustworthy consumer. To achieve this it is necessary to establish trust across the cloud, between the user and the service provider.

Trust is a complex subject relating to an entity's belief in honesty, trustfulness, competence and reliability of another entity. In most of the existing distributed heterogeneous networks, trust between a consumer and a service provider is established based on identity and reputation. This identity-based trust model is concerned with verifying the authenticity of an entity and what it is authorized to do. This however does not ensure consistency, promptness of service and Quality of Service, resulting in loss to the consumers. This problem is overcome in reputation-based trust management. Reputation of an entity is a measure derived from direct or indirect knowledge of the entity's earlier transactions. In this model, a certification process verifies the consistency of services offered by a service provider. The consumers who have had transactions with the service providers provide feedback on various aspects of the services provided by the service providers. The feedback received for a service provider from various consumers is aggregated over a period of time. This forms the reputation of the specific service provider and the consumer first confirms the behavior of the service provider as being trustworthy

or not, before proceeding to use the service provider. This ensures Quality of Service for the consumer. This scheme is very appropriate in a cloud environment where entities are distributed geographically.

Trust management is an intrinsic element of commercial aspect of cloud. An important goal of trust management in cloud resources is to establish faith and confidence on resource providers in the internet based distributed environments. Trust is the major complex issue in the Cloud Computing arena and there is no specific trust model available for cloud computing. The companies like e-bay, Amazon have implemented the reputation based trust management system for e-transactions and it helps them to improve the quality of service based on the user's feedback value. The efficacy of a reputation based trust management system depends on the trust model behind the system. E-bay is a typical example for reputation based system that is built on centralized model of trust, in which every entity in the centralized model. The other trust model is called as Transitive Trust Model, in which the recommendation from the recommender is highly emphasized for the trustworthiness. There is little work carried out to evaluate the trustworthy of the resources available in the cloud environment. In our proposed reputation based novel trust model, the trust value is computed based on the values such as identity level of the resources as identity-based trust, capability of the resources as capability-based trust and behavior of the resources called as behavior-based trust.

3. Introduction to Cloud Middleware

In our proposed approach we are using Eucalyptus as cloud middleware and it is open source middleware and pioneer of the cloud-computing world [19]. It is based on popular open-source Linux systems and it is compatible with the Amazon Elastic Cloud Computing (EC2) SOAP interface. The Eucalyptus platform has a three-level hierarchical architecture. The top-level hierarchy consists of Cloud Controller Node and its role is to aggregate and coordinate the cloud resources as a whole and to handle client management requests. The middle-level contains the Cluster Controller and it is responsible for keeping track of resource usage in its cluster. The lower level contains the Node Controller, which is responsible for monitoring resource usage and managing virtual resources. Our proposed Trust Resource Broker considers the Eucalyptus enabled cloud resources.

4. Background and Related work

There is lot of reputation based trust management systems available, which has dealt mainly based on the history of experience from others. Grandison et al [3] have surveyed the several existing trust models mainly focused on Internet applications and they define the trust "the firm belief in the capability of an entity to act consistently, securely and reliably within a specified context". They also claim that the trust is the composition of multiple attributes such as reliability, honesty, truthfulness, dependability, security, competence, timeliness, Quality of Service (QoS) and Return on Investment (ROI) in the context of an environment. The main contribution of this paper is a good conceptual definition for trust and the establishing of some trust properties. They have not addressed the computational trust management models, they have focused more on trust based on certification, and they have not addressed the reputation-based trust. Ganeriwal et al [4] have designed the reputation based trust management framework for sensor networks. This framework evaluates the trustworthiness of sensor nodes based on their behaviors and they have not addressed the issue in cloud resources. Rochwerger et al [5] have proposed the reservoir model and architecture for Open Federated Cloud Computing. Josang et al [6]

have proposed the various approaches related to online activities where trust is relevant and where there is a need for trust management. Vishwas et al [8] have presented a comparative analysis of various approaches of identity based trust management in practice that integrates technology with other factors. Torsten et al [9] have proposed a reputation-based conceptual framework and it consider the economic issues for commercial grid and it describes the role of reputation in grid environments incorporating three basic perceptions such as technology, business, and policy. Chapin et al [10] have surveyed modern state-of-the-art technology in trust management authorization, focusing on features of policy and rights to guarantee the committed security properties. Ian Foster et al [11] have compared and contrasted cloud computing with grid computing from various perspectives and give an insight into the essential characteristics of both. Marty Humphrey et al [12] have described the security aspects for grids with the set of challenges that are applicable for cloud also. Shyamsundar et al [13] have described the design and implementation of the Role-based Authorization and Delegation System, which give the motivation for Role-based Authorization in our proposed trust management system. Dan Jong Kim et al [14] have described multi-dimensional trust model for on-line exchange that may be applicable for cloud too. Urquhart [15] explains the biggest cloud computing issue is trust and he mentions that there is need of more trust between customers and service providers because of the dynamic nature of cloud. Nuno Santos et al [16] have proposed a design of trusted cloud computing platform (TCCP). This design enables IaaS providers such as Amazon EC2 to provide a closed box execution environment that guarantees confidential execution of guest virtual machines. The TCCP does not consider the reputation, identity and capability based trust. Ashish C.Morzaria [17] has given emphasis to trust and he mentioned that trust is the secret to cloud computing success. Rui He et al [18] have proposed the novel cloud-based trust model for pervasive computing. Sheikh et al [19] have proposed trust-based secure service (TSSD) model for truly pervasive environment. This model is hybrid one that allows both secure and non-secure discovery of services and it allows service discovery and sharing based on mutual trust. Sheikh et al [20] have described omnipresent Formal Trust Model (FTM), which is context specific, and reputation-based trust model suitable for peer-to-peer and ad-hoc environments. Abdul-Rahman et al [21] have proposed the reputation is an expectation about and agent behavior based on information about or observations of its past behavior. Josang et al [22] have proposed reputation is the belief about the persons or things character or standing and also they have argued the reputation is the meaning of building trust using this trust value, one can trust another based on reputation. Therefore, reputation is a measure of trustworthiness in the sense of reliability.

