IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 30, 2020, accepted July 18, 2020, date of publication July 23, 2020, date of current version August 5, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3011477*

# A Data Security Enhanced Access Control Mechanism in Mobile Edge Computing

**YICHEN HOU[1], SAHIL GARG[2,3], (Member, IEEE), LIN HUI[1], DUSHANTHA NALIN K. JAYAKODY[3], (Senior Member, IEEE), RUI JIN[4], AND M. SHAMIM HOSSAIN[5], (Senior Member, IEEE)**

[1]College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China
[2]École de Technologie Supérieure (ETS), Montreal, QC H3C 1K3, Canada
[3]School of Computer Science and Robotics, Tomsk Polytechnic University, 634050 Tomsk, Russia
[4]College of Engineering, Mathematics, and Physical Sciences, University of Exeter, Exeter EX4 4QF, U.K.
[5]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Lin Hui (linhui@fjnu.edu.cn)

This work was supported in part by the Competitive Enhancement Program of the Tomsk Polytechnic University, Russia No VIU-ISHITR-180/2020; and in part by the Researchers Supporting Project number (RSP-2020/32), King Saud University, Riyadh, Saudi Arabia.

**ABSTRACT** Mobile edge computing, with characteristics of position awareness, mobile support, low latency, decentralization, and distribution, has received widespread attention from industry and academia, and has been applied to application areas such as intelligent transportation, smart city, and real-time big data analysis. However, it also brings the new security threats, especially data security threats during data access that leads to unauthorized/unauthorized access, alteration and disclosure of data, affecting the confidentiality and integrity of the data. Therefore, access control, as an important method to ensure the security of user data during data access, began to be applied to mobile edge computing. However, the existing access control has the disadvantages of coarse-grain, poor flexibility and accuracy, lack of internal attack considerations, etc., which cannot meet the needs of data security in practical applications of mobile edge computing. In this paper, a data security enhanced Fine-Grained Access Control mechanism (FGAC) is proposed to ensure data security during data access in mobile edge computing. In FGAC, a dynamic fine-grained trusted user grouping scheme based on attributes and metagraphs theory was first designed. Secondly, the scheme was combined with the traditional role-based access control mechanism to assign roles to users based on user group credibility. And then, based on attribute matching the user authentication further verifies whether the user is allowed to perform the access operations to achieve fine-grained data protection. Experimental results show that FGAC can effectively identify malicious users and make group adjustments, while achieving fine-grained access control and assure the data security during the data access process in mobile edge computing.

**INDEX TERMS** Mobile edge computing, access control, data security, data confidentiality, data integrity, metagraph theory.

## I. INTRODUCTION

In recent years, the development of intelligent mobile terminal technology such as smartphones, tablets, various Internet of Things devices, and mobile communication technologies s uch as 5G, the types of mobile applications such as face recognition, augmented reality, virtual reality, live webcasting, etc. are also constantly enriched. Due to constraints such as size, many mobile devices still have relatively scarce resources such as computing, storage, network, and electrical energy, and cannot meet application requirements. To this end, scholars have proposed the Mobile Cloud Computing (MCC) [1] that expanding physical resources of device by migrating tasks to cloud data center to meet all kinds of application of resource requirements. However, since the rapid growth of the mobile devices and applications, the mobile cloud computing mode is overly centralized, and the number of server connections is extremely large, which will cause huge pressure on the server and the network, resulting in server downtime and excessive network delays, which seriously affects the user experience [2]. In view of the above problems, the traditional centralized computing model needs

The associate editor coordinating the review of this manuscript and approving it for publication was Md Zakirul Alam Bhuiyan.

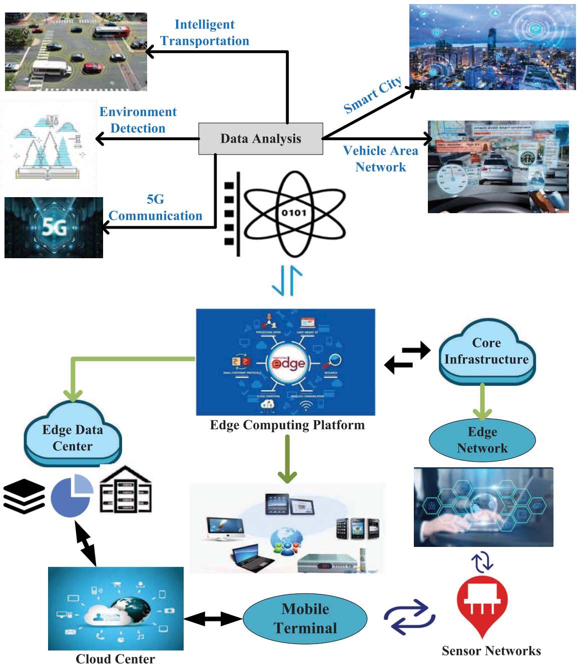


**FIGURE 1.** Architecture of mobile edge computing.

to be further optimized and improved, and is developing towards flattening and marginalization. In this context, as an emerging technology, Mobile Edge Computing (MEC) [3], [4] integrates the mobile access network with various network services and has become an inevitable product that conforms to this trend of development. By migrating the server from a cloud data center to the mobile network edge, MEC reduces physical distance between the mobile terminal and the server. On the one hand, it can reduce the transmission delay and ease the pressure on the backbone network. On the other hand, it can also share the concentration heavy server load.

As shown in Fig. 1, a typical MEC is divided into 4 layers, mobile terminal layer, edge network layer, edge data center layer, and core infrastructure layer [5], [6]. In the MEC, the edge terminal equipment is responsible for data perception and reception, and performs some preliminary data processing. The wireless network is connected to the edge network, and the edge network integrates a variety of communication networks to interconnect the mobile terminal and the sensor network to upload the data to the edge data center. The edge data center is deployed at the edge of the network and is connected to the cloud center. And, the edge data center performs data fusion processing according to the processing results to feedback information or provide related services, or transfer the processed data to the core infrastructure. The of data storage, processing, and access operations are performed at the core infrastructure layer. The MEC architecture built on this can provide a platform for data analysis of Intelligent transportation, smart cities, and the Vehicle Area network, etc.

With the vigorous development of technologies such as 5G, Internet of Things, and artificial intelligence [7], new service models and services based on mobile edge computing [9] will show an explosive growth trend, and generate ‘‘massive’’ data [10]. And, it also brings new security threats to mobile edge computing [11], [12], especially data security threats during data access. These security threats will lead to unauthorized/unauthorized access, alteration and disclosure of data [13], affecting the confidentiality and integrity [8] of the data. Therefore, access control, as an important method to ensure the security of user data during data access, began to be applied to mobile edge computing. At present, the access control mechanisms used in mobile edge computing are mainly divided into two categories: Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) [14]. However, existing mechanisms have the disadvantages of coarse-grain, poor flexibility and accuracy, lack of internal attack considerations, etc., which cannot meet the needs of data security in practical applications of MEC.

To enhance the data security such as data confidentiality and data integrity during data access process, a data security enhanced Fine-Grained Access Control mechanism (FGAC) is proposed, and the contributions of this work include:

(1) Combining the traditional RBAC with metagraph theory based user grouping strategy and user attributes, in FGAC, a novel role and attribute based access control mechanism is proposed to achieve fine granularity of data confidentiality and integrity assurance through fine-grained grouping and access rights settings for users.

(2) In order to realize the fine-grained grouping of users, a dynamic fine-grained trusted user grouping scheme based on user attributes and metagraph theory is proposed. The scheme divides user groups according to the attribute relevance between users and uses the metagraph theory to establish trust relationships based on the access behavior between users. At the same time, a user group update module is also designed to achieve the dynamic adjustment of user groups within the user group.

