Asian Journal of Information Technology 15 (22): 4541-4545, 2016
ISSN: 1682-3915

Multi Attribute Behavior Analysis Model Based Access Control for Performance Development in Collaborative Environment

[1]S. Rajeshwari and [2]A. Chandrasekar
[1]Saveetha School of Engineering, Saveetha University, Kuthambakkam, India
[2]Department of CSE, St. Joseph's College of Engineering, Tiruchirappalli, India

Abstract: The problem of access control in collaborative environment has been studied in various situation and there are number of methods has been studied in detail. Still the methods suffers with the poor performance in access control and affects the performance of the collaborative systems. To improve the performance in security and throughput performance, we propose a novel multi attribute behavior analysis model which uses different attributes to compute the trustworthy of the user. The method receives the request from user and identifies the set of all attributes being accessed to complete the process. Based on identified attributes, the method collects the traces produced by accessing the attributes. Using the traces available, the method performs behavioral analysis to computes the trustworthy of accessing the same attributes and others. Based on the trustworthy value the method decides the access of the request generated. The method improves the performance of the collaborative environment and improves the throughput performance.

Key words: Collaborative environment, secure computing, behavior analysis, access control, QoS development

INTRODUCTION

The growing technology sector has various impact in different domain of engineering and has various applications in other sectors. The development of information technology has great impact in various domains and could be used to improve the performance of any problem. The same can be applied in the collaborative environment where the task can be performed in a collaborative nature. For example, the task T can be performed and shared by more than one resource R to achieve in a short period. In a collaborative environment, the process can be performed in shared manner where the update done by any of the user will get reflect in others view and vice versa.

In general phenomena, the organization maintains more number of units in different geographic region of any country or world. The peoples working in different units works together to perform the task where they cannot assemble in a single location is not possible. To perform the specified task the users shares the same copy of the resource and whatever the modification performed by any person will get reflect on the others copy. Such processing approach is named as collaborative working and such environment is named as collaborative environment.

However, the resource present in the collaborative environment has to be secured from unauthorized access because the access protocol could be breached easily due to the loosely coupled nature. To overcome the difficulty of unauthorized access the resources must be restricted from access using strategic access protocols. The basic password based approaches are not suitable for these kind of problems where it can be overridden by the malicious user easily. Also the usage of key based approaches are not useful in this problem of collaborative environment. In general case, the users of collaborative environment is restricted based on their profile or based on some other factor. Whatever the protocol being used, the efficiency of restricting the malicious access could not be achieved efficiently.

The problem of enforcing security in collaborative environment has been studied in different study but most of them uses attribute based access control methods. The methods restricts the users from accessing certain attributes based on their rights where the protocol maintains different restriction meta data. Eventhough the legitimate user would produce an malicious access in some times, so that the protocol enforced to secure the resource will not be effective at all the times. To overcome this issue, the necessary of statistics approaches are essential. Also the quality of service of the collaborative environment is depending on various factors like throughput, tampering efficiency and many more. To achieve such high quality parameters, some efficient protocols has to be enforced. In this study, we discuss

Corresponding Author: S. Rajeshwari, Saveetha School of Engineering, Saveetha University, Kuthambakkam, India

about such an efficient access restriction protocol to improve the quality of service of the collaborative environment.

Literature review: There are number of access control mechanism has been declared in the literature and discuss about some of them related to the problem.

Trust and security in collaborative environments (Mihok *et al*., 2008) purpose of this study is to summarize how trust can be considered in collaborative environments. Partial results of the field studies of two European IST projects, FLUID-WIN and SEAMLESS, are presented. Identity management problems and trusted operational scenarios are treated.

STORM: Collaborative security management environment (Ntouskas *et al*. 2011), discusses that the security management is a necessary process in order to obtain an accurate security policy for Information and Communication Systems (ICS). Organizations spend a lot of money and time to implement their security policy. Existing risk assessment business continuity and security management tools are unable to meet the growing needs of the current, distributed, complex IS and their critical data and services. Identifying these weaknesses and exploiting advanced open-source technologies and interactive software tools we propose a secure, collaborative environment (STORM) for the security management of ICS's.

