Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1098 – 1107

RESEARCH ARTICLE

Ancillary Multi Trust Virtual Dissemination for Capability Fortifying Systems

S. Sundar Raj[1], Dr. Ashish Chaturvedi[2]

[1]Research Scholar, Department of Computer Science and Engineering,
Himalayan University, Arunachal Pradesh, India, rajsundar1003@gmail.com

[2]Professor and Associate Director, Arni School of Computer Science and Applications,
Arni University, Indora (Kathgarh), Himachal Pradesh, India, dr_ashysh@yahoo.com

Abstract— Virtualized services can take benefit of statistical multiplexing across solicitations to yield momentous cost savings to the operator. However, achieving similar benefits with real-time services can be an encounter. In this paper, we pursue to lower a provider's costs of real-time IPTV amenities through a virtualized IPTV design and through intelligent time shifting of service delivery. We take modernization of the differences in the deadlines supplementary with Live TV versus Video-on-Demand (VoD) to effectively multiplex these services. We provide a generalized framework for computing the amount of resources needed to support multiple services, without missing the deadline for any service. We construct the problem as an optimization formulation that uses a generic cost function. We consider multiple forms for the cost function (e.g., maximum, convex and concave functions) to reflect the different pricing options. The solution to this formulation gives the number of servers needed at different time instants to support these services. We implement a simple mechanism for time-shifting scheduled jobs in a simulator and study the reduction in server load using real traces from an operational IPTV network. We also show that there are interesting open problems in designing mechanisms that allow time-shifting of load in such environments.

Keywords—: Virtualized services, IPTV, Video-on-Demand, Dynamic Resource Allocation

I. INTRODUCTION

Access control, which is used to restrict the use of resources, is an important safeguard in network security. Nowadays, most of access control models have been studied extensively in centralized and static environment, and they seldom meet the requirements of some open and dynamic environments, such as Grid and P2P. Traditional access control models do not work in these environments. The entities that a system well will interact with or the resources that will be accessed are not always known in advance. Thus, it is almost impossible to predefine permissions to an entity. Since almost all traditional access control models rely on successful authentication of predefined users, they become unsuitable for open and dynamic environments. Access control in these environments must dynamically adapt to dynamic addition and deletion of entities.