(3) In order to reduce the probability of internal attacks and achieve fine-grained data protection, a user re-authentication based on attribute matching is proposed. The new authentication mechanism further verifies the matching of user attributes and access data attributes after the user passes preliminary identity verification, restricts the malicious unauthorized access of authorized users, and realizes the fine-grained protection of data.

## II. RELATED WORK

In order to achieve more secure, efficient, and dynamic access control to meet various application requirements, recently, researchers combine RBAC and ABAC [14], and propose some improved solutions.

Kuhn *et al.* [17] combined attribute-based and role-based access control schemes for the first time to achieve effective distributed access control and support dynamic role assignment and permission management. Wang *et al.* [18] proposed an attribute encryption based novel RBAC scheme to provide more flexible access control by introducing the user attributes into RBAC to implement attribute-based user roles and permission assignment. Mon and Naing [20] provide an attributes and roles based access control method, and formulate corresponding access policies to ensure personal data and clouds private. Barkha and Sahani [21] designed a context-based role activation and permission revocation method. The proposed method effectively overcome the shortcomings of traditional ABAC and ABAC, and achieve the advantages of context-aware, fine-grained, etc. For the SaaS model of cloud computing, Geetha and Anbarasi [22] proposed a role-based and attribute-based Web service access control mechanism to ensure the security of the service composition by ranking the possible chains of services based on user's role and sensitivity of related data. Yu *et al.* [23] combined attribute encryption algorithm with FAHP-based user trust evaluation methods, and proposed an attribute and user trust based RBAC to implement the fine-grained dynamic authorization of access control.

Although the existing research results can provide certain data access security, the implementation of the program will generate a lot of additional overhead and cannot be directly applied to mobile terminals with limited resources. At the same time, these solutions lack the flexibility to meet the fine-grained data security requirements associated with different scenarios and multiple services in mobile edge computing and the need to ensure that multiple categories of users access different data. Besides, the lack of consideration of internal attacks also makes these methods impossible to apply directly to practice. Therefore, introducing an internal attack defense mechanism and designing a fine-grained, flexible, and accurate security access control mechanism against internal attacks will be a powerful guarantee for improving the security of mobile edge computing data.

## III. ATTACK MODEL

In FGAC, all users are divided into different groups, and each user accesses data resources according to the role assigned by the user group's credibility. We consider collusion attacks and self-improvement attacks initiated by internal attackers. Attackers can increase their access to important resources through collaboration, thereby threatening data security. The specific attack is defined as follows:

- *Collusion attack:* Multiple attackers can cooperate and provide false information to increase the reputation value of malicious users and reduce the reputation value of normal users, thereby affecting the security level of users.
- *Self-promotion attacks:* Attackers try to increase their reputation by mistake by providing false information or exploiting calculation loopholes, thereby improving their security level.

## IV. A DATA SECURITY ENHANCED FINE-GRAINED ACCESS CONTROL MECHANISM (FGAC)

Because of the existing access control problems such as coarse-grained access control strategy, poor flexibility, and accuracy, lack of internal attack considerations, etc., which cannot meet the data security access requirements in practical applications of mobile edge computing, this section proposes a data security-oriented fine-grained access control mechanism FGAC. Table 1 shows the main symbols used in this paper and their meanings. The overall architecture of FGAC is shown in Fig. 2, which mainly contains two modules: user role assignment and authority assignment. Among them, the user role assignment module divides all users into different groups according to the evaluation result of the user attribute relevance, and then assigns roles to each user group according to the user group's credibility. The rights assignment module re-authenticates the module based on the user based on the attribute matching degree assign appropriate permissions to users. FGAC converts the user-role-permission relationship into a user-user group-role-permission relationship, divides users into different groups according to the user's attribute values and access requirements, assigns corresponding roles and permissions to the user group, and also validates the user role Perform user authentication with the attribute matching degree, and then screen more qualified users for access operations, and meet the different access needs of users under the premise of ensuring user data security.

TABLE 1. Main symbols.

| Symbol | Definition |
|---|---|
| $SH$ | Sensitivity hierarchy of data |
| $SL$ | Security level of user |
| $AR$ | Attribute relevance between users |
| $AM$ | Attribute matching degree |
| $TR(u, u')$ | Trust relationship between user $u$ and user $u'$ |
| $R_i^{sum}$ | Comprehensive reputation value of user $i$ |
| $C_G$ | Reputation threshold set by user group $G$ |
| $GUM$ | User group update module |

The constituent elements in FGAC are defined as follows:

1) Users: a collection of data access requesters, denoted as U, defined as:

$$U = \{u_1, u_2, \ldots, u_n\}, \quad (n \in N)(i, j, if\ i \neq j\ then\ u_i \neq u_j). \quad (1)$$

2) Attribute relevance ($AR$): The similarity of the user's own attribute set. The higher the attribute correlation between users, the closer the functions, access data preferences, and security levels of different users are, and the easier they are to be classified into a user group.
3) User group ($G$): a group divided according to the evaluation results of the user attribute relevance, and the user group is used as a transition between connecting users and roles to form a user-user group-role authorization method. Users in the same user group have similar functions, similar security levels, access requirements, and so on.
4) User group credibility: Measure the value of user group credibility. Each user has a different security level, and users in the same user group have similar security levels. User group credibility is determined by the minimum security level of users in the group.

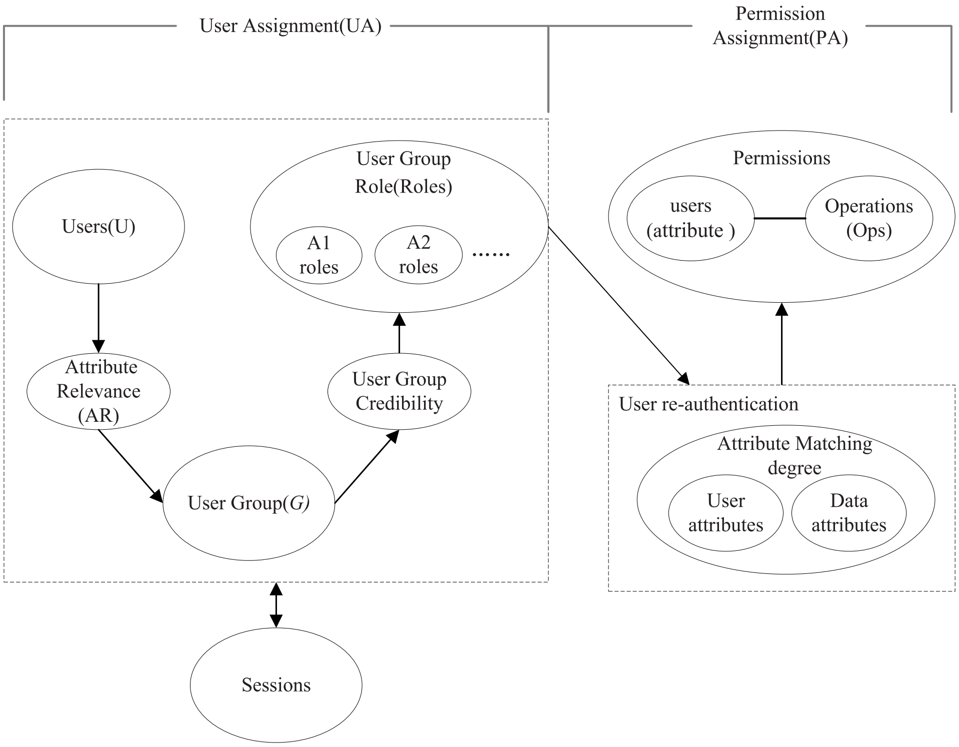


**FIGURE 2.** **Overall architecture of FGAC.**

5) User group role (*Roles*): A role is a collection of responsibilities and access rights. In FGAC, role assignment is performed for user groups, and different roles are assigned to user groups with different credibility. At the same time, the user roles in the group are divided into A1 level roles and A2 level roles according to the security level. The highest level A1 role is responsible for updating users in the group, etc.; the other level roles are responsible for access operations without change User group permissions. The roles and role sets are collectively denoted as r and R, respectively, defined as:

$$\begin{cases} r_i = \{u_{i1}, u_{i2}, \ldots, u_{ik}\}, & (k \in N) \\ R = \{r_1, r_2, \ldots, r_m\}, & (m \in N). \end{cases} \tag{2}$$

6) Permissions: It represents the specific access permission for different information content. Data owners will add attributes to resources and data according to their requirements, thereby restricting access by unauthorized users; operations are specific access modes that users can perform, such as readable, modifiable, or denied access, etc.