5. Architecture of Trust Resource Broker for IaaS Providers

The proposed Cloud Trust Management System (CTMS) integrated with the Trust Resource Broker computes the reputation based trust value of the cloud resources in IaaS based on the following and it is depicted in Figure 1.

- The identity trust is calculated based on the security level of the resources available in the IaaS providers.
- The capability trust is calculated based on the power of processor, memory, bandwidth, and storage capacity of the resources available in the IaaS providers.
- The behavior of the resources is calculated based on the availability, success rate and the user's feedback about the computational/storage transactions takes place in the cloud resources available in IaaS providers.

The trust resource broker allows only the authenticated users allowed to perform the

operation/transaction in cloud resources. The users are authenticated through the Kerberos [24] & [25] based authentication mechanism and it allows the authenticated user to access the cloud resources based on the access control rights the user may have.

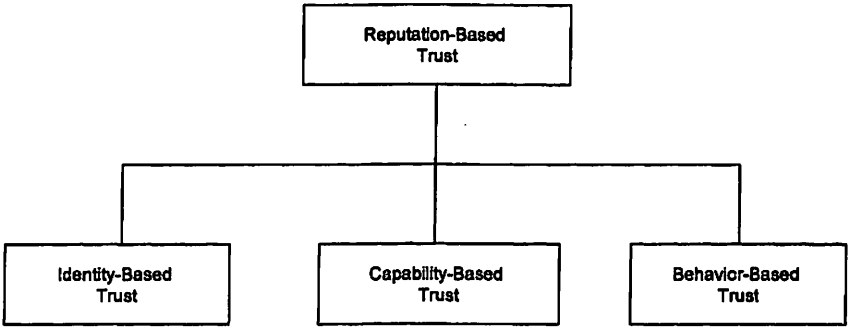

Figure 1. Reputation Based Trust

The users are assigned with specific roles and permissions using PERMIS [26] based authorization. The Trust Resource Broker is developed using the Simple Access Object Access Protocol (SOAP) based web services. By incorporating the CTMS in the Trust Resource Broker, we demonstrate that the Trust Resource Broker can able to find trustworthy cloud resources. The proposed architecture of Trust Resource Broker for cloud resources is shown in Figure 2.

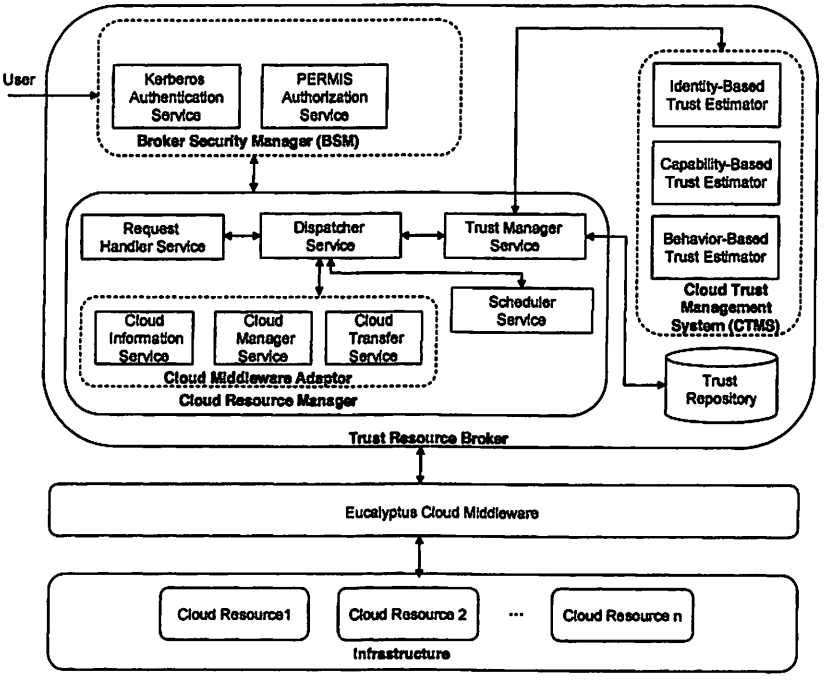

Figure 2. Trust Resource Broker for IaaS Providers

The Trust Resource Broker comprises of three main modules as follows:

1. Broker Security Manager (BSM)
2. Cloud Resource Manager (CRM)
3. Cloud Trust Management System (CTMS)

5.1 Cloud Security Manager (CSM)

The Cloud Security Manager comprises of Kerberos Based Authentication Service and PERMIS Role Based Authorization Service. Kerberos [24] & [25] is network authentication protocol and it was developed by MIT in mid 1980s. Kerberos is an authentication mechanism for authenticating the user using their credential without transmitting a password either in the form of clear of hashed manner. Kerberos is designed to prove the user's identity and it has been enhanced with single sign-on property. The conventional authentication systems which challenge a user for a user ID and password but Kerberos issues the authentication tickets. It works around the principle of Kerberos server or Key Distribution Center (KDC).

The PERMIS [3] Role Based Authorization Service authorizes and allows the operations based on the user and the roles in the LDAP repository. PERMIS was developed as role based access control infrastructure and it is based on X.509 attribute certificates (ACs) to store the users' roles. The access control decisions are managed by authorization policy and it is stored in an X.509 attribute certificate to guarantee the integrity of the user. The Attribute Certificates are stored in Light Weight Directory Access Protocol (LDAP). PERMIS has a tool called Privilege Allocator and it is used to sign the attribute certificate and store in an LDAP directory for Access Control Decision.

