

# An Efficient Computational Dynamic Trust Model for P2P Network

**Aditya Verma**

Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

## **Abstract**

With today's multi-agent systems, security and privacy concerns are of utmost importance. Multi-agent systems are often open and dynamic by design. By offering protected communication, this nature undoubtedly creates an issue. Because of the rapid growth of multi-agent systems, security and privacy problems have taken on a fundamental importance. The majority of network applications, including ubiquitous computing, grid computing, and peer-to-peer (P2P) networks, may be thought of as open, anonymous, and dynamic multi-agent systems. These multi-agent system features create weaknesses and dangers for delivering encrypted communication. Evaluating the reliability and standing of the interacting agents is one practical technique to reduce the dangers. Several trust/reputation models have attempted to achieve this, but they fall short of accurately assessing trust when hostile actors begin to act in an unexpected manner. A further drawback of these models is their inability to react quickly to the fluctuating behavior of a hostile actor. The equitable allocation of workload across service-providing agents is another feature of multi-agent systems that is increasingly important for maintaining high service quality. This problem has not yet been solved by the majority of trust/reputation models. Current methods include context into the computation of trust. Their use is restricted to certain domains. The system presented an integrity belief model in this study. The suggested approach was evaluated against various trust models. The suggested approach performs better than alternative trust models in terms of efficiency. The suggested method separates trusting confidence in competence from that in integrity.

## **1. INTRODUCTION**

The authorisation of access to data on a network is known as network security, and it is within the network administrator's authority. The goal of malicious agents is to find any existing network flaw and exploit it. Multi-agent Systems (MAS) are gaining popularity for sending safe and important data through networks. As conventional network security methods like firewalls, access controls, and approved certification cannot forecast agent behaviour from a "trust" perspective, trust issues have become more prevalent. To decrease storage overhead while calculating the trust of agents, we have employed an unique approach that makes use of the exponential averaging function.

According to how data is compiled from the viewpoint of an evaluator, reputation-based trust designs may be classified into two groups. Direct/Local experience mode is generated from direct contacts or observations (personal knowledge), while indirect reputation is built from judgements in accordance with information collected indirectly (informal proof, such as reports from others). When using a global reputation model, an agent gathers input from every agent that has ever engaged with the target agent in order to swiftly come to a better conclusion.

When malevolent actors have the potential to generate misleading feedback, the global reputation design is more difficult to regulate instead of the local experience model. When malevolent agents behave in a predictable manner, the majority of global reputation models can successfully isolate them, but when agents start to display dynamic personalities, they suffer severely. This model also struggles

when agents adjust their actions strategically since it cannot adjust to the sudden shift in behaviour. The right allocation of workload among dependable service providers is another factor that is becoming more crucial for the effective maintenance of service quality. The load immensely respected service providers will be enormous without a good load-balancing technique, eventually leading to a stumbling block in the performance of the system. By outsourcing data storage, cloud service providers (CSPs) have evolved as a way to lessen the burden of expensive local data storage and upkeep.

Storage-as-a- Service entails the physical handover of private information to a distant CSP by the data owner. Provable data ownership approach has been offered as a means of ensuring the data integrity on cloud servers. To aid agents in making trust decisions, promote trustworthy conduct, as well as deter participation by dishonest agents, reputation-based trust models gather, distribute, and aggregate input about participants' prior behaviour. Direct/Local Experience Models along with Indirect/Global Reputation Models are the two divisions of these models. Although hostile actors have the potential to offer misleading feedback, managing global reputation models is far more difficult than managing local experience models.

For the right upkeep of service quality, it is also becoming more and more crucial to distribute the job among the dependable service providers. The load at immensely regarded service providers will be enormous without a good load balancing technique and eventually result in a stumbling block in the performance of the system.

In this study, a feedback-based dynamic trust computation paradigm called Secured Trust is proposed. This model can efficiently identify abrupt strategic changes in malevolent behaviour and also balances the burden across service providers. Secured Trust takes into account a wide range of variables when establishing an agent's level of trust, including contentment, similarity, feedback credibility, current and historical trust, unexpected deviations from trust, and trust erosion.

In order to decrease storage requirements while calculating agent trust, it employs a unique strategy of using exponential averaging functions. Also, a brand-new load balancing technique predicated upon an approximation of the workload at various service providers is used. Service requesters can programmatically access and alter web services, which are reusable components with a set of linked functions, from the service provider. Several researchers have developed various trust-based web services access control models to stop harmful requesters in order to safeguard web services against malicious requesters. This examination of the literature also looked at how a service provider's access control policy uses the idea of a trust level to let service requesters to access online services.

