Research on Access Control Model Based on User Trust Degree and Resource Life Cycle under Mobile Environment

Xiaoyan Zhang* and Kai Kang
Xi'an University of Science and Technology, China
*Corresponding author

***Abstract*—Traditional role-based access control models cannot meet the changing requirements of the roles and users under the mobile Internet environment due to their static attributes. To address such issue, this paper proposes an access control model, which is based on the user trust degree and the resource life cycle. From the perspective of subject, the proposed model takes the trust degree's impact factor and the trust degree's fading factor into consideration. From the perspective of object, it takes life cycle of resources into consideration. By using factors given above together, the model accomplishes the function of switching constraints dynamically in the mobile environment. At last, this paper analyzes the main characteristics of the proposed model and other traditional models, the results of analysis show that the proposed access control model has more advantages than other models in the mobile environment.**

Keywords—access control model; mobile environment; user trust degree; resource life cycle

I. INTRODUCTION

With the development of mobile networks, mobile applications have become one of the indispensable parts in modern life, which contribute conveniences as well as unsafe elements towards networks. On the one hand, more and more private information is exposed to the mobile networks. On the other hand, the resources available to the mobile networks may be attacked by unauthorized users. Under such circumstances, it is worthy to research the access control model, especially the model working under mobile environment. Traditional RBAC models have acted as a bridge between the subject and the object, which realized mapping users into the fixed roles. In other words, the constraints between subject and object are unchanged. Obviously, it is difficult for the traditional RBAC models to meet the needs of unremitting changes of users and roles under mobile environment.

To solve the above problem, this paper presents an access control model, which is appropriate for mobile Internet environment. The model meets the requirements of mapping users into different roles automatically by adjusting the synthesized users' trust degree and the life cycle of resources under mobile environment.

II. RELATED WORKS

In 1994, the SANDHU's group came up with the principles of access control [1]. In 1996, they proposed the concept called RBAC96 [2]. This model was based on the previous RBAC model and could be spitted into four nested models with the change of environments. After that, formal definition of access control models was put forward by SANDHU [3]. In 2008, Kulkarni e with other researchers came up with the context-aware role-based access control (CA-RBAC) model [4] basing on the SANDHU' works. CA-RBAC model could activate corresponding sessions and roles if contexts match the constraints.

In recent years, TOAHCHOODEE M [5] proposed the Spatial-temporal Role-based Access Control (STRBAC) model to deal with the access constraints of specific scenarios. In these usage scenarios, roles, space-time positions and access time are all restricted by constraints. The reference [6] devised a workflow-based access control model worked in a specific mobile scenario, and completing the mechanism of access control through a workflow manager. The reference [7] introduced Ebbinghaus's forgetting curve, and further proposed a trust-based access control model working under mobile environment. However, the final conclusion of the reference [7] does not consider the impacts of users' location in time and space as well as their behaviors. The reference [8] put forward another type of access control model, which was based on the evaluation of trust degree. Unlike reference [7], this model calculated the synthesized trust degree by adopting the combination of ANP theory and the super decision-making software. However, the model does not take resources into account. Therefore, the paper overlooked the dynamic change of resources in real mobile networks.

In summary, the existing access control models cannot meet the requirements between the diversified access control conditions under the mobile environment and the resource access control strategies needs to be dynamically and adaptively adjusted. Thus, the study of putting forward a feasible model which is suitable for the mobile environment is urgent.

III. MODEL DESCRIPTION

A. Mechanisms of Altering User Trust Degree

1) Impact factors

Impact factors in access control models refer to the factors that affect the change of user's trust degree under the mobile environment. As shown in Figure I, the impact factors include access time, users' location and user's behaviors.

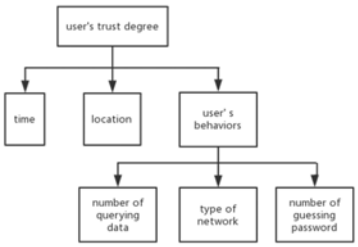

FIGURE I. IMPACT FACTORS OF USER TRUST DEGREE

To handle the time factor, we divided the discrete access time into a set of time periods. The lasting time of period is 2 hours during the daytime, and 4 hours during the nighttime results from the frequency of users' accesses to mobile Internet. In such cases, the time factor can be expressed as T=$\{t_1, t_2, \dots, t_9, t_{10}\}$. What's more, we denoted the user i's trust degree in period j as D($u_{i,j}$), the duration of access time as L($u_{i,j}$), and the duration threshold as S_{t_j}. The calculating formula of D($u_{i,j}$) is as belows if the time factor works alone.