A constraint and attribute based security framework for dynamic role assignment in collaborative environments (Cruz *et al*., 2008), investigate a security framework for collaborative applications that relies on the Role-Based Access Control (RBAC) model. In our framework, roles are pre-defined and organized in a hierarchy (partial order). However, we assume that users are not previously identified, therefore the actions that they can perform are dynamically determined based on their own attribute values and on the attribute values associated with the resources. Those values can vary over time (e.g., the user's location or whether the resource is open for visiting) thus enabling or disabling a user's ability to perform an action on a particular resource. In our framework, constraint values form partial orders and determine the association of actions with the resources and of users with roles. We have implemented our framework by exploring the capabilities of semantic web technologies and in particular of OWL 1.1 to model both our framework and the domain of interest and to perform several types of reasoning

Assessing collaboration framework in multi cloud environment (Pandey and Gonnade, 2014), surveyed every one of those system that are zone of concern when an existing model is to be changed the architecture to manufactured environment, the stage on which the services are to be imparted and finally the business sector perspective that is its cost viability contrasted with the accessibility. The multi-cloud environment can end the vendor lock-in of the consumer which is a trait in the single cloud. The significant zone of concern in this field is the understanding between the cloud service providers for collaboration of their services in multi-cloud. The purchaser will get exceptionally profited with multi-cloud environment and acquire services dependent upon his inclination and prerequisite and not dependent upon his cloud service provider.

MATERIALS AND METHODS

The design and implementation of collaboration service integration platform based on context-aware role based access model (Lu *et al*., 2014), designs and implements the Collaboration Service Integration Platform (CSIP) which combines Business Process Model and Notation (BPMN) and Context-Aware Role-Based Access Control (CARBAC) model. The context information is considered to enhance RBAC and adjust the authority of user role dynamically. For implementation, the logic gateways and connectors are added in the tasks and workflows for adjusting the authority dynamically. The right information can be accessed by the right user in CSIP based on CA-RBAC.

Currency exchange rates prediction based on linear regression analysis using cloud computing (Lin *et al*., 2013), proposed a novel cloud computing approach to do linear regression prediction for dynamic currency exchange rates. We adopt an Intelligent Exchange Rates Prediction System (IERPS) based on cloud computing to collect real-time exchange rates information and predict the future exchange rates in efficient computing time. The system can process large amounts of historical and dynamic data more efficiently and accurately. The experimental results showed that the average error ratios of using linear regression are 94.6% which is a very good performance.

An architecture of document control system for blocking information leakage in military information system (Eom *et al*., 2012), architected a document control system for monitoring leakage of important documents related to military information. Our proposed system inspects all documents when they are downloaded and sent. It consists of 3 modules authentication module, access control module and watermarking module. The authentication module checks insider information for allow to log on system. The access control module control

access authorization to do operations by insiders according to their role and security level. The watermarking module is used to track transmission path of documents. The document control system controls illegal information flow by insiders and does not allow access to documents which are not related to the insider's duties.

A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC (Jin *et al*., 2012), takes a step towards this end by constructing an ABAC model that has "just sufficient" features to be "easily and naturally" configured to do DAC, MAC and RBAC. For this purpose we understand DAC to mean owner controlled access control lists, MAC to mean lattice based access control with tranquility and RBAC to mean flat and hierarchical RBAC. Our central contribution is to take a first cut at establishing formal connections between the three successful classical models and desired ABAC models. All the above discussed approaches has the problem of restricting malicious access and produces poor results in access control.

Multi attribute behavior analysis approach: The multi attribute behavior analysis model maintains trace about the access of various uses of the collaborative environment. The method monitors the behavior of users of the environment and generates patterns of access at each time window. Based on that the method computes the trust weight for the user on the request using which the user is restricted and controlled from malicious access.

Figure 1 shows the architecture of the proposed multi attribute behavior analysis model and shows the functional stages in detail.

Preprocessing: The method maintains large set of logs about the access performed by various users. Whenever a user access the resource from the collaborative environment and at the time when a request is being processed, the method monitors the list of properties or attributes has been modified or accessed. Such information has been stored in form of trace and at the preprocessing stage, the method identifies the number of attributes the request will access and collects the traces produced in accessing the same attributes. From the traces the method removes the incomplete one and using the rest the method splits each attribute access and their status.

