

AN AGENT BASED FRAMEWORK FOR INSIDER THREAT, PRIVACY AND ADAPTABILITY MANAGEMENT

Ghulam Ali Mallah, Noor Ahmed Shaikh and Zubair Ahmed Shaikh

Department of Computer Science, Shah Abdul Latif University, Khairpur, Pakistan, Department of Computer Science, Shah Abdul Latif University, Khairpur, Pakistan and National University of Computer & Emerging Sciences, Karachi campus, Pakistan

Received January 2010, accepted April 2010

Abstract: This paper targets Network Security and more specifically deals with Insider Threat. Software Agents have been used as a technology in this research. The literature survey shows that FIPA (Foundation for Intelligent Physical Agents) and MASIF (Mobile System Interoperability Facility) agent standards have many limitations, therefore their combination or a new standard is proposed for a true agent system. Various milestones were set and bottom-up approach is used to achieve the overall task. Agent based vulnerability assessment model has been developed in which various practical issues have been identified and appropriate solutions have been proposed. Platform-dependent and platform-independent approaches were used to achieve the task and results of both approaches are compared. Profiling is the key source of identifying insider threat therefore an Agent-based Profiling model has been developed that considers an individual's personality profile to identify real personality. A FIPA-compliant agent framework (ACENET) for profiling has been developed to achieve the task. The framework allows identifying, online and offline, anomalies in user activities. The ACENET (Agent collaborative Environment on .NET) scores every user of the organization and maintains a detailed profile of whether a legitimate user is doing any malicious activity. The framework checks out whether user activities are in accordance with organization's policy or not. ACENET is adaptable to deploy in any organization where agents are designed as services on the top layers of the model. The threats have been categorized in various classes and for each category agents have been designed. Considering privacy as a major concern, the professional issues were studied and it is proposed that the organization may announce in advance what can be monitored and what cannot be monitored through a user monitoring policy. The framework has been tested on real data and the performance has also been evaluated on the basis of specified parameters. The results were analyzed to match with the targeted objectives.

Keywords: Insider threat, software agents, privacy, agent framework, .NET framework, network security

Introduction

Software agents have been in use for quite some time and the field is still evolving in distributed applications. The concept stands from the traditional thread based systems to message passing systems and ultimately to software agents where it is expected that the nodes on which the software agents could be deployed may or may not be accessible all the time, and they could have heterogeneous nature. Numerous research applications have been done in the area of the software agents [1].

Statistics has shown that most of the security breaches take place because of users' own behavior, attitude and related actions or activities. Various factors have been studied and based on these factors, the vulnerable elements by which a network is generally breached, have

been identified. According to Phua *et al* [2], the vulnerability assessment model shows that the biggest threat to the organizations is their employees. Mobile agents have been used to monitor user profiles. The work pertaining to user profiles has received many names by many researchers such as social computing, social behavior, social networks [3]. Those agents are named as the social agents that can monitor the social profiles and the user behavior and can therefore portray the behavior of the user. Due to cultural and social limitations of the rating systems, an enhancement in the solution has been proposed to rate Internet users and contents.

Since agents can be developed in various models currently available, a comparative study has also been conducted to thoroughly understand which platform is the most suitable for such applications. An agent framework has been developed in which all basic operations can be

performed on the agents. Some research solutions have been proposed in which agents target intended machine to acquire required information such as running applications, processes, open ports and Websites. Communication that takes place between agents has been encrypted. All necessary modules such as Agent Management System, Directory Facilitator and Communication Channels have been included in the framework. The framework follows FIPA (Foundation for Intelligent Physical Agents) standard to avoid interoperability problems. Different applications have been implemented and tested over the framework. The framework was tested by performing a demonstration of an application in which many nodes (a cluster of nodes) represented in the matrix format were made to communicate using simple matrix operation. The matrix numbers are not simple numbers but are nodes that were developed and managed by the modified algorithms. The problem of task decomposition and their execution on the idle nodes to utilize CPU cycles to get full advantages of distributed environment through agents was also addressed.