$$\mathrm{D}(u_{i,j}) = \begin{cases} \mathrm{D}(u_{i,j-1}) - 1, & \mathrm{L}(u_{i,j}) = 0 \\ \mathrm{D}(u_{i,j-1}), & 0 < \mathrm{L}(u_{i,j}) \le S_{t_j} \\ \mathrm{D}(u_{i,j-1}) + 1, & \mathrm{L}(u_{i,j}) > S_{t_j} \end{cases} \quad (1)$$

To handle location factor, we adopted two-dimension coordinate. Within the coordinate, we considered the sites where time period is longer than 2 hours as safe point (SP), and the rest locations called relative point (RP) are calculated as the relative distance from SP to their real coordinates. Furthermore, we represented user i's trust degree in location RP_jas D(u_{i,RP_j}), the threshold of RP as S_{RP_j}. It means the D(u_{i,RP_j}) decrease when RP_j is greater than S_{RP_j}, and the D(u_{i,RP_j}) remains unchanged when the RP is within a certain range.

To handle user's behavior factor, we regulated the model from three aspects, including the number of querying data, the types of networks and the number of guessing passwords. The detailed regulations as bellow.

a) When the number of access times within a certain time period less than the threshold, the trust degree presents positive correlation with the number of access times; when the number of access times within a certain time period greater than the threshold, the trust degree presents negative correlation with the number of access times; when the number of the user access times within a certain range in a time period, trust degree remains unchanged.

b) When the network connected to the user is not a frequently used network, the trust degree presents negative correlation with the number of access times with in a certain time period.

c) When the number of guessing password greater than the threshold in a certain time period, the trust degree presents negative with the number of guessing time.

2) Fading factors and synthesized user trust degree

According to the trust theory, the trust degree would gradually reduce as time went on [8]. Let t_i indicates the time interval between the last access and the i-th access. We recalculate the trust degree at the beginning of each time period based on the Table 1., and the calculation formula as in [10] as follow.

TABLE I. COMPARISON OF DIFFERENT ACCESS CONTROL MODELS

Type	Time	Location	User behavior	User Truse degree	Resource Life Cycle	Confidentiality	Integrality	Flexibility
RBAC	×	×	×	×	×	×	√	low
STRBAC	√	√	×	×	×	√	√	medium
CA-RBAC	×	×	√	×	×	√	√	medium
Mobi-CosWAC	√	√	√	×	×	√	√	medium
DTDAC	√	√	√	√	×	√	√	medium
reference[7]	×	×	√	√	×	√	√	medium
Proposed model in this study	√	√	√	√	√	√	√	medium

$$\alpha(t_i) = \begin{cases} 1 & t = 0 \\ \frac{1}{e^{t_i}} & t \neq 0 \end{cases} \quad (2)$$

The value of $\alpha(t_i)$ keeps reduced with the time increasing, and it will approach zero when t_i increases to a certain value. Therefore, This trend is consisitent with the trust theory mentioned previously.

With regard to the synthesized user's trust degree, which is based on the impact factors of user's trust degree and further takes fading factor into account. That is, we calculate the sum of user's trust degree, after that, multiplying the sum by the fading factor $\alpha(t_i)$. The calculation fumula of the synthesized user's trust degree (D_{Syn}) is

$$D_{Syn} = \sum_{i=0}^{n} \alpha(t_i) = \sum_{i=0}^{n} \frac{1}{e^{t_i}} \quad (3)$$

B. Mechanisms of Altering Resource Life Cycle

Users can join and leave at any time under the mobile Internet environment, so the network nodes are generally uncertain, the state of the resources are also uncertain in the same way. As shown in Figure II, taking the activity diagram of publishing documents in a certain company as an example. The states of resources at different stages are distinctive. Therefore, the access control model requires to dynamically update the access control strategies for different stages according to the environment in which the object is located.

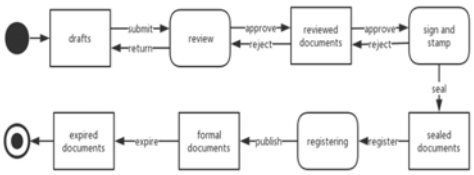

FIGURE II. ACTIVITY DIAGRAM OF PUBLISHING DOCUMENTS IN A COMPANY

C. Description of the Access Control Model

Based on the part C and part D discussed above, this paper proposes an access control model for mobile environment as shown in Figure III. This model is different from the traditional RBAC model due to the model has two modules – user's synthesized trust degree manager and the resource's life cycle manager.

The two modules are not independent of each other, the synthesized user trust degree is the basis of the model, and the life cycle manager work on it. The two together make mobile access control policies more flexible and secure.

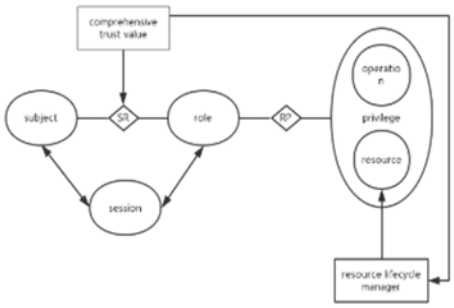

FIGURE III. THE DESCRIPTION OF ACCESS CONTROL MODEL UNDER MOBILE ENVIRONMENT

Specifically, the model uses the following strategy to alter the policies of access control model.