Algorithm:

Pseudo Code of Preprocessing:
Input: Access Trace At, Request Req
Output: Preprocessed Trace Pt.
State

Identify traces belongs to the user access. User trace Ut= $\int^{SIZE(At)}_{i=1}$ Σat(i).User= = Req. User && At(i). Res = = Req. Res

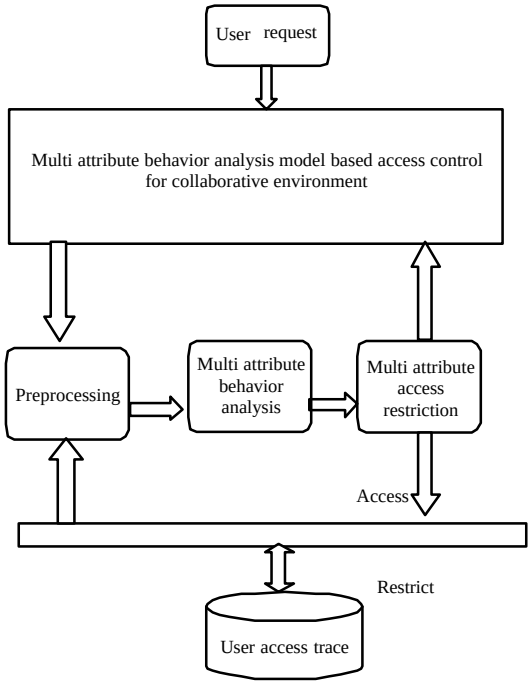

Fig. 1: Architecture of multi attribute behavior analysis model

For each trace Ti from Ut
Verify the completeness of the trace.
If $\int^{SIZE(Ut)}_{i=1}$ ΣUt(i)∈∀(Attr) then
Remove the trace.
Ut = Ut∩Ut(i)
Else Pt = Pt∪Ut(i)
End End
Stop

The above discussed algorithm, performs preprocessing of traces and removes the noisy one.

Multi attribute behavioral analysis: Using the result of preprocessing, the method computes the trust factor for each attribute based on the previous trace. According to the behavior of the users which is represented by the access trace the method computes the trust factor on each attribute which is computed 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 to decide the access control for the user.

Algorithm:

Pseudo Code of MABA:Input: Preprocessed Trace PtOutput: Multi Attribute Trust Factor MATF.Start
For each attribute Ai of request Req
Compute Total number of access.
Tna = $\int^{SIZE(Ut)}_{i=1}$ Σpt(i)∈ Ai
Compute number of completeness.
Nc =

$\int^{SIZE(pt)}_{i=1}\Sigma(pt)(i)\epsilon Ai)\&\&Pt(i).\ Status==success$
Compute trust factor of Ai.
$Tai = Nc/Tna \times size(Pt)$
End
Compute Multi attribute trust factor MATF.
$MATF = \int \Sigma^{SIZE(Accy)} Tai(Ai)/size(Attr)$
Stop

The above discussed algorithm computes the multi attribute trustworthy measure by computing the multi attribute trust factor to decide the trust of any user request.

Multi attribute access restriction: At this stage, the method uses the above mentioned two modules to perform access control. Upon receiving the request from the user the method performs preprocessing and multi attribute behavioral analysis. Based on the result of multi attribute behavioral analysis the method computes the trust factor to allow or deny the user request.

RESULTS AND DISCUSSION

The proposed multi attribute behavior analysis approach has been implemented and evaluated for their efficiency. The method produces efficient results in all the factors of quality of service in collaborative environment. The method has been tested and evaluated using various simulation parameters.

Table 1, shows the details of simulation parameters being used to evaluate the performance of the proposed approach. Figure 2 shows the comparison of security efficiency produced by different methods and it shows clearly that the proposed method has produced higher efficiency than other methods. Figure 3 shows the comparative results on false classification ratio produced by different methods and it shows clearly that the proposed method has produces less false classification ratio than other methods. Figure 4 shows the comparison of time complexity produced by different methods and shows that the proposed method has produces less time than other methods.

