Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 5 (2013) 183 – 188

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Parallel and Distributed Computing and Systems

A New Proposal for Distributed System Security Framework

Vijay Prakash[a], Manuj Darbari[b]

[a]Department of Computer Science & Engineering, BBD University, Lucknow, India, E-mail: vijaylko@gmail.com
[b]Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, India, E-mail: manujuma@gmail.com

Abstract

Trust among entities of a distributed system supports secure environment. In this paper, the authors propose an approach to compute trust values using fuzzy based approach. The main focus of the approach is on the dynamic behaviour of trust values. Mutual authentication is ensured among the communicating entities using trust values. These trust values are transmitted securely using cryptography. The trust values have also been used to generate access control policies.

Keywords: Distributed environment, Grid, Fuzzy Logic, Trust.

1. Introduction

Security methodologies in grid systems [1, 2, 3] is an important aspect. Security features required in distributed system are identified as: trust, authentication, encryption and access control. 'Trust' is used to ensure secure communication. It can be used for implementing security methods in grid environment. A distributed trust model has been developed for ad hoc mobile networks in [4]. A trust and access control based model for distributed system has been developed in [5]. Trust and reputation based access control mechanism have been discussed in [6]. For wireless communications, a rendezvous node based trust based security is proposed in [7]. A behavioural pattern based security system is proposed in [8, 9]. A new access control model is proposed in [10] that ensures data security in distributed system. TrustWebRank based security approach is proposed in [11]. Fuzzy logic can be used for calculating trust. Many models have been proposed to compute trust using fuzzy. Alfarez Abdul-Rehman and Stephen Hailers have proposed a trust model [12] where trust is defined in terms of direct trust and recommended trust. In our framework we have direct trust

doi:10.1016/j.aasri.2013.10.076

values based on direct communication and updated trust value based on direct and feedback trust values. Fixed weighted [13] and variable weighted [14] fuzzy based models have been proposed for evaluation of trust. As evaluation parameters have dynamic significance, hence variable weighted method is used here.

This paper is divided into 5 sections; section 2 defines the terminology we have used for defining our grid system also with the data structures used for maintaining the trust values. Section 3defines the fuzzy approach used to calculate the trust value. Then section 4 defines the various security measures used in this framework. Section 5 is conclusion and future scope.

2. Proposed Framework

Grid is composed of a number of independent domains. Here, we refer to these domains as Organizations. Each organization is an autonomous domain with its own administrative and security policies. These are denoted as vector O={O_1, O_2, O_3..... O_n}, where, O_i is the i^{th} organization of the grid environment. These organizations comprises of entities. An entity is represented as e_{ij}^{x}if where i represents the organization to which entity e belongs, j represents the grade of an entity within the organization x is used as a name for entity to differentiate from different entities. Grade of an entity refers to the level of trust that an organization has over its own entity. Two entities of the same organization can have the same grade.

Each organization has a manager. M_i denotes the manager of organization O_i. Grades are allotted by the organization manager, which is responsible for maintaining the trust values of an organization and its entities. Initially M_i assigns same grades to all the entities e ϵ O_i. Gradually, with feedbacks from communicating entities, grade is updated.

For any entity e, we have following types of trust values:

a) Initial Trust Value: The Trust value assigned for it by any entity with which no communication has occurred in the past. They are based on authentication queries. And its value can be either 0 or t_0. The scope of these values is before completion of any transaction. (b) Direct Trust Value: The Trust generated after an entity has carried out a job. It is based on, initial trust, job success rate, error rate, turnaround time. Its value ranges from [t_0, 1] and the scope of these values is before completion of job. (c) Reputation: It depends on trust values by other entities. Its value depends on feedbacks after job completion, trust on an organization and grade within organization.

For any organization, we have various trust values,

(a)Initial trust value: It is based on the authentication queries from the highest grade entity. In case, all entities are of the same grade, randomly any entity can be selected. (b) Direct Trust Value: With the competition of job, direct trust values of entities of organization are updated.

Direct Trust for O_i = Aggregate function (direct trust values of all communicating entities of O_i).