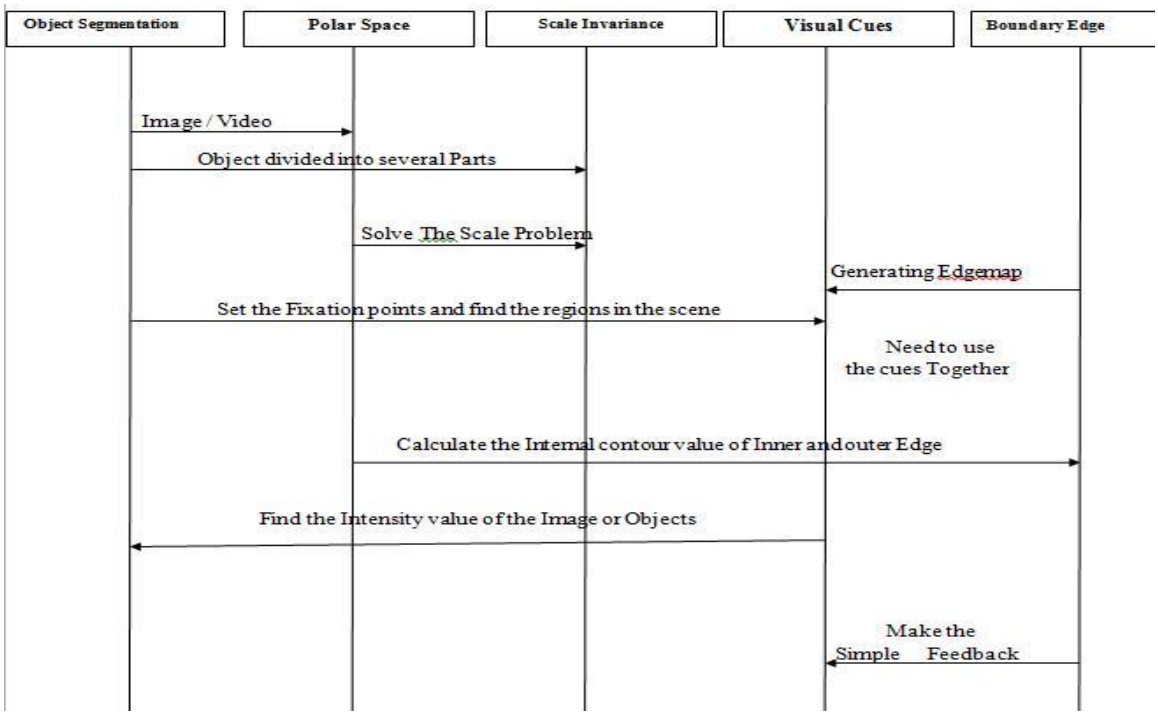

Fig 1.1 Sequence View of Fixation points in various Edges

In this paper, we propose an access control model based on multi-factors trust. We compute trust using several factors, and we present a trust based access control model. Trust is a part of our daily life and thus can be used as a tool to reduce the complexity of making access decisions, which can be accomplished by using trust to provide security [1]. In recent years, many researchers have applied trust to the dynamic environments. In [2], trust models are proposed to control anonymity, unpredictability and uncertainty. However, there is several factors affect trust. For example, entities attribute, time, network condition and history behavior. ICC adds a demand that is proportional to the number of users concurrently initiating a channel change event [1]. Operational data shows that there is a dramatic burst load placed on servers by correlated channel change requests from consumers (refer Figure 1). This results in large peaks occurring on every half-hour and hour boundaries and is often significant in terms of both bandwidth and server I/O capacity. Currently, this demand is served by a large number of servers grouped in a data center for serving individual channels, and are scaled up as the number of subscribers increases. However this demand is transient and typically only lasts several seconds, possibly upto a couple of minutes. As a result, majority of the servers dedicated to live TV sit idle outside the burst period. In a virtualized environment, ICC is managed by a set of VMs (typically, a few VMs will be used to serve a popular channel). Other VMs would be created to handle VoD requests. With the ability to spawn VMs quickly [3], we believe we can shift servers (VMs) from VoD to handle the ICC demand in a matter of a few seconds.

II. LITERATURE SURVEY

There are mainly three threads of related work, namely cloud computing, scheduling with deadline constraints, and optimization. Cloud computing has recently changed the landscape of Internet based computing, whereby a shared pool of configurable computing resources (networks, servers, storage) can be rapidly provisioned and released to support multiple services within the same infrastructure [7]. Due to its nature of serving computationally intensive applications, cloud infrastructure is particularly suitable for content delivery applications. Typically LiveTV and VoD services are operated using dedicated servers [2], while this paper considers the option of operating multiple services by careful rebalancing of resources in real time within the same cloud infrastructure. Arrival of requests that have to be served by a certain deadline have been widely studied [8], [9]. For a given set of processors and incoming jobs characterized by arrival time and requirement to finish by certain deadline, EDF (Earliest Deadline First) schedules the jobs such that each job finishes by the deadline (if there are enough processors to serve) [10]. In this paper, there are multiple sets of services providing

jobs. Each of these services send request for chunks with different deadlines. For a fixed number of processors, EDF is optimal schedule. In this paper, we find the region formed by server tuples so that all the chunks are serviced such that no chunk misses deadline. Optimization theory is a mathematical technique for determining the most profitable or least disadvantageous choice out of a set of alternatives. Dynamic optimization is a subbranch of optimization theory that deals with optimizing the required control variables of a discrete time dynamic system.

In this paper, we consider finite-horizon optimization where the optimal control parameters with finite look-ahead are to be found [11] [12]. More specifically, we know the arrival pattern of the IPTV and VoD requests with their deadlines in the future. We wish to find the number of servers to use at each time so as to minimize the cost function. In this paper, we consider different forms of cost functions. We derive closed form solutions where possible for various cost functions.

III. METHODOLOGY

3.1 EXISTING METHOD

Semantic access control (SAC) is a access control model, which uses machine reasoning at a semantic level to determine whether let the requests pass according to the semantic descriptions of the policies, requests, resources and other entities. Compared with traditional access control, SAC is more scalable, more applicable to dynamic environments with heterogeneous and complex access criteria.