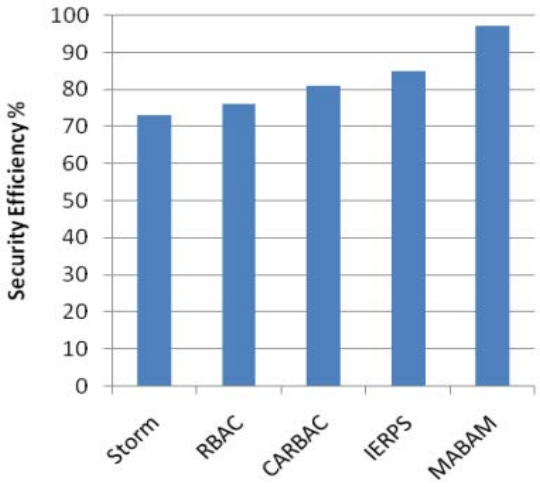

Fig 2: Comparison of security efficiency

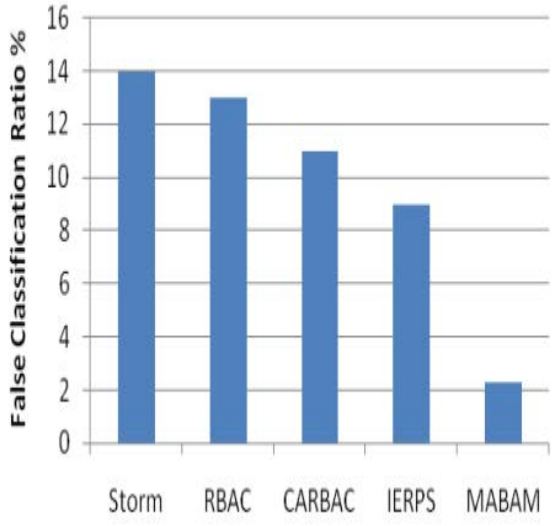

Fig. 3: Comparison of false classification ratio

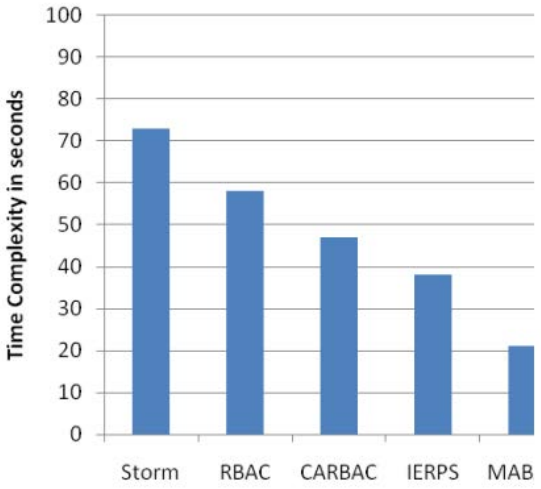

Fig. 4: Comparison of time complexity

Table 1: Details of simulation Parameters

Parameter	Value
Tool used	Advancedjava
Number of resources	100
Number of users	500
Size of trace	1 million

CONCLUSION

In this study, we propose a novel multi attribute behavior analysis model to improve the security in the collaborative environment and improve the quality of service of the system. The method preprocess the previous traces to eliminate the noisy data traces. At the second stage, the method computes the trust factor for each attribute being identified that the request would access. Based on the trust factor being computed the method computes the multi attribute trust factor which represents the trustworthy of the request. Based on the value the user request is handled to produce efficient results. The method has been evaluated for its efficiency and has produced efficient results in all the factors of collaborative environment.

REFERENCES

Cruz, I.F., R. Gjomemo, B. Lin and M. Orsini, 2008. A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments. In: Collaborative Computing: Networking, Applications and Worksharing. Elisa, B. and B.D.J. James (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-642-03353-7, pp: 322-339.

Eom, J.H., N.U. Kim, S.H. Kim and T.M. Chung, 2012. An architecture of document control system for blocking information leakage in military information system. Int. J. Sec. Appl., 6: 109-114.

Jin, X., R. Krishnan and R. Sandhu, 2012. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. In: Data and Applications Security and Privacy XXVI. Boulahia, N.C., F. Cuppens and G.A. Joaquin (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-642-31539-8, pp: 41-55.

Lin, S.Y., C.H. Chen and C.C. Lo, 2013. Currency exchange rates prediction based on linear regression analysis using cloud computing. Int. J. Grid Distrib. Comput., 6: 1-10.

Lu, S.P., K.K. Shao, Y.N. Chao, K.S. Luo and C.H. Chen, 2014. The design and implementation of collaboration service integration platform based on context-aware role based access model. Int. J. Sec. Appl., 8: 295-306.

Mihok, P., J. Bucko, R. Delina and D. Palova, 2008. Trust and Security in Collaborative Environments. In: Enterprise Interoperability III. Mertins, I.K., R. Ruggaber, K. Popplewell and X. Xiaofei (Eds.). Springer London, England, ISBN: 978-1-84800-220-3, pp: 135-143.

Ntouskas, T., G. Pentafronimos and S. Papastergiou, 2011. STORM-Collaborative Security Management Environment. In: Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication. Ardagna, C.A. and Z. Jianying (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-642-21039-6, pp: 320-335.

Pandey, R. and S. Gonnade, 2014. Assessing collaboration framework in multi-cloud environment. Int. J. Innovative Technol. Exploring Eng. (IJITEE.), 3: 24-27.