The description of the data structures are as follows:

Direct Trust Matrix: An entity e_{ij}^{x} has a trust matrix

	e_{kl}^{y}	e_{mn}^{z}	e_{op}^{Q}
C_1	.5	.7	.3
C_2	.2	.9	.6
C_3	.1	.1	0

where columns represents the communicating entities and rows represents the contexts of communications. Above matrix represents that e_{ij}^{x}has .5 trust over $e_{kl}^{y}$for context C_1 and .2 for context C_2. So, we can say that

entity e_{kl}^{y} is better for context C_1 in view point of e_{ij}^{x}.

Feedback matrix: this matrix is sent to the manager of the entity's organization. For example, lets assume that e_{jk}^{y} ε O_j communicates with ∃e ε O_i then, based on its communications its will generate feedbacks and send it to M_j. M_j will aggregate all the received feedback matrices and send to M_i.

	e_{lh}^{y}	e_{in}^{z}	e_{ip}^{Q}
C_1	.5	.7	.3
C_2	.2	.9	.6
C_3	.1	.1	NA

So in the above matrix we can see, that column represents all the entities of organization O_i. With respect to different contexts, trust values are assigned to the entities with which communication took place. Since there was no communication of e_{jk}^{y} with e_{ip}^{a} in terms of C_3 hence it takes value as NA.

Update Trust Matrix: This matrix is generating by updating the trust matrix with the feedbacks received from different entities. So a join operator is used here to get a combined result from both the matrices.

Updated Trust Matrix = Trust Matrix (+) feedback matrix, here (+) represents join operator.

3. Applying Fuzzy Inference Engine in Trust Computation

It is a variable weight based fuzzy evaluation.

3.1 Computation of direct trust matrix: Direct Trust depends on following parameters, initial trust, job success rate, Error rate, turnaround time.

Now we need to assign weights to these parameters. Importance of a parameter depends on the instant of time, the trust value is computed. For example, if two entities are going to compute for the first time, then whole weightage will be given to initial trust value. Whereas, after few successful job completions, initial trust will have least weightage. Therefore, these weights will be variable. W_i is weight for Evaluation parameter E_i, where $E = (E_1\ E_2\ E_3\ E_4)$ is the evaluation parameter vector. Value of evaluation is denoted as u_1, u_2, …. u_n where u_i ε {0, μ_m} so, when E_i is best $u_i = \mu_m$

When E_i is worst $\mu_i = 0$

M_i will be a non increasing differential function in $(0,\mu_m)$

$$\lambda i\,(u) \leq 0 \quad \text{Where } u \in (0,\mu_m)$$

so, $W_i = (u_1, u_2 \ldots\ldots u_n) = \dfrac{\lambda i(\mu i)}{\sum_{j=1}^{n} \lambda j(\mu j)}$

3.2 Computation of Feedback matrix

Say few entities of O_j communicate with entities of O_i. After completion of job, O_j entities will give feedback of O_i entities to M_j. On the basis of which feedback matrix will be generated.

Depending upon the grades of e_j entities (which would be variable); then feedback values will be computed.

$E = \{f_1, f_2, f_3 \ldots\ldots..\}$ f_i – feedback from the entity.

$\mu = \{\mu_1, \mu_2, \mu_3 \ldots\ldots\}$ μ_i – grade value of i^{th} entity

So, here weight values α grade values

So $W_i = (u_1, u_2 \ldots\ldots u_n) = \frac{\lambda i(\mu i)}{\sum_{j=1}^{n} \lambda j(\mu j)}$ condition, entities provide feedback for same context. So, for different contest, different matrices can be developed.

3.3 Computation of update matrix

Here joint operation will be used as:

As, feedback will be received from different managers

So $E = [Mf_1, Mf_2, \ldots\ldots\ldots Mf_{12}]$ where Mf_i is feedback from M_i

$\mu = (\mu_1, \mu_2 \ldots\ldots\ldots \mu_n)$

μ = trust value of any organization.

So, here weights α Organization trust value.

