information

MDPI

Article

CaACBIM: A Context-aware Access Control Model for BIM

Rongyue Zheng [1], Jianlin Jiang [1], Xiaohan Hao [2], Wei Ren [2,*], Feng Xiong [3] and Tianqing Zhu [2,4]

1 Faculty of Architecture, Civil Engineering and Environment, Ningbo University, Ningbo 315211, China; rongyue@nbu.edu.cn (R.Z.); jiangjianlin@nbu.edu.cn (J.J.)
2 School of Computer Science, China University of Geosciences, Wuhan 430074, China; xhhao@cug.edu.cn (X.H.); Tianqing.Zhu@uts.edu.au (T.Z.)
3 School of Business Administration, Zhongnan University of Economics and Law, Wuhan 430073, China; xiongfeng@zuel.edu.cn
4 School of Software, University of Technology Sydney, Ultimo, NSW 2007, Australia
* Correspondence: weirencs@cug.edu.cn

Received: 22 December 2018; Accepted: 23 January 2019; Published: 1 February 2019

Abstract: A building information model (BIM) is of upmost importance with a full life-time cycle in architecture engineering and construction industry. Smart construction relies on BIM to manipulate information flow, data flow, and management flow. Currently, BIM has been explored mainly for information construction and utilization, but there exist few works concerning information security, e.g., audits of critical models and exposure of sensitive models. Moreover, few BIM systems have been proposed to make use of new computing paradigms, such as mobile cloud computing, blockchain and Internet of Things. In this paper, we propose a Context-aware Access Control (CaAC) model for BIM systems on mobile cloud architectures. BIM data can be confidentially accessed according to contexts in a fine-grained manner. We describe functions of CaAC formally by illustrating location-aware access control and time-aware access control. CaAC model can outperform role-based access control for preventing BIM data leakage by distinguishing contexts. In addition, grouping algorithms are also presented for flexibility, in which basic model (user grouping based on user role permissions) and advanced model (user grouping based on user requests) are differentiated. Compared with the traditional role-based access control model, security and feasibility of CaAC are remarkably improved by distinguishing an identical role with multiple contexts. The average efficiency is improved by $2n/(2n-p-q)$, and time complexity is $O(n)$.

Keywords: access control; BIM; construction automation; mobile cloud;

1. Introduction

BIM (Building Information Model) has been envisioned as a key approach for smart construction, such as construction automation, construction supply chain management, building information exchange, and building data sharing [1,2]. BIM can provide a uniform presentation, data framework, and organizing architecture to enable Information and Communication Technology (ICT) to manage the full life-time information of a building in smart construction. BIM information can be accessed to facilitate engineering procedures such as design, construction, maintenance, re-construction, and even destruction [3–5].

The recent ICT architecture for BIM applications is usually traditional client/server mode or single work station mode. It is worth noting that mobile cloud computing becomes pervasive in current personal computing. For example, cloud servers provide storage for the large volume of BIM data, which can be accessed remotely. Mobile computing devices help designers, monitors, construction

workers or suppliers access BIM information in cloud servers, any time and anywhere. The BIM cloud can greatly shorten information accessing delay, and make BIM information available to all demanders. In other words, mobile cloud architecture allows BIM information to be pervasively accessible, and is scalable for a large number of users.

However, access control of BIM data is subtle in mobile cloud environment. For example, consider entities in a construction project as follows: owners of a bank building are members of a bank company; designers are engineers in design institute; contractors are managers in contracting companies; and builders are workers of construction companies. They may access BIM information with different privileges. Even for the same information and entity, the privileges may be different at various times or locations, as, in mobile cloud, access may occur any-time any-where.

RBAC (role based access control) is mainstream model in current access control research [6–9], in which roles are assigned to each user. When the number of users grows, the management complexity obviously increases. Besides, RBAC may be inflexible due to the restriction of user's login authority. Mobile cloud for BIM provides the convenience of information access, but it also raises several security issues [10–12].

Access control for critical and sensitive BIM data presents the following challenges: (1) Users are mobile and access may be any-time, thus requiring a more efficient and secure enhancement in access control mechanism. (2) When the number of users is much larger than that in traditional RBAC, it experiences difficulties in scalability assigning each user privileges. (3) An attack is possible in which the credential of a role is leaked, whether due to intentional attacks or unintentional mistakes and random failure.