7) Attribute matching degree (*AM*): The data owner further restricts access users after verifying the user role and can screen more suitable users for access operations to ensure the security of their own data. The data owner not only requires the user to have the relevant role to obtain access qualification but also further authenticates the access user. It requires that the matching degree between the user attribute and the access data attribute is greater than the set threshold before the user is allowed to access related data.

### A. USER GROUPING SCHEME BASED ON ATTRIBUTES AND METAGRAPHS

In this scheme, firstly, the data needs to be divided into different levels according to the data sensitivity hierarchy (*sh*). The data sensitivity hierarchy is determined by the data owner. The higher the hierarchy, the greater the need for confidentiality and data security. Secondly, according to the evaluation results of Attribute Relevance (AR) between users, all users are divided into different groups by using the metagraph theory [16], [19].

Assume that each user has a set of attributes that including specialty, access data preference, security level, etc., and denoted as $UAS = \{uas_1, uas_2, \ldots, uas_k\}$. The attribute relevance $AR_{(i,j)}$evaluated by user *j* for user *i* can be calculated as follows:

$$AR_{(i,j)} = R_{(i:j)} \times \tau \times \left[ \frac{1}{n} \times \sum_{int=1}^{n} \frac{\left|\mathrm{UAS}_i^{int} \cap \mathrm{UAS}_j^{int}\right|}{\left|\mathrm{UAS}'\right|} \right]$$
$$s.t. \left|\mathrm{UAS}_i^{int} \cap \mathrm{UAS}_j^{int}\right| > w. \tag{3}$$

where $\mathrm{UAS}'$ is the attribute set used in this interaction.$\mathrm{UAS}_i^{int}$ and $\mathrm{UAS}_j^{int}$ are the attribute set used in each interaction between users *i* and *j*, respectively. *n* is the total number of interactions between users *i* and *j*. *w* is the threshold of the proportion of attribute intersections.$R_{(i,j)}$ is the reputation of *j* versus *i* stored in *i*'s local reputation database.$\tau$ is a

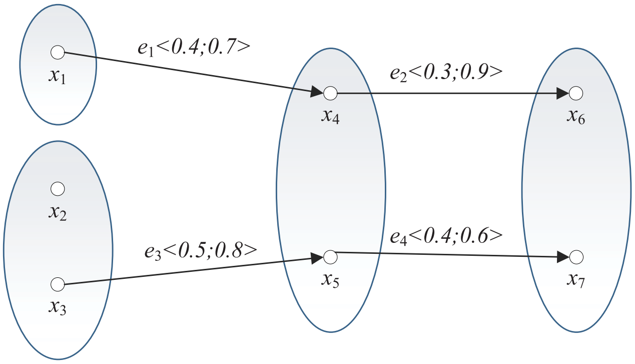


**FIGURE 3. User grouping based on attributes and metagraphs.**

time factor that determines how much interaction time affects $R_{(i,j)}$. Then, $\tau$ is defined as follows:

$$\tau = \tau_{i:j,T_n} \times \theta_{T_n}. \tag{4}$$

where $\theta_{T_n}$indicates the frequency of historical interactions between users $i$ and $j$ up to time T$_n$. $\tau_{i:j,T_n}$is a weighting factor, which determines the degree of influence of the distribution of the historical interactions of users $i$ and $j$ on $R_{(i,j)}$ up to T$_n$. The calculation of $\tau_{i:j,T_n}$ and $\theta_{T_n}$ is as follows:

$$\theta_{T_n} = 1 - e^{(-\frac{\sum_{sh=1}^{|SH|} N_{sh}}{m\times n})}. \tag{5}$$

$$\tau_{i:j,T_n} = \sum_{l=1}^{n} (\frac{T_l}{m} \times \frac{l}{n}). \tag{6}$$

where $N_{sh}$ is the number of historical interactions performed by users $i$ and $j$ based on the data sensitivity hierarchy($sh$), and $m$ and $n$ are the number of time slots and period T, respectively.

The user grouping method based on metagraph theory is defined as follows:

1) Construct the metagraph $S$ $=< X, E >$ into a graph construction specified by its generation set $X$ (user set) and a set of edges $E$ defined on the generation set.
2) Among them, the generation set $X$ represents the user; the edge between the meta nodes users) represents the trust relationship between them. For example, edge $e$ $=< V_e, W_e >\in E$ indicates that there is a trust relationship between user $V_e$ and user $W_e$.
3) The weight of the edge $e$ $=< V_e, W_e >\in E$ is represented by a binary <$ar$; $wr$>, where $ar$ represents the attribute correlation between the user $V_e$ and the user $W_e$; $wr$ represents the trust relationship between the user $V_e$ and the user $W_e$, and the value range is [0,1].

As an example, consider the metagraph $S$ $=< X, E >$ in Fig. 3. Generate set $X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ with edge set $E = \{e_1, e_2, e_3, e_4\}$, where $e_1 =< x_1, x_4 >, e_2 =< x_4, x_6 >, e_3 =< x_3, x_5 >, e_4 =< x_5, x_7 >$. First, divide $X$ into 4 groups $(G1, G2, G3, G4)$ according to the attribute correlation between users, where $G1 = \{x_1\}, G2 = \left\{x_{2,}, x_3\right\}, G3 = \left\{x_{4,}, x_5\right\}, G4 = \left\{x_{6,}x_7\right\}$. Then, the trust relationship between users is established according to the historical interaction between users. For example, $e_1$ $< 0.4; 0.7 >$ indicates that the attribute correlation between user $x_1$ and user $x_4$ is 0.4 and there is a trust relationship. The trust relationship between the two is 0.7.

### 1) TRUST RELATIONSHIP BETWEEN USERS

According to the evaluation result of attribute relevance, all users are divided into different groups using metagraph theory. Assuming that user $u$ and user $u'$ belong to different groups, the trust relationship between user $u$ and user $u'$ is expressed as $\left(TR\left(u, u'\right)\right)$, which is calculated as follows:

(1) When user $u$ and user $u'$ have direct interaction, the trust relationship $TR^{direct}_{(u,u')}$ between $u$ and $u'$ is calculated as follows:

$$TR^{direct}_{(u,u')} = \frac{1}{|\mathrm{SH}|} \times \sum_{sh=i}^{|\mathrm{SH}|} \left(\frac{SI^{sh}}{TI^{sh}} \times \xi_{sh}\right). \tag{7}$$

$$\begin{cases} \xi = E(\gamma_t) \\ \gamma_t = \sum_{j=i}^{|\mathrm{SH}|} IA_j \Big/ \sum_{j=1}^{|\mathrm{SH}|} IA_j, \end{cases} \quad (t = 1 \ldots N_{slot}). \tag{8}$$

where $i$ is the lowest data sensitivity level. $SI^{sh}$ and $TI^{sh}$ represent the number of successful data interactions with the sensitivity hierarchy($sh$) and the total number of interactions, respectively. $\xi$ is a weighting factor, which determines the degree to which the sensitivity hierarchy ($sh$) affects $TR^{direct}_{(u,u')}$ when the two interact. $\gamma_t$ is the ratio between the number of interactions with a sensitivity hierarchy higher than the currently required sensitivity hierarchy $i$ and the total number of interactions at all sensitivity hierarchies. $IA_j$ represents the number of times the sensitivity hierarchy in the historical interaction is confirmed as $j$, and $N_{slot}$ represents the number of time slots.

