A Congenial Access Control Technique for Knowledge Management Systems

Julius Olatunji Okesola & Oluwafemi Shawn Ogunseye

GJCST Classification
H.2.8,K.6.5

***Abstract*-Usability is of extreme importance in any system design. In knowledge management systems, the need for usability is heightened by the inertia to use the system by workers. The current popular access control technique used by in KMS and portals is not exactly suitable for such a sensitive system because it does not amend to the fuzzy nature of a KMS and KM functions and ends up making the system difficult to use and violates the overall objective of the system. The research highlights usability issues as one of the problems of KMS and a potent cause of failure it was therefore treated with such seriousness. A more congenial access control technique was proposed which allows for the fuzziness inherent in KMS for large organizations. The model was evaluated through a real-world implementation – the dotCSC and the design proved viable. The system had a 0% false positive and an initial 2.1% false negative rate which was quickly corrected. It eliminated the stress of continuous role engineering and modifications. The system also recorded a high level of usability based on an online survey conducted through it. Overall, we achieved adequate security and usability, a goal which has been elusive to KMS and other systems.**

Keywords-Knowledge management systems, Access control, Information security, semantic web, web mining, FOAF

I. Introduction

Saying knowledge is the world's most important resource is not entirely far from the truth. The status of an organization as far as competitiveness is concerned is dependent on the knowledge of the organization's workers. Knowledge Management describes how organization's manage and apply this knowledge. Interest in knowledge management has been very high and impressive with organizations deploying projects to manage knowledge worth millions of dollars[1]. As stated by [2], knowledge management projects would amount to a waste of time and money if organizations are not successful in its mediation and use. Knowledge management systems are information systems that help organizations acquire, manage and provide knowledge to solve their problems. They are systems that serve as mediators and are supposed to provide knowledge to users when, how and where they need them depending on the organization's policy. No organization would want their high cost knowledge management system to fail. One of the major causes of poor attitude to KMS leading to its eventual failure is the usability. This is true for most information systems[3]. Security has been known to have an inverse relationship with usability of systems[4]. The problem is basically the more intense the security the less usable a system becomes. This effect is amplified in knowledge management systems due to the already present reluctance users exude towards knowledge sharing and knowledge management systems [5,6]. Once people start to get discouraged or the system proves too difficult to use, the apprehension is quickly transferred into others discouraging them from using the system. The most prominent type of security measure used in KMS is Access control. Access control involves users providing the system with their valid identity and the system verifies the supplied identity in order to determine eligibility for access and the allowed activities for such legitimate user. Access control techniques are primarily classified into discretionary access control (DAC) and Non Discretionary Access Control (NDAC). DAC is an access control policy controlled by the owner of an object [7]. NDAC is directly opposite to DAC and does not involve the owner specifying the access policy to his/her resource[8]. Most KMS portals use Role based access control (RBAC). RBAC is a NDAC and involves assigning roles to users that will determine how they can access the {knowledge} resources [9&10]. Despite its wide use, knowledge management systems are undoubtedly more sensitive than portals and other information system applications and the unsuitability of RBAC as the access control technique is beginning to show. RBAC restricts all users to one role or the other in a finite set of roles. It does not appreciate the fuzzy nature of user roles in organization and which might not be exhaustible by a predefined role or set of roles [11]. This actually becomes more pronounced in the globalized state of large corporations today. So many mergers, collaboration and acquisition leading to so many established communities and systems coming together. KMS use in such systems require hitch free integration despite the different organizational structure. The predefined role in RBAC makes it tasking adapting to such growth or development. Knowledge requirement can also be fuzzy, how do we say for certain that a particular staff does not need to know a certain thing. This can be easy atimes and can also be very difficult. We therefore propose a more congenial access control technique which will use the user's reputation to determine their access rights to knowledge resources. Access is determined based on semantic information used to generate a reputation/authorization score that determines a user's access rights. The perspective taken therefore involves looking at the user as a member of a community regardless of our dispersed in time and space the other members of the community might be. His right to a

About[1] - Department of computer science;University of Agriculture, Abeokuta, Ogun State, NigeriaStatetunji_okesola@yahoo.co.uk, ogunseyeoluwafemi@yahoo.com

particular knowledge resource is therefore built on this relationship he has with the creator or owner of the knowledge resource and the collaborative knowledge community.

