A Cooperative RBAC-Based IoTs Server with Trust Evaluation Mechanism

Hsing-Chung Chen[1,2](✉)

[1] Department of Computer Science and Information Engineering,
Asia University, Taichung City, Taiwan
shin8409@ms6.hinet.net

[2] Department of Medical Research, China Medical University Hospital,
China Medical University, Taichung City, Taiwan

Abstract. With the recent advances in ubiquitous communications and the growing demand for low-power wireless technology, smart mobile device (SMD) access various Internet of Things (IoTs) resources through heterogeneous wireless networks (HWNs) at any time and place alternately. There are some new requirements for integrating IoTs servers in which each one is individually gathering its local resources in HWNs, which cooperatively supports SMD to get some flexibility or temporary contract(s) and privileges in order to access their corresponding desired service(s) in a group of collaboration IoTs servers. However, traditional access control schemes designed for a single server are not sufficient to handle such applications across multiple cooperative IoTs servers to get rich services in IoTs environments. It does not take into account both security and efficiency of IoTs servers, which securely share their resources. Therefore, the cooperative IoTs-based RBAC (Role-based Access Control) model with trust evaluation function for reducing internal security threat in the RBAC servers is proposed in this paper, where RBAC is an access control mechanism via managing the users' roles and giving their corresponding access rights. Finally, a cooperative RBAC model with both trust evaluation function and cooperation trust evaluation function is designed and presented for reducing internal security threats in collaborative IoTs servers.

Keywords: Role-based Access Control (RBAC) · Cooperative RBAC Internet of Things · Trust evaluation

1 Introduction

Due to the development of communication technology among Internet of Things (IoTs) [1, 2] and heterogeneous wireless networks (HWNs), many emerging application services have been developed. These application services include the following features or disadvantages. First, these application services often use Location Based Services (LBS) to provide information to the smart mobile device (SMD). Although LBS services bring huge incomes for the SMD manufacturers, APP (application) software development companies and telecommunication operators, these new application services have suffered a lot of new challenges in access control. Second, some services are accessed by SMD from a remote server in HWNs. It cannot provide handover function

Y.-B. Lin et al. (Eds.): IoTaaS 2017, LNICST 246, pp. 36–42, 2018.
https://doi.org/10.1007/978-3-030-00410-1_5

in order to get the access rights for continuous access to server. Therefore, leaving the wireless coverage area of the Base Station or AP (Access Point), the SMD which is accessing some services will be interrupted. Furthermore, the SMD logs in to the server with the privileges provided by the original registration server. It can get the privileges to similar servers through the cooperation negotiation mechanism among these servers. Thus, new access control (AC) techniques are required to meet this situations.

At present, AC has been researched for various applications, and there are different AC approaches for different environments. The general RBAC model is one of the AC technologies formally was first proposed by Ferraiolo et al. [3] in 1992. Their model defined that there is a user's assigned a role to access the resources managed by a remote server. The user's access rights should be determined by his assigned role. Each role has its associated set of some individual member(s). The role is the basis component of the RBAC model that categorizes users based on their various properties. The basic model [4–10] of the RBAC as shown in Fig. 1 [10] includes the sets of five basic data elements such as *Users* (U), *Roles* (R), *Objects* (OBJ), *Operations* (OPT) and *Permissions* (P). *Users* are considered to be human beings, machines, networks, smart devices or intelligent agents that could perform some activities. *Roles* are defined as a set of permissions to access the specific resources. *Permissions* are approvals to execute operations on one or more objects. *Operations* are the executions of a specific function that is invocated by a user. *Objects* are entities that contain or receive information, or have exhaustible system resources. Moreover, the basic model of the RBAC is introduced its concept of role activation as part of a user's session within a computer system [3–5, 10]. There are three relations in the traditional RBAC model, which are hierarchical roles relations, static separation of duty relations, and dynamic separation of duty relations. It also provides the user-to-role assignment and permission-to-role assignment functions.

The remainder of this paper is organized as follows: in Sect. 2, we first formalize the cooperative IoTs-based RBAC model. In Sect. 3, we present discussions comparisons, and security analyses. Finally, we draw our conclusions and examine future work in Sect. 4.

