ORIGINAL RESEARCH PAPER

Information Technology

ACCESS RESTRICTION EFFICIENCY OF MULTI ATTRIBUTE BEHAVIOUR ANALYSIS BASED RESTRICTION IN COLLABORATIVE ENVIRONEMNT

KEY WORDS: Collaborative environment; Privacy Protection; Users; User restriction; multi Attribute Behaviour

V.Samatha Lecturer in Computer Applications, PRR & VS Govt. college, Vidavalur

Dr M.V.Srinath* Sengamala Thayaar Educational Trust Women's Colelge, Mannargudi *Corresponding Author

ABSTRACT

The collaborative environment (CE) is one which contains large number of users as actors and each actor can perform different actions in the same resource which is shared. All the users do not have access to the entire resource present in the collaborative system, to restrict data tampering, misuse and illicit use. It is a major problem to provide privacy protection and control for the individuals who use the environment. Ensuring privacy in CEs requires the use of privacy policies which allow individuals to outline how they wish their private information to be used by others. Number of approaches have been proposed earlier for the restriction of users in the collaborative environment. In this paper, we discuss the efficacy of Multi Attribute behavior Analysis Based Restriction as a privacy protection tool in collaborative environment.

INTRODUCTION:

Collaborative environment has become the back bone for modern information technology sector which supports various activities of the IT sector to be performed in different locations without contradicting location dependency. In a software development system, a number of components are present, performing different tasks. Collaborative environment includes a number of users who have differential access to the resources being used for development of a particular software/program. To protect privacy and operate securely, users are often restricted by user profile based approach. Collaborative Environments (CEs) are distributed software applications and platforms that support both individual and group shared work in many areas, including research, business and learning (Q. Li, M. Abel, J. Barthčs, 2014). Privacy protection is a considerable problem in CEs, and any privacy protection system for CEs must be able to determine and infer how information should be shared as the situation changes.

ATTEMPTS AT PRIVACY PROTECTION FOR CEs:

Management of personally identifaiable information (PII) and the challenges involved are studied well. An agent-based prototype is described to support automated enterprise management of PII (Korba et.al., 2007). Several data mining techniques are combined to achieve the life cycle of private data, including individual data discovery, social network analysis, knowledge visualization, and effective human-computer interaction. The developed prototype can automate the management of PII within an organization by collecting, analyzing and applying security policies on that PII. One drawback of this approach is that it has the potential to actively monitor and analyze all user activity and behaviours within a collaborative environment. This monitoring can cause concerns among the users of the prototype. The work by Korba et al., (2007) is concerned with the discovery of PII through data mining, the collection of the discovered PII and the management of the collected PII. This differs from the collaborative privacy architecture which does not collect and analyze personal information. As well, while the work by Korba et. al., (2007) discusses the use of privacy policies, it does not detail what these privacy policies should look like.

Kanovich, Rowe and Scedrov (2007) propose an abstract formal model of collaboration which addresses privacy concerns. A state transition system is used to model private data through the use of a syntactic convention on a predicate symbol. The goal of this model is to describe how to generate a collaborative plan by providing some privacy guarantees to the participants. The created concerted plan is a sequence of transitions which will transform the environment from an initial state into a specific goal state. The work by Kanovich, Rowe and Scedrov (2007) has a different definition of privacy. The authors equate privacy with secrecy and are focused on developing a proper balance between the protection and release of information and resources (2007). This differs from the approach to privacy, as privacy is not considered to be just the isolation of private information. Instead, privacy includes the ability to understand how information is being used, why it is being used, and to have some influence over these decisions.

Burnap et. al., (2012) describe a method of using "sticky policies" to retain access control even after information has been moved to an autonomous computer system outside the control of the information owner. This ability is achieved by attaching a privacy policy alongside the private information, while at the same time distributing the access control elements. By attaching the policy with the information, the information gatherer will always have access to the access control document they must check against. Similarly, distributing the access control elements allows both the information collector and the information owner to access the policy decision maker even from different environments. This access will let for the information collector to check their access rights and will allow the information owner to change the access rights (Burnap et. al., 2012). The idea of being able to retain a measure of control over information that has been released into a collaborative environment is an important one.

This approach by Burnap et. al., (2012). shows one technical method to how this could be accomplished. This work differs from the architecture as the access control available through sticky policies only permit access based on roles, and does not take into consideration how an individual may be using the information.

Malik and Dustdar (2011) describe a method for sharing private information in a collaborative working scenario through an expansion to the RBAC NIST standard (2014) The scenarios considered by the authors of this work are similar to the situation, where overlapping teams work to complete shared tasks. In the approach taken by Malik and Dustdar, five main data elements are identified: enterprise, team, task, role and user (Malik and Dustdar, 2011). The use of a task element differs from the approach, which instead considers projects. Malik and Dustdar do not formally describe their privacy policy. However, Malik and Dustdar do identify some privacy requirements that are similar to the privacy rules introduced. The work by Malik and Dustdar is complementary, as they describe issues related to access control, considers information usage and provides extended features through the CPM.