Step1: reading the user set $\{u_1, u_2, \ldots, u_n\}$;

Step2: judging the value of $D(u_i)$, if $D(u_i) \geq D$, turn to step3; otherwise, stopping the accessing;

Step3: initializing the policies of access control;

Step4: reading the stage of resource's life cycle;

Step5: judging whether stepping into another stage, if the answer is yes, turn to step6; otherwise, stopping the accessing;

Step6: updating the policies of access control.

The following figure shows the process of updating access control policies.

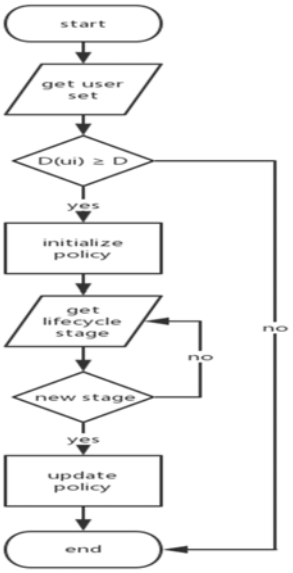

FIGURE IV. FLOWCHART OF DYNAMICALLY UPDATING ACCESS CONTROL POLICIES

IV. MODEL ANALYSIS

In this study, we refined the attributes of the subject and object by considering the synthesized user trust degree and resource life cycle respectively. The RBAC models can control the security of assigning rights, and the proposed model can satisfy the further requirements of the flexibility of the mobile environments.

In the subject aspect, the factors that could in-fluence user trust degree are obtained by combining the user's temporal state, position state and concrete behaviors. Based on this, the trust degree's fading factor is introduced, and a relatively objective synthesized trust degree could be obtained. In the object aspect, the correlation and dynamic of resource's life cycle stage and access control strategy are considered, so that the access control strategy can change with the resource's life cycle, and the access control flexibility and adaptability in a mobile network environment is improved. Table I shows the main characteristics of traditional models and the proposed model.

V. CONCLUSION

In this work, we have proposed an access control model suitable for mobile environment. This model was based on the traditional RBAC model, and further explored the concept of resource life cycle and the synthesized user trust degree. It included the structure of the model, the process of access control and the mechanism of updating policy. Finally, we have compared it with other access control models. The results showed that the proposed model is more suitable for the mobile

network environment. The next work plan is to consider putting forward a more accurate formula for calculating the fading factor as well as the classification of the trust level, so as to further improve the reliability of the model.

VI. ACKNOWLEDGMENT

This research was supported by Industrial Project of Science and Technology Department of Shaanxi Province, the project number is 2014K05-37. Besides it, the research was also supported by Serving Local Project of Education Department of Shaanxi Province, the project number is 14JF016.

REFERENCES

[1] SANDHU R S, SAMARATI P. Access Control: Principle and Practice[J]. IEEE Communications Magazine, 1994, 32(9): 40-48.

[2] SANDHU R. Rationale for the RBAC96 Family of Access Control Models[C]. ACM. The First ACM Workshop on Role-based Access Control, November 30-December 1, 1995, Gaithersburg, MD, USA. New York: ACM, 1996: 9.

[3] R. Sandhu. Role-based access control models. IEEE Computer, February1996.

[4] Devdatta Kulkarni, Anand Tripathi. Context-aware role-based access control in pervasive computing systems. In SACMAT'08 Proceedings of the 13th ACM symposium on Access control models and technologies, pp. 113-122, 2008.

[5] TOAHCHOODEE M, RAY I. On the formalization and analysis of a spatio-temporal role-based access control model[C]. IFIP Wg 11.3 Working Conference on Data and Applications Security. Springer-Verlag, 2008:399-452.

[6] Shaocan Chen. Research and application of access control of scientific workflow in mobile environment [D].Fudan University, 2014.

[7] Jianyu Shao, Fuzhen Chen, Pengyu Qin, Jiujun Cheng. Research on access control method based on dynamic trust degree in mobile Internet environment. [J]. Netinfo Security, 2016(08):46-53.

[8] Yundong Fan, Xiaoping Wu, Xiong Shi. Research on cloud computing access control model based on trust degree evaluation. [J]. Netinfo Security, 2016(07):71-77.

[9] Yuyu Bie. Research on trust - based access control technology in cloud computing environment. [D]. China University of Mining and Technology, 2014

[10] Saizhe Zuo. Trust value Update Model Based on the Memory Theory [J]. The Journey of Southeast University (Natural Science Edition), Nov.2016