The Kerberos based authentication service and PERMIS based authentication service enhances the security measures of the broker compared to the conventional security mechanism.

5.2 Cloud Resource Manager (CRM)

The Request Handler Service is responsible for handling user requests and identifying suitable cloud resources based on the user requirements. The Dispatcher Service is responsible for invoking the Scheduler Service, Trust Manager Service and Eucalyptus Adaptors based on the situation. The Scheduler Service is responsible for selecting the most trustworthy resources from the matched resources. The Trust Manager Service invokes the Cloud Trust Management System computes the trust values of the cloud resources. The Cloud Information Service aggregates the resource information such as Processor Speed, Free RAM, and Hard Disk space, number of virtual machines running, bandwidth, and latency. The Cloud Transfer Manager Service is responsible for transferring the images of the operating system demanded by the user and the user required libraries, input files, and executables if the user is trying to perform any computational operations. The Cloud Manager Service is responsible for invoking the cloud middleware to provision the required resources. The resource may be created on demand as virtual resource or the freely available resource may be provisioned.

5.3 Cloud Trust Management System (CTMS)

The Cloud Trust Management System consists of the following major components to compute the trust value of the resources.

1. Identity-Based Trust Estimator (IBTE)
2. Capability-Based Trust Estimator (CBTE)
3. Behavior-Based Trust Estimator (BBTE)

5.3.1 Identity-Based Trust Estimator (IBTE)

The Identity-Based Trust Estimator is responsible for measuring different security levels in cloud resources. In cloud computing a single application or platform or infrastructure has been shared by multiple users/tenants. Tenants/Users may be separate users, companies, or departments within a company, or even just different applications. Cloud computing takes the advantage of web based mechanisms that allow scalable, virtualized storage or computational resources to be provided as a service over a network. The main requirement for multi-tenant computational or storage resource is to ensure the security of tenant/user data. The resource provider should protect the user data from the following security threats such as:

- Snooping - The user data could not able to gain unauthorized access to another user's data. The user data must be restricted to their own computational or storage resources.
- Spoofing – The authentication mechanisms must ensure that no one can access a user's identity to gain data access.
- Deletion – The accidental or malicious action external to the virtual resource should cause user data within the resource to be deleted or corrupted.
- Denial of service – The user data access should not be disrupted by direct denial of service attacks against the resources.

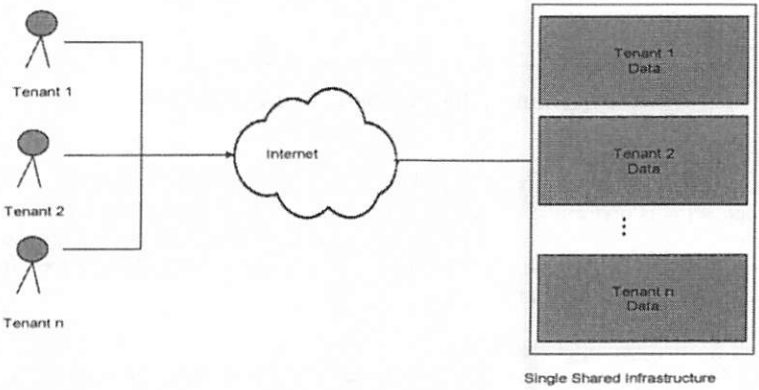

Figure 3. Multi-tenant Architecture

The multi-tenant security is achieved by isolating one user's virtual resources from another user's. The efficient and careful tenant/user security measures are necessary to ensure security against possible malicious attacks. Encryption of data as it is stored on the underlying storage may also be provided as an option to meet the security concerns of the most sensitive tenants. In our proposed architecture of Cloud Trust Management System, the security level is considered as an important factor for computing the trust value of the resource provider. The security attributes repository as shown in Figure 4 is used for storing the available security levels of each resource provider. The security level of the resource provider has been classified into the following security levels in our proposed architecture:

A. Authentication level
B. Authorization level
C. Self-Security competence level
D. User Protection level

E. Data Security level
F. Data Recovery level

A. Authentication level

Authentication deals with verifying the identity of an entity in the network. An identity may be a user, a resource or a service provider. The Authentication level of the cloud resources is verified by the authentication mechanism implemented in the cloud resources. The Kerberos based authentication and X.509 based authentication is more secure compared to simple password based authentication.

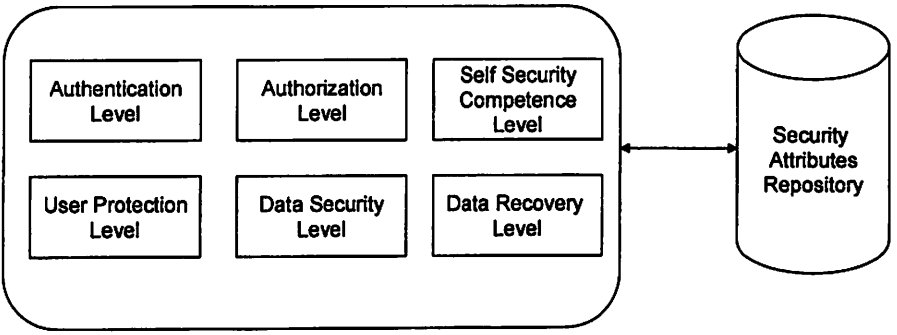

Figure 4. Identity-Based Trust Estimator

B. Authorization level

Authorization deals with verifying the action that an entity can perform once the authentication is performed successfully. The Authorization level of the cloud resources is verified based on the type of authorization mechanism used by the service providers. The identity-based and attributed-based authorization is more secured compared to simple password-based authorization.