(2) When users $u$ and $u'$ do not directly interact, assume $DirR = \{dir - rec_i | i = 1 \ldots m\}$ is a set of direct recommenders. The direct recommender $u_j$ has direct interaction with the user $u'$ and has the result of direct trust relationship evaluation about $u'$. Then the indirect trust relationship $TR^{indirect}_{(u,u')}$ between $u$ and $u'$ is calculated as follows:

$$TR^{indirect}_{(u,u')} = \frac{1}{m} \times \sum_{j=1,u_j\in DirR}^{m} \left(\frac{sl_j}{sl_{\max}} \times TR^{direct}_{(u,u_j)}\right). \tag{9}$$

where $sl_{\max}$ is the maximum security level of the person directly recommended in DirR.

Then, each user updates the reputation value of the interacted user according to the calculated trust relationship value between users. Assuming that user $i$ sends an access request to user $j$, hoping that $j$ provides corresponding services, then the credibility value from $j$ to $i$ can be calculated as follows:

$$R_{(i,j)} = UQ_i \times TR_{(i,j)}. \tag{10}$$

Among them, $TR_{(i,j)}$ is the trust relationship between the current users $i$ and $j$. $UQ_i$ is the user qualification of user $i$ in the user group. Because each user may have different status and influence in a group, the higher the user's $UQ$ in the group, the more likely their behavior will meet the group's standards. Let $\bar{g}$ be the group, and the $UQ$ of the user in $\bar{g}$ is defined as follows:

$$\begin{cases} UQ = \kappa_1 \times \frac{1}{|\bar{g}|} \times \sum_{u \in \bar{g}, u \neq \bar{u}} AR(\bar{u}, u) + \kappa_2 \times \frac{1}{|\bar{g}|} \\ \times \sum_{u \in \bar{g}, u \neq \bar{u}} TR(\bar{u}, u) \\ TR(\bar{u}, u) = \rho_1 \times TR^{direct}_{(\bar{u},u)} + \rho_2 \times TR^{indirect}_{(\bar{u},u)} \\ \kappa_1 + \kappa_2 = 1 \\ \rho_1 + \rho_2 = 1. \end{cases} \tag{11}$$

Because user $i$ will interact with multiple users, according to the change of the trust relationship between the data owner and user $i$ and the update of the reputation value after each interaction, the comprehensive reputation value $R_i^{sum}$ of user $i$ can be calculated as follows:

$$R_i^{sum} = \frac{1}{k_n} \sum_{n=1}^{k_n} SL_j^{k_n} \times \lambda_{sl} \times R_{(i,j)}. \tag{12}$$

where $k_n$ is the total number of interactions between user $i$ and other users. $SL_j^{k_n}$ is the security level of the data owner $j$ during the $k_n$ interaction of user $i$. $\lambda_{sl}$ is the proportion of the reputation value of user $i$ provided by data owners with different security levels.

Assuming that the security level is divided into $n$ levels, the security level of user $i$ is divided according to the comprehensive reputation value of user $i$. When $R_i^{sum} \in [TS_j, TS_{j+1}]$ is satisfied, the security level of user $i$ is $j+1$, $j \in [j, n]$, where $TS_{j+1}$ and $TS_j$ is the upper limit of the credibility value corresponding to different security levels.

### 2) USER GROUP UPDATE

After the initial grouping of users, it is assumed that user $x$ belongs to user group g. After some access operations, the change of user attributes may no longer meet the requirements of user group g. At this time, user $x$ needs to be comprehensively evaluated to determine whether the user still meets the Group g requirements.

(1) If the following constraints are met, the original grouping remains unchanged, and user $x$ still belongs to user group g;

$$\begin{cases} \frac{1}{|G|-1} \times \sum_{u \in G, x \neq u} AR(u, x) > \theta \\ \frac{1}{|G|-1} \times \sum_{u \in G, x \neq u} TR(u, x) > \theta' \\ R_x^{sum} > C_G \\ TR(u, x) = \rho_1 \times TR^{direct}_{(u,x)} + \rho_2 \times TR^{indirect}_{(u,x)} \\ \rho_1 + \rho_2 = 1. \end{cases} \tag{13}$$

where $C_G$ is the reputation threshold set by the current user group $G$. $\theta$ and $\theta'$ are the thresholds of attribute relevance and trust relationship set by group $G$, respectively.

(2) If the user $x$ does not meet the constraints set by the user group g, the user group update module (GUM) is used to update the user $x$ grouping.

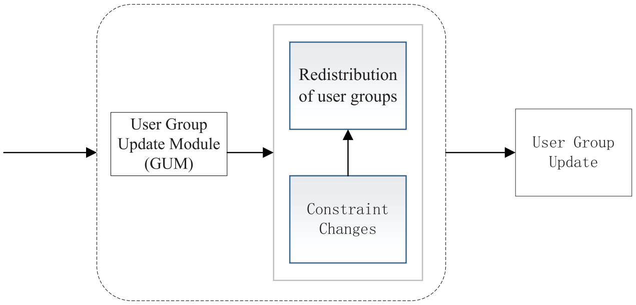


**FIGURE 4.** User group update module.

The user group update module (GUM) mainly provides two functions, as shown in Fig. 4.

One is the redistribution of user groups. This function first integrates the constraints set by all user groups into a list, then calculates the relevant value of user $x$ according to the constraints set by the user group, and finally compares the calculation results with the constraints in the list to assign user $x$ to In the corresponding group.

The second is the change of constraints. The constraints here refer to the constraints set for each group in the user group redistribution function list. This function mainly provides the update of user group constraints. If the user group has not changed much within a certain period of time, this function will regularly update the constraints set by the user group; if the user changes within the user group are too large, the originally set constraints will no longer meet the group status, the user The group can immediately submit the constraint condition update to the user group update module, and replace the constraint condition of the group in the user group redistribution function list.

## B. USER AUTHENTICATION BASED ON ATTRIBUTE MATCHING DEGREE

The user requests access to certain data. After verifying that the user role is qualified to access the data, the data owner needs to further authenticate the access user by calculating the attribute matching degree. Assume that $UcA = \{uca_i | i = 1 \ldots n\}$ is a set of user attributes corresponding to the data attribute requirements. When user $x$ sends an access request to data owner $z$, indicating that he wants to access data $y$, the attribute matching degree of user $x$ and data $y$ is calculated as follows:

$$AM_{(x,y)} = \sum_{j=1, a_j \in UcA}^{n} \gamma_j^y \times uca_j. \tag{14}$$

where $\gamma_j^y$ is a weighting factor, which determines the importance of the jth attribute of the attributes required by the data $y$, and $\gamma_j^y$ is set by the data owner.

Finally, the data owner $z$ compares the attribute matching degree $AM_{(x,y)}$ of the user $x$ and the data $y$ with the attribute matching degree threshold $Ts_y$, where is the threshold of the attribute matching degree set by the access data $y$. If $AM_{(x,y)} \geq Ts_y$, it is determined that user $x$ is granted relevant permissions and user $x$ is allowed to perform the access operation.