The goal of this work is to demystify security concerns specific to cloud environments and to make security-related issues more understandable. It offers a security solution that frees clients from the responsibility of security by putting their faith in a third party. The research strategy used to accomplish this aim is based on information systems design and software engineering methodologies. Peer-to-peer (P2P) network security state-of-the-art research and analysis provide key insights into why these totally decentralised and dynamic networks lack realistic security methods. The purpose of this thesis is to describe, create, and evaluate a secure P2P content distribution strategy based on the usage of digital certificates, similar to those used in the supply of public key authenticity, for file sharing situations.

## **2. LITERATURE SURVEY**

A project called Message-Digest5 tries to deal with concerns about security and privacy in multi-agent systems. It presents the secured trust dynamic trust computation paradigm, which reduces the accurate identification of actors' real identities to authentication. The authentication and authorisation processes are made easier by applying the Multi-Agent System (MAS) ideas. To encrypt/decrypt electronic data or transactions, or to sign/authenticate the sender and receiver, the key pair and Certification Authority are used. The necessity of using an appropriate load-balancing strategy for maintaining service quality is covered in this paper. In establishing an agent's level of trust, Secured Trust takes into account a number of variables, including satisfaction, similarity, feedback credibility, current with historical trust, along with unexpected deviations from historical trust, and trust erosion. The Multi-Agent System offers a model for assessing trust, a heuristic load-balancing mechanism for dividing the workload

between service providers, and support for run-time validation and verification for watch agents as well as agents to verify any violation of invariants. In order to decrease storage requirements for calculating agent trust, it also employs a unique policy of using the exponential averaging function. In unsupervised virtual communities like multi-agent environments, trust is calculated and measured using complicated factors like peer agent credibility ratings. The Key Pair Generator class is used to create pairs of agents who work together to accomplish a specific goal that they could not accomplish separately [1].

This study developed a work flow management system and grid authorisation model with dynamic roles. The access control object is a service, and the technique is service-oriented. The Trust Value Database updates the trust value of the person who owns these services and records the trust value of the services after each invocation. WFMS gives WFMS information on roles and privileges, while TVDB keeps the level of trust for each subject and service. There are two suggested grid resource management models. In Beth's concept, trust was quantified and split into recommended trust and direct trust. The trust connection between two grid entities according to Reference's model was separated into trust between domains and trust inside domains. In a grid context, the paper developed a dynamic role-based access control in accordance to a trust mechanism. Conventional static access control system is unable to fulfil the grid's sharing and dynamic requirements. To make CAS authorization simple, paper created a role-based CAS that does not have access to services and only has rights that are controlled by WFMS [2].

The trust management technique is the foundation of the trust-based content distribution presented in this research for peer-to-peer overlay networks. A node's trust index is determined by how well it delivers data and how quickly it searches for it. If the aggregated trust index of its peers falls below a certain level, it is regarded as distrusted, and the traffic associated with it is banned. The suggested technique produces a higher success percentage with less latency and drop, according to simulation data. The Bit Torrent packet-level simulator for P2P networks is tested with the NS2 simulator. One drawback is that when trust evaluation is used, the client nodes' success ratio rises; however, when trust is not used, it falls [3].

A dynamic trust computation paradigm known as "SecuredTrust" is presented in this work. It examines the many aspects of judging an agent's level of trust and suggests a thorough quantitative model for calculating that level of trust. It also suggests a brand-new load balancing algorithm depending upon many model-defined variables. According to the simulation results, the model can efficiently allocate workload between the service-providing agents amid constant circumstances and deal with the strategic behavioural changes of malevolent agents. The open, anonymous, as well as dynamic nature of multi-agent systems raises security along privacy concerns, which are highlighted in this study. The trust as well as reputation of the interacting agents have been assessed using trust/reputation models, however these models are unable to assess trust when malevolent actors begin to operate in an unpredictable manner. The proper allocation of workload among the dependable service providers is crucial for maintaining high service quality. The SecuredTrust trust computation paradigm, which is new and is presented in this research, may assure safe agent communication by successfully identifying malevolent agents' strategic activities. It offers a thorough mathematical explanation of the many trust-related criteria, a model for integrating these aspects to measure trust, and a heuristic load-balancing method for dividing the work-load within service providers. According to simulation data, SecuredTrust is more resistant to attacks from opportunistic hostile agents, and the straightforward averaging function used to determine local trust gives each transaction the same weight. As conventional network security techniques are not capable of predicting agent behaviour from a "trust" perspective, trust issues have becoming more prevalent [4].