3.2 DISADVANTAGES

Unfortunately, the foundation of SAC is the semantic web technologies. So it cannot be applied in all access control fields.

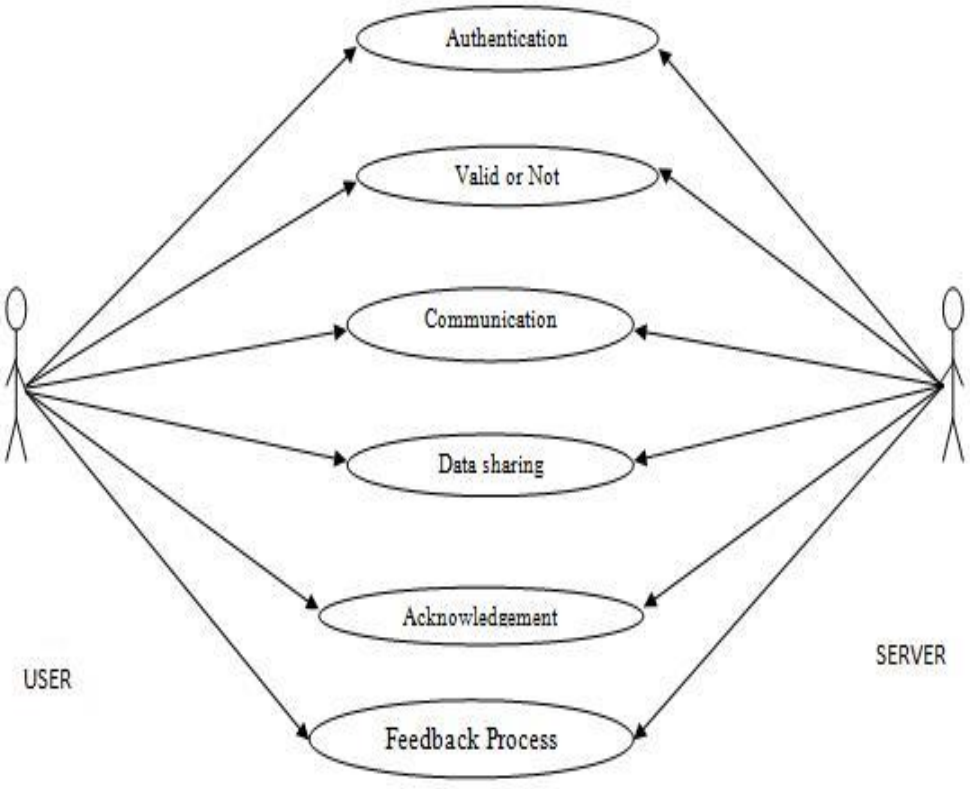

Fig 3.1 Use Case View of the Proposed System

3.3 PROPOSED METHOD

With the development of ontology and semantic web, a new access control, context-based access control has been designed. Different from the traditional access control, context-based access control looks context as the key of access control. It uses the context of requestor to decide whether to give the requestor the warranty or not. Change of its trust value. When there is deception, the owner of the resource can modify mapping relationship between the access permission set and the trust intervals.

Multi-factors Trust based Access Control Model:

The mapping method mentioned above is used for access control and an access control model based on multi-factors trust is thus proposed. The model includes three layers: request management, access control management and access feedback management. The model also includes four modules: subject request, multi-factors trust computation, access permission mapping and access feedback.