II. Related Work

[12] used a Friend Of A Friend (FOAF) architecture based web mining techniques to study relationship between users of a semantic web based social network site. They also were able to rank users by calculating trust values for them in the network. The EigenTrust [13] computes global trust values for peers based on their previous behavior. [14] proposed a strategy for calculating global trust for individuals in the network from the perspective of the designated seeds. The strategy uses group assertions for determining membership within a group. [15] created a method that involves certifying users at three levels. This method is very good in identifying ―bad" nodes and resisting their effect in the computation of trust. [16] used a local metric to calculate trust values for individual on a network. A similar method was also used in [17] but defers in that it uses a probabilistic interpretation of global belief combinations. [18] proposed an efficient algorithm for generating locally calculated reputation ratings from a semantic network and applied it to a mail application to rate mail according to relevance. This method was mathematically tested and proved to be highly effective and one of the most realistic. All these approaches are highly effective but not suitable for this work because we need a technique that can compute local trust values and does not involve a user manually ranking other users. To achieve this, we therefore build on the algorithm proposed by [18] and [12].

III. Method

First we view the organization‘s organogram as a multilevel tree structure (organizational tree structure). The chairman/president is at the root of the tree. We then assign values to each of the levels. Depending on the depth of the tree. The root has the highest value and highest weight and it decreases down the tree.Previous reputation networks are made of ratings given from one node to another[18] implying that each node (user) ranks each node on a particular scale e.g. 1-9. In this work we use a defined rank of 2 if there is a relationship between the users and 0 if there isn‘t. we assign the value of 1 to indirect relationships. When a user wants to access a knowledge resource, the user is evaluated to see if they have a direct connection with the owner of the resource i.e. they are in the same group. If they do, they are allowed to use that resource. If they do not then they are evaluated to see if they have an indirect relationship (see figure 1). The nodes are therefore traversed to find out. The level a node is on the tree also has its effect. For instance, the president should be able to access any knowledge resource on the system therefore a score of 1 on level 3 is different from 1 on level 5. Since level 5 is higher, the relationship is stronger and the score will therefore be higher. The data is gotten through a customized FOAF semantic data (figure 2) which applies to all user and keeps a record of their groups and affiliations. To detect relationship or authorization mark, the user is first probed using a web mining technique and then each member of their group is also probed to detect indirect relationship. The result is then used to calculate the user‘s authorization score.

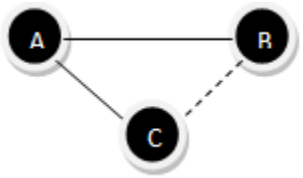

Figure 1: the possible relationships between nodes.

Direct relationship is shown with the straight thick line and indirect relationship is shown by the dashed line. C is the resource, and A has a direct link to it, and A has a direct link to C then B has an indirect link to C. from [12]

```
<rdf:RDF
xmlns:rdf=”http://www.w3.org/1999/02/22-rdf-syntax-ns#”
xmlns:foaf=”http://xmlns.com/foaf/0.1”
xmlns:unaab=”http://www.dotcsc.com/
okesola/tasued/0.1”>
<foaf:Person>
<foaf:mbox rdf:resource=”Okesola@tasued.edu.ng”/>
<foaf:name>okesola</foaf:name>
<foaf:interest rdfs:label=”Character agent”
rdf:resource=”http://www.dotcsc.com”/>
<foaf:currentProject rdfs:label =”CACT”
rdf:resource=”www.dotcsc.com”/>
<foaf:workplaceHomepage rdfs:label=”department of
computer science”
rdf:resource=”www.dotcsc.com/”/>
<dotcsc:group>programming
</position:seniorlecturer>
</level:5>
<foaf:Person>
<foaf:mbox rdf:resource=”Ogunseye@tasued.edu.ng”/>
<foaf:name>ogunseyeoluwafemishawn</foaf:name>
</foaf:Person>
</group:linux group>
</group:programmers group>
</position:analyst>
</level:3>
</foaf:Person>
```

Fig. 2. An example of a FOAF file based on extracted information from users

1) *The Algorithm*

The algorithm for our proposed access control technique is as follows:

Step 1: Login the user logs in to his computer and the KMS [the KMS can use the system‘s login so the user will not have to log in to the KMS as a separate entity. This is an optional feature]

Step 2: User profiling

The user is immediately profiled and his FOAF file pulled from the database

Step 3: Resource Requisition and Resource Owner Profiling
When the user requests a resource, the FOAF file of the owner is immediately pulled to an active memory.

Step 4: Processing Authorization and FOAF Mining
To achieve this step, the FOAF file is mined and the data it contains is extracted to be used for computation of reputation score.

This step involves four stages.

1. Get the prescribed threshold score for access authorization set by the KMS administrator.
2. Check if the user is directly connected to the resource owner, if yes, grant access if no then goto 3
3. Check if the members of the group are connected to the owner or a member of the owners group and compute their authorization score
4. If authorization score > threshold then access granted else, ask user to request permission from owner.

The FOAF data would contain, the person's name, the group(s) they belong to, their position {used in computing the level in the organogram scale}

The algorithm implies a member of a group can request resources belonging to someone or a group which he is not directly connected to but indirectly connected to {through a colleague that knows a colleague that knows a colleague…… } which would not be possible in a role based architecture. This is illustrated in figure 3.