C. Self-Security competence level

The self-security competence or self-defense capability level of cloud resources is computed by considering the following security attributes in the cloud resources. The physical and virtual infrastructure is more vulnerable to security attacks if they are not properly protected. To identify the resource, which is less vulnerable to attacks are based on the following values such as follows:

- Firewall – Number of firewall rules present in the resources.
- Protection Against Virus – How much the antivirus software is protecting the data?
- Malware Protection – How much the malware is protected based on the protection mechanism?
- IDS – Availability of Intrusion Detection System

D. User Protection level

The cloud computing or any type of online application should consider the protection of the data related to the users. The private data related to the user such as phone number, credit card number, personal identity etc and it should not misuse and alter by others. The value may be low or high ranging between 0 and 1.

E. Data Security level

The resource provider has to give the protection of data by encrypting the data based on encryption algorithm. The value may be low or high ranging between 0 and 1.

F. Data Recovery Level

In addition to prevention, the recovery mechanism is also important. The resource provider should consider the data recovery in case of any loss of data due to any disaster. The value may be low or high ranging in between 0 and 1.

Based on the above said six security levels and it each level varies from 0 to 1. The six security level value is taken and the average value of the six security level is calculated and the calculated trust value based on the security level is T_I using the Equation (1).

$$T_I\left(R_i\right) = AU_L + AZ_L + SS_L + UP_L + DS_L + DR_L / TS_L \quad \text{Equation (1)}$$

Where AU_L represents the authentication level of resource, AZ_L represents the authorization level of resource, SS_L represents the self security competence level of resource, UP_L represents the user protection level of resource, DS_L represents the data security level of resource, DR_L represents the data recovery level of resource and TS_L represents the total security level consider for trust calculation.

5.3.2. Capability-Based Trust Estimator (CBTE)

The current capability of the cloud resources should affect the performance of the application execution and file transfer or data transfer. The capability based trust value of the resources is calculated using the Equation (2) and it is based on Computational Parameters such as Processor Speed and RAM Speed and Network Parameters such as Bandwidth and Latency is considered in our trust computation.

$$T_B\left(R_i\right) = (2 * \mathrm{P}\,Speed + RSpeed) + (Bandwith / latency) \quad \text{Equation (2)}$$

Where *PSpeed* represents the processor speed of the i^{th} resource, *RSpeed* represents the Ram Speed of the i^{th} resource, *Bandwidth* represents the amount of data transferred at time of the i^{th} resource and *Latency* represents the delay to reach i^{th} resource.

5.3.3 Behavior-Based Trust Estimator (BBTE)

The Behavior-Based Trust Estimator computes the trust value of a cloud resource based on the performance factors such as availability (A_{Ri}), success rate (S_{Ri}) and user's feedback (F_{Ri}) about the resources over a period time using the Equation (3).

$$T_B\left(R_i, n\right) = A_{Ri} \times S_{Ri} \times F_{Ri} \quad \text{Equation (3)}$$

A. Availability

The availability of the resource refers to number of times the resources available versus total number of times the resource has been queried for transaction. The availability of the resource provider is calculated using the Equation (4).

$$A_{Ri} = \mathrm{NTA}_{Ri} / \mathrm{TNTQ}_{Ri} \quad \text{Equation (4)}$$

Where NTA_{Ri} represents the number of times resource available and $TNTQ_{Ri}$ represents the total number of times the particular resource available.

B. Success Rate

The success rate of resource refers to number of successful transactions take place in the resource versus total number of transactions place in the particular resource. The success rate of the resource provider is calculated using the Equation (5).

$$S_{Ri} = \mathrm{NST}_{Ri} / \mathrm{TNT}_{Ri} \qquad \text{Equation (5)}$$

Where NST_{Ri} represents the number of successful transactions by the resource provider and TNT_{Ri} represents the total number of transactions over the particular resource provider.

C. Feedback

The user submits the feedback or rating of the resource provider to the Trust Resource Broker once the service requested by the user has been completed. The feedback reflects the quality of service provided by the resource provider during a transaction. The Feedback collector collects the feedback, identifies the biased and unbiased values and computes the trust value based on feedback and updates the trust value feedback repository database. User feedback is an important factor in the resource provisioning of cloud resources, because the feedback of the user can ensure the reliability of cloud resource. The user's feedback also helps to improve the performance of the resource provider's to adapt them to the changes demanded by the user's requirements. The feedback is given over a range of values from 0 to 1, where 1 represents the most trustworthy and 0 represents the non trustworthy resource. Initially the feedback value of the resource has been assigned to 0; it indicates that there is no trustworthy information available about the resources. The trust value can be modified dynamically during the course of transactions it reflects the current or latest behavior of cloud resources.

The existing trust models which have been implemented in peer-to-peer networks distributed computing, grid computing have taken all the feedback about the resources given by the user. There may be some malicious user who can give the false feedback about the cloud resources which has been accessed by them. In general these false feedbacks about the resource may alter the decision of choosing the resource by the trust resource broker. In real world scenario there may be lot of malicious users purposefully entering into the cloud to distract the cloud resources by giving false feedbacks. The existing approach simply uses the feedback values given by the users and evaluates the trustworthiness of the resource provider based on the feedback values. But the existing approach does not have answer for the following questions such as

- Whether the feedback value given by the user is reliable?
- Whether the feedback value given by the user is unbiased?
- Whether the feedback value given by the user is trustworthy?

The proposed approach compares the feedback value given by the user about the cloud resources with the other user's feedback value. If there is a positive correlation of user given feedback with other user's feedback value it has to be taken into account else the feedback has been discarded by the feedback evaluator.

i. Feedback Collector

The Feedback Collector collects the user's feedback about the resource provider's quality of service and the user's satisfaction. It computes the trust value based on the feedback. The values are obtained through the Feedback Portal of the Trust Resource Broker. The user feedback of the cloud resources in IaaS provider has been calculated based on the following parameters:

- User/Customer Satisfaction – whether the user/customer is satisfied with the particular transaction in the cloud resource?
- Deadline – whether the user's request is completed within the deadline?