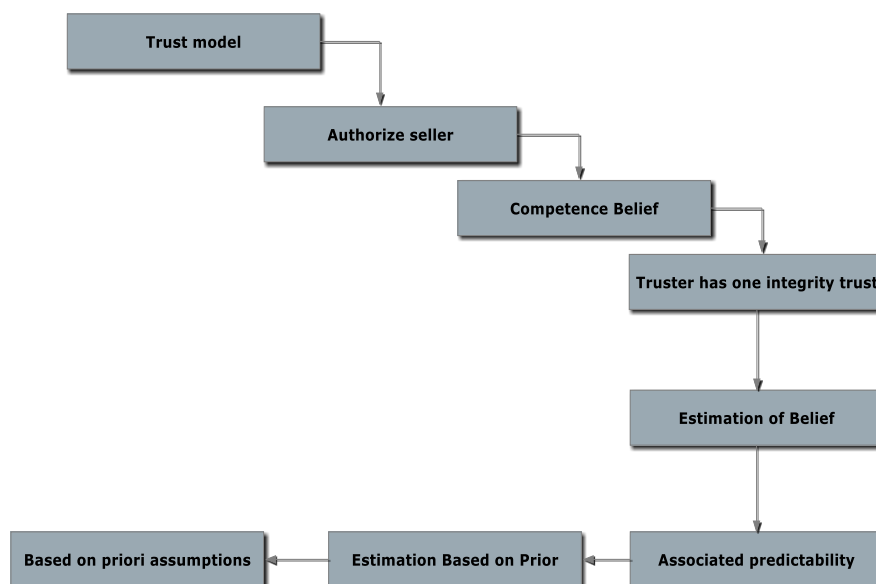
The strategy for choosing cloud service providers (CSPs) for outsourcing that considers performance and security is presented in this article. It suggests a technique for choosing between options that calculates and ranks security SLA clauses, computes and ranks using a quantitative assessment methodology, and obtains a set of trust weights from other linked service providers. The system evaluates potential services in real time and is applicable to any scenario involving cost and security in a quantitative service evaluation. It focuses on the fundamental issue of organisational security assessments in a dynamic distributed cloud environment and how to calculate the security weight based on SDTs and SLOs with regard to financial restrictions. Through a case study that demonstrates how

our solution may best fulfil the organisational security and cost goals, the recommended strategy is verified. The quantitative assessment technique analyses the potential services in real time and may be used in any security and cost-related service evaluation situation. Most crucially, this algorithm can update security evaluations as SLA changes spread throughout the business. It becomes challenging to find CSP that not only satisfies corporate security requirements but also manages financial costs [5].