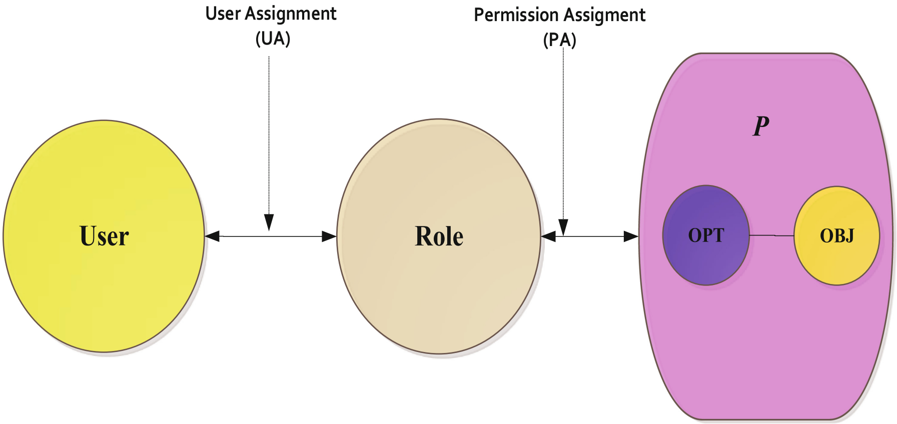

Fig. 1. Basic traditional RBAC model [10].

2 A Cooperative IoTs-Based RBAC Model

In this section, the basic definitions and cooperative IoTs-based RBAC model are formulated in Subsects. 2.1 and 2.2 below.

2.1 Basic Definitions of Cooperative IoTs-Based RBAC Model

The cooperative IoTs-based RBAC model is shown in Fig. 2. The components of the core cooperative IoTs-based RBAC model are illustrated in Fig. 2. They are denoted below. First, the set of SMDs (D, for short), and the results of both trust evaluation as well as cooperation trust evaluation will be recorded for all assignment. Second, the set of trust values T is consisting of local trust evaluation (T_L, for short) and cooperation trust evaluation (T_C, for short). Third, the set of sessions (S, for short). Fourth, the set of roles is denoted as R, where $R = R_L \cup R_V$, R_L is a local role set mapping to a local role hierarchy (LRH) and R_V is a virtual role set mapping to a virtual role hierarchy (LRH). Fifth, the set of permissions is represented as P consisting of a local role set P_L and a virtual role set P_V where and $P = P_L \cup \left(\cup_{x=1,2,\ldots l} P_{V_x} \right) = P_L \cup P_{V_1} \cup P_{V_2} \cup \ldots \cup P_{V_1}$. Sixth, the set of the objects $O = \{O_L \cup O_V\}$ accessed by SMDs is consisting of local IoTs objects (O_L, for short) and virtual IoTs objects (O_V, for short). Moreover, the two major relations of the cooperative IoTs-based RBAC model are also explained in next subsection. First, the smart device assignment (DA) is the smart device-to-role assignment relation consisting of the smart device-to-local role assignment relation (LDA) and the smart device-to-virtual role assignment relation (VDA). Second, the permission assignment (PA) is the role-to-permission assignment consisting of the local role-to-local IoTs objects assignment relation (LPOA) and the virtual role-to-virtual IoTs objects assignment relation (VPOA).