### C. FINE-GRAINED ACCESS CONTROL MECHANISM BASED ON USER GROUPING

To ensure the security of user data, the FGAC access control strategy is mainly divided into two parts: role assignment strategy and user authorization strategy.

- *Role assignment strategy*
  FGAC first divides all users into different groups based on user attribute relevance. Users in the same user group have similar functions, similar security levels, and access requirements, etc. Therefore, role assignment is performed for the entire user group, only the user group When the credibility is greater than the threshold set by the role, users in the user group can obtain the corresponding role.
- *User authorization strategy*
  When a user wants to access a certain item of data, the data owner will often further set the access rights for the item of data according to his requirements, not just the role constraints. After verifying that the user role is qualified to access the data, the data owner will re-authenticate the user based on the attribute matching degree, and calculate the matching degree between the user attribute and the data attribute. Only when the matching degree of the two attributes is greater than the threshold set by the data owner can the user obtain the corresponding authority, and then access the data for related operations. This can ensure the security of the data owner's data, and prevent users with relevant roles and attributes who do not meet the requirements from accessing relevant data.

The specific implementation process of FGAC is shown in Fig. 5, and the access control process is described as follows:

(1) User $u$ sends an access request to a certain data;

(2) The data owner performs an authorization check on the access request of user $u$, first verifying whether the role owned by user $u$ is in the set of roles defined in the data and determining whether user $u$ is qualified to access the data. If the role of user $u$ is in the set of accessible roles of this item of data, step (3) is performed; otherwise, the access request of user $u$ is denied;

(3) After the user role is verified, the user re-authentication based on the attribute matching degree is then performed to calculate the matching degree between the user $u$ attribute and the data attribute. If the attribute matching degree of the two meets the threshold defined by the data, the user is granted the corresponding permission to allow user $u$ to perform the access operation; otherwise, the access request of user $u$ is denied;

(4) After the user, $u$'s visit is over, first update the trust relationship between users according to the user's access behavior, and then update the user's reputation value to adjust the user's security level.

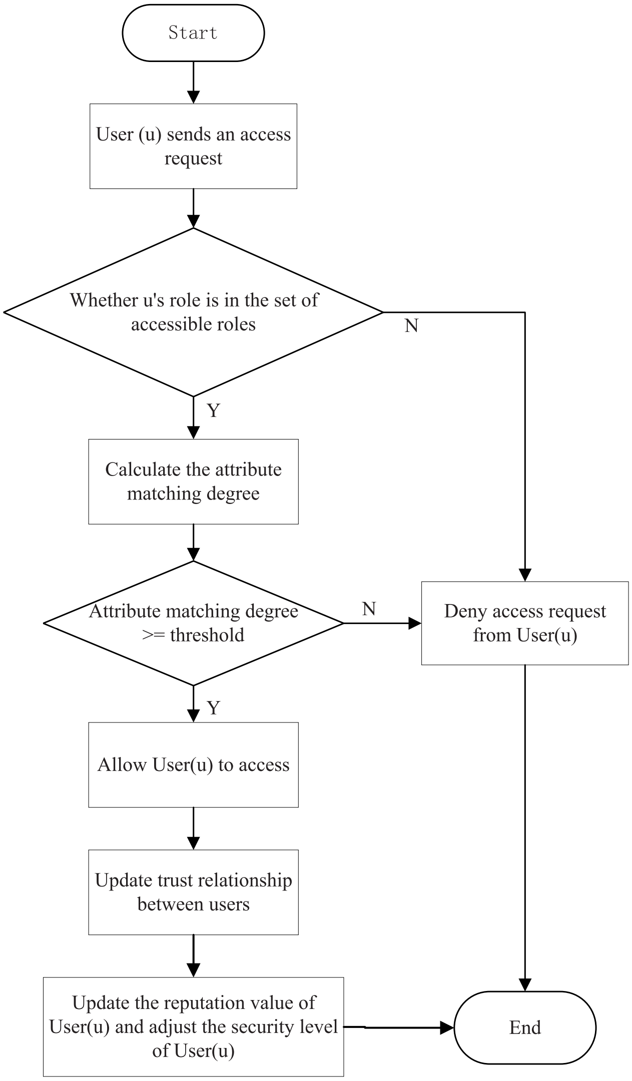
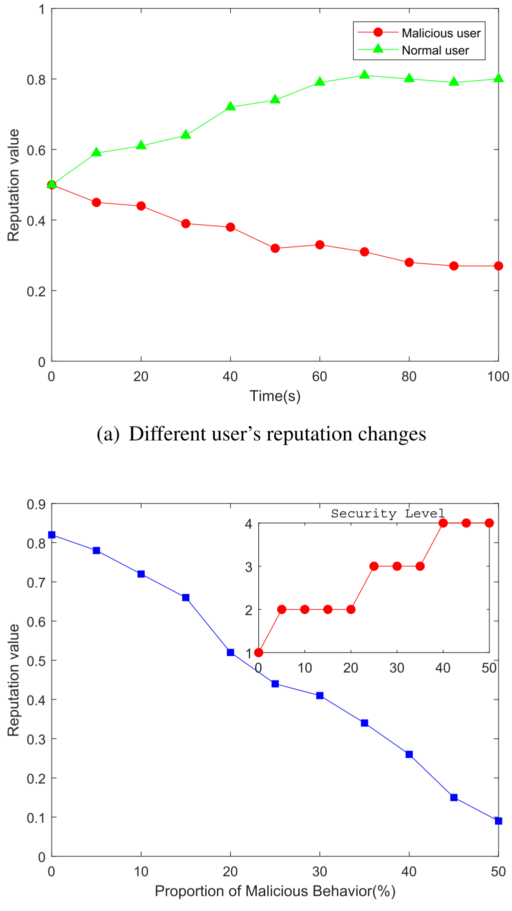

Start
User (u) sends an access request
Whether u's role is in the set of accessible roles
N
Y
Calculate the attribute matching degree
Attribute matching degree >= threshold
N
Deny access request from User(u)
Y
Allow User(u) to access
Update trust relationship between users
Update the reputation value of User(u) and adjust the security level of User(u)
End

**FIGURE 5. FGAC implementation process.**

## V. SIMULATION VERIFICATION AND ANALYSIS

The experiments in this section mainly verify and analyze the user security and authorization fine-grained aspects. In the Windows 7 environment, the configuration is i7-5500U CPU, 8.0GB memory, 1TB hard disk, and simulation verification using MATLAB2017b. In the experiment, we assume that there are 100 mobile terminal users, among which a certain number of malicious users. Malicious users are not always performing malicious visits, while normal users' visits are always benign.

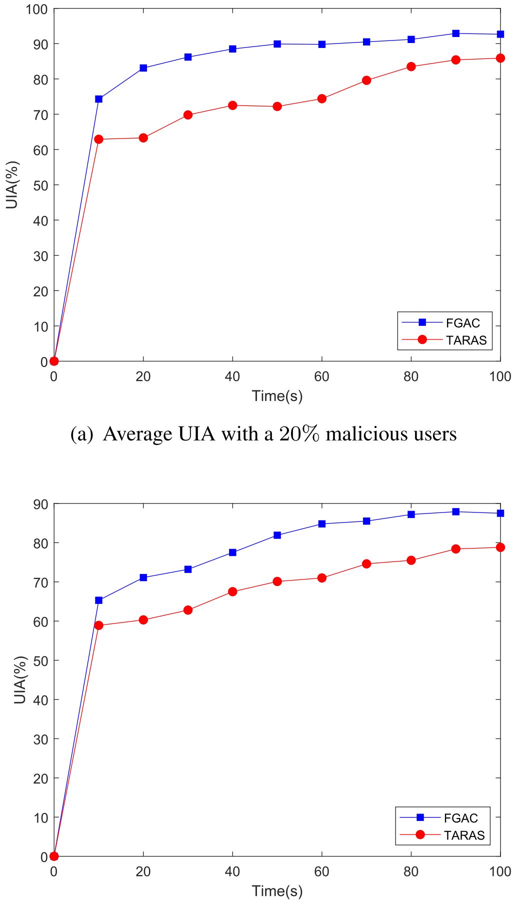
Among the parameters used in this paper, $\kappa_1$ and $\kappa_2$ are the weighting factors of equation (11). We set $\kappa_1$ and $\kappa_2$ to 0.4 and 0.6 respectively, which determine the degree of influence of attribute relevance and the trust relationship between users on user qualifications($UQ$); $\rho_1$ and $\rho_2$ are the weighting factors in equation (11) and equation (13). We set $\rho_1$ and $\rho_2$ to 0.6 and 0.4 respectively, which determine the degree of influence of the direct and indirect trust relationship between users on the trust relationship($TR$).



