http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (1): 134-140, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.134.140

Collaboration Framework and Trust Mechanism Model of Context-Aware Computing

[1,2]Zhaobin Liu, [1]Wenzhi Liu, [1]Ligang Fang and [2]Yazhe Tang
[1]Suzhou Vocational University, Suzhou Jiangsu, 215104, China
[2]School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, China

Abstract: How to establish a flexible, robust and smart collaborative working environment of scene perception? How to solve the assertion description based on trust system of identity and the trust problem of role reversal in the circumstances? In order to bridge this gap, a collaborative system framework and a trust mechanism model of trustworthiness factor based on role transformation is proposed. This framework senses the context of entities which affects the trust relationship and transforms them into different input values. In this trust mechanism model, the methods of mutual-trust relationship in grid environment and trustworthiness factor evaluation are adopted to evaluate the trust relationship between the entities. The simulation is compared with Monte Carlo model by changing time and the context of entities. The result indicates the model is effective and feasible.

Key words: Context aware computing, collaboration framework, trust mechanism model

INTRODUCTION

With the expansion and Increase in applications of IoT (Internet of Things), Context-aware computing architecture of IoT must be able to support the acquisition of real-time environmental information and knowledge representation of the information. Including the realization of semantic interoperability, information fusion, low-layer scene information collaboration and the active service of high-layer information can be recognized. However, tightly-coupled way will result in the complexity of context aware computing (Baldauf *et al*., 2007). So, there was a based on middleware structure which is a layered structure in context-aware system (De *et al*., 2012; Gao *et al*., 2011). It is located between the sensor and the application. This layer to shield the details of underlying sensor operation to upper layer and to provide a unified information access interface, at the same time, the layer down to drive the physical or logical sensor information acquisition. Middleware technology to build the bridge of the application program and the sensor data sources, integrate the modeling of situational information and simplify the development of context-aware applications for IoT, at the same time, enhance the scalability of the system. Context Toolkit (Dey *et al*., 2001) is a middleware which Georgia Institute of Technology proposes and achieves to support for context-aware applications. In the Context Toolkit architecture, it provides a unified data interface for upper layer application, server and interpreter encapsulates the analysis process of the information process. But Toolkit architecture uses a specific object-oriented information modeling methodology, the lack of scene information sharing, there are some limitations.

Gaia (Roman *et al*., 2002; Henricksen *et al*., 2005) provides the ability to reason on the uncertain context-aware computing and support for inference mechanism of Bayes network. Among them, the underlying physical and logical sensor is responsible for the information collection of scenarios. The middle-layer fusion and infer high-layer scene information by accessing information and provide historical context storage services. The scene information of the application layer decides to take the appropriate action. However, a huge number and variety of the underlying sensor can cause transmission problems of Gaia' network, it will lead to information gaps and noise data.

In actual research, the thought that context information aware be separated from actual application was initially proposed (Jun-Zhong, 2009) and the middleware framework form was used, the context information by analytical processing was provided outside. Universal concept level generally consists of four parts: context information aware, context information processing, context information management and context information application. The agent-based framework was proposed (Mangalwede and Rao, 2009; Khedr and Karmouch, 2005), each agency play different roles, through mutual coordination, the context information was processed and released. A context-aware

Corresponding Author: Zhaobin Liu, Suzhou Vocational University, Suzhou Jiangsu, 215104, China
Tel: 008615506155880 Fax: 0086051266503531

service-oriented platform based on OSGI was presented (Gu *et al*., 2004) which also is based on the ontology modeling. The whole framework includes context information acquisition, discovery, explanation and visit etc. In addition, the framework' security, privacy trust issues and quality of service, also must be considered when the framework of context-aware system was designed.