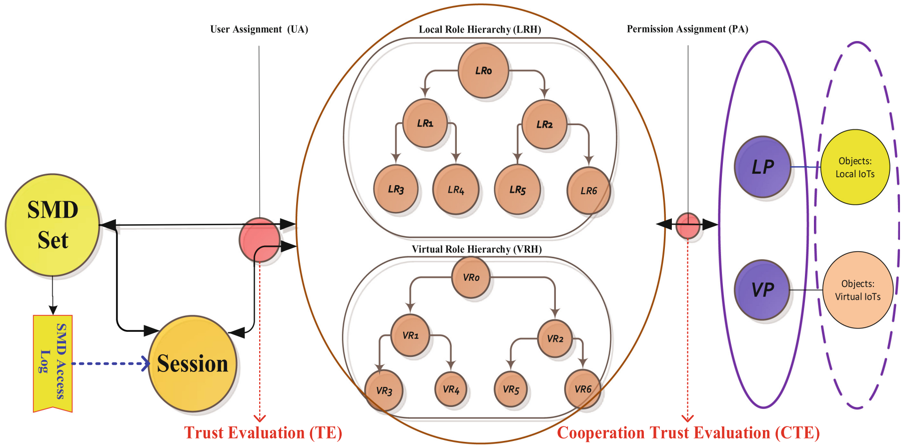

Fig. 2. A cooperative RBAC-based model designed for the architecture of IoTs server.

2.2 Cooperative IoTs-Based RBAC Model

According to the basic explains of the sets: D, O, T, S, R, and P, which are mentioned above, several functions are then given their further definitions in this subsection. The relation function of the smart device assignment DA consisting of the smart device-to-local role assignment relation (LDA) and the smart device-to-virtual role assignment relation (VDA) represents the assignment function based on the success of both SMD trust evaluation function (TE function, for short) and cooperation trust evaluation function (CTE function, for short) from a smart device set D mapping to the roles set $R = R_{\mathrm{L}} \cup R_{\mathrm{V}}$, R_{L} is a local role set and R_{V} is a virtual role set. The both trust evaluation functions TE function and CTE function used to associate SMDs with their corresponding trust values calculated by the cooperative trust evaluation (CTE) algorithm in [10]. The permission assignment (PA) represents the assignment of the role-to-permission assignment consisting of the local role-to-local permission (LPA) and the virtual role-to-virtual permission assignment relation (VPA). The permission-to-object assignment consisting of both the local permission-to-local IoTs object assignment relation (LPOA) and the virtual permission-to-virtual IoTs objects assignment relation (VPOA). In addition, the trusted SMD assigned to a single session s ∈ S, which is evaluated by both trust evaluation functions TE function *γl_trust evaluation*(●) and CTE function *vr_cooperative trust evaluation*(●) representing SMDs associated with this single session *s*. The detail of the generalization definitions of the cooperative IoTs-based RBAC model are defined and shown in *Definition* 1.

Definition 1: The generalized model of the cooperative IoTs-based RBAC;

- *D, O, T, S, R, and P represent the finite sets of SMDs, the set of objects O accessed by SMDs consisting of* O_L *and* O_V, trust values $T = T_L \odot T_C$ where $\odot$ *is the sum operation function inputted by both* T_L and T_{C}, *sessions, roles* $R \subseteq \{R_L \cup R_V\}$ *and permissions P consisting of* P_L *and* P_V *plus* $P = P_L \cup \left(\bigcup_{x=1,2,\ldots,l} P_{V_x} \right) = P_L \cup P_{V_1} \cup P_{V_2} \cup \ldots \cup P_{V_l}$, *which are assigned by the cooperative IoTs-based RBAC model, respectively;*
- $TE \subseteq D \times T \times O_L \times O_V$, *the trust evaluation function that associates SMDs with their corresponding trust values calculated by the CTE algorithm in* [10] *by cooperative evaluating of their access local IoTs objects* O_L *and virtual IoTs objects* O_V *via the co-members in a specific session* $s \in S$ *during the serving time period;*
- $CTE \subseteq D \times T \times O_V$, *the trust evaluation function that associates SMDs with their corresponding trust values calculated by the CTE algorithm in* [10] *by cooperative evaluating of their access virtual IoTs objects VO via the co-members in a specific session s during the serving time period;*
- $DA \subseteq D \times T \times R_L \times R_V$, *the SMD assignment relation function that associates SMDs with roles available upon the successful SMD's trusted evaluation;*
- γ_l*_trust evaluation*$(\gamma_l \in R_{\mathrm{L}}) \rightarrow 2^D$, *the mapping of a local role* γ_l *onto a set of trusted SMDs, where the function* γ_l*_trust evaluation*(●) *is defined as* γ_l*_trust evaluation*$(\gamma_l) = \{d \in D | (u_x, \gamma_l) \in DA\}$;