Flight planning in the future collaborative environment (Stéphane Mondoloni, 2015) focused on obtaining using feedback, data sharing and simulation. Enforcing Context-Sensitive Policies in Collaborative Business Environments (Alberto Sardinha, Jinghai Rao, & Norman Sadeh 2007) includes enforcing access control policies whose elements are tied to changing contractual relationships or to information obtained from external sources (e.g. ratings, credit worthiness, export restrictions, etc.). Path-Restricted Parallel Q-Learning Algorithm in Collaborative Virtual

Environment (Zhigang Wang and Li Xiao, 2007) proposed to improve the application effect of the collaborative navigation control, a Q-learning algorithm based on the path restriction is proposed by constructing the absolute distance between a mobile agent of the virtual environment and its destination into a status function of reinforcement learning. Poster's Collaborative data exploration using two navigation strategies (Omar Gomez et. al., 2009) shows how two different modes of collaboration can affect user performance in a specific exploration task. Fair Trade Metaphor as a Control Privacy Method for Pervasive Environments: Concepts and Evaluation (Abraham Esquivel et.al., 2015), presents a proof of concept from which the metaphor of "fair trade" is validated as an alternative to manage the private information of users. This privacy solution deals with user's privacy as a tradable good for obtaining environmental services. Supporting Fine-Grained Concurrent Tasks and Personal Workspaces for a Hybrid Concurrency Control Mechanism in a Networked Virtual Environment (Jun lee et. al., 2012) propose a hybrid concurrency control mechanism that reduces restrictions of non-owners' behaviour and task-surprises in a networked virtual environment. Regulation was proposed as an Enabler for Collaborative Software Development (Allyson F Hardwin, 2015). Widespread availability and adoption of social channels has led to a culture where today's developers participate and collaborate more frequently with one another. TAMRI presents TAMRI, a planning tool for identifying task assignments based on multiple criteria and weighted project goals. Its implementation combines a distributed systems approach with Bayesian networks. The tool can be adapted to specific organizational environments by exchanging the underlying Bayesian network. A Tool for Supporting Task Distribution in Global Software Development (Lamersdorf, A. & Munch, J. 2009) presents an overview of task distribution approaches, gives three application scenarios for the tool, and shows the implementation of the tool as well as its application in the scenarios.

Multi Attribute Behavioural Analysis

Using the result of pre-processing, the method computes the trust factor for each attribute on the basis of the previous trace. The method computes the trust factor on each attribute on the basis of the users' behaviour represented by the access trace and based on the completeness of the access and how genuine the user has accessed the attributes in earlier days. Based on multi attribute trust factor the method computes trustworthy measure called CAM to decide the access control for the user.

Algorithm:

Input: Pre-processed Trace Ts
Output: CAM
Step1: start
Step2: read preprocessed trace Ts
Step 3: identify list of all attributes of the access

Attribute set As = $\sum_{i=1}^{size(Ts)} Ts(i).Attribute! \in As$

Step 4: for each attribute Ai
Compute number of access Na = $\sum_{i=1}^{size(Ts)} Ts(i).Attribute == Ai$

Compute number of successful access Nsa = $\sum_{i=1}^{size(Ts)} Ts(i).Attribute == Ai \&\&Status == Success$

Compute trust factor Tf = $\frac{Nsa}{Na} \times size(Ts)$
End

Step 5 : compute cumulative access measure $CAM = \frac{\sum Tf}{Numberofattributes}$

Step 6: stop
The algorithm discussed above computes the trust factor for each attribute and based on them the cumulative access measure is computed.

Multi Attribute Access Restriction

At this stage, the method first performs pre-processing using the input user request and the user access trace. Then the method performs the multi attribute behaviour analysis using the pre-processed trace. Based on computed trust factor and the cumulative access measure the method performs access restriction.

Algorithm:
Input: User Request Ur
Output: Boolean
Step1: start
Step2: read user request Ur.
Step 3: perform preprocessing
Step 4: cumulative access measure CAM = perform multi attribute behaviour analysis
Step 5: if CAM >TTh //trust threshold
Allow access
Else
Deny the request.
End
Step 6: stop.
The above discussed algorithm computes the access trust measure and cumulative access measure from behaviour analysis. Based on the trust measure the method performs the access restriction.

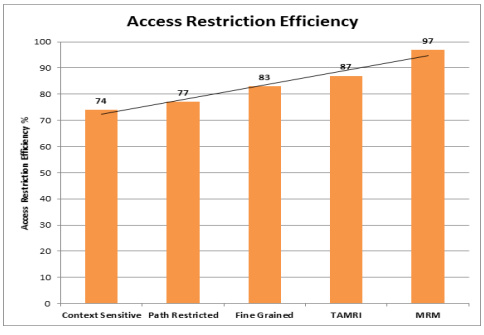
RESULTS AND DISCUSSION:

The proposed multi attribute behaviour analysis based restriction model has been implemented and evaluated for its efficiency. The method has been evaluated for its performance by simulating in different conditions. The method has produced the following results and the details of the simulation are presented below.