Trust issues in context-aware computing environment have been the research hotspot of scholars (Ghelawat *et al*., 2010; Mistry *et al*., 2009). People in daily life always worried that their information could be easily leaked to others. A widely accepted view is that there is no transitivity relationship of trust. Therefore, in collaborative work, even if twenty-two participants trust each other, there may be two participants in a situation of distrust. Meanwhile, in addition to the issue of trust between participants and participants, the trust between participants and task should also be issues that are needed to be considered.

The above-mentioned middleware based on Context-Aware Computing support for traditional sensor networks, it lacks the collaborative management. As mentioned earlier, several middleware and agent there are limitations in the Internet of Things environments.

This paper provided a new method for the collaboration system high level modeling, evaluation and confirmation of the context-aware computing.

SYSTEM FRAMEWORK OF CONTEXT-AWARE COLLABORATION

System framework of context-aware collaboration mission work as the center, intended to provide participants with a shared space collaborative workspace, to be more concerned about plan, division, coordination, state aware and knowledge sharing of collaborative tasks in the design. The concept level of Collaborative work generally consists of three layers: first, the underlying communication layer which determines the whole organizational model of collaborative work systems and gradually shifts from the fixed network to mobile network development. Secondly, the service level or system level, this layer is the core of collaborative work systems, responsible for task management, including planning, division, coordination, etc. The top is the application layer, with humanized human-machine interaction interface for users. Therefore, the following gives application-layer system framework of context-aware collaboration of flexible, robust and intelligent, shown in Fig. 1.

In this context-aware system context-aware goes along modeling by means of ontology, whose benefit is in its convenience for knowledge sharing in different areas and facilitation of the knowledge management. Ontology model supported context-aware and cooperative work needed to solve the following questions:

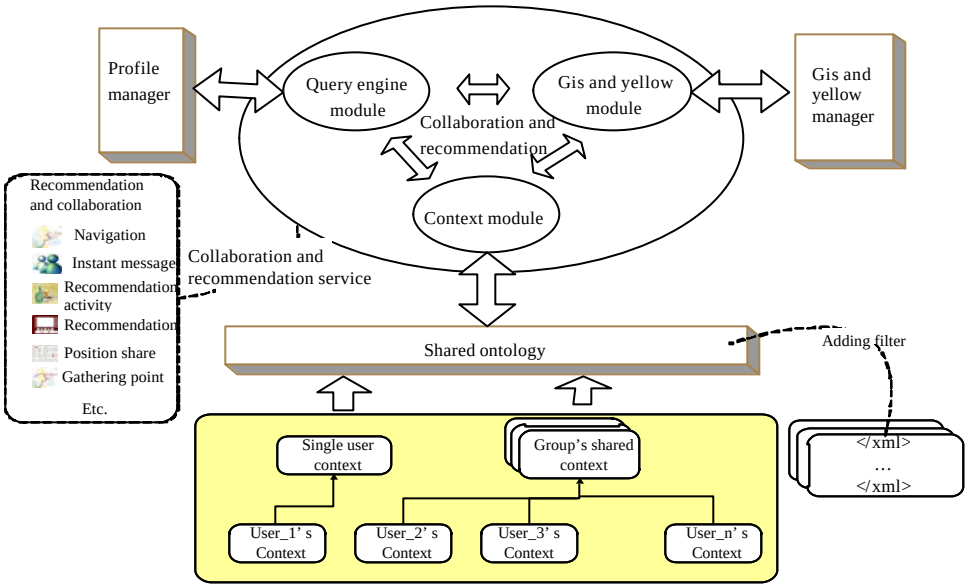

Fig. 1: Collaborative framework for context-aware services management

- Ontology construction, including computing context, participant context, external physical context, coordination task context and privacy and trust context, etc
- Context reasoning mechanism (Niu *et al*., 2011), the upper context information should be obtained by needed reasoning on the underlying information. Typical information such as user location and time can be inferred to obtain the current user activities (home, office work, etc.). In addition, the user's habits and preferences can be obtained by analyzing the user's historical data

Therefore, the following framework has been proposed which deals with data management using ontology and information derivation according to user queries. This paper illustrates how existing techniques can be extended and combined in a logical multilayer framework. Clearly, the actual techniques to be applied for trust mechanism depend on the current context (users' situation, available services, network and environmental conditions). However, this framework is considered flexible enough to provide effective trust mechanism in most pervasive and mobile computing scenarios. The framework is composed of the following layers.