Finally, an agent based environment to run intelligent agents on the platform of .Net has been deployed to monitor user-behavior. It has been proved through many surveys that the user is an unpredictable entity that is a possible threat in an organization. Even in the existence of technology, the network remains insecure because of humans. There is need of an agent framework, adaptable enough so that every corporate can use it by just asking the required features according to their environment. At low level, organizations are using different kinds of technology, protocols, procedural security measures, but an agent based autonomous system at high level is needed for profiling to monitor user activities in an organization to avoid insider threat. The proposed framework uses a service-

oriented architecture. Therefore it is flexible enough so that every corporate can use it by just setting the required social features according to their environment. Profiling for security is a very important factor where activities of all users can be analyzed to know whether user's behavior is acceptable or not. This framework provides security both at low level and high level. At low level, security is provided through protocol or procedural mechanisms, while at high level security is provided through profiling or monitoring user behavior.

Various researchers have defined an agent according to their own point of view. Some researchers have described a software agent as "an umbrella term for a heterogeneous body of research and development" [4]. Software agents are not merely confined to computer science but also involve diverse fields such as sociology, psychology, etc [5]. Domain-specific definitions have also been given by researchers. Some common and related definitions are given below. According to the definition of Russell and Norvig [6], an agent performs two tasks: It senses its surrounding environment through sensors and performs actions into it with its effectors. According to another definition "Autonomous agents are computational systems that inhabit some complex dynamic environment; sense and act autonomously in this environment and by doing so realize set of goals or task for which they are designed" [7]. Some researchers view agents as special software that involve in communications, bargaining, and coordination, and perform so many other actions autonomously, as it is done in real life [8].

Security is a general term that is generally defined as "the condition of being protected against danger or loss" [9]. The circumstances or conditions that have potential to cause loss or harm the computing systems are called threats.

Vulnerability is the weakness in the system and its exploitation is known as attack. A computer system is made up of three valuable components: hardware, software and data. There is always threat for these three components that can be vulnerably exploited by the attacker.

The area of vulnerability assessment is not new, but the use of mobile agents, is still an evolving area. Many researchers are working in the area either commercially or academically to enhance the security of the systems. Few projects or models are presented that are related to our work. Their limitations and difference of these models from our work are also pointed out. The related work presented here is related to intrusion detection and insider threat.

Social profiling is not purely domain of computer science, but it has roots in various areas such as psychology, social sciences, cognitive sciences and many other areas. The intention in this research was to focus on computer science. Therefore, papers related to this particular domain have been referred. Next we present the projects and research work that is related to the proposed model.

POSTAGE (POSTman AGEnt), was developed to involve software agents for communications with human that has strong philosophical foundation in speech act theory, argumentation theory, and social commitments [10]. Another agent based approach has been used in social computing that discusses socio-affective agent model to support the diagnostic reasoning development of domains with complex and uncertain knowledge [11]. To interact with users and provide necessary services to avoid expensive and powerful mobile devices an agent based social model (Agent and Profiling Management System) has been developed by Huang and Yang [12]. In social networks a model of opinion formation has been proposed

where dynamic confidence in agent-mediated social networks is implemented [13]. To track user behavior regularity measures have been proposed to examine patterns in the four aspects: day count, day-of-week, time zone and time zone with day-of-week with three months transition patterns [14]. The project of CASA (Computers are Social Actors) has also been developed to describe how intelligence technology needs to anticipate the need of humans to build up social relationships [15]. Social interaction arises from individual social action and mind. Sociological agents can model their social environment. The effective social agents must be sociological in modeling agents and agent relationships.

This study aimed at targeting Network Security, especially insider threat. Since profiling is key source to identifying insider threat, an Agent-based Profiling model has been developed here that considers an individuals personality profile to identify real personality. Platform dependent and platform independent approaches have been used to achieve the task. A FIFA compliant agent framework, ACENET (Agent Collaborative Environment on .NET), for profiling has been developed to achieve the task. The framework was tested on real data and the performance was also evaluated on the basis of specified parameters. Along with other characteristics, mobility is the major property that is exploited in the dissertation. Therefore, terms such as agents, software agents and mobile agents, will be interchangeably used. The second part of the research is network security that is the other well defined area where problems and issues can be addressed and resolved at various levels. Computing systems are subject to threats. So, one objective of the study was to focus on computer science. In this dissertation the problem of user-profiling and user-behavior has been addressed. As a specified security problem, insider threat was taken where

identified problem has been addressed and appropriate solution has been proposed. Insider threat can be addressed in many ways but user-behavior was a major focus of this research.

