

MULTI-AGENT CO-ORDINATION IN DISTRIBUTED E-LEARNING ENVIRONMENTS: PROVIDING ACCESS PERMISSIONS

Shantha Visalakshi. U[#], Shyamala. K^{*},

[#] Department of Computer Science, Ethiraj College For Women, Egmore, Chennai – 600 008, Tamil Nadu.

shan_shrivisa@yahoo.com

^{*} Department of Computer Science, Dr. Ambedkar Govt. College, Vyasarpadi, Chennai – 600 039, Tamil Nadu.

shyamalakannan2000@gmail.com

Abstract— E-Learning, the new technology of supporting education and training, in recent times has been gaining a lot of attention. Content retrieval in e-learning refers the way by which the learning content is provided by means of electronic medium. It is an effective web-based learning paradigm, where many agents can be assigned with unique responsibilities to cope-up with the content retrieval by various users. Agent based system can manage the information stored in the e-learning environment, accessing and granting access permissions. Each task can be carried out by an autonomous agent and various such agents are grouped to form a multi-agent based system. Existing architectures do not consider the enhanced security measures, where it holds security as one among the agents. In the proposed architecture, security is enhanced at the network level and it wraps up all the other agents providing an enhanced security.

Keywords - Multi-agent architecture, Multi-agent co-ordination, e-learning, Security, distributed e-learning environments.

I. INTRODUCTION

E-learning in recent times has been gaining a popular name. Education and training is being carried out through the electronic medium and e-learning is one such technology used now- a-days. Simply put, e-learning refers to the use of various electronic media to impart knowledge. E-learning has paved the way for learning anytime and anywhere.

Content retrieval is the technique through the user request is provided by means of electronic technologies. E-learning facilitates the user to gain knowledge conveniently and it replaces the traditional learning system.

But security is often ignored although e-learning is gaining importance [2]. Security, literally put is protecting something from harm. Information security or security in e-learning means defending information from unauthorized access. Information access in e-learning is performed through the digital media, which really consists of a lot of risks.

Basically, security issues or security gaps are managed by identifying the assets, calculating the risks involved, setting security precedence, implementing a control mechanism for lesser risk and keep on monitoring the system for further issues or risks [4]. Identifying the assets includes the worth of the e-materials and the effort put up for the creation of the material. When the assets are identified, the risks involved, in publishing the contents over the internet are calculated. On identification and calculation of risks involved, the security precedence for the materials is set up based on the risks and security mechanisms are implemented. The task of providing security does not end here and it extends until the existence of the contents over the internet for the users. The maintenance is carried-out by monitoring the system for further issues.

Security breaches are often identified by the following ways that include checking the integrity of the content, checking accessibility, maintenance of the secrecy of the content and non-repudiation.

The existing system concentrates on multi-agent co-ordination but it is not concerned with the governance of the security issue of the entire system as a single entity [1]. Access control for content retrieval is one of the main issues in providing security to the e-learning system. Accessibility to the geographically dispersed content in the e-learning system also involves security issues [1].

In this paper, the architecture is proposed with an enhanced security agent along with the other agents of the system. When this system is implemented, it will concentrate on a security in e-learning as a whole and in co-ordination with the other agents security will become an enhanced one. Thus in co-ordination with the multiple agents of the system, the proposed system governs the overall security of the system by lying on top of all other

agents and a special declaration on the network layer. The main concentration of security in this paper lies on the network layer by an IP capturing mechanism.

II. LITERATURE REVIEW

The concept of using agents to oversee the responsibilities of the e-learning system has grabbed attention. The use of this multi-agent architecture is based on autonomic knowledge acquisition wherein the agents organize themselves dynamically and co-operate among themselves and provide interactive medium between the e-learning system and the users [6].

Security model for the wrapped security in the middleware or the business layer has to be done in such a way that the security attributes for the users as well as the administrator, instructor, technician, developer and institution should be taken into consideration [7]. Each and every entity of the system has an influence on the other entity's security attribute and thus the interdependencies must be well accomplished.

The comparative study that was illustrated in the paper [5] helped in relating the social aspects and importance of secure identity of the collaborative e-learning environment. The basic requirements of security are integrity, confidentiality and availability. These attributes are considered in order to enhance the security by identifying the identity of an entity that is a set of distinctive characters of an e-learning environment.

Today's e-learning environment is based on the service oriented architecture [8] where the contents tools and the functionalities are reusable which increase the security challenges for which this enhanced security mechanism provides a clear way out of security breaches.

Most of today's e-learning system is based on the service oriented architecture does not concentrate on integrating all the agents that are required for the effective security enhancement in the system[1]. This system aims at integrating multi-agent support into a generic architecture that considers feature such as interoperability, dynamism and etc.

A security perspective for the e-learning environment needs to be seen from the point of the learner as well as provider's[8]. Infrastructure, quality and cost are the three major perspectives received by the learning providers whereas readiness is the only perspective from the learner's side that throws security challenges.