Collaborative and recommendation: To locate data sources, it keeps the organization hierarchy of local or even global data sources. It firstly checks repository, if failed, then it tries to find information from data repositories according to the query semantics. To keep frequent hit queries and their answers which are in XML or GML format for quick response and further modification? Repositories can be differentiated based on their regions or domains. So, the information in repository is mainly derived from data repositories. Furthermore, repositories also reflect changes of user's attentions in particular duration:

- **Query engine module:** To locate the user according to the GPS data, analyze and decompose the query based on the user profile and his/her actual location. It is assumed that every query message is composed of user's position, user's profile and user's request body. In LBS (Location-Based Service), the user's current location is significant since most of queries have evident region-dependent characteristic. Usually users care about surrounding and objects within the current or neighboring city or region, including real-time monitoring, historical track playback, data analysis, reporting, etc
- **Profile manager:** To analyze and define user profiles. The format and domain of user profile should be consistent with the Profile Manager's specifications. Thus, the Profile manager can provide some hints to the Data Handler by analyzing specific user profiles
- **GIS and YELLOW module/manager:** The system supports the basic operation of zoom in, zoom out and distance measuring on map. It also supports multiple ways of yellow page information retrieval of surface features, in line with the actual operation of the various needs of users. After the terminal made a navigation requests to the GIS and YELLOW Manager, the navigation information is formed according to the terminal location and the navigation map by path planning and return to the terminal. It requires minimal changes to starting mobile GIS architecture and minimizes processing requirements on the client side. On the server side, context information is handled separately from the user commands. It is inserted into rules and facts database and analyzed by rule based expert system. Every change in rules and facts database can lead to either insertion of new context information at the higher logical level into database or entering new state. Reaching new state results in picking out profile that most adequately fits new change in user's context
- **Context module:** This includes context-aware interface that exchanges context data with the lower layers through encrypted channels using energy-efficient cryptographic protocols. It is assumed that this module is within the trusted domain of the user

Shared ontology: To organize and manage data from heterogeneous sources using ontology. Each data source has its own local ontology to specify the content of its data. However, they are grouped by the shared ontology. The approach can make it easier to access relevant data sources, as is discussed (Yu *et al*., 2003).

Adding filter: To evaluate and decide if an answer can be added into TOP Hits Repository. It serves as a mechanism to count the frequency of a query and be responsible for transformation from data's original format to XML or GML format:

- **Shared ontology structure:** In order to solve the matching problem between the different ontologies, each data source is described by their own ontology (user ontology, trust ontology, coordination application ontology), as shown in Fig. 2. User ontology is inherited by the shared ontology and expanded. It is used to formalize a description for single/group user context information and personalized data. It is essential that user ontology be introduced to describe user information for the

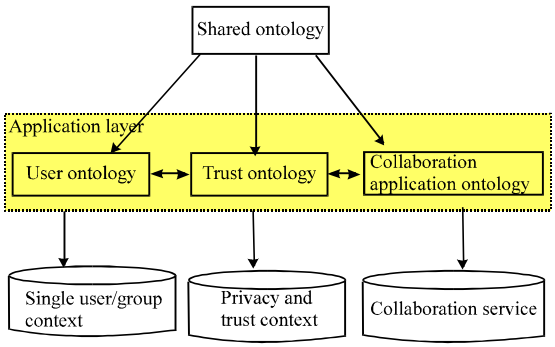

Fig. 2: Collaborative ontology structure

service query of context aware computing, the trust ontology is based on Gruninger TOVE method (Park *et al*., 2010) to create trust domain ontology. Dynamic trust property to use deductive reason in the action and behavior, the formal description of the ontology of trust and other attributes in the semantic level. By actual association to capture the trust scenarios, using formal methods solves the collaboration problem. Application ontology is used to describe the coordination and cooperation between the profile, GIS and the context. It can make the data sources of context information more clear. Different services to interoperate, you can use the concept of shared ontology or the use of shared ontologies to establish the concept of collaborative ontology mapping.