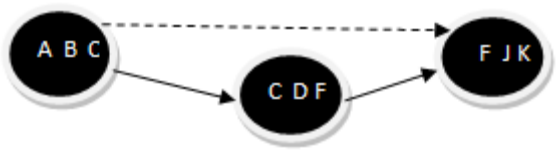

Figure 3. access control through user relationship and reputation

In figure 4, the assumption is that any user in the group made up of members A,B,C can request access to a knowledge resource from another group with members F,J,K which it might not have any knowledge of or direct connection to. This will be made possible through the use a link group which user C from the first group and user F from the owner's group both belong to. If this were defined in terms of roles a user A will not be able to access knowledge resources belonging to owner J in an independent group structure.

2) *The Authorization Score Computation Model*

The model used for computing the authorization score is built on the popular PageRank made popular and used by Google to rank web pages and sites based on links and has been established as an efficient model. This model had been used effectively in [12][19] to rank user based on trust and reputation. In explaining our application of the model we consider the authority value for a node ***v*** that requests a knowledge resource has an authorization value $\mathbf{A_n(v)}$ on iteration **n**. The authorization value propagates to neighboring nodes in proportion to the node's relevance.

$$A_{n+1}(v) = c \sum_{v' \in Neighbor(v)} \frac{R(v,v')}{Rsum(v)} A_n(v') + cE(v)$$

$$Rsum(v) = \sum_{v'' \in Neighbor(v)} R(v,v'')$$

Where **Neighbor(*v*)** represent a set of nodes, each of which Is connected to node **v**, **c** is a constant for normalization and E represents a source of authorization value in this case the level of node **v**. The owner of the document represents our target and is represented as $\mathbf{v_{target}}$. The final score is then compared to a threshold value which determines if access is granted or not. Note that the score are rounded up to the nearest integer value before comparison. See [12] and [20] for more details of the mathematical model.

3) *Assigning the threshold value*

The flexible threshold value gives the KMS administrator an opportunity to vary the strictness of access to knowledge resources and therefore the strictness of security for the system. By default, the system could be set to a score which will equal the attainable score if the user and the owner was on the same team. In this case that would be a score of 2.

Our implementation is discussed in the next section to serve as a sample.

IV. Application of the Model

The original influence for this research was the failure of the RBAC to meet the need for the Social Networking/KMS dot CSC" a web based wireless intranet portal designed by the second author for the department of computer science UNAAB in 2008 based on issues already discussed in the Introductory section of this paper. The proposed congenial model was therefore implemented as a replacement for the RBAC. The figure x show the screenshot of the SNA.

The model is therefore evaluated based on the reasons for its creation, these are: Security and Usability

1) *Security*

To evaluate for security, after four months of full scale deployment of the dotCSC wireless intranet portal, the

portal had 346 registered users. Upon implementing the congenial access
control model proposed in this paper, The security capabilities was tested by separating user access along class lines which could be overcame by the users due to due to group affiliations. Lecturers where given a rank of 5 and 100level students 1.The users are grouped as follows:

Table 1: Groups according to class

Level	Number
100	*50*
200	*63*
300	*121*
400	*106*

There are also 5 lecturers registered on the site Total:346

Table 2: Groups according to Interest

AVERAGE LIKERT SCALE RATINGS FOR THE DOTCSC USIN THE SCALE 1 = DISAGREE AND 4=AGREE	
Accessing knowledge resources on tl tCSC was easy	3.8
I enjoyed conversing and sharing eas on the dotCSC	3.9
The flow of operation was straight rward	3.9
It was easy using the portal to solve y problems	3.6

below; 127 people participated in the polls. The results for the usability test is shown in table 3 below.

Group Name	*Number*
Linux Groups	*15*
Programmers Club	*191*
Information Systems Group	*23*
Artificial Intelligence Group	*47*
Number of users not in a group	*70*

From the system log after 5 weeks of active use the results are analyzed as follows(see figure 4).

Total amount of login session = 1722
Total amount of distinct users= 313
% of False positives based on affiliation = 0.00%
% of False Negatives based on affiliation= 2.1%
% accuracy level of the system = 96%

Figure 4: the results of access log analysis

2) *Usability*

To estimate this, we poled the users through the portal: Questions relevant to this survey are shown in the table

V. Discussion

The sample implementation the viability and accuracy of our design. Though not perfect the false negative was quickly corrected by increasing the threshold. The system also proved to be acceptable to users who hardly realized any difference. The system was designed to monitor user login and also the attempts to access resources which triggers the authorization score computation. The system performed better than RBAC which was about 89% accurate in terms false positive and false negative computation and peaked at 91% when we used it. It also did not deny anyone access to resources who should have been allowed table 3: results of the usability poll

limitation

The model assumed a collaborative society where knowledge is allowed to be shared with almost everybody and where they are work groups and units.The implementation also showed that the initial computation of authorization score can be processor and memory intensive as the organizations grows. This we hoped can be solved by caching computation result in a fast memory.