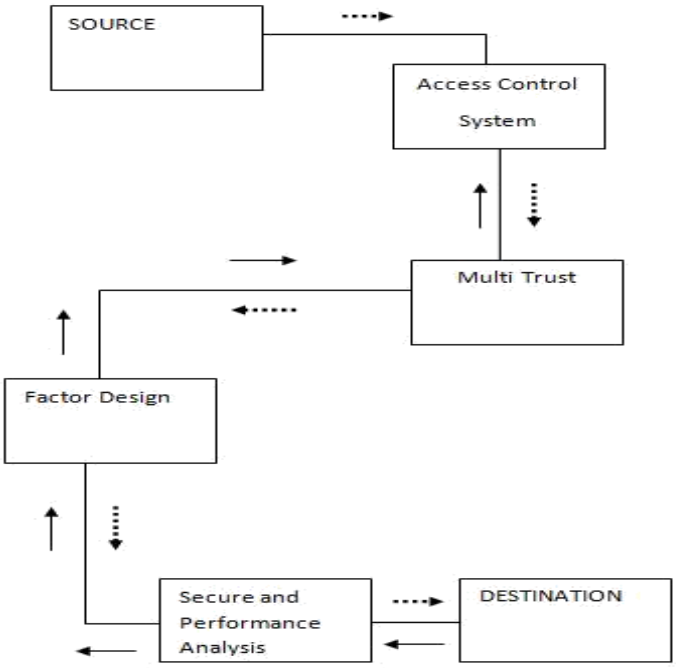

Fig 3.2 Collaboration of Source Accessing over the Multi Trust party to the Destination

3.4 ADVANTAGES

The main merits in the proposed syst4em are the components reduce the complexity of making access decisions, which can be accomplished by using trust to provide security and it access control model based on multi-factors is feasible.

IV. MULTI TRUST VIRTUAL DISSEMINATION SYSTEMS

List of Modules

1. **Module Description**
2. **Mapping between Trust and Permission**
3. **Multi-factors Trust based Access Control Model**

Mapping between Trust and Permission:

A trust value is mapped to access permissions for providing fine-grained access control over sensitive resources. Meanwhile, access permissions can be dynamically adjusted based on the change of the trust values.

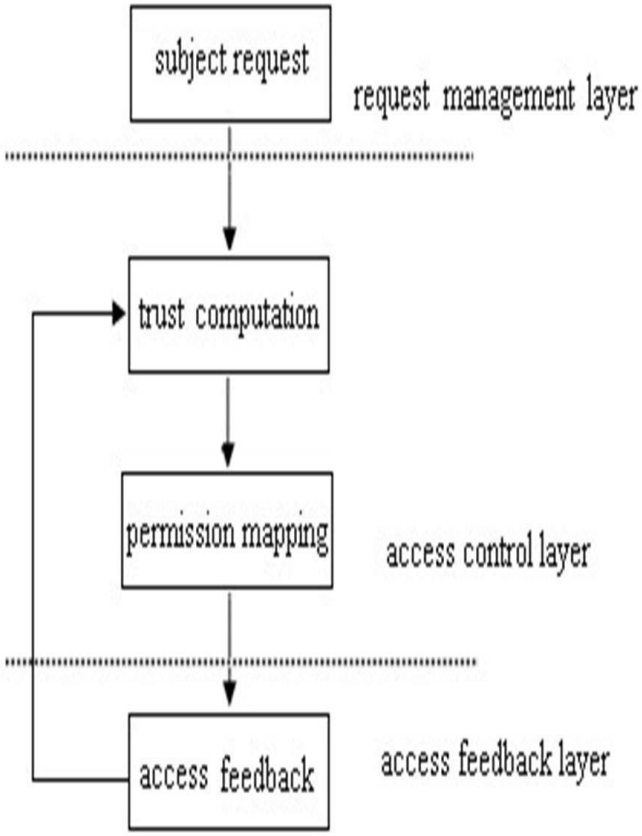

Fig 4.1 Architecture View of the Proposed System

Multi-factors Trust Computation:

Given IP attribute affects trust computation, we suppose that IP attribute has four possible cases. Trust interval is then divided into four disjoint subintervals in which every case of the IP attribute corresponds to a subinterval. According to interaction results between entities, the history behavior can be divided into four possible cases, such as trusted behavior, hostile behavior, attempted hostile behavior and hostile behavior. Every case corresponds to a subinterval.

V. EXPERIMENT RESULT

The code that targets .NET, and which contains certain extra Information - "metadata" - to describe itself. Whilst both managed and unmanaged code can run in the runtime, only managed code contains the information that allows the CLR to guarantee, for instance, safe execution and interoperability. The multi-language capability of the .NET Framework and Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft's old favorites Visual

Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family. Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, custom attributes and also supports multi-threading.. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. Subject A and subject B are both honest nodes. Subject A and objects are in very safe network segment. Subject B and objects are in safe network segment. Two honest subjects randomly access objects 10 times respectively. The experiment executes 50 times and we randomly extract one of them.