Materials and Methods

Multiagent systems support many agents to collaborate and cooperate to achieve the overall goal of the organization. Since agents can be developed in various models currently available, a comparative study was conducted to thoroughly understand which platform is the most suitable for such applications. An agent framework has been developed in which all basic operations can be performed on the agents. Some research solutions have been proposed in which agents target intended machine to acquire required information such as running applications, processes, open ports and Websites. Communication that takes place between agents has been encrypted. All necessary modules such as Agent Management System, Directory Facilitator and Communication Channels have been included in the framework. The framework follows FIPA standard to avoid interoperability problems. Different applications have been implemented and tested over the framework. The framework was tested by performing a demonstration of an application in which many nodes (a cluster of nodes) represented in the matrix format were made to communicate using simple matrix operation. The matrix numbers are not simple numbers but are nodes that were developed and managed by the modified algorithms. The problem of task decomposition and their execution on the idle nodes to utilize CPU cycles to get full advantages of distributed environment through agents was also addressed.

FIPA and MASIF are two renowned agent standards that define rules to offer multiagent

systems execution environment. MASIF supports mobility while FIPA focuses on communication and interaction protocols. The architecture that provides implementation environment to multiagent systems for organization of the agents, coordination, communication, negotiation, etc. is called agent platform or toolkit. The agent toolkits provide agent builders with enough height of generalization to let them to employ intelligent agents with preferred characteristics and convention. Figure 1 shows the major components of the proposed agent framework.

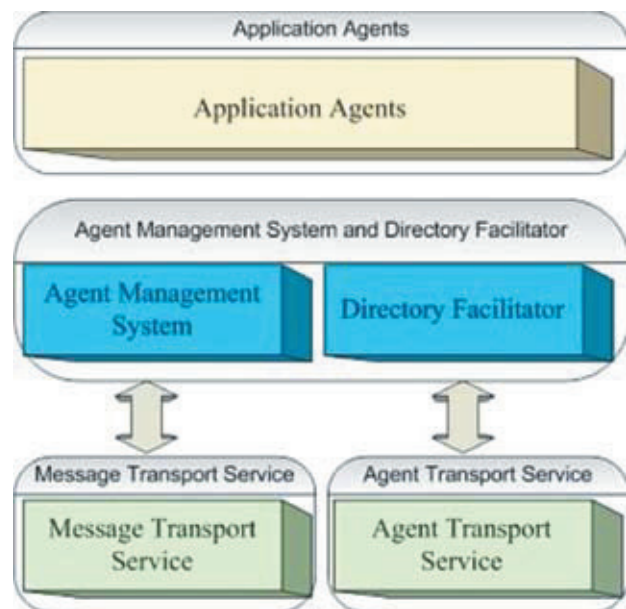


Figure 1: Major components of ACENET.

The Net framework was selected to build multi-agent systems for many reasons. Net is a rising technology; it is widely used by maximum users and supports many programming languages. It is treated as one language due to CLR (Common Language Runtime) and is excellent web supporting technology. Another motivation behind it was that till the end of 2004, more than one hundred agent platforms for the execution of multiagent systems, commercially and academically, have been built but not a single platform exists on NET. In 2005, the research