So, $W_i = (u_1, u_2 \ldots\ldots u_n) = \frac{\lambda i(\mu i)}{\sum_{j=1}^{n} \lambda j(\mu j)}$

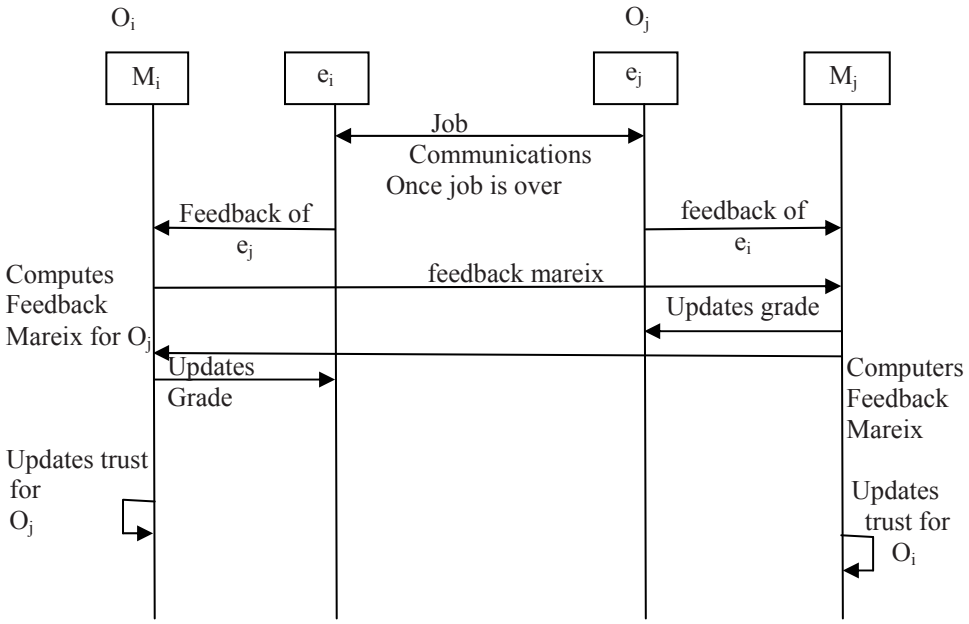

Fig. 1 Space Time Diagram Values for Trust and Grade Values

4. Defence in depth security

Whenever a new entity/organization wishes to be the part of grid, authentication is required. Security threat could be both ways, it may be possible that a hacker is trying to be a part of grid or, it may be possible that a legitimate user is getting connected to a spoofed grid component.

So Mutual Authentication is required. In our framework authentication takes place at two levels. Time line diagram below shows how authentication is carried out.

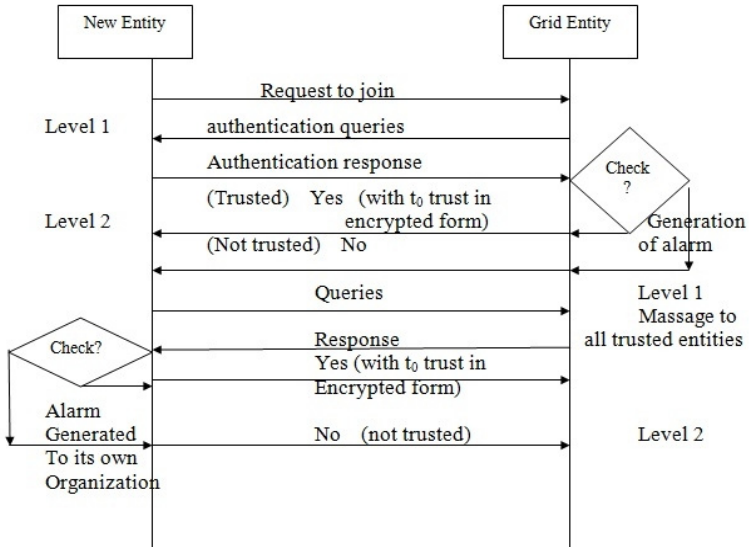

Fig. 2 Time Line Diagram for Mutual Authentication

Level 1, whenever a new entity wishes to join a grid, it will send request to particular grid entity to which it wants to communicate. This grid entity will check for authentication, by generating certain queries. Only legitimate user will have the correct answers to those queries. In case correct responses are received, grid entity will sent initial trust value (t_0).Else if wrong response will be there then grid entity will assign trust = 0, and an alarm will be generated for all grid entities informing about this unidentified entity.