- *vr_cooperative trust evaluation*$(v\gamma \in R_V) \rightarrow 2^D$, *the mapping of a virtual role* γ_v *onto a set of trusted SMDs, where the function vr_cooperative trust evaluation*$(\bullet)$ *is defined as* $\gamma_v\_trust\ evaluation(\gamma_v) = \{d \in D|(u_x, \gamma_v) \in DA\}$;
- *The permission assignment (RPA) represents the assignment of the role-to-permission assignment consisting of both local role-to-local permission (LRPA) and the virtual role-to-virtual permission assignment relation (VRPA), where* $LRPA{\subseteq}R_L \times P_L$ *represents the local permission assignment relation function that it assigns a local permission* p_l *to a local role* γ_l, *and* $VRPA{\subseteq}R_V \times P_V$ *represents the virtual permission assignment relation function in which it assigns a virtual permission* p_v *to a local virtual* γ_v;
- *The permission-to-object assignment POA consisting of both the local permission-to-local IoTs object assignment relation (LPOA) and the virtual permission-to-virtual IoTs object assignment relation (VPOA), where* $LPOA{\subseteq}P_L \times O_L$ *represents the local IoTs object assignment relation function that it assigns a local IoTs object* O_l *to a local permission* p_l, *and* $VPOA{\subseteq}P_V \times O_V$ *represents the virtual IoTs object assignment relation function in which it assigns a virtual IoTs object* O_v *to a virtual permission* p_v;
- $r\_p\&o(\gamma \in R, (d_x, t_x) \in T) \rightarrow 2^O$, *the mapping of a role* $\gamma = (\gamma_l, \gamma_v) \in R \subseteq \{R_L \cup R_V\}$ *onto a power set of IoTs objects* 2^O *based on the availability of the trust pair* $(d_x, t_x) = TE(d_{x-1}, t_{x-1}) \odot CTE(d_{x-1}, t_{x-1})$, *where* $O \subseteq \{O_L \cup O_V\}$, $t_x \in T$ *and the function* $r\_p\&o(\bullet)$ *is defined as* $r\_p\&o(\gamma \in R, (d_x, t_x)) = \{o \in 2^O| (\gamma(d_x, t_x)), p \in P\} \in RPA \cup POA$;
- $trust\_s(d_x \in D, t_x \in T) \rightarrow 2^S$, *where the function* $trust\_s(\bullet)$ *assigns a trusted SMD onto a set of sessions;*
- $s\_r(\varsigma \in S) \rightarrow 2^R$, *the mapping of each session* ς *to a set of roles;*
- $s\_rpa\&poa\_trusted\ pair(\varsigma \in S, (d_x, t_x) \in T) \rightarrow 2^O$, *a power set of IoTs objects* 2^O *available only a trust pair* $(d_x, t_x) = TE(d_{x-1}, t_{x-1}) \odot CTE(d_{x-1}, t_{x-1})$ *for a session s, such as* $\bigcup_{\gamma \in s\_rpa\&poa\_trusted\ pair} r\_rpa\&poa(\gamma, (u_x, t_x))$, *where* $O{\subseteq}\{O_L \cup O_V\}$.

■

3 Discussions and Security Analysis

In this section, the features of our cooperative IoTs-based RBAC model are discussed and their corresponding security issues are also analyzed.

1. Two specific roles which are local roles set and virtual roles set are introduced in this cooperative IoTs-based RBAC model. At first, both local roles set and virtual roles set are organized in a hierarchy privileges, individually. Each local role with high privilege could be allowed to access the permissions belonging to the local role with low privilege. In the same way, each local role with high privilege could be allowed to access the permissions belonging to the local role with low privilege. Each local role will be assigned to a local permission which is allowed to access a group of local IoTs coordinators or devices. Similarly, each virtual role will be assigned to a virtual permission which is allowed to access a group of external IoTs

coordinators or devices depending to the contract between serving IoTs-based RBAC server and cooperative IoTs-based RBAC server.