To tackle the above challenges, in this paper, we propose a Context-aware access control model called CaAC for BIM data auditing in mobile cloud BIM architecture. CaAC can support many users with fewer roles. Although the number of roles is decreased, CaAC can guarantee access control within the same role by differentiating contexts, which provides fine-grained control. We group users and user groups are granted roles. The contributions of the paper are listed as follows:

1. We propose a Context-aware Access Control mechanism (CaAC) to guarantee pervasive access control in mobile cloud paradigm that provides scalable storage and fast retrieval.
2. We propose a user grouping method to improve scalability and efficiency. We also propose an authentication scheme by dynamic electronic signature to reduce the aggressiveness of role leakage attacks.

The rest of the paper is organized as follows. Section 2 gives an overview of the relevant previous work. In Section 3, we propose the mobile cloud BIM architecture. Section 4 analyzes access control problems, and presents the detailed description of our proposed methods and algorithms. In Section 5, we evaluate the security and performance of CaAC model. Finally, Section 6 concludes the paper.

2. Related Work

BIM model is largely used in smart construction and sustainable buildings. Ren et al. [13] discussed BIM model for sustainable construction, such as energy saving, pollution reduction, costs saving and construction efficiency. BIM-based design method for energy efficiency was discussed by Yoon et al. [14]. They proposed a BIM-based system that can be scheduled to be built by reducing the amount of energy. Vozzola et al. [15] described a practical application of BIM in construction processes. Kokorus et al. [16] suggested using BIM software to shorten project time and costs for improving efficiency and accuracy in substation design.

Some works discuss BIM with other ICT to enhance smart construction. Wang et al. [17] explored the real-time communication and integration of BIM into site and task conditions. They proposed to use Augmented Reality (AR) to visualize BIM data in the physical context of each construction activity or task. Garcia-Fernandez et al. [18] focused on semantic enrichment process of models, especially in the field of cultural heritage. They discussed different approaches on HBIM generation: from 3D

point cloud data collection to semantically enriched parametric models. Bottaccioli et al. [19] proposed a software architecture for the management of energy behaviors in buildings that integrates data such as BIM, IoT, GIS (Geographical Information System), and meteorological services. Their system allows real-time visualization of energy consumption and builds performance evaluation, through energy modeling and simulation, by exploiting data from the field and real weather conditions. Pasini et al. [20] defined a digitally enabled framework for operating cognitive buildings by exploiting IoT and BIM.

Recently, Desogus et al. [21] proposed a sensor-based plan for monitoring indoor thermo-hygrometric conditions, and defined a set of interventions, which should be compatible with building preservation issue and oriented at improving its energy performance. They adopted a cognitive building concept and then applied it to the icon building at the University of Cagliari Campus called "Mandolesi Pavilion". Arslan et al. [22] developed a prototype system using Hadoop for data storage and processing. The results of processing BIM and sensor data in a Hadoop architecture demonstrate that the system can effectively provide data visualizations to facility managers. Building Life Cycle Assessment (BLCA) of energy consumption is an important issue in the field of sustainable development and green building. Yuan et al. [23] summarized the features of Building Life Cycle Energy Consumption (BLCEC) data. They also proposed the method of information exchange and integration management by BIM, and utilized cloud computing technology to achieve wide-area BLCEC data management. As part of a larger, modular and extensible framework, the application of Linked Data View (or Semantic View) was introduced by Ferguson et al. [24]. Their framework provides a method to automatically query, understand BIM instances and convert them into linked data to support more accurate decision-making.

Regarding BIM application potential, Ding et al. [25] proposed a BIM application framework, which describes the process of expanding from 3D to computable *n*D. Dawood et al. [26] proposed to integrate between BIM and Genetic Algorithm (GA) for reaching the minimum LCC. BIM is the simulation tool to generate the building design and dynamical analysis for the energy consumption of houses. According to the measures and characteristics of BIM barriers in China, Pan et al. [27] drafted a road map for the adoption and application of BIM in China. Mohd et al. [28] discussed the application of BIM in architectural planning. BIM was used to conduct semi-structured interviews with customers. The interviews revealed the necessity and benefits of BIM implementation in construction planning, as well as the challenges faced by customers in implementing BIM. Ferreira et al. [29] used a simplified method, combining the location information generated by interaction between beacon propagation signals and mobile device sensors (accelerometers and gyroscopes) with local building information to provide real-time positioning and guidance for users in buildings.