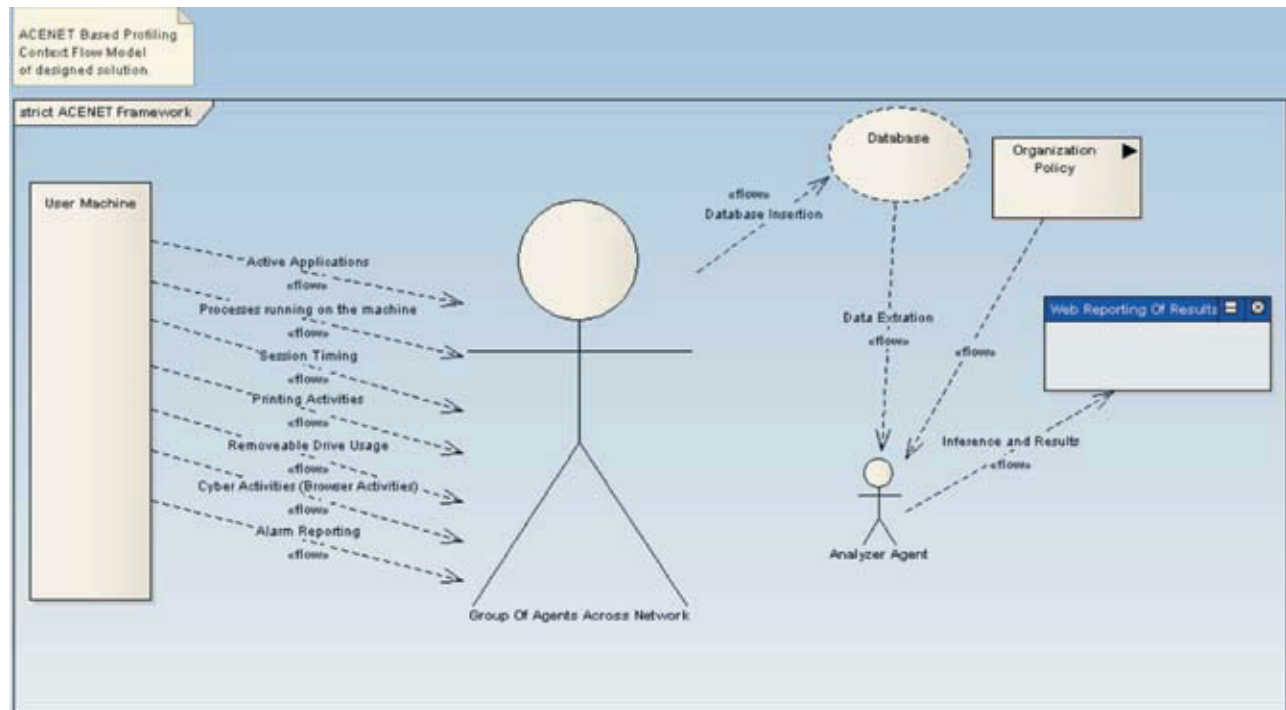


Figure 2: Context flow diagram of the profiling through ACENET.

community and agent-oriented programmers commenced to work on the framework as the high level application developer may explore agents in such a rising technology. Due to these motivations software agents on NET framework for profiling based security are proposed. An interface was developed with which users may interact with agents to assign them tasks. On the ground of the added features, ACENET (Figs. 1 and 2) is the first .NET based fault-tolerant agent platform that provides a decentralized architecture by implementing separate communication layer among different machines. It is reliable having both peer to peer and client-server architecture. All machines are independent to connect or disconnect that favors the decentralized architecture.

Results and Discussion

The ACENET is completely distributed as there is no server or controlling machine as generally occurs in other platforms. The

disadvantage of client-server architecture is that in case of server's failure the entire system and agents will go astray. In ACENET, all instances of the platform have the ability to work as server when it has to provide some services. Similarly, when it needs some services from other machines (agents) it will work as client and can be connected to any machine by just sending request. All machines are independent to connect or disconnect the model. In case of failure of a node the entire system will not be shutdown but only the services of the agents of that particular machine will not be available. The platform is executable over both local area network within the organization and internet.

Application agents interact with AMS and DF, and use the services of Agent Transport Service (ATS) and Message Transport Service (MTS) through AMS. AMS coordinates with all the modules of the ACENET. It acts as a mediator to all the components and performs administrator level tasks. DF provides directory

services to agents for searching agents and their services at runtime by specifying such search criteria such as Agent ID, Agent Name and Service Type. MTS supports asynchronous messaging between agents within the same platform and between ACENET to ACENET. ATS offers message passing service to agents between ACENET to ACENET. In future, the functionality of ATS will be extended for mobility as well. Because of that if one node does not work properly or fails to run and remains isolated, the other nodes remain intact and function without disturbance. Instead of shutting-down the entire system, only the agents of that machine will not be available to provide services. Therefore the architecture ensures high assurance using peer to peer architecture which brings scalability, fault tolerance and load balancing among distributed peers. There was the extensive use of the NET Remoting in the implementation of ACENET mainly for the communication and management purpose. Besides other implementations, the platform also provides configuration tools for Agent Management System, Directory Facilitator and Message Transportation [16].

As earlier discussed, privacy in this research has been handled in two different perspectives. The privacy of any employee may be ensured at implementation level when various agents are working at backend having profiles of all users. Agents of one user may not violate the privacy of the other. The second perspective is concerned with the deployment of the framework. When an organization is deploying ACENET, the professional issues pertaining to privacy must be ensured to resolve the probable conflict between the user and the organization.