Collaboration between the different ontologies in the shared ontology approach is more flexible. An additional advantage is that the new ontology can be added to the structure to make any changes. It does not need the shared ontology or mapping and it supports ontology effectively access and evolution.

User context: User context is responsible for and manage the user's personal data information (such as personal information, interests and preferences) and privacy policies. Moreover, User context is in charge of fusing context data provided by body-worn mobile terminal and transferring them in an aggregated form to the upper layer on a per-request basis. This layer is deployed on the user's device which is assumed to be trusted (traditional security issues are not addressed here); communications with the upper layer are performed through encrypted channels.

TRUST MECHANISM MODEL

Because of the scale and openness of context aware computing environment, the traditional identity-based trust system can't operate effectively. The certificate exchange is used to establish trust relationships. The so-called evidence is the kind of document that used to prove certain facts 0 be true which describes one or more properties of certificate owner that is approved by the certificate issuer, the concrete manifestation is attribute name/value pairs.

However, in context aware environment, the certificate itself has a lot of uncertainty. As the lack of authority recognized by commonality in context aware computing environment and interaction frequently occurs between multiple administrative domains, so that the certificate issued by outside domain can't be granted full trust. Even if the certificate can be fully trusted, it can't guarantee that the entity holding the certificate must be in accordance with expectations. Moreover, in a different context, the credibility proof strength of the different certificate holders would differ.

In view of trust issues based on role transformation, this paper puts forward a method for reliability-aware computing through Credential Possessed Trustworthiness Fact and Credential Unpossessed Trustworthiness Factor between entities, so as to establish reliability, flexibility and predictability of the trust relationship in grid environment and to improve and complement the role-based Trust system. Especially for the trust establishment issues in grid cross-realm, autonomy and distributed environment, it provides more realistic situation and more convincing credibility assessment.

Definition 1: Modeling model an autonomous network as a directed graph G(V, E), in which nodes are the entities in the network and links represent trust relations.

Definition 2: A directed link from node i to node j in G, expressed as C(i, j) ($0 \le C(i, j) \le 1$), denoted as:

$$V \times V \to [0,1].\ C(i, j) = 1$$

Represents completely positive confidence i has on j and C(i, j) = 0 represents completely negative confidence. C(i, j) = 0.5 means total uncertain, so if i and j have no interactions, i.e., $(i, j) \in E$, C(i, j) may set to be 0. Trust relations are asymmetric, so generally $C(i, j) \neq C(j, i)$. Throughout, this study, it is assumed that nodes' opinions are fixed for the sake of analysis. It is defined as that the neighbor set of node i:

$$N_i = \{j \mid (i, j) \text{ or } (j, I) \in E\} \subseteq V \quad (1)$$

Definition 3: Credential Possessed Trustworthiness Fact (CPTF) (Kocher, 1998; Ma *et al*., 2001), expressed as H(i, j). It shows the relative degree of credibility that i hold j:

$$H(i,j) = (C(i, j)-C(j))/(1-C(j)) \quad (2)$$

where, C(j) (0<C(j),1) means a priori credibility as i did not produce j, C(i, j) represents the posterior credibility for i hold on j. Since, C(i, j)≥C(j)0.5, the value of H(i, j) should be between 0 and 1.

Definition 4: Credential Unpossessed Trustworthiness Factor (CUTF): expressed as M(i, -j), it shows relative degree as the lack of j reduce credibility of i, as shown in Eq. 3:

$$M(i, -j) = C(i, -j)-(j))/C(j) \quad (3)$$

Because C(i, -j)≤C(j), the values of should be between 0 and -1. Obviously, when the value of M(i, -j) becomes lower, the credibility between i and j declines more.