SCREENSHOTS

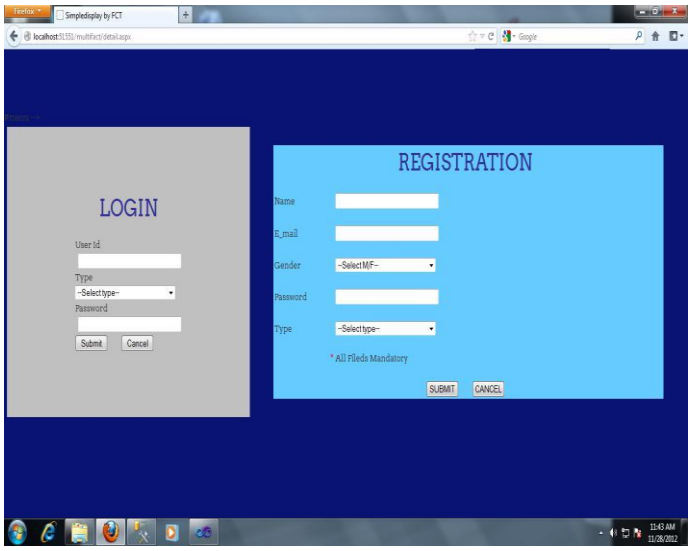

Fig 5.1 Access Control Based Multi Factors Trust Login Details

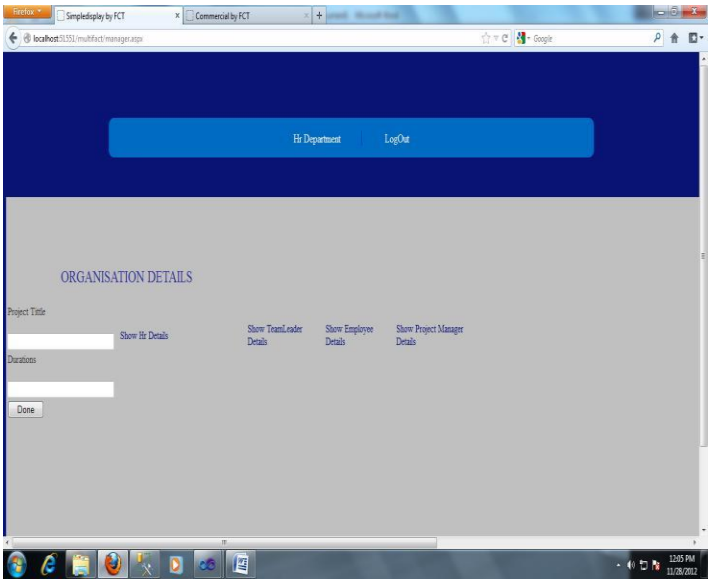

Fig 5.2 Organisation Details are Verified on Multi Factors Trust

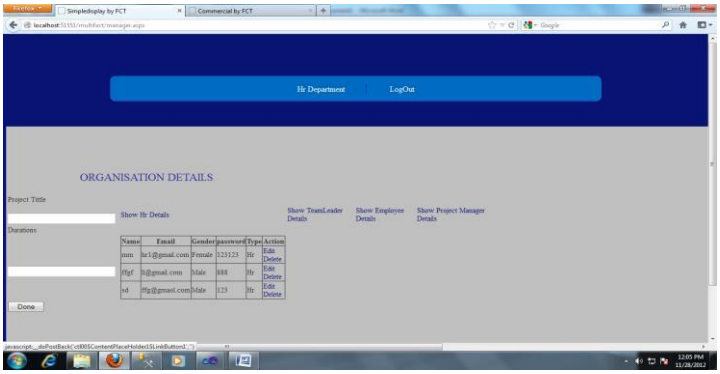

Fig 5.3 Displaying the Organisation Employee Details

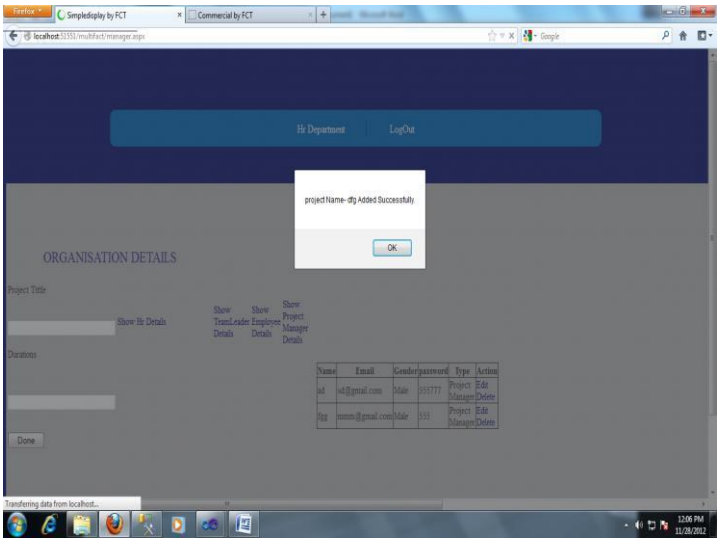

Fig 5.4 Adding New Project Name over the Multi Trust Network