### 3. PROPOSED SYSTEM

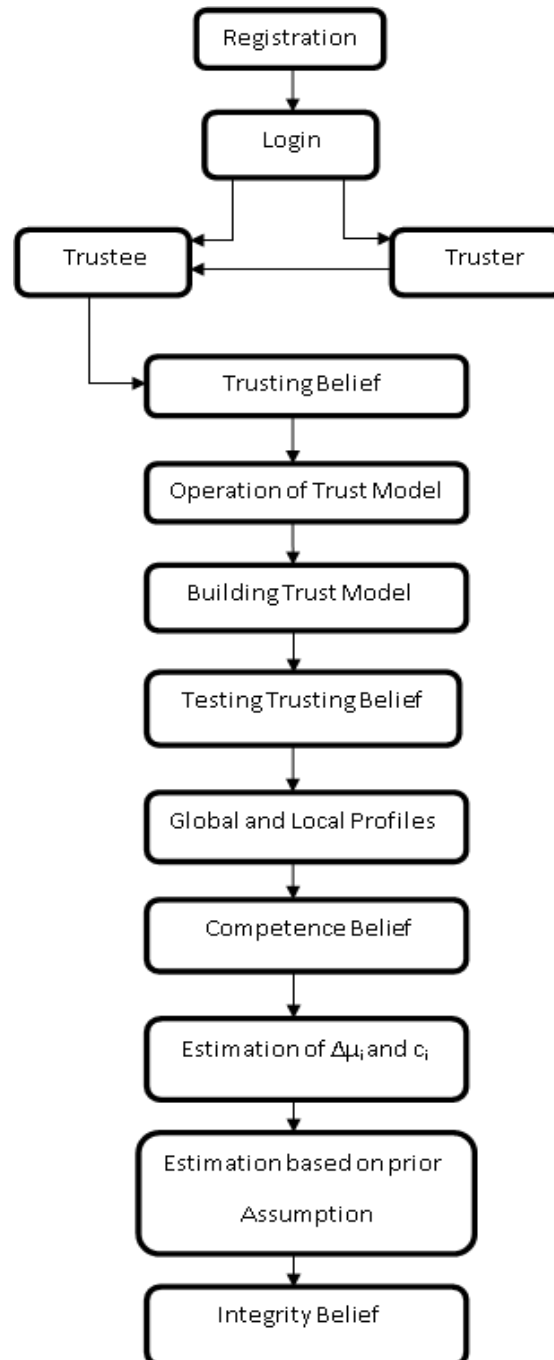
The system offers a computational dynamic trust paradigm for user authorization. The model includes components for forming reliable beliefs using both first- and second-hand data. As a result of the model's foundation in social science research, it provides automated trust management that mimics trusting social behaviour, bringing trust computation for the digital world closer to the evaluation of trust in the real world. In contrast to other trust models that have been proposed in the literature, the recommended model takes into account a variety of kinds of trust. It distinguishes between a trusting confidence in integrity and a belief in competence. The approach incorporates a method that takes into account the subjectivity of trust assessments and removes the effect of subjectivity in reputation aggregation by various institutions.

Assume that customer B must choose between allowing seller S to charge his credit card for a product I. The purchasers who have registered on the auction site are trusted. The sellers listed on the auction website are known as trustees. The context makes clear how crucial S's expertise in shipping, packing, and item quality for item I is to B. It also expresses the significance of S's honesty to B in this transaction. Via a site-maintained database or a reliable third party, B can learn S's level of trust. This data covers the evaluations of S's honesty and S's skill with regard to packaging, shipping, and product quality from customers. Also, it has ratings for S for various things as well as reviews left by customers for vendors other than S. When a buyer scores a transaction with a seller on the website, the trust rating is saved in the database. According to this concept, each trustee has a single integrity trust for all situations. A truster's confidence in a trustee's integrity is damaged if they let them down. Contexts don't need to be separated for honesty and trust. Competency and trust are situational. Even if Bob is a fantastic lecturer, you shouldn't put your faith in him to be your leader. To determine the type and amount of ability required in a situation, a representation is developed. There are two specified context-related functions.



**Fig 1: System Architecture**

The difficulty of parameter estimation is how competence belief building is put out. For the purpose of estimating the stable mean and variance, used as the belief value respecting the trustee's competency plus the corresponding predictability, statistical methods are applied to the rating series. An estimation's accuracy is evaluated using a confidence interval. For  $m$  and  $s^2$ , 90 percent confidence intervals are generated. The corresponding predictability  $pc$  is calculated using the size of the confidence interval of  $m$ . The observations must be taken from a normal distribution in order for this strategy to work. This presumption might not be accurate, and the outcome might be deceptive. Tests for goodness-of-fit could indeed determine if the assumption is true or not. This encourages the use of trust management for authorization, where the authorizer may decide permissions depending upon the properties of the principles that are scattered across multiple places without requiring the identities of the principles.



**Fig 2; Flow Diagram**

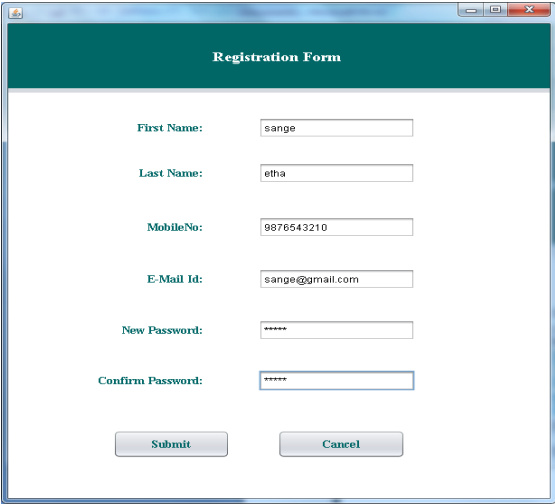
Moreover, the transferable ownership of data and resources in the cloud requires that a distributed authorization system utilising trust management offer a chain of delegation at several levels. In this research, we provide a distributed authorization system for a multi-provider intercloud context with dynamic trust formation. These are the contributions. First, our suggested system gives an attribute-based trust model approach that is supported by logical formulae and is predicated upon fundamental attribute-based access control design. The dynamic trust formation method, which is a component of a dynamic access control infrastructure for on-demand provisioned clouds, is then proposed using the trust model. Finally, employing Multi-type Intervals Decision Diagrams, we provide a realistic implementation of attribute-based trust that outperforms existing straightforward ABAC implementations. As it relates to Cloud authorisation, In our definition, trust is the confidence that one entity (the trustor) has in the trustee that the trustee would act safely, predictably, and reliably in a given situation.