III. SYSTEM ARCHITECTURE

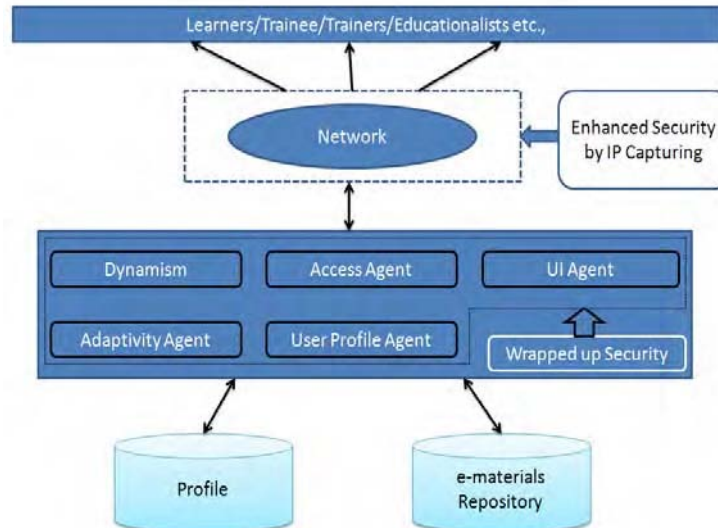


Fig.1. System Architecture

The system consists of databases that contain the registered users profile and a repository containing all the e-learning materials. The business layer of the system contains all the agents for the proper and excellent performance of the e-learning system.

The agents inside the business layer of the system are responsible for all the functions.

Dynamism agent:

This agent is responsible for the dynamic response from the e-learning system for the tasks performed on behalf of the learning community.

Access agent:

The access agent guards the accessibility of the contents of the e-learning system by providing access permissions for the users. It is also responsible for the access of the contents that are dispersed throughout many servers in various geographic areas.

User Interface agent:

The user interface must be user friendly and it must provide good communication between the user and the system. Since the learning systems now-a-days has increased and have been using a blended mode of learning techniques and adaptable mode of learning it becomes the responsibility of the system to provide a compatible and more user friendly interface.

Adaptive agent:

This agent predicts the response of the user by monitoring the activities of the user and acts accordingly. Thus the adaptability of the system is increased and the user's actions are interpreted by the system providing good dynamism for the system.

User Profile agent:

This agent ponders on personalization of the user profiles. The e-learning system must be able to adopt itself to changes on personalization of the user profiles. The user may have their own schedule for learning the contents and plan their own learning tests and interaction with other learners.

The business layer thus consists of these agents and these are wrapped up into a single unit and then a security agent is put upon that. This security agent is responsible for the security breaches in the agents that are wrapped up into a single unit. Each agent may have to satisfy a particular responsibility in which the agent can have certain security that would have been left without notice.

The UI consists of the learners, trainees, and trainers who access the e-learning contents from the system. There are chances of misuse of the network to hack the system and alter or copy the e-learning materials from the system. So, another set up that covers the network is put up in order to capture the IP addresses of the host that are accessing the e-learning environment.

IV. IMPLEMENTATION

Once when the e-materials repository and the other agents are set up for the publishing of the e-learning environment the system can be tested for security.

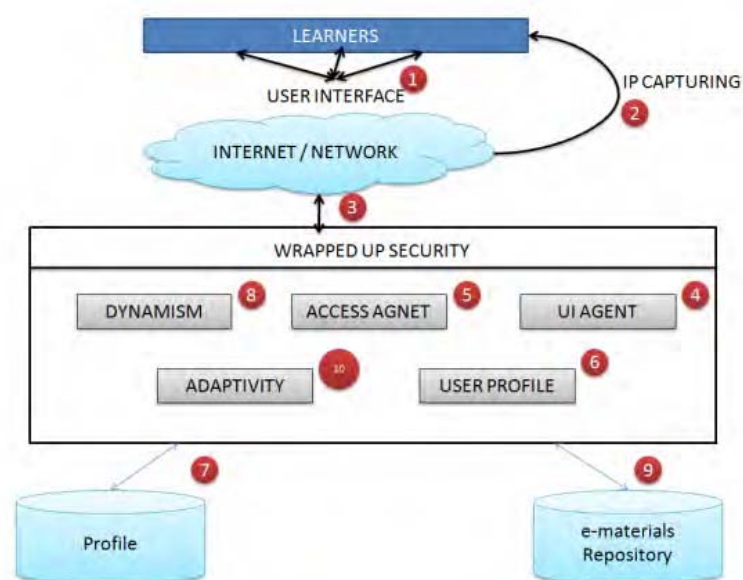


Fig. 2. Implementation steps

Implementation of the multi-agent co-ordination in e-learning security is discussed step by step in the following section:

Step1: Learners can interact with the e-learning environment by logging into the system with registration where the profiles of the learners and the trainers are stored in the profile databases. The system uses RSA algorithm in preserving the details of the user in the database.

Step 2: IP capturing is the second step where the IP address of the user who is entering into the e-learning environment is captured and stored in order to avoid illegal access of the contents in the system. IP capturing is legal and without IP capturing it can be noted that Apache and Tomcat will not turn the home page. So, IP capturing is used here to authenticate the user of the system.