We observe that some upcoming computing paradigms are promising to be integrated with BIM system as a new architecture, such as mobile cloud computing, blockchain, and Internet of Things. However, the marriage of them with BIM has been explored by few related works. The hand-held devices such as smart phones and tablet computers have already been pervasively used as an ordinary computing tool for many engineers. Those devices perform as convenient productivity tools, because hardware capabilities grow sufficiently powerful, and more productivity applications are available at application stores. The work on the marriage between mobile cloud and BIM model is few. Betarte et al. [30] proposed a framework—ACTkit—for the definition and enforcement of dynamic access control. Their work is independent of ours.

3. Problem Formulation

3.1. System Model

The main weakness in security for current BIM are as follows: The access control of BIM data is not fine-grained. BIM data can be accessed by roles, but same roles may have different privileges for the same subject. In addition, with the development of pervasive data sharing in BIM data,

access control becomes more critical because some data may not be accessible to the same role in different contexts, e.g., times or locations. For some sensitive buildings, such as cross-sea bridges and critical infrastructures, it is necessary to carry out fine-grained access control of BIM data.

Five basic elements are concerned: users, roles, objects, operations and permissions. At least one permission is assigned to each role, and at least one role is assigned to each user. The same access rights can be assigned to different roles. Users and roles are many-to-many, which means users can have different roles in different scenarios. For example, a project manager can also be a designer. Certainly, a role can be given to multiple users. The separation of user and role can make authorization be more flexible. Roles and permissions are also many-to-many, which means roles can have multiple rights and the same right can be delegated to multiple roles. RBAC refers to the association of a user with permissions through roles, where a user has multiple roles and each role has multiple permissions. In this way, an authorization model such as user–role–permissions is built. In this model, ordinary people have many-to-many relationships between users and roles, as well as roles and permissions.

When the number of users is large, it is cumbersome to give each user authorization (to delegate roles) one by one. Thus, we consider organizing multiple users in one group, and authorizing users by authorizing groups. As a result, all permissions that a user possesses consist of permissions possessed by the user personally and permissions possessed by the user group. The model is shown in Figure 1, and the specification is discussed in details in the following.

In addition, we propose two models on grouping rules: basic model and advanced model. In the basic model, grouping is based on user's privileges. That is, the user knows the privileges upon login. Once the basic model is not sufficiently flexible, the advanced model is proposed in which grouping corresponds to context requests.