2. There are two trust evaluation functions are defined in this cooperative IoTs-based RBAC model, which are both trust evaluation functions TE function γ_l*_trust evaluation*(●) and CTE function *vr_cooperative trust evaluation*(●) in *Definition* 1. The reputation evaluation for each local role assignment together with the virtual role assignment during a time period or a short session *s* will be calculated the trust values by the cooperative trust evaluation (CTE) algorithm proposed in [10]. In this model, the strength of the security depends on the robustness of among two trust evaluation functions and the evaluation algorithm [10].
3. For each session, SMD will be assign a local role together with a virtual role. He could access the resources from local IoTs coordinators or devices managed by his serving RBAC server as well as cooperative IoTs coordinators or devices managed by the cooperative RBAC server. All access records consisting of the local records regarding to local IoTs coordinators or devices and the remote access records regarding to virtual IoTs coordinators or devices will be logged in a database. Finally, each assignment of local role and virtual role to a SMD will be logged its trust data evaluated from the serving RBAC server and cooperative RBAC server (s). In the other words, the trusted SMD assigned to a single session s ∈ S, which is evaluated by both trust evaluation functions TE function γ_l*_trust evaluation*(●) and CTE function *vr_cooperative trust evaluation*(●) representing SMDs associated with this single session *s*.

4 Conclusions

The model we proposed in this paper will provide future mobile e-commerce servers that could be developed with a high potential to exploit an internal security threat that can be developed or can be applied to a multi-server service that could reduce the internal security threat. The research results will provide a new generation of IoTs resources based on cooperative and hierarchical control, and therefore our approach has a very large application field and development space.

Acknowledgements. This work was supported in part by Asia University, Taiwan, and China Medical University Hospital, China Medical University, Taiwan, under Grant ASIA-105-CMUH-04. This work was also supported in part by the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under Grant MOST 104-2221-E-468-002.

References

1. Chen, H.-C., Chang, C.-H., Leu, F.-Y.: Implement of agent with role-based hierarchy access control for secure grouping IoTs. In: The 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), 8–11 January 2017, Las Vegas, USA, pp. 120–125 (2017)
2. Zhong, S., Zhang, L., Chen, H.-C., Zhao, H., Guo, L.: Study of the patterns of automatic car washing in the era of internet of things. In: The 31st IEEE International Conference on Advanced Information Networking and Applications (AINA-2017), 27–29 March 2017, Tamkang University, Taipei, Taiwan, pp. 82–86 (2017)
3. Ferraiolo, D.F., Kuhn, D.R.: Role-based access controls. In: Proceedings of the 15th National Computer Security Conference, 13–16 October 1992, pp. 554–563 (1992)
4. Odelu, V., Das, A.K., Goswami, A.: Scheme for a user hierarchy based on a hybrid algorithm. Smart Comput. Rev. **3**(1), 42–54 (2013)
5. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Computer **29**, 38–47 (1996)
6. Balamurugan, B., Krishna, P.V.: Enhanced role-based access control for cloud security. Artif. Intell. Evol. Algorithms Eng. Syst. **324**, 837–852 (2015)
7. Akl, S.G., Taylor, P.D.: Cryptographic solution to a problem of access control in a hierarchy. ACM Trans. Comput. Syst. **1**(3), 239–248 (1983)
8. Ghodosi, H., Pieprzyk, J., Chames, C., Naini, R.S.: Algorithm for hierarchical croups. In: Proceedings of 1'st Security and Privacy Conference, pp. 275–285 (1996)
9. Cao, J., Yao, Z.A.: An improved access control scheme for hierarchical groups. In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications, pp. 719–723 (2005)
10. Chen, H.-C., Hui-Kai, S.: A cooperative trust bit-map routing protocol using the ga algorithm for reducing the damages from the InTs in WANETs. J. Internet Serv. Inf. Secur. (JISIS) **4**(4), 52–70 (2014)
11. Chen, H.-C.: TCABRP: a trust-based cooperation authentication bit-map routing protocol against insider security threats in wireless ad hoc networks. IEEE Syst. J. **99**, 1–11 (2015). https://doi.org/10.1109/JSYST.2015.2437285
12. Chen, H.-C.: A trusted user-to-role and role-to-key access control scheme. Soft Comput. 1–13 (2015). https://doi.org/10.1007/s00500-015-1715-4