Level 2:- When grid entity sends the initial trust, the trust value is sent using public key cryptography. Therefore, an entity can have access to the trust value, only if it has the key to it. Suppose a hacker in any way gets the responses of initial queries, he will be able to cross the first level authentication, but cannot cross level 2 unless presence of key.

Keys should be changed periodically because in grid computing, entities may join and leave the grid dynamically, even during the execution. So, Stateless Key Management can be used to securely maintain the keys.

The new entity joining the grid must also be sure of the authentication of grid. Therefore, mutual authentication is necessary. New entity will also generate queries to which grid responses are checked and accordingly trust is established. Here also two levels of security are maintained.

4.1 Access Control

Initially, a new entity will have limited access to resources corresponding to the initial trust t_0. As the trust values of a new member increases, he is allowed to get more access to resources.

Thus, access control policies vary according to the trust values. The manager's of each entity are responsible for maintaining the access control. Managers maintain the trust value of each entity of other organizations, on the basis of feedback from its own entities.

Say, e_{ij}^{x} want to communicate to e_{kl}^{y}then M_k is responsible for access control. M_k checks the trust value from feedback matrices and accordingly allows e_{ij}^{x}

5. Conclusion and Future Scope

In this paper, trust values have been used to carry out authentication and access control, ensuring a secure grid environment. Fuzzy logic concept is utilized for evaluating the trust. In future, authors would be working for decreasing the computations required for generating and updating trust values. Also reputation parameter can be added to ensure secure communication.

References

[1] Shehab M, Ghafoor A, Bertino E., Secure collaboration in a mediator free distributed environment", IEEE Transactions on Parallel and Distributed Systems, 2010:19(10), pp.1338-1351.
[2] Pallickara S., Ekanayake J., Fox G, A scalable approach for the secure and authorized tracking of the availability of entities in distributed systems, IEEE International Parallel and Distributed Processing Symposium, pp. 1-10, 2007.
[3] Anderson R., Security engineering: a guide to building dependable distributed systems, Wiley, 2010.
[4] Omar M, Challal Y, Bouabdallah A, Reliable and fully distribted trust model for mobile ad hoc networks", Computers and Security, 2009: 28(3-4), pp. 199-214.
[5] Feng F, Chuang L, Peng D, Li J, A trust and context based access control model for distributed system, 10th IEEE International Conference on High Performance Computing and Communications, pp 629-634, 2008.
[6] Marmol FG, Derez GM, Security threats Scenarios in trust and reputation models for distributed systems, Computers and Security, 2009: 28, pp 545-556.
[7] Cheng N, Govindan K. and Mahopatra P., Rendezvous based trust propagation to enhance distributed network security, International Journal of Security and Networks, 2011: 6(2-3), pp 112-122.
[8] Ukil, Arijit, Secure Trust Management in Distributed Computing Systems, Sixth IEEE International Symposium on Electronic Design, Test and Application(DELTA), pp. 116-121, 2011.
[9] Uzunov AV, Fernandez EB and Falkner K, Securing distributed systems using patterns: a survey, Computers and Security, 2012: 31(5), pp. 681-703.
[10] Aneta PM, Implementation of Access Control Model for Distributed Information Systems Using Usage Control, Security and Intelligent Information System, vol. 7053, 2012, pp. 54-67.
[11] Carchiolo V, Longheu A, Malgeri M and Mangioni G, Trust assessment: a personalized, distributed, and secure approach, Concurrency and Computation: Practice and Experience, 2012: 24(6), pp. 605-617.
[12] Abdul-Rahman A, Hailes S, Supporting Trust in Virtual Communities, 33rd Hawaii International Conference on System Sciences, vol. 6, Dec. 2007, pp. 6007.
[13] Tang W, Chen Z, Research of subjective trust management model based on the fuzzy set theory, Journal of Software, 2003:14(8), pp. 1401-1408.
[14] Liao H, Wang Q and Li G, A Fuzzy Logic Based Trust Model in Grid, International Conference on Networks Security, Wireless Communications and Trusted Computing NSWCTC, pp. 608-614, 2009.