Sl.No	Parameter	Value
1	Number of Services	20
2	Number of Users	100
3	Size of Trace	500
4	Tool Used	Advanced Java

Table 1: Details Of Simulation

Table 1, shows the details of simulation and the number of services and users being considered for the evaluation purpose.



Graph 1: Comparison On Access Restriction Efficiency

Graph 1 shows the comparison on access restriction efficiency produced by different methods. The access restriction efficiency achieved by the proposed system MRM is 96%. The results show that the proposed approach has produced higher efficiency than other methods. This study claims that the proposed mechanism is best to compare than other existing systems regarding access restriction.

When we compared the throughput performance produced by various methods, The throughput value of our proposed system is 98 %. The proposed method shows better results when compared to the other existing systems. So the deduction of access restriction is accurate by this MRM model when compared to other systems.

CONCLUSION:

In this paper, an efficient Multi Attribute Restriction Model (MRM) has been proposed to improve the access restriction in collaborative environment. The method first receives the user request and identifies the component being claimed. Then the method identifies the list of attributes being required. Then the method collects the traces being accessed on the attributes. Each trace has been validated for its complete and noisy records have

been removed from the trace. Then the method performs the multi attribute behaviour analysis to compute the trust factor. Based on the trust factor, the method computes the cumulative access measure. The computed trust factor and the access measure have been used to restrict the user from accessing the component maliciously. The method has produced efficient results on access restriction and increases the throughput performance.

REFERENCES:

1. Abraham Esquivel, Pablo Haya, and Xavier Alamán, 2015. Fair Trade Metaphor as a Control Privacy Method for Pervasive Environments: Concepts and Evaluation, Journal of sensors, vol.15, issue 6.
2. Alberto Sardinha; Jinghai Rao ; Norman Sadeh 2007. Enforcing Context-Sensitive Policies in Collaborative Business Environments, IEEE, Data Engineering Workshop.
3. Allyson F. Hadwin, 2015. Regulation as an Enabler for Collaborative Software Development, Cooperative and Human Aspects of Software Engineering (CHASE)
4. Burnap P, Spasic I, Gray W, Hilton J, Rana O, Elwyn G 2012. "Protecting Patient Privacy in Distributed Collaborative Healthcare Environments by Retaining Access Control of Shared Information," in the Proceedings of the 2012 International Conference on Collaboration Technologies and Systems, IEEE, Denver, CO, USA, May 21-25, pp. 490-497
5. Jun Lee ; Mingyu Lim ; Hyung Seok Kim ; Jee In Kim, 2012. Supporting Fine-Grained Concurrent Tasks and Personal Workspaces for a Hybrid Concurrency Control Mechanism in a Networked Virtual Environment, IEEE, Presence Volume: 21, Issue: 4
6. Kanovich M, Rowe P, Scedrov A, 2007. "Collaborative Planning With Privacy," in the Proceedings of the 20th IEEE Computer Security Foundations Symposium, IEEE, Venice, Italy, July 6-9,pp. 265-278.
7. Korba L, Song R, Yee G, Patrick A, Buffett S, Wang Y, Geng L, 2007 "Private Data Management in Collaborative Environments," in the Proceedings of the 4th International Conference on Cooperative Design, Visualization, and Engineering, Springer, Shanghai, China, Sept. 16-20, pp. 88-96.
8. Lamersdorf, A. & Munch, J. 2009 "TAMRI: A Tool for Supporting Task Distribution in Global Software Development" Projects Proc. Fourth IEEE International Conference on Global Software Engineering ICGSE. Pp 322-327.
9. Li Q, Abel M, Barthčs J, 2014. "Facilitating Collaboration and Information Retrieval: Collaborative Traces Based SWOT Analysis and Implications," in Distributed Systems and Applications of Information Filtering and Retrieval, C. Lai, A. Giuliani,G. Semeraro (ed.). Springer Berlin Heidelberg, Studies in Computational Intelligence, vol. 515, pp. 65-78.
10. Malik and Dustdar S, 2011. "Enhanced Sharing and Privacy in Distributed Information Sharing Environments," in the Proceedings of the 7th International Conference on Information Assurance and Security, IEEE, Malacca, Malaysia, Dec. 5-8, 2011, pp.286-291.
11. National Institute of Standards and Technology Computer Security Resource Center,2014. "Role Engineering and RBAC Standards," U.S. Department of Commerce, NIST.
12. Omar Gomez ; Helmuth Trefftz ; Pierre Boulanger ; Walter F. Bischof, 2009. Poster: Collaborative data exploration using two navigation strategies, 3D User Interfaces, 2009. 3DUI .
13. Stéphane Mondoloni, 2015.Flight planning in the future collaborative environment, Digital Avionics Systems Conference (DASC).
14. Zhigang Wang ; Li Xiao, 2009. Path-Restricted Parallel Q-Learning Algorithm in Collaborative Virtual Environment, Computational Intelligence and Software Engineering.