Normally the IP address of the system can be captured from the DHCP server using the control panel options where the 'obtain DNS server address automatically' is enabled to capture the address of the host. Programmatically this is achieved and stored in the database corresponding to the user of the e-learning environment. The *IP.getHostByName()* and *IP.getHostEntry()* functions helps receiving the host IP address and this can be stored in the database. In this IP capturing mechanism, by registering the node with the system, security for the download of editable format of content is made available only to authorized nodes while only non-editable format of content is available for the other viewers from unregistered node.

Step 3: In this step the IP capturing and the user login details are sent to the business layer with the wrapped up security.

Step 4: The UI agent interacts with the network, receives the information from the UI and sends it to the next agent.

Step 5: The Access agent verifies the user profile for the accessibility of the user. The access agent is responsible for the grant of access rights to the users of the e-learning environment. By using the RSA and MD5 algorithms the accessibility of the contents are secured.

Step 6: User profile agent concentrates on the profile of the user and depending on the plans of the user that has been saved in the profile databases serves the needs of the learner.

Step 7: The user profile verifies the details sent to the business layer from the network layer and responds to the user request.

Step 8: The dynamism agent co-ordinates with the response from the user profile agent to endow with the needs of the user. This agent dynamically responds to the tasks performed on behalf of the learner.

Step 9: Dynamism agent fetches the contents based on the tasks of the user from the e-materials repository and returns it back to the UI.

Step 10: The final step is the Adaptivity wherein the user activities are interpreted by the system providing good dynamism. Thus the complete cycle of a user request ends here.

The implementation involves IP capturing and enhanced security where the Security is wrapped around the multiple agents responsible for various tasks carried out in the collaborative distributed e-learning environment. Also, it is ensured that only to the intended IP captured node, the editable retrieved content can be downloaded else the non-editable can only be viewed.

V. FUTURE ENHANCEMENTS

Future enhancements to this system includes a generic architecture that will enable IP capturing with voice recognition in the network layer merged together to improvise the security at the network level. Security provisioning for the database must be increased, as anyone who has an authenticated access can also break the database and copy the contents from the database. These are the future enhancements to be carried out that will enable authenticated access a safe one too.

Moreover the security here in this paper is based only at the network level, host level and the business level. But the security has to be enhanced at other levels to avoid unauthorized access.

VI. CONCLUSION

In recent times, e-learning has become a major part of training and education. E-learning has made learning possible anywhere anytime. The advancements in information technology have made a very great impact in e-learning environment resulting in this construction of the multi-agent architecture to enhance security. This paper proposed the generic architecture that co-ordinate the multiple agents to provide an enhanced security for the e-learning environment. The IP capturing security provision and enhanced security wrapped around the multiple agents thus provides intelligent security fit for the e-learning environment.

REFERENCES

- [1] K.Sakthiyavathi and K.Palanivel. A generic architecture for agent based e-learning system, *International conference on Intelligent Agent and Multi-Agent Systems (IAMA-2009)*, 2009, Pages 1-5.
- [2] P.R.Lakshmi Eswari. A process framework for securing an e-learning ecosystem, *International Conference on Internet Technology and Secured Transactions (ICITST)*, 2011, Pages 403 – 407.
- [3] M.Wareen and W. Hutchinson. Information Security – An e-learning problem, advances in web-based learning, *International conference on ICWL, Springer* 2003, ISBN 3-540-40772-3 Pages 21-26.
- [4] Available: <http://www.elearnmag.acm.org/securityissuesinelearning/>
- [5] Ruth Raitman, Leanne Ngo, Naonni Augar, and Wanlei Zhou. Security in the online e-learning environment, *Fifth IEEE International Conference on Advanced Learning Technologies (ICALT 2005)* Pages 702-706.

- [6] Alexandr Seleznyov, Mohamed O.Ahmed, and Stephen Hailes. ADAM:An agent- based middleware architecture for distributed access control,*The Twenty-Second International Multi-Conference on Applied Informatics: Artificial Intelligence and Applications*, 2004, Pages 200 – 205.
- [7] Jianming Yong. Security modelling for e-learning, *First IEEE International Symposium on Information Technologies and Applications in Education (ISITAE '07)*, 2007, Pages 1-5.
- [8] Najwa Hayaati , Mohd Alwi and IP Shing Fan, Information Security in e-learning, Technology Enhanced Learning , *Communications in Computer and Information Science, Springer Publication* , 2010,Volume 73, Pages 285-291.
- [9] A. Tripathi, M.Koka, K.Karnath, I.Osipkov, H.Talkad, T.Ahmed, D.Johnson and S.Dier, Robustness and security in a Mobile-Agent based network monitoring system, *International Conference on Autonomic Computing*, 2004, Pages 320-321.
- [10] V.Thiagarasu and T.Devi, Multi-agent coordination in project scheduling: Priority rules based Resource Allocation, published in academypublisher.com., *International Journal of Recent Trends in Engineering*, 2009, Pages 42-46.