The method is perfection and complement of trust-based system, especially for the trust establishment issues in grid cross-realm, autonomy, distributed environment and it provides a more realistic situation, a more convincing assessment of the credibility.

SIMULATION AND PERFORMANCE ANALYSIS

In order to validate the algorithm, we selected a network shown in Fig. 3. The network contains 12 nodes and 12 edges, as shown in Fig. 3, the network has a more obvious level and these nodes are divided into four levels according to the characteristics. The Credential Possessed Trustworthiness Fact (CPTF) value of H(i, j) and Credential Unpossessed Trustworthiness Factor(CUTF) value of M(i, -j) as shown in Table 1.

Table 1: The CPTF relationship of the node

Layer	Node	CPTF	CUTF
1	N1, N2, N3	H(N1, N4) (N1, N5), H(N2, N5), H(N3, N6), H(N3, N7)	
2	N4, N5, N6, N7	H(N4, N1) (N4, N8), H(N4, N9) (N5, N10), H(N6, N3) (N7, N10), H (N7, N12)	M(N5, -N1), M(N5, -N2), M(N7, -N3)
3	N8, N9, N10, N12	H(N9, N4) (N9, N11), H(N10, N11), H(N10, N7), H(N12, N7)	M(N8, -N4), M(N10,-N5), M(N12, -N7)
4	N11	H(N11, N10)	M(N11, -N9)

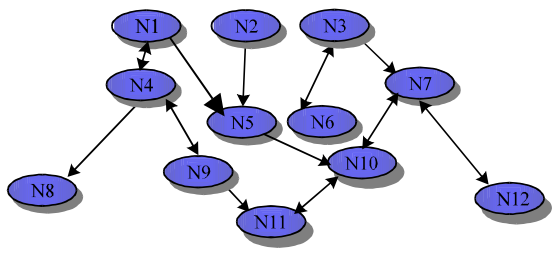

Fig. 3: Experimental network topology

Finally, using Monte Carlo algorithm, it had been generated seven groups of unbiased data shown in Fig. 3. Its data were 10, 20, 50, 100, 200, 300, 400 and 500. Use these data to examine the impact of the trust mechanism model and collaboration framework performance.

Figure 4 shows that, the elapsed time of executing the two services increases gradually with respect to the number of CPTFs. The increase of the number of CPTFs results in the increase of the number of network I/O events of the backbone network. Thus, it takes more time waiting for the response packets from all CPTFs. The long waiting time can be improved by decreasing the numbers of the interacting CUTFs. For example, we can store all CPTFs nodes' locations into the trust maintenance server. when a CPTF executes a service of building all group members, it obtains the location context information from the CPTFs maintenance server instead of sending broadcast packets to all other CPTFs. This is consistent with the theoretical analysis of the situation.

This used to simulate multi-node shared ontology collaborative workspace, along the node does not cache data link information which can be seen from Fig. 5, the context-aware collaboration model has a high perceived success rate, even in the case of increase in the amount of data, it can maintain the success rate of 90% or more but it takes a larger network overhead to achieve that:

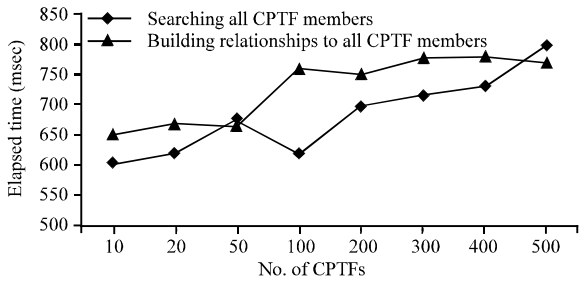

Fig. 4: The elapsed time of group services with number of CPTFs

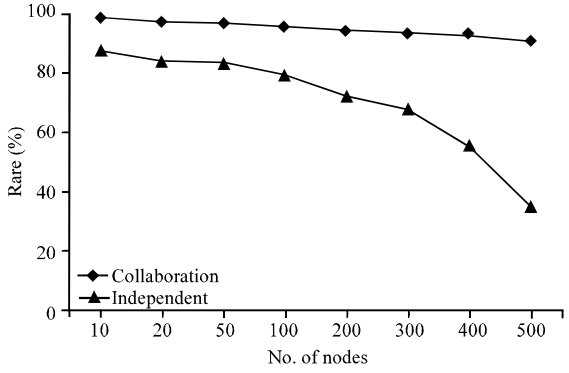

Fig. 5: Node perceived success rate

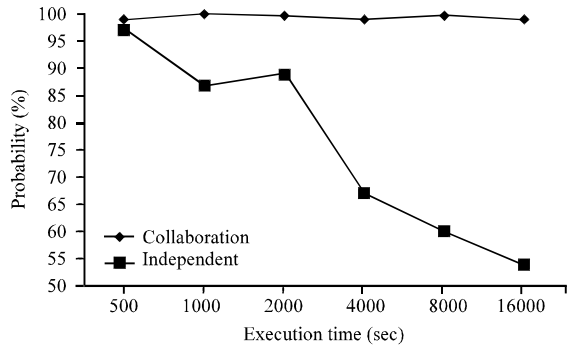

Fig. 6: Correct probability

- **Independency:** The nodes do not collude with each other. It is assumed that their probabilities of isolated identifying whether a node is cooperative or independent
- **Collaboration:** Nodes know each other. They always support friendly node in collaborative work environment for organization services, activity service, interaction service, scene service and location aware service

Figure 6 shows the relationship between correct probability and computation time system takes to perform the trustworthiness fact of independent and collaborative nodes. Y-axis represents the graph Correct Probability, the X-axis represents the execution time in seconds.

Through, the trust mechanism definition model, especially the issue of autonomy and distributed environments to build collaboration and trust, it provides a more realistic and more convincing proof.

Simulation approach is used to compare two types of nodes. In each simulation, the only difference is the behavior of Independent nodes. In order to verify trust mechanism model, the curve for all collaboration nodes and independent nodes is plotted except for some small random perturbations. The performance of independent nodes does not change with respect to the percentage of nodes in the network.

Surprisingly, the curve of collaboration nodes which use the algorithm for trust mechanism model performs better than the ones for independent nodes. This is because the trust ontology rules have considered credential possessed trustworthiness fact and CUTF. In the independent case, the worst performance is that the some nodes cannot gain trust from good nodes. Then they are much easier to be detected. Because our model rule does not capture such isolated behavior.

CONCLUSION

The context aware computing has gained increasing attention because of their wide applications and difficulties of reasoning trust mechanism. In this study, it has been introduced that a new architecture and describe for context-aware collaboration will be useful for context-aware applications. The interactions in such isolation management can only be local. Without the global management and control on the scene perception, a small change in local domain may result in dramatic behavior changes on the whole network collaboration environment. Therefore, it is essential to understand the behavior of such collaboration framework and trust mechanism before conducting any context aware computing management and control. In this work, the context aware computing characteristics have been studied under distributed trust management of context. Our analysis shows extraordinary complexity in terms of the system performance. The analytical results enable us to design the algorithm that can achieve desired performance.

A framework has been presented for providing trust mechanism services in context-aware environments and applications. In addition, it has been explored that through the context aware trust mechanism, an implementation of the Generalized Role-Based Access Control model. Our study is just the first step on the exploration of understanding autonomous networks. The simple local voting is not necessarily the best scheme however, it performs well in certain scenarios.

In the future people will live in a more intelligent environment, based on the shared ontology of context-aware framework is essential. The introduction of the body in the framework of context-aware systems theory, unified semantic description of the build environment and agent between the uses of ontologies for the semantic information of the communication interaction is the focus of our future work. The future research will focus on ontology reasoned technology and trustworthiness evolution of aware computing.