(a) Different user's reputation changes

(b) Malicious user's reputation changes

**FIGURE 6. User's reputation changes.**



(a) Average UIA with a 20% malicious users

(b) Average UIA with a 30% malicious users

**FIGURE 7. Average UIA with different proportions of malicious users.**

## *A. USER SAFETY ANALYSIS*

The user security is determined by the user's security level, and the user security level is adjusted by updating the trust relationship between users and the user's reputation value after each interaction. The trust relationship between users reflects the historical interaction between users based on different data sensitivity hierarchies.

In Fig. 6(a), it is assumed that two users are in the same user group and the reputation values are equal. To prevent malicious users from excluding the user group and thereby update the user group, we set the user group reputation threshold $C_G = 0$. From the results in the figure, it can be found that with the increase of time, the reputation values of the two users change significantly. On the one hand, when normal users interact with other users, their normal and benign behavior causes their reputation value to continue to increase; on the other hand, when malicious users interact, their malicious behavior makes their reputation value continue to decrease, This is the same as what we estimated. Fig. 6(b) shows the changes in the reputation value and security level of users with high reputation values when their proportion of malicious behavior continues to increase. As can be seen from the results in the figure, even users who performed well in the previous historical interactions will have their reputation value lower as the malicious behavior continues to increase in the later period, and the user's security level will gradually adjust from the high level "1" To the lower level "4", the user's safety is re-evaluated.

Besides, based on the historical interaction between users, we consider comparing and evaluating FGAC, TARAS [15], and RBE in terms of user recognition accuracy and successful acceptance rate, because they are all role-based access control mechanisms, in which TARAS provides users with permissions based on the estimation of the dynamic trust relationship between users, similar to the FGAC mechanism.

- User identification accuracy(UIA): the accuracy of identifying normal users and malicious users;
- Successful acceptance rate(SAR): The ratio of the number of access requests that do not meet the security requirements to the total number of access requests.

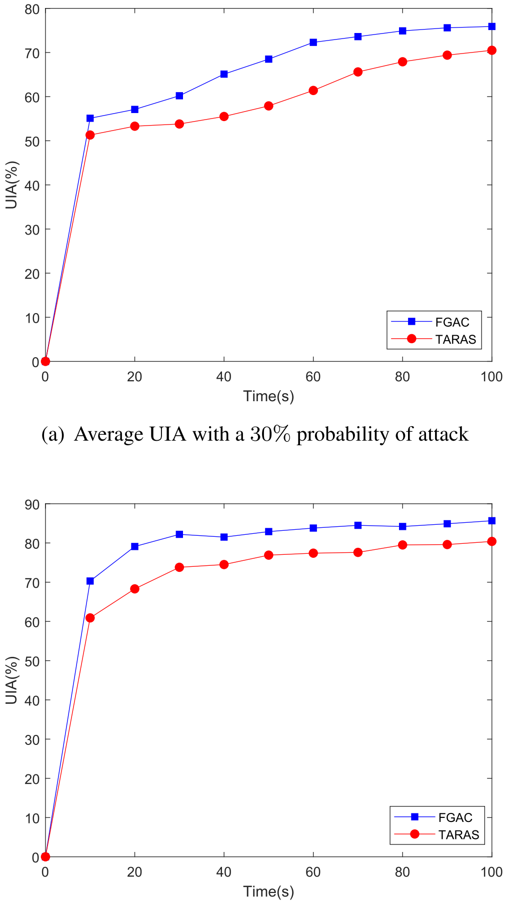
### 1) USER IDENTIFICATION ACCURACY

First, we compared the accuracy of user identification between the two schemes of FGAC and TARAS under the proportion of 20% and 30% malicious users with an attack probability of 1, where the attack probability determines the possibility of malicious users attacking. The greater the probability, the higher the frequency of malicious user attacks. Fig. 7(a) and Fig. 7(b) show the comparison between the accuracy of identifying normal users and malicious users when the proportion of malicious users is 20% and 30%, respectively. It can be seen from the figure that as the proportion of malicious users increases, the accuracy of user identification in both schemes decreases. But at the same time, it can also be found that in the case of a fixed proportion of malicious users (20% or 30%), after a long period of observation and comprehensive evaluation of users, the accuracy of user identification in both schemes has increased, and the accuracy of the FGAC scheme is higher. Although both schemes restrict the access of malicious users by setting thresholds, FGAC combines the division of user groups based on attribute correlation and the establishment of trust relationships, and FGAC sets trust thresholds for user groups. The range of users in the group is small and similar, so users in the group can provide more accurate evaluation references, which improves the accuracy of evaluating users' security level, and it is easier to detect malicious users and adjust the user group. Therefore, the accuracy of user identification is slightly Higher than TARAS.

At the same time, we also compared the accuracy of user identification of the two schemes under different malicious user attack probabilities when the proportion of malicious users was 20%. Fig. 8(a) and Fig. 8(b) show the comparison between the accuracy of identifying normal users and malicious users when the attack probability of malicious users is 30% and 70%, respectively. As can be seen from the figure, as the probability of malicious user attacks increases, the possibility of malicious user exposure increases accordingly, so the accuracy of user identification in both schemes has increased. But at the same time, it can also be found that, regardless of the increase in time or the probability of malicious user attacks, the accuracy of FGAC user identification is still higher than that of TARAS. The reason is that the user group division scheme based on attribute relevance in FGAC divides users with similar security levels into a group. If there is a malicious user in the group and the proportion of the user's malicious behavior increases, GRM can identify the malicious user in time by establishing a trust relationship between users and setting a user group trust threshold.

### 2) SUCCESSFUL ACCEPTANCE RATE

Fig. 9 is a comparison of the successful acceptance rate of the three schemes of FGAC, TARAS, and RBE. As can be seen from the figure, as the number of interactions, and the proportion of malicious users increase, the successful acceptance rate of the three schemes has increased. In general, the successful acceptance rate of FGAC and TARAS is better than RBE. As shown in Fig. 9(b), when the proportion of malicious users is 0-20%, the overall successful acceptance rate of the two schemes is not much different. As the proportion of malicious users continues to increase, TARAS's successful acceptance rate has increased, while FGAC's successful acceptance rate has changed less and is relatively stable. This is because the establishment of the trust relationship between users makes the adjustment of the user's security level more accurate so that more credible users can be selected during data access. Besides, the user re-authentication based on attribute matching proposed in the FGAC can screen out users who are more in line with the access requirements based on the user's true attributes and reduce the probability of collusion attacks, which also improves the security of the data access process, and decreases the successful acceptance rate of FGAC.