In the field of computer science, privacy is separated in information privacy and communication privacy. Information privacy engages

the making of laws commanding the gathering and controlling individual's data such as credit information, medical and government records. The second one is the privacy of communications that involves the security and privacy of mail, telephones, email and other forms of communication. To facilitate reliable privacy, identity management has to be user controlled as it could be partially done at user's own machine [17].

The proposed framework addresses the issues of privacy as the user may not engage in any activities that create a conflict of interest with the user's responsibilities and obligations with the organization. Researchers are in agreement with the following guidelines that will assist in developing a model for user-profiling.

- a) Organization may publicize what can be monitored and what cannot be monitored, by providing a clear policy. No one will ever be surprised on this behavior of the organization, and it will avoid all kinds of risks of privacy rights law violation.
- b) Find a sense of balance between ethics, best practices in monitoring and keeping users in high spirits and creative. The most excellent way to do it is to come up to the concept of user monitoring as something that requires to be glowing thought out in advance and agreed upon by the management of the organization.

In accordance with the provided guidelines, policy-making is the foundation to resolve all kinds of probable conflicts.

The ACENET framework was deployed over corporate network to monitor behavior of the users to generate and keep up profiles. Agents running in the framework perform their tasks in hidden mode and are activated as users log into the system, as shown in Fig. 2. According

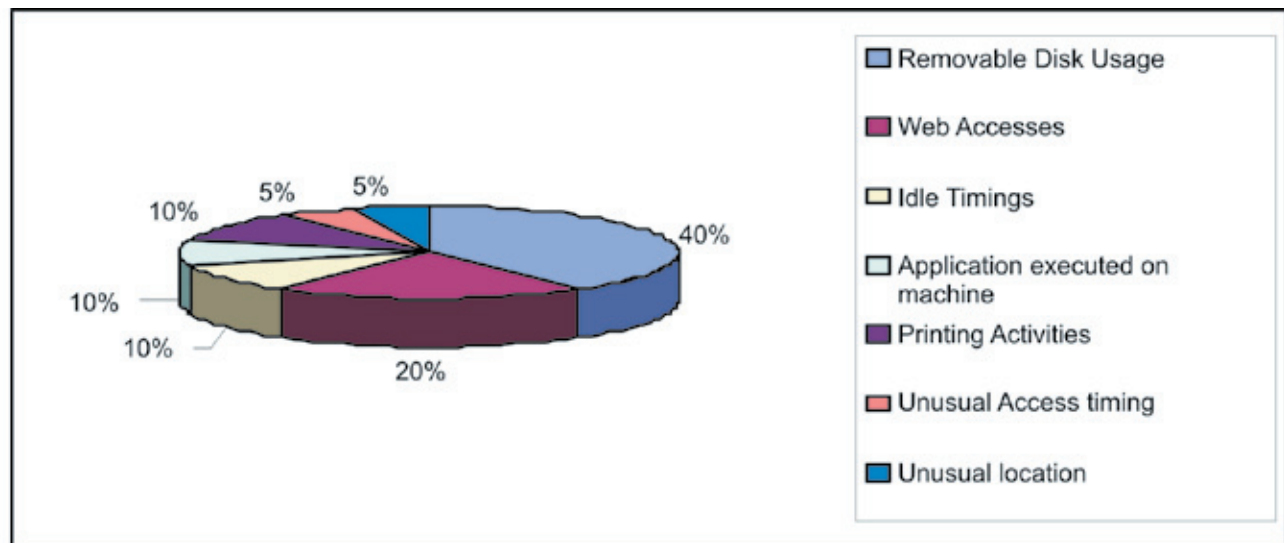


Figure 3: Organization's policy showing threat percentage of the activities

to local needs of the organizations, the agents were created to gather information of at least seven activities; justification already discussed. A brief overview has been presented here to explain what and how deployed framework monitors the behavior.

To estimate the level of overall threat to the organization, each individual activity threat was assigned by means of a weighting procedure. The maximum threat level to the organization was set up to 1. In order to bring the monitored activities into quantifiable form, threshold limits were set to estimate the behavior of the user [18].

The framework produces and maintains a profile consisting of all observed activities. It compares with the threshold values to decide the type of the user behavior. Fig. 3 shows the threat percentage of each activity.