- Reliability of Network – whether the network connectivity is reliable throughout the user interaction?
- Success/failure – whether the user's request is successfully completed or not?
- Economical Feasibility – whether the cost is affordable or not?

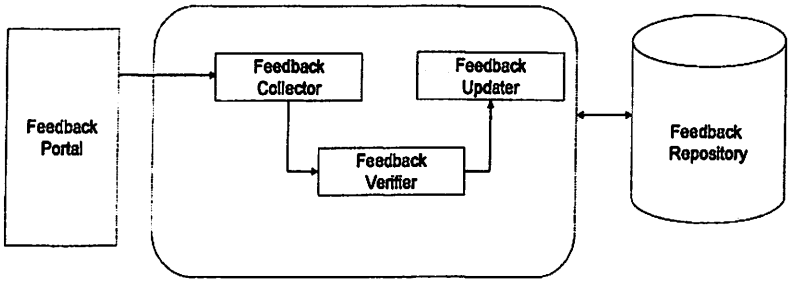

Figure 5. Feedback Collector and Verifier

The above feedback values may be 0 for NO and 1 for YES. The final feedback value is calculated by averaging the values and the computed trust value is F_{RI}.

ii. Feedback Verifier

The Feedback Verifier verifies the feedback submitted by the user about the resource provider's service. The Feedback Verifier maintains a threshold value and the allowable minimum threshold difference value be T 0.05 is used as minimum threshold value.

Algorithm 1 Feedback Verifier to find biased and unbiased feedbacks

1. Let the consumer feedback rating be $cf_1 = \{CFR_0, CFR_1, \ldots CFR_n\}$
2. Let the broker feedback rating be $bf_1 = \{BFR_0, BFR_1, \ldots BFRn\}$
3. Compute the expectation values $E(cf_1)$ and $E(bf_1)$ of the sets cf_1 and bf_1.
4. Compute the standard deviations of the set cf_1 and bf_1 of SD_1 and SD_2 using the Equation (6) and Equation (7) respectively as follows.

$$SD_1 = \sqrt{E(cf_1^2) - [E(cf_1)]^2} \qquad \text{Equation (6)}$$

$$SD_2 = \sqrt{E(bf_1^2) - [E(bf_2)]^2} \qquad \text{Equation (7)}$$

5. Using the same expectation values and standard deviation formula from the previous algorithm, compute the regression line using Equation (8) as

$$\frac{cf_1 - E(cf_1)}{SD_1} = \frac{r(bf_1 - E(bf_1)}{SD_2} \qquad \text{Equation (8)}$$

Here r is the correlation coefficient where

$$r = \frac{E(x_1 x_2) - E(x_1)E(x_2)}{SD_1 SD_2}$$ Equation (9)

6. Assign the r value to FRi such as $FR_i = r$

If this correlation coefficient value of F_{RI} > threshold value then the feedback from the consumer is considered as biased one as it deviates from the broker's threshold value of 0.05.

iii. Feedback Updater

The Feedback Updater receives the verified user's feedback from the Feedback Verifier and updates the user's feedback in the Feedback Repository.

iv. Feedback Repository

The Feedback Repository is the database, which is used to store the user's feedback on the resource providers and to make use of them for future trust computation.

6. Trust Calculation

The trust value based on the identity is T_I, the trust value based on the capability is T_C, and the trust value based on the behavior is T_B. The initial values of T_I, T_C and T_B values are assumed a small value, say 0.01.The Total Trust value of the resource T_T has been calculated as shown in Equation (10) and the final total trust value should be 0 to 1. The weightage factors a, b, c are assigned with values in proportion of 0.3, 0.4, 0.3. The weights can be assigned and varied based on the needs.

$$T_T = a * T_I + b * T_C + c * T_B$$ Equation (10)

$$\text{where } a + b + c = 1$$ Equation (11)

In our trust computation the initial trust value of the capability and identity level trust value is considered. The behavioral trust is taking into account after some transactions on the resource. Let us consider the three resources R1, R2 and R3 respectively based on our real experimental setup. The resource R2 has provided with maximum-security level compared to other two resources R1 and R3. The identity-trust value of the resources has been shown in Table 1.

Table 1. Identity-Based Trust Value

S. No	Resources	Identity-Based Trust Value $T_I(R)$
1	R1	0.5
2	R2	0.7
3	R3	0.4

The capability-trust value of the resources has been shown in Table 2. The resource R1 has more capable compared to R2 and R3.

Table 2. Capability-Based Trust Value

S. No	Resources	Capability-Based Trust Value $T_C(R)$
1	R1	0.6
2	R2	0.5
3	R3	0.3

The behavior-trust value of the resources has been shown in Table 3. The past behavior of the resource R2 is excellent over others based on the availability, successful execution of jobs and the feedback about the resources.

Table 3. Behavior-Based Trust Value

S.No	Resources	Availability Trust Value (A_R)	Success Rate Trust Value (S_R)	Feed back based Trust Value (F_R)	Total Behavioral Trust Value (T_B)
1	R1	0.8	0.18	0.6	0.240
2	R2	0.9	0.2	0.7	0.504
3	R3	0.5	0.3	0.4	0.006

The Total trust value of the resources has been computed as shown in Table 4. The weightage factors of a, b, c are 0.3, 0.4 and 0.3 respectively.

Table 4. Total Trust Calculation

S.No	Resources	Identity-Based Trust Value (T_I) * (a)	Capability-Based Trust Value (T_C) *(b)	Behavioral –Based Trust Value (T_B) * (c)	Total Trust Value (T_T)
1	R1	0.15	0.6	0.072	0.822
2	R2	0.21	0.5	0.151	0.861
3	R3	0.12	0.12	0.002	0.242

From this table we infer that the resource R2 is the most trustworthy resource, followed by R1 and R3. Our proposed Trust Management System identity the most reliable and the most capable resource to execute the job with minimal execution time in a reliable mode.