(a) Average UIA with a 30% probability of attack

(b) Average UIA with a 70% probability of attack

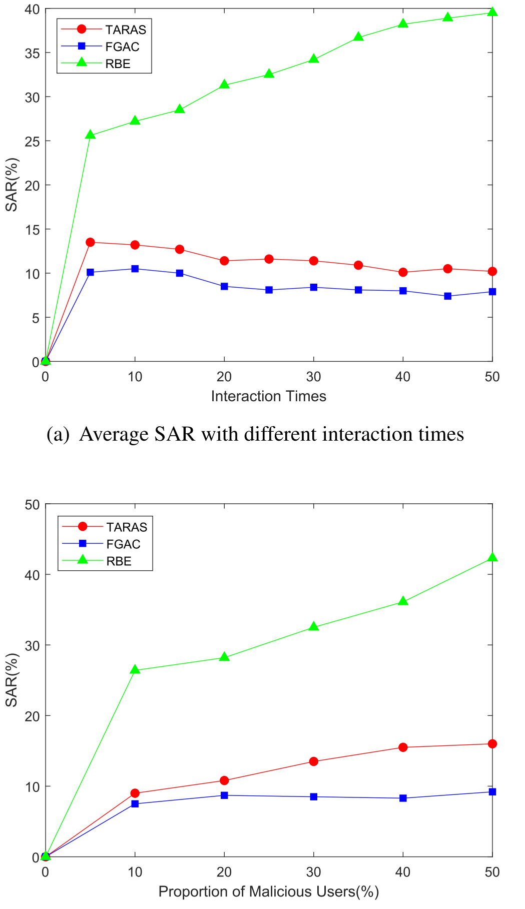
**FIGURE 8. Average UIA with different attack probabilities.**

## B. AUTHORIZED FINE-GRAINED VERIFICATION

Authorized fine-grained verification is mainly to determine whether more fine-grained access control is achieved than the traditional RBAC model. In the simulation experiment, 7 users are specifically set, and each user's attribute set includes ID, name, department, job title, work experience, the annual number of operating tables, and security level. The security level is determined by the user's comprehensive reputation value. Table 2 lists the detailed information of each user.

After preliminary experiment setting, the threshold of user group credibility corresponding to the role is shown in Table 3. Table 4 is the attribute requirements set by the data *Data*_1 and the data *Data*_2.

The user access results are shown in Table 5. If user *Staff* _0 and *Staff* _3 request access to data *Data*_1 at the same time,



(a) Average SAR with different interaction times

(b) Average SAR with different proportions of malicious users

**FIGURE 9.** Average SAR.

**TABLE 2.** User information.

| User | Department | Title | Work experience (years) | Number of operating tables (year) | User group | User group credibility |
|---|---|---|---|---|---|---|
| Staff_0 | Neurology | director physician | 9 | 120 | G1 | 3 |
| Staff_1 | Respiratory Medicine | assistant director physician | 8 | 100 | G3 | 4 |
| Staff_2 | Neurology | director physician | 9 | 110 | G2 | 2 |
| Staff_3 | Neurology | director physician | 11 | 90 | G1 | 3 |
| Staff_4 | Neurology | assistant director physician | 8 | 90 | G2 | 2 |
| Staff_5 | Respiratory Medicine | director physician | 10 | 90 | G3 | 4 |
| Staff_6 | Neurology | director physician | 10 | 80 | G1 | 3 |

**TABLE 3.** The credibility of the user group corresponding to the role.

| Role | Threshold for user group credibility |
|---|---|
| Role_1 | 4 |
| Role_2 | 3 |
| Role_2 | 2 |

**TABLE 4.** Data attribute requirements.

| Data | Accessible role | Department | Title | Work experience (years) | Number of operating tables (year) |
|---|---|---|---|---|---|
| Data_1 | Role_2<br>Role_3 | Neurology | director physician | 10 | 100 |
| Data_2 | Role_1<br>Role_2 | Respiratory Medicine | director physician | 8 | 80 |

**TABLE 5.** Access results.

| User | User group | User group credibility | Role | Accessed data | Result |
|---|---|---|---|---|---|
| Staff_0 | G1 | 3 | Role_2 | Data_1 | Allow |
| Staff_1 | G3 | 4 | Role_1 | | |
| Staff_2 | G2 | 3 | Role_3 | | |
| Staff_3 | G1 | 3 | Role_2 | Data_1 | deny |
| Staff_4 | G3 | 2 | Role_3 | | Allow |
| Staff_5 | G3 | 4 | Role_1 | Data_2 | Allow |
| Staff_6 | G1 | 3 | Role_2 | Data_2 | deny |

first verify whether the roles of the two users meet the requirements of data *Data*_1. At this time, the roles owned by both users are *Role*_2, which is consistent with the data *Data*_1 request. Then further verify other attributes. User *Staff*_0 and *Staff*_3 are the director physicians of the Department of Neurology. The work experience and the number of operating tables are different. At this time, the matching degree of the user attribute and the data attribute can be calculated according to equation (14). Assuming that the weight of work experience in the data *Data*_1 is 0.4 and the weight of the annual number of operating tables is 0.6. According to the calculation, the user *Staff*_0 is more in line with the requirements of the data *Data*_1, then the user *Staff*_0 is allowed to perform the access operation, and the user *Staff*_3 is denied the access request.

In addition, if user *Staff*_6 and user *Staff*_5 request access to data *Data*_2 at the same time, the roles owned by the two users meet the requirements of *Data*_2. Although user *Staff*_6 and user *Staff*_5 belong to internal medicine, user *Staff*_5 belongs to respiratory medicine, which is more in line with the requirements of data *Data*_2. After attribute matching calculation, user *Staff*_5 is allowed to perform access operations. In the traditional RBAC model, for example, the user *Staff*_0 and the user *Staff*_3 are all assigned the role of *Role*_2, so in the subsequent data access process, the two have the same permissions. The FGAC scheme proposed in this article adds the user re-authentication module based on the attribute matching degree. According to the matching degree of different attribute values and data attributes of the user, even if the user *Staff*_0 and the user *Staff*_3 have the same role, the permissions they have will be different, thus enabling more fine-grained authorization to ensure the security of user data.

## VI. CONCLUSION

Aiming at the problems that the existing access control policies have coarse granularity, poor flexibility and accuracy, and lack of internal attack considerations, which cannot meet the data security access requirements in practical applications of MEC, this paper proposes a data security enhanced

Fine-Grained Access Control mechanism(FGAC) based on user grouping. First, the attribute relevance evaluation for users is carried out, and a dynamic fine-grained trusted user grouping scheme is designed based on the above evaluation results and metagraph theory. Then, combined with role-based access control, the scheme assigns roles based on the credibility of user groups and further verifies users based on attribute matching, to achieve fine-grained protection of data and reduce the risk of internal attacks. Experimental results show that FGAC can effectively limit the access of malicious users and update user groups in time, and ensure the security of user's data by implementing more fine-grained access control. For future work, we intend to introduce blockchain technology into the access control mechanism in mobile edge computing to solve data security issues in the process of data access further.

## REFERENCES

[1] J. X. Zhai, "Research on authentication protocol in mobile cloud computing," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., JiangSu, China, 2019.

[2] Y. Chen, D. J. Xu, and L. Xiao, "Survey on network security based on blockchain," *Telecommun. Sci.*, vol. 34, no. 3, pp. 10–16, Mar. 2018.

[3] K. Kaur, S. Garg, G. Kaddoum, M. Guizani, and D. N. K. Jayakody, "A lightweight and privacy-preserving authentication protocol for mobile edge computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[4] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

[5] X. Y. Ma, "Research on trusted cooperative mechanism based on edge computing," M.S. thesis, Dept. Abbrev., Beijing Univ. Posts Telecommun., Beijing, China, 2019.