The dynamic trust formation technique is then proposed as part of a dynamic access control infrastructure for on-demand supplied clouds, using the trust model as a basis. Ultimately, we provide a realistic implementation of attribute-based trust utilising Multi-type Intervals Decision Diagrams, which performs significantly better than previous fundamental ABAC implementations As it relates to Cloud authorisation, In our definition, trust is the assumption that one entity (the trustor) can act in a trustworthy, dependable, and secure manner towards another entity (the trustee) in a given situation. The following are a few of benefits of the suggested strategy:

- It offers automatic trust administration.
- It denotes a reliable conviction in honesty.
- To reduce subjectivity's influence on reputation aggregation.

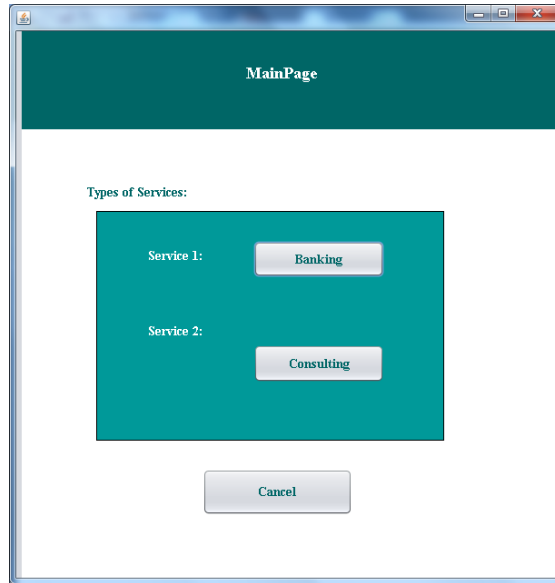
#### 4. RESULTS

So that we may evaluate the reliability and trustworthiness of the interacting agents in multi-agent systems, this research suggests an integrity belief model. The suggested technique outperforms previous trust models in terms of performance and distinguishes between trusting confidence in competence and believe in integrity, as seen in the accompanying screenshots. It also addresses the equitable task sharing among service providers, which is becoming increasingly important for maintaining high service quality. Current methods include context into trust calculation, but they are only applicable in a small number of domains.

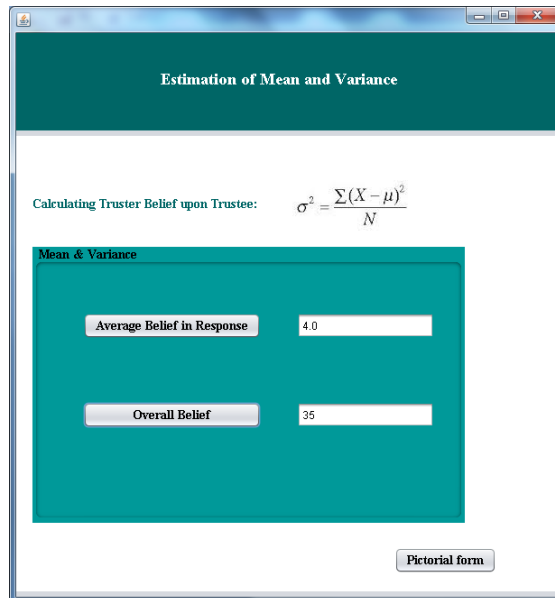


The image shows a web browser window displaying a registration form. The form has a dark green header with the text "Registration Form". Below the header, there are several input fields with labels and values: "First Name" with "sange", "Last Name" with "etha", "MobileNo" with "9876543210", "E-Mail Id" with "sange@gmail.com", "New Password" with "\*\*\*\*\*", and "Confirm Password" with "\*\*\*\*\*". At the bottom of the form, there are two buttons: "Submit" and "Cancel".