7. Implementation Details

The proposed architecture is developed using the Netbeans 6.7 as development environment, oracle 11g as database for storing trust values and Eucalyptus-2.0.0 as cloud middleware. The Kerberos authentication and PERMIS authorization mechanisms are incorporated with Trust Resource Broker to enhance the security measures of the resource broker. All the services that are listed below are implemented as SOAP based web services in Netbeans 6.7 and it has been deployed in the Glassfish Sun Server v3.

7.1. Kerberos Authentication Service

The SOAP based web service is developed to act as an interface for Kerberos authentication mechanism and the user. This service retrieves the user id and generates the authentication ticket for a period of time. Once the user has been authenticated it invokes the PERMIS based authorization service.

7.2. PERMIS Authorization Manager Service

This service uses the Kerberos tickets to hold users roles/attributes. This service maintains the roles for each user based on the roles the user can able to perform specific action in the cloud resources. Once the user role has been verified, the user request has sent to the Request Handler Service.

7.3. Request Handler Service

The authenticated and authorized request is parsed by the Request Handler Service creates the user requirements in the Request Pool. The Request Handler Service invokes the match making algorithm and the match making algorithm matches the user requirements with the resource information available in the Resource Pool to identify suitable resources for creating virtual resources. The request id and matched resources or capable resources which can able to satisfy the user request is sent to the Dispatcher Service.

7.4. Dispatcher Service

The Dispatcher is the central core component of the Trust Resource Broker. It invokes the appropriate components based on the input that it receives from other services like Request Handler Service, Scheduler Service, File Transfer Manager Service and Virtual Infrastructure Manager Service.

7.5. Scheduler Service

The Scheduler is responsible for choosing the trustworthy resource from the matched resource. The Scheduler invokes the Cloud Trust Management System for computing the trust value of a cloud resource. Based on the trust values of the cloud resources, the Scheduler schedules the cloud resources to the Dispatcher for virtual resource creation.

7.6. Trust Manager Service

The Trust Manager Service is responsible for computing the trust value of cloud resources. The Trust Manager Service computes the overall trust value of the cloud resource using the identity-based trust estimator, capability-based trust estimator and the behavior-based trust estimator. The computed trust value is sent to the scheduler.

7.7. Cloud Information Service

The Cloud Information Service is responsible for aggregating the physical resource information and the virtual resource information. This information is maintained in the Resource Pool of the Trust Resource Broker and updated dynamically.

7.8. Cloud Transfer Service

The Cloud Transfer Service uses the File Transfer Protocol (FTP) and it is responsible for transferring input files (data) from the user to the cloud resource and it is also responsible for transferring the output files (processed data) to broker/user if the user is performing any computational operations.

7.9. Cloud Manager Service

The Cloud Manager Service is responsible for invoking the user's operation in the remote resource. This module interfaces with Eucalyptus middleware for virtual resource creation and deletion.

8. Experimental Setup and Evaluation

The following experimental setup as shown in Figure 6 has made in our research laboratory for testing the proposed work in real world scenario. The experimental setup consists of the trust resource broker named cloudtrustbroker.mit.in and three cloud resources namely cloudserver1.mit.in, cloudserver2.mit.in, and cloudserver3.care.mit.in and it is managed by the cloud middleware of Eucalyptus 2.0.0. The cloud resources are virtualization enabled by the use of Xen 3.0.0 hypervisor over the physical resources.

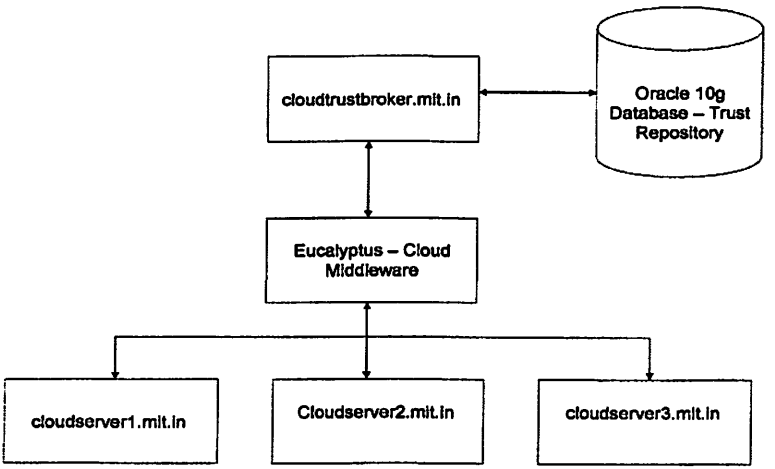

Figure 6. Experimental Setup

9. Simulation experimental results and Inferences

Simulation is techniques for performing experiments on a system other than construct a real system. It is a simpler and effective approach for analyzing and evaluating designed mechanisms, protocols, algorithms. Cloud is a simulation toolkit developed by Buyya et al. (2009) for creating cloud simulation environment. The simulated cloud environment

consists of m resources and each resource has characterized with different capabilities of computational parameters such as different processor speed, hard disk memory, ram memory and network parameters of varying bandwidth and latency to incorporate the heterogeneous concept. The simulation has been carried out using the latest beta version of cloudsim-2.0.0, java environment as jdk1.6.0_21 and ant compiler as ant-1.7.1 version. The Trust Management System is integrated with cloud simulation toolkit to select the resources based on trust value other than time based and spaced based resource allocation. The simulation is carried out by varying the task number from 10 to 100 with different user requirements of processor speed, ram memory, hard disk memory and number of nodes requirements.

10. Simulation results and discussions

In our simulation experimental results, we mainly concentrate on two factors such as job success rate, execution time and utilization of the resources. The simulation experiment has been carried by varying the capability trust values the resource which is having capability trust value executes the job from the queue with minimal execution time as compared to non-trusted resources and the measures has been shown in Figure 7.