[6] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

[7] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6242–6251, Jul. 2020.

[8] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2679–2689, Apr. 2020.

[9] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[10] W. S. Shi, H. Sun, J. Cao, Q. Zhang, and W. Liu, "Edge computing-an emerging computing model for the Internet of everything era," *J. Comput. Res. Develop.*, vol. 54, no. 5, pp. 907–924, Feb. 2017.

[11] H. Li, G. Shou, Y. Hu, and Z. Guo, "Mobile edge computing: Progress and challenges," in *Proc. 4th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Oxford, U.K., Mar. 2016, pp. 83–84.

[12] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: Convergence of computing, caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779, Mar. 2017.

[13] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, G. Wang, T. Wang, M. M. Ahmed, and J. Li, "Economic perspective analysis of protecting big data security and privacy," *Future Gener. Comput. Syst.*, vol. 98, pp. 660–671, Mar. 2019.

[14] J. L. Zhang, Y. C. Zhao, B. Chen, F. Hu, and K. Zhu, "Survey on data security and privacy-preserving for the research of edge computing," *J. Commun.*, vol. 39, no. 3, pp. 1–21, Mar. 2018.

[15] B. Gwak, J.-H. Cho, D. Lee, and H. Son, "TARAS: Trust-aware role-based access control system in public Internet-of-Things," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, New York, NY, USA, 2018, Aug. 2018, pp. 74–85.

[16] Y. Zhu, B. Li, H. Fu, and Z. Li, "Core-selecting secondary spectrum auctions," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2268–2279, Nov. 2014.

[17] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *Computer*, vol. 43, no. 6, pp. 79–81, Jun. 2010.

[18] Y. Wang, Y. Ma, K. Xiang, Z. Liu, and M. Li, "A role-based access control system using attribute-based encryption," in *Proc. Int. Conf. Big Data Artif. Intell. (BDAI)*, Beijing, China, Jun. 2018, pp. 128–133.

[19] M. Ezhei and B. T. Ladani, "GTrust: A group based trust model," *Int. J. Inf. Secur.*, vol. 5, no. 2, pp. 155–169, Mar. 2014.

[20] E. E. Mon and T. T. Naing, "The privacy-aware access control system using attribute-and role-based access control in private cloud," in *Proc. 4th IEEE Int. Conf. Broadband Netw. Multimedia Technol.*, Shenzhen, China, Oct. 2011, pp. 447–451.

[21] P. Barkha and G. Sahani, "Flexible attribute enriched role based access control model," in *Proc. Int. Conf. Inf., Commun., Instrum. Control (ICICIC)*, Indore, India, Aug. 2017, pp. 1–6.

[22] N. Geetha and M. S. Anbarasi, "Role and attribute based access control model for Web service composition in cloud environment," in *Proc. Int. Conf. Comput. Intell. Data Science(ICCIDS)*, Chennai, India, Jun. 2017, pp. 1–4.

[23] B. Yu, X. Q. Tai, and Z. J. Ma, "Research on RBAC model based on attribute and trust in cloud computing environment," *Comput. Eng. Appl.*, vol. 56, no. 9, pp. 84–92, May 2020.

**YICHEN HOU** received the bachelor's degree in software engineering from Xinyang Normal University, China, in 2018. She is currently pursuing the master's degree with the School of Mathematics and Information, Fujian Normal University. Her research interests include blockchain, access control, and network security.

**SAHIL GARG** (Member, IEEE) received the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently a Postdoctoral Research Fellow at École de technologie supérieure, Université du Québec, Montréal, Canada. He has many research contributions in the area of machine learning, big data analytics, security & privacy, internet of things, and cloud computing. He has over 60 publications in high ranked Journals and Conferences, including 40+ top-tier journal papers and 20+ reputed conference articles. He was awarded the IEEE ICC best paper award in 2018 at Kansas City, Missouri. He is currently a Managing Editor of Springer's Human-centric Computing and Information Sciences (HCIS) journal. He is also an Associate Editor of the IEEE Network Magazine, IEEE System Journal, Elsevier's Applied Soft Computing, Elsevier's Future Generation Computer Systems (FGCS), and *Wiley's International Journal of Communication Systems* (IJCS). In addition, he also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications. He guest-edited a number of special issues in top-cited journals, including IEEE T-ITS, IEEE TII, IEEE IoT Journal, IEEE Network, and Future Generation Computer Systems (Elsevier). He serves/served as the workshop chair/publicity co-chair for several IEEE/ACM conferences, including the IEEE Infocom, IEEE Globecom, and IEEE ICC and ACM MobiCom. He is a member of ACM.

**LIN HUI** received the Ph.D. degree in computing system architecture from the College of Computer Science, Xidian University, China, in 2013. He is currently a Professor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, where he is also a M.E. Supervisor. He has published more than 50 papers in international journals and conferences. His research interests include mobile cloud computing systems, blockchain, and network security.

**DUSHANTHA NALIN K. JAYAKODY** (Senior Member, IEEE) received the M.Sc. degree (Hons.) in electronics and communications engineering from Eastern Mediterranean University, Turkey (under the University Graduate Scholarship), and the Ph.D. degree in electronics and communications engineering from University College Dublin, Ireland, under the supervision of Prof. M. Flanagan (Science Foundation Ireland Grant). From 2014 to 2016, he has held a Postdoctoral position at the Coding and Information Transmission Group, University of Tartu, Estonia, and the University of Bergen, Norway. Since 2016, he has been a Professor with the School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Russia. He has held various visiting positions at the Texas A&M University, Qatar, the University of Jyväskylä, Finland, and the National Institute of Technology, Trichy, India. He has served as the Session Chair or a Technical Program Committee Member for various international conferences, such as IEEE PIMRC 2014–2020, IEEE WCNC 2014–2020, and IEEE VTC 2015–2019.

**RUI JIN** received the bachelor's degree in computer science from the University of Science and Technology Beijing. She is currently pursuing the Ph.D. degree in computer science with the University of Exeter, U.K. Her research interests include network security, machine learning, and mobile edge computing.

**M. SHAMIM HOSSAIN** (Senior Member, IEEE) is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa, Canada. He has authored and coauthored more than 260 publications including refereed journals (200+ SCI/ISI-Indexed papers, 100+ IEEE/ACM Transactions/Journal papers, 10+ ESI highly cited papers, 1 hot paper), conference papers, books, and book chapters. Recently, he co-edited a book on "Connected Health in Smart Cities", published by Springer. He has served as cochair, general chair, workshop chair, publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. He is currently the cochair of the 3rd IEEE ICME workshop on Multimedia Services and Tools for smart-health (MUST-SH 2020). He is a recipient of a number of awards, including the Best Conference Paper Award and the 2016 ACM Transactions on Multimedia Computing, Communications and Applications (TOMM) Nicolas D. Georganas Best Paper Award, and the 2019 King Saud University Scientific Excellence Award (Research Quality). He is on the editorial board of the IEEE TRANCTIONS ON MULTIMEDIA, the IEEE NETWORK, the IEEE MULTIMEDIA, the IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, the Journal of Network and Computer Applications (Elsevier), and the International Journal of Multimedia Tools and Applications (Springer). He also presently serves as a lead guest editor of IEEE Network, ACM Transactions on Internet Technology, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) and Multimedia systems Journal. Previously, he served as a guest editor of IEEE Communications Magazine, IEEE Network, the IEEE TRANCTION INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), the IEEE TRANCTIONS ON CLOUD COMPUTING, *International Journal of Multimedia Tools and Applications* (Springer), *Cluster Computing* (Springer), *Future Generation Computer Systems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *Sensors* (MDPI), and *International Journal of Distributed Sensor Networks*. He is a senior member of the ACM.

• • •