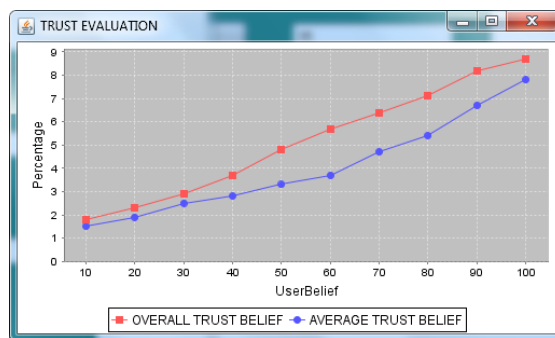
**Fig 3: Registration Form**



**Fig 4: Types of Services**



**Fig 5: Overall Belief Calculation**



**Fig 6: Trust Evaluation**

## 5. CONCLUSION

The system in this project presents a dynamic trust concept. For assessing agents in multi-agent contexts, we have introduced a brand-new trust computation paradigm called Secured Trust. Secured Trust may guarantee safe agent communication by successfully identifying malevolent agents' strategic activities. The many elements involved in computing trust have all been thoroughly mathematically defined in this study. Ultimately, we provide a heuristic load balancing approach for dividing the workload among service providers. In addition, we offer a sample for incorporating all of these elements to evaluate trust. According to simulation data, Secured Trust is more resistant to assaults from opportunistic hostile agents and effective against them, while also being able to distribute the burden across service providers.

## REFERENCE

- [1] G.R. Barnes and P.B. Cerrito, "A Mathematical Model for Interpersonal Relationships in Social Networks," *Social Networks* , vol. 20, no. 2, pp. 179-196, 1998.
- [2] R. Brent, *Algorithms for Minimization without Derivatives*. Prentice-Hall, 1973.
- [3] A. Das and M.M. Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems," *IEEE Trans. Dependable and Secure Computing* , vol. 9, no. 2, pp. 261-274, Mar./Apr. 2012.
- [4] C. Dellarocas, "Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior," *Proc. Second ACM Conf. Electronic Commerce*, pp. 150-157, 2000.
- [5] L. Fan, "A Grid Authorization Mechanism with Dynamic Role Based on Trust Model," *J. Computational Information Systems* , vol. 8, no. 12, pp. 5077-5084, 2012.
- [6] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications," *IEEE Comm. Surveys* , vol. 3, no. 4, pp. 2-16, Fourth Quarter 2000.
- [7] J.D. Hamilton, *Time Series Analysis*. Princeton University Press, 1994.
- [8] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A Robust and Efficient Feedback Credibility-Based Distributed P2P Trust Model," *Proc. IEEE Ninth Int'l Conf. Young Computer Scientists (ICYCS '08)*, pp. 1963-1968, 2008.
- [9] B. Lang, "A Computational Trust Model for Access Control in P2P," *Science China Information Sciences*, vol. 53, no. 5, pp. 896-910, May 2010.
- [10] C. Liu and L. Liu, "A Trust Evaluation Model for Dynamic Authorization," *Proc. Int'l Conf. Computational Intelligence and Software Eng. (CiSE)*, pp. 1-4, 2010.
- [11] X. Long and J. Joshi, "BaRMS: A Bayesian Reputation Management Approach for P2P Systems," *J. Information & Knowledge Management*, vol. 10, no. 3, pp. 341-349, 2011.
- [12] S. Ma and J. He, "A Multi-Dimension Dynamic Trust Evaluation Model Based on GA," *Proc. Second Int'l Workshop Intelligent Systems and Applications* , pp. 1-4, 2010.
- [13] S. Marsh, "Formalizing Trust as a Concept," PhD dissertation-Dept. of Computer Science and Math., Univ. of Stirling, 1994.
- [14] P. Matt, M. Morge, and F. Toni, "Combining Statistics and Arguments to Compute Trust," *Proc. Ninth Int'l Conf. Autonomous Agents and Multiagent Systems (AAMAS '10)*, pp. 209-216, 2010.
- [15] D. McKnight, V. Choudhury, and C. Kacmar, "Developing and Validating Trust Measures for E-Commerce: An Integrative Topology," *Information Systems Research* , vol. 13, no. 3, pp. 334-359, Sept. 2002.
- [16] D. McKnight and N.L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationship Model," *Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS '01)* , 2001.