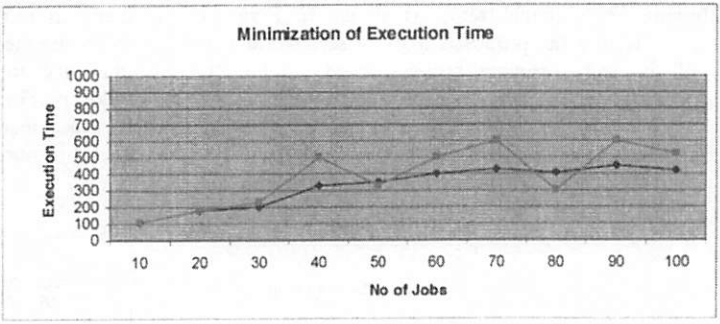

Figure 7. Minimization of Total Execution Time

The simulation experiment has been carried out with behavioral trust and without behavioral level trust and the performance has been analyzed as shown in Figure 8. The trust based resources increases the job success rate gradually increases in a steady state manner and it has been represented in blue line but the non-trusted resources has the variations in the job success rate and it has been represented in pink color.

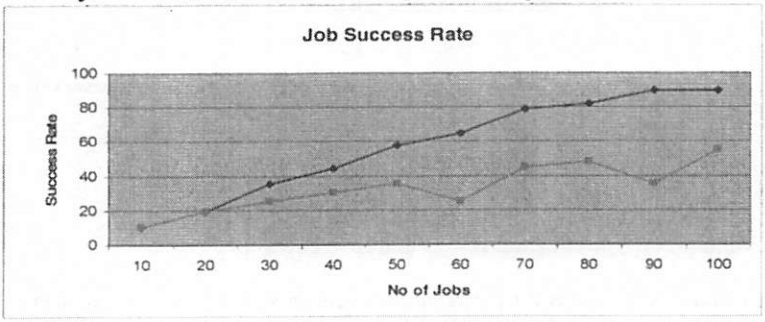

Figure 8. Job Success Ratio

The simulation experiment has been carried out by combining the identity trust, capability trust and behavioral trust and the performance has been analyzed as shown in Figure 9. The overall utilization of trust resources are more compared to non-trusted resources.

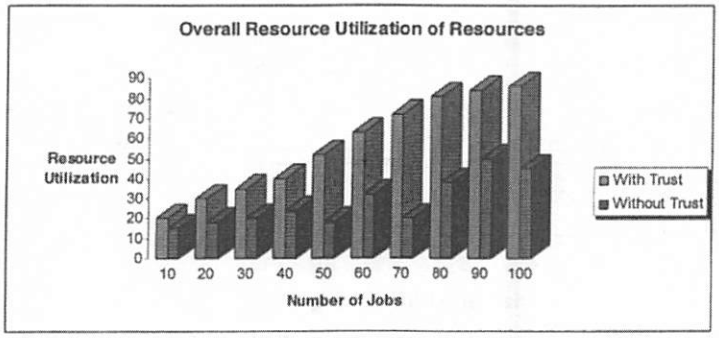

Figure 9.Overall Utilization of Resources

The proposed trust model/protocol is simulated using the CloudSim toolkit and sample of 200, 400, 600, 800, 1000 requests and 5000 nodes of cloud resources and the request has been submitted to the Trust Resource Broker. The above requests is tested both with trust based model and non-trust based model. The percentage of requests handled successfully with respect to the submitted requests is plotted as shown in Figure 10. The proposed trust model increases the success rates, user satisfaction, and utilization of resources in a best manner. The success rates in case of trusted resources are above 80% whereas the success rate is very low in case of non-trusted resources.

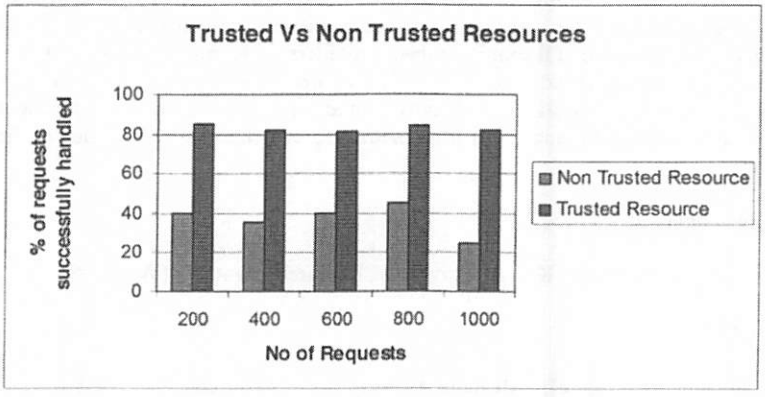

Figure 10. Successful Requests Handled

The user's satisfaction level is plotted based on the feedback given by the user. The user's satisfaction increases for the trustworthy resources over a period of time whereas the satisfaction level is fluctuating and it is unpredictable for non-trusted resources as shown in Figure 11.