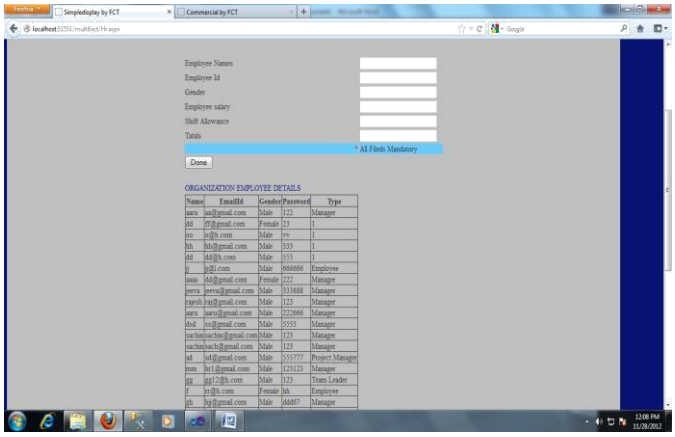

Fig 5.5 Organization Employee Details Monitoring & Sharing

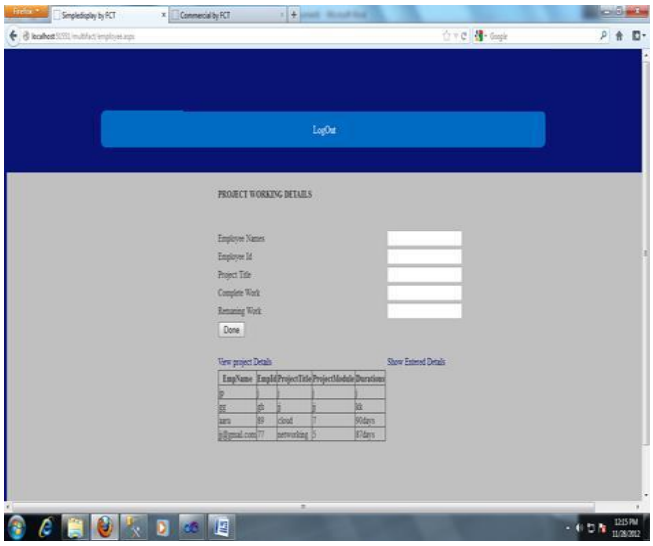

Fig 5.6 Project Working Details Sharing Over Multi Trust Network

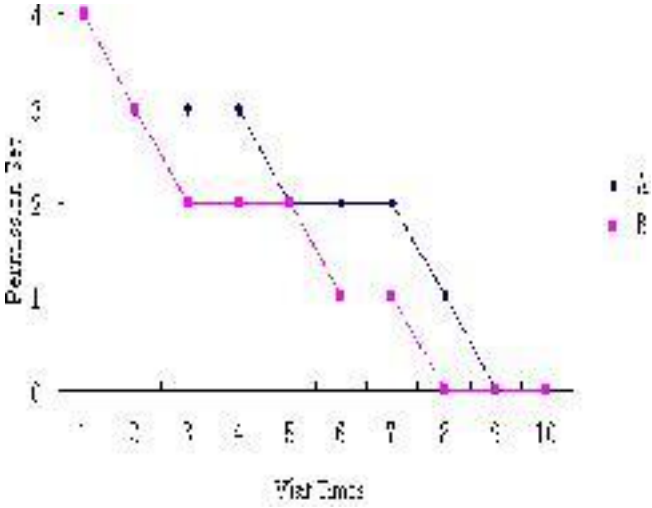

Fig 5.7 Subject A and objects are in very safe network segment. Subject B and objects are in safe network segment