VI. Conclusion and Future Work

In this work, we have proposed a congenial access control for knowledge management system based on the peculiarities of knowledge management and the unsuitability of the commonly used role based access control technique to address those needs. Through our methodology and evinced in the sample, the simplicity this model brings to access control for KMS is unique and achieves the desired and erstwhile elusive goal of accurately blending security and usability. This is highly due to the user focused design. This work will serve as a model for KMS developers to follow in their search for a more usable KMS. The effect of an increase in usability of a system is positive and multiplier and can be adopted even beyond the field of KM.

VII. Reference

1) Awad E.M. and Ghaziri H.M. (2004), Knowledge Management", Pearson Education, Inc.
2) Eva Maaninen-OlssonMay Wisme´n andSven A. Carlsson, (2009), Permanent and temporary work practices:knowledge integration and the meaning ofboundary activities, Knowledge Management Research & Practice (2008) 6, 260–273
3) Wing Lam & Alton Chua (2005) KNOWLEDGE MANAGEMENT PROJECT ABANDONMENT: AN EXPLORATORY EXAMINATION OF ROOT CAUSES, Communications of the Association for Information Systems (Volume 16, 2005) 723-743

4) Lorrie Faith Cranor, Simson Garfinkel (2005) Security and Usability:Designing Secure Systems that People Can Use,O'Reilly Media
5) Jean-Grégoire Bernard,(2006) "A Typology of Knowledge Management System Use by Teams," hicss, vol. 7, pp.155a, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 7, 2006
6) Kamla Ali Al-Busaidi, Lorne Olfman, Terry Ryan, and Gondy Leroy(2010), Sharing Knowledge to A Knowledge
Management System: Examining the motivators and the benefits in anOmani organization, Journal of Organizational Knowledge Management, IBIMA PublishingVol. 2010 Article ID 325835, [online]
http://www.ibimapublishing.com/journals/JOKM/jokm.html
7) Cavale, M., & McPherson, D. (2003). *Cu, Role-based access control using Windows Server 2003 Authorisation*
Manager. Microsoft Corporation. Retrieved from http://www.microsoft.com/technet
8) Ferraiolo, D., Kuhn, D., & Chandramouli, R. (2003). *Role-based access control*. Artech House, Computer Security Series.
9) Kamvar, Sepandar D. Mario T. Schlosser, Hector Garcia-Levien, Raph and Alexander Aiken. (1998) "Attack resistant trust metrics for public key certification." *7th USENIX Security Symposium*, San Antonio, Texas.
10) Hu, V. C., Ferraiolo, D. F., & Kuhn, D. R (2006). *Assessment of access control systems*. NIST Interagency Report 7316.
11) Mori J., Matsuo Y. Hashida K. Ishizuka M., Web Mining Approach for a User-centered Semantic Web, [online] http://swoogle.umbc.edu. Accessed 9/august/2010
12) Molina, The EigenTrust Algorithm for Reputation Management in P2P Networks", *Proceedings of the 12thb International World Wide Web Conference*, May 20-24, 2003, Budapest, Hungary.
13) The Advogato Website: http://www.advogato.org
14) Golbeck, Jennifer, Bijan Parsia, James Hendler, (2003), Trust Networks on the Semantic Web," *Proceedings of Cooperative Intelligent Agents 2003*, August 27-29, Helsinki, Finland.
15) Kumar, Ravi, Prabhakar Raghavan, Sridhar Rajagopalan,
D. Sivakumar, Andrew Tomkins, and Eli Upfal. (2000) "The web as a graph". *Proceedings of the Nineteenth ACM SIGMODSIGACT-SIGART Symposium on Principles of Database Systems*.
16) Richardson M, Agrawal R, Domingos P.Trust Management for the SemanticWeb", available at http://citeseerx.ist.psu.edu/viewdoc/download?doi 10.1.1.3.6539&rep rep1&type pdf. Accessed 19/august/2010.
17) Golbeck J. and Hendler J. ()Inferring Reputation on the Semantic Web
18) Y. Matsuo, H. Tomobe, K. Hasida, and M. Ishizuka. Finding Social Network for Trust Calculation, *In Proc. 16th European Conf. on Artificial Intelligence (ECAI2004)*, 2004.
19) S. Brin and L. Page. The anatomy of a large-scale hypertextual web search engine, *In Proc.*
20) *7th WWW conf*, 1998.