ACKNOWLEDGMENTS

This research was supported by the National Natural Science Funds (No.61170245), This study was supported by Science and Technology Plan Project of Suzhou (No. SYG201257) and Science and Technology Plan Projects of Jiangsu Province (No. BK2012164).

REFERENCES

Baldauf, M., S. Dustdar and F. Rosenberg, 2007. A survey on context-aware systems. Int. J. Ad Hoc Ubiquitous Comput., 2: 263-277.

De, D. and S. Tang, W.Z. Song, D. Cook and S.K. Das, 2012. ActiSen: Activity-aware sensor network in smart environments. Pervasive Mobile Comput. 10.1016/j.pmcj.2011.12.005.

Dey, A.K., G.D. Abowd and D. Salber, 2001. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. Human-Comput. Interact., 16: 97-166.

Gao, H., S. Wang and H. Lu, 2011. Local positioning systems for mobile devices based on ontology. Inform. Technol. J., 10: 168-174.

Ghelawat, S., K. Radke and M. Brereton, 2010. Interaction, privacy and profiling considerations in local mobile social software. Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction, November 22-26, 2010, Brisbane, Australia, pp: 376-379.

Gu, T., H.K. Pung and D.Q. Zhang, 2004. Towards an OSGI-based infrastructure for context-aware applications in smart homes. IEEE Pervasive Comput., 3: 66-74.

Henricksen, K., J. Indulska, T. McFadden and S. Balasubramaniam, 2005. Middleware for distributed context-aware systems. Proceedings of the OTM Confederated International Conferences on the Move to Meaningful Internet Systems, October 31-November 4, 2005, Agia Napa, Cyprus, pp: 846-863.

Jun-Zhong, G., 2009. Context aware computing. J. East China Normal Univ., 5: 1-20.

Khedr, M. and A. Karmouch, 2005. ACAI: Agent-based context-aware infrastructure for spontaneous applications. Network Comput. Appl., 28: 19-44.

Kocher, P., 1998. On certificate revocation and validation. Proceedings of the 2nd International Conference on Financial Cryptography, February 23-25, 1998, Anguilla, British West Indies, pp: 172-177.

Ma, J., J. Liu and Y. Xu, 2001. A method of Uncertainty reasoning by using information. Proceedings of 31st IEEE International Symposium on Multiple-Valued Logic, May 22-24, 2001, Warsaw, pp: 73-377.

Mangalwede, S.R. and D.H. Rao, 2009. Context-aware intelligent multi-agent technology in knowledge grid environments for e-Learning systems. Proceedings of the International Conference on Advances in Computing, Communication and Control (ICAC' 09), Mumbai, India, pp: 257-263.

Mistry, O., A. Gursel and S. Sen, 2009. Comparing trust mechanisms for monitoring aggregator nodes in sensor networks. Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems, Vol. 2, May 10-15, 2009, Budapest, Hungary, pp: 985-992.

Niu, W., G. Li, H. Tang, X. Zhou and Z. Shi, 2011. CARSA: A context-aware reasoning-based service agent model for AI planning of web service composition. J. Network Comput. Appl., 34: 1757-1770.

Park, J., W. Cho and S. Rho, 2010. Evaluating ontology extraction tools using a comprehensive evaluation framework. Data Knowledge Eng., 69: 1043-1061.

Roman, M., C. Hess, R. Cerqueira, A. Ranganathan, R.H. Campbell and K. Nahrstedt, 2002. Gaia: A middleware infrastructure to enable active spaces. IEEE Pervasive Comput., 1: 74-83.

Yu, S., M.A. Aufaure, N. Cullot and S. Spaccapietra, 2003. Location-based spatial modelling using ontology. Proceedings of the 6th AGILE, April 24-26, 2003, Lyon, France.