Conclusion

The paper investigated the research areas of mobile agents and network security both from theoretical and practical aspects by focusing professional and ethical issues of privacy. The

problems of multi-agent systems and agent toolkits were investigated by surveying literature as well as practical implementation. Alternate and better solutions have been presented to address the pointed problems. The problem of network security has been further specified and the problems related to insider threat have been pointed out. The privacy issues, from organization and users perspectives, have been addressed. The solution of both insider threat and the user privacy have been presented in the shape of profiling. Finally, integrating all components an agent framework, ACENET, has been presented that provides most of the solutions identified in various components. It is concluded that along with the deployment of the framework there is need of understanding the business process and a clear policy of the organization that will be a threshold to monitor overall behavior of the users.

Acknowledgements

This work is part of PhD dissertation submitted to Shah Abdul Latif University Khairpur, Sindh, Pakistan and Higher Education Commission, Islamabad in December 2009.

References

1. **Nourani, C.F.** 1998. Software Agents and Intelligent Object Fusion. ACM SIGSOFT Software Engineering Notes archive, Volume 23, Issue 1, pp. 98-104.
2. **Phua, C., Alahkoon, D. and Lee V.** 2004. Minority report in fraud detection: classification of skewed data. ACM SIGKDD Explorations: Special issue on learning from imbalanced datasets, Volume 6, Issue 1, pp. 50 – 59.
3. **Mika, P.** 2005. Social Networks and Semantic web: The next challenge. IEEE Intelligent Systems proposed by Microsoft Research group.
4. **Sakarkar, G. and Upadhye, S.** 2010. A Survey of Software Agent and Ontology. International Journal of Computer Applications (IJCA), Volume 7, Issue 4, pp. 29-40.
5. **Tosic, P. and Agha, G.** 2004. *Towards a Hierarchical Taxonomy of Autonomous Agents*. Proceedings of IEEE International Conference on Systems, Man and Cybernetics (IEEE-SMC'04), The Hague, The Netherlands.
6. **Russell, S. and Norvig, P.** 2002. Artificial Intelligence: A Modern Approach. Englewood Cliffs, NJ: Prentice Hall, pp. 375-410.
7. **Maes, P.** 2005. *Designing Autonomous Agents*. Cambridge, MA: MIT Press, pp. 102-110.
8. **Pazzani, M. and Billsus, D.** 2004. Learning and Revising User Profiles: The Identification of Interesting Websites. Journal of Machine Learning (MACH LEARN), Volume 27, pp. 313-331.
9. **Charles, P. and Shari, L.** 2003. *Security in Computing*. Third Edition, pp. 7 – 28.
10. **Boff, E. and Santos, E.** 2006. Social Agents to Improve Collaboration on an Educational Portal. Proceedings of Sixth International Conference on Advanced Learning Technologies, pp. 896 – 900.
11. **Ramirez-Cano, D. and Pitt, J.** 2006. *Follow the Leader: Profiling Agents in an Opinion Formation Model of Dynamic Confidence and Individual Mind-Sets*. Proceedings of IEEE/WIC/ACM International Conference on Intelligent Agent Technology, (IAT'06), pp. 660-667.
12. **Huang, T. and Yang, C.** 2003. *An agent and profile management system for mobile users and service providers*. Proceedings of 17th International Conference on Advanced Information Networking and Applications (AINA'03), pp. 574-280.
13. **Yamakami, T.** 2007. *Classification of Mobile Internet User Behaviors using Qualitative Transition Patterns*. Proceedings of International Conference on Information Technology, (ITNG'07), pp. 890-892.
14. **Huber, M.J.** 2007. *Agent Autonomy: Social Integrity and Social Independence*. Proceedings of International Conference on Information Technology (ITNG'07), pp. 282-290.
15. **d'Inverno, M. and Luck, M.** 2000. *Sociological agents for effective social action*. Proceedings of Fourth International Conference on Multi-Agent Systems (ICMAS'00), pp. 379-402.
16. **Wanger, A.** 2009. *Creating and using Matrix Representations of Social Interaction*. Proceedings of ACM/IEEE International Conference on Human-Robot Interaction, pp. 125-132.
17. **Katrin, B., Marit, H., Katja, L., Andreas, P. and Sandra, S.** 2006. What user-controlled identity management should learn from communities. Information Security Technical Report, Volume 11, Issue 3, pp. 119-128.
18. **Ali, G., Shaikh, N.A. and Shaikh, Z.A.** 2009. Integration of Grid and Agent Systems to Perform Parallel Computations in a Heterogeneous and Distributed Environment. *Australian J. Basic appl. sci.* 3:3857-3863.