VI. CONCLUSION

6.1 CONCLUSION

In this paper, In open and dynamic network applications, not every resource requestor can be known beforehand by the resource owners because of the open property. Trust can be used as a tool to reduce the complexity of making access decisions, which can be accomplished by using trust to provide security. By considering several factors which affect trust, we computed trust using several factors, and we proposed an access control model based on multi-factors trust.

6.2 FUTURE WORK

In the model, we described how trust values can be mapped to access permissions. In the future, we will design the mapping algorithm in the model to make it more suitable for fine-grained access control.

REFERENCES

[1] X. Ni and J. Luo, "A Trust Aware Access Control in Service Oriented Grid Environment". Proc. 6th International Conference on Grid and Cooperative Computing, 2007.

[2] A. Alfarez and H. Stephen, "Supporting Trust in Virtual Communities". Proc. 33rd Annual International Conference on System Sciences, Vol. 6, Maui, Hawaii, 2000.

[3] P. Samarati etal, "Access control: Policies, models, and mechanisms". In Foundations of Security Analysis and Design, LNCS, Vol. 2171, Springer-Verlag, pp.137–196, 2001.

[4] L. Snyder, "Formal models of capability-based protection systems". IEEE Trans. Computers, Vol. 30, pp. 172-181,1981.

[5] X. Qian, L. T. F, "A MAC policy framework for multilevel relational database". IEEE Transactions on Knowledge and Data Engineering, 8(1), pp. 1-14, 1996.

[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models". IEEE Trans.Computers, Vol. 29, pp.38- 47, 1996.

[7] G. Ahn and R. Sandhu, "Role-based authorization constraints specification". ACM Trans on Information and System Security, pp. 21-30, 2000.

[8] K. Taylor and J. Murty, "Implementing role based access control for federated information systems on the web". Pro. Australasian Information Security Workshop, Adelaide, Australia, 2003.

[9] X. Wang, J. Luo, A. Song and T. Ma, "Semantic Access Control in Grid Computing". Proc. 11th International Conference on Parallel and Distributed Systems, 2005.

[10] D. Chadwick, A. Otenko, and E. Ball, "Role-Based Access Control with X.509 Attribute Certificates". IEEE Internet Computing, 7(2), pp. 62–69, 2003.

[11] T. Alessandra et al, "A semantic context-aware access control framework for secure collaborations in pervasive computing environments". Proc. ISWC2006, Athens, GA, USA, pp. 473-486, 2006.

[12] Y. Guo, H. Fan, Q. Zhang and R. Li, "An Access Control Model for Ubiquitous Computing Application". Proc. 2nd International Conference on Mobile Technology,Applications and Systems, Guangzhou, China, 2005.

[13] S. Chakraborty and L. Ray, "TrustBAC: integrating trust relationships into the RBAC model for access control in open systems". Proc. 11th ACM symposium on Access control models and technologies, pp. 49–58, 2006.

[14] F. Feng, C. Lin, D. Peng and J. Li, "A Trust and Context Based Access Control Model for

Distributed Systems". Proc. 10th IEEE International Conference on High Performance Computing and Communications, pp. 629-634, Washington, 2008.

[15] A. Z. Lin, E. Vullings, and J. Dalziel, "A Trust-based Access Control Model for Virtual Organizations". Proc. 5th International Conference on Grid and operative Computing Workshops, 2006.

[16] R. Bhatti, E. Bertino and A. Ghafoor, "A Trust-based Context-Aware Access Control Model for Web-Services".Proc. IEEE International Conference on Web Services,2004.

[17] J. Jiang, H. Bai and W. Wang, "Trust and cooperation in peer-to-peer systems". Springer-Verlag, pp. 371-378,2004.

[18] D. Huang. Means of Weights Allocation with Multi-Factors Based on Impersonal Message Entropy [J]. Systems Engineering-Theory Methodology Applications, 12(4), pp. 321-324, 2003.