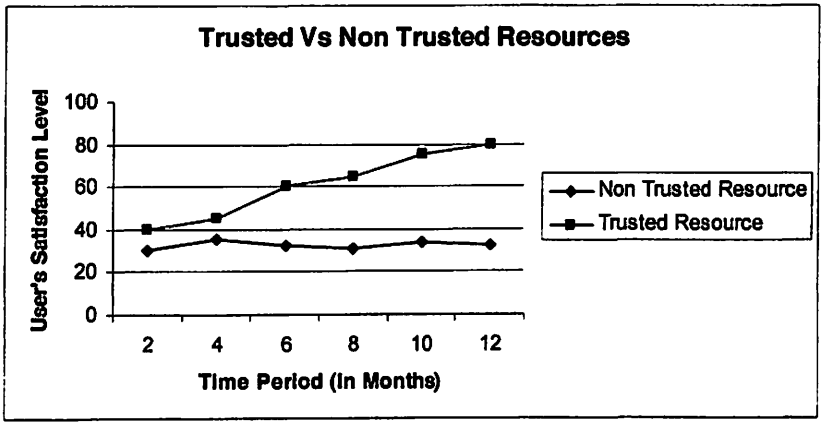

Figure 11. Level of User's Satisfaction

11. Conclusion and Future Work

This research paper proposes a Trust Resource Broker for cloud resources of IaaS providers. The Resource Broker is implemented with Kerberos authentication and PERMIS authorization service enhances the security measures of the trust resource broker. This proposed Trust Resource Broker evaluates the trust value of the cloud resources provided by the IaaS providers and resource selection based on the computed trust value improves the QoS of cloud resources of IaaS providers. The Behavior-Based Trust Estimator computes the trust value of a cloud resource based on the performance factors such as availability, utility, capability of the cloud resource provider per unit time and security level of the cloud resources in IaaS providers. The proposed trust model increases the reliability of the cloud resources, it is an important factor in the cloud. It is also possible to extend our work to SaaS providers and PaaS providers. As future work, it is proposed to incorporate additional trust metrics to evaluate the trust values of the cloud resources.

Acknowledgement

This work is supported by Kuwait University, Research Grant No. [WI 02/08]

References

1. Luhmann, N. (1990d), "Meaning as sociology's basic concept", In Essays on self-reference, pp. 21–79, New York: Columbia University Press.
2. Diego Gambetta, "Trust: Making and Breaking Cooperative Relations", chapter Can We Trust? Pages 213–237, Department of Sociology, University of Oxford, 1988 http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf.
3. T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications", IEEE Communications Survey and Tutorials, 3(4) September 2000.
4. S.Ganeriwal and M.B.Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks", Proceedings in the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004), Washington DC, USA, pp.66-77.

5. B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. Caceres, M. Ben-Yehuda, W. Emmerich, and F. Galán, "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research & Development, Volume 53, Number 4, 2009.
6. Matt Blaze, Joan Feigenbaum and Jack Lacy, "Decentralized Trust Management", Proceedings of IEEE Conference on Security and Privacy, IEEE Computer Society. Oakland, CA, USA, pages 164-173, May 1996.
7. Audun Jøsang, Claudia Keser and Theo Dimitrakos, "Can we manage trust?" proceedings of International Conference on Trust Management, (iTrust), LNCS, Volume 3477, pages 93–107, 2005
8. Vishwas Patil and R K Shyamasundar, "Trust management for e-transactions", Sadhana: Academy Proceedings in Engineering Sciences, Volume. 30, pp 2-3, 141–158, April 2005.
9. Torsten Eymann, Stefan König and Raimund Matros, "A Framework for Trust and Reputation in Grid Environments", Journal of Grid Computing, Volume 6, pp 225–237, 2008.
10. Chapin, P. C., Skalka, C., and Wang, X. S. "Authorization in trust management: Features and foundations", ACM Computing Survey, Volume 40, Issue 3, Article 9, 2008.
11. I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", proceedings of IEEE Grid Computing Environments Workshop, pp. 1-10, 2008.
12. Marty Humphrey, Mary R. Thompson and Keith R. Jackson, "Security for Grids", proceedings of the IEEE, Volume 93, No.3, pages 644-652, March 2005.
13. Shyamasundar and Vishwas Patil, "ROADS: Role-based Authorization and Delegation System – Authentication, Authorization and Applications". International Conference on Computational & Experimental Engineering and Sciences, (ICCES-03), Corfu, Greece, July 2003.
14. Dan Jong Kim, Yong Song, Sviatoslav. B. Braynov, and H. Raghav Rao, "A B-To-C Trust Model for ON-LINE EXCHANGE", Americas Conference on Information Systems (AMCIS), AMCIS 2001 Proceedings, Association for Information Systems Year 2001.
15. J. Urquhart, "The Biggest Cloud-Computing Issue of 2009 is Trust", C-Net News, 7 Jan. 2009; http://news.cnet.com8301-19413_3-10133487-240.html.
16. Nuno Santos, Krishna P, Gummadi, and Rodrigo Rodrigues, "Towards Trusted Cloud Computing", Proceedings of the Workshop on Hot Topics in Cloud Computing (HotCloud), San Diego, CA, June 2009.
17. Ashish C. Morzaria, "Trust is the Secret to Cloud Computing Success", Quest for the Cloud Making the Cloud Safe for IT, July 2009, www.questforthecloud.com/2009.
18. Rui He, Jianwei Niu, Man Yuan, and Jianping Hu, "A Novel Cloud-Based Trust Model for Pervasive Computing", proceedings of the Fourth International Conference on Computer and Information Technology, pages: 693 – 700, 2004
19. Sheikh I. Ahamed and Moushumi Sharmin, "A trust-based secure service discovery (TSSD) model for pervasive computing", Computer Communications, Volume 31 issue 18, pages 4281-4293, December 2008.
20. Sheikh I. Ahamed, Munirul M. Haque, Md. Endadul Hoque, Farzana Rahman and Nilothpal Talukder, "Design, analysis, and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments", Journal of Systems and Software, Volume83 Issue.2, pages 253-270, February, 2010.

21. A.Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities" in HICSS '00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 6, page 6007, Washington, DC, USA, 2000 IEEE Computer Society.
22. A.Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", Published in Decision Support Systems, 43(2):618–644, March 2007.
23. eBay, http://www.ebay.com.
24. http://gost.isi.edu/publications/kerberos-neuman-tso.html
25. http://web.mit.edu/kerberos/dist/index.html
26. D.W.Chadwick and O.Otenko, "The PERMIS X.509 Role Based Privilege Management Infrastructure", SACMAT'02, June 3-4, 2002, Monterey, California, USA.