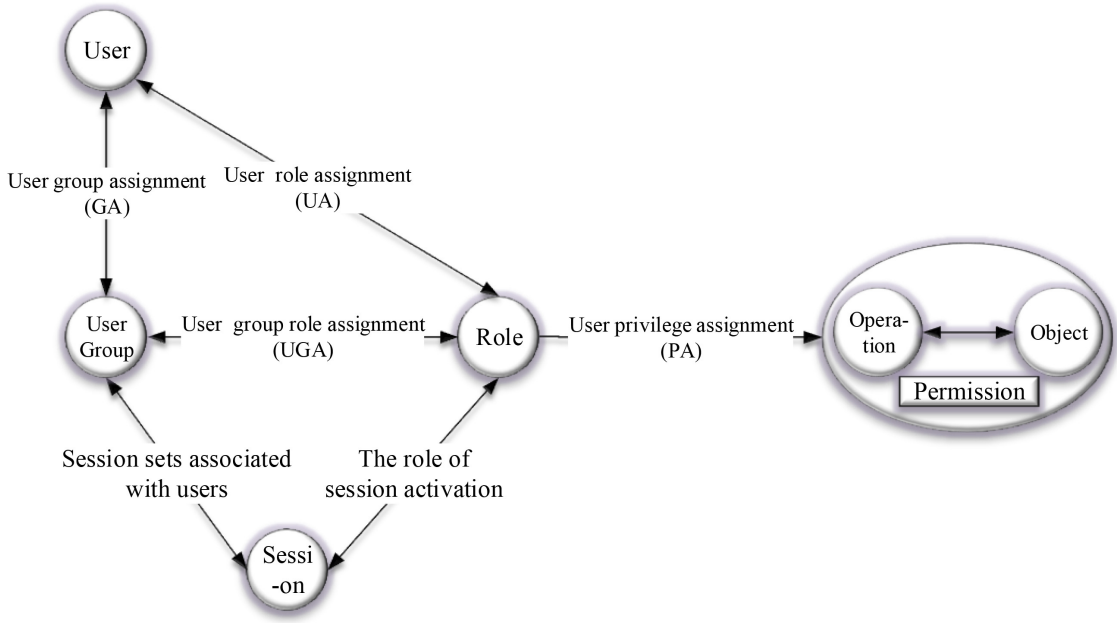

Figure 1. Context-aware Access Control with grouping

It is worth stressing that the main difference between a role and a user group is that a user group is a group of users, instead of a group of permissions. In contrast, a role is a group of users and permissions, and it indeed connects two groups as a mediation. In a system where permissions and members of a user group can only be modified by system administrator, user grouping mechanism is very similar to role mechanism. Roles can also be implemented based on user groups, in which a role links to the privileges of the user group.

3.2. Adversary Model

In this section, we pinpoint three potential weaknesses that could be exploited by adversaries as follows: role credential leakage, administrator compromise, and a mismatch between the number of users and roles.

The role's credential may be disclosed, whether it is an intentional attack, an unintentional error, or a random failure. Attackers can impersonate designated roles to obtain unauthorized permissions by obtaining the credentials, e.g., a login password.

During the grouping process, all user groups are grouped by administrators. We assume that administrators may be compromised. As a result, attackers can be included into any groups they want to join. Although it is difficult in reality, it is preferable to assume stronger adversary for better security.

We observe that, in the BIM model, the number of users may be much larger than the number of roles, thus mismatch exists between them. This mismatch leads to potential risks for BIM models. For example, some critical models (e.g., architecture, construction, and infrastructure data) may be revealed by unintended users and exposed to potential attackers that intend to access data illegally.

4. Proposed Scheme

4.1. Context-Aware Access Control

As BIM data are stored in cloud servers, the data may be accessed by requestors, or be updated by corresponding users who are responsible to the information. A secure data management issue thus arises: access control for the BIM data in cloud servers.

The access control has been explored for many years, and the mechanism becomes mature in traditional ICT domains. For example, RBAC is a typical one in which access rights are controlled according to requestor's roles. The data have different access rights, such as read, write, and execute (if applicable), and a user is assigned one role or multiple roles, corresponding to access rights to specified data. The key advantage of RBAC access control mechanism is that it can support a large number of users within much fewer roles and access control tables can be created easily. Furthermore, assigning rights to roles is more flexible than assigning rights to users directly. For example, if the right for accessing certain data is changed for a user, it can be done easily by changing the role of the user to another role.

We observe that the number of roles in BIM system context is usually rare. There exist four main roles in the BIM model:

1. Host: It represents investors for a building construction.
2. Designer: It represents building devisers or revisers.
3. Constructor: It represents executive and concrete builders of the building.
4. Supplier: It represents material providers for the constructors.

It is straightforward to deploy RBAC to facilitate access control in BIM. However, we observer that the numbers of users and subjects in terms of BIM models are usually large but the number of roles is usually small, thus there exists a mismatch between them. Such mismatch will induce certain risks of BIM model breach. Besides, passwords for designated roles may be incidentally exposed or hacked by attackers intentionally. As there are much fewer roles are than users, it may not be flexible to change the accessing privileges of a role. (It will influence all users in this role.) To tackle these problems, we propose incorporating the context information along roles in access control for BIM in the following.

We list certain major notations used in the remainder of the paper in Abbreviations.

For better understanding and emphasis, we induce the following notation.

Definition 1. *Role Revealing Attack (RRA). It works for leaking the credential of a role, whether by intentionally attack, or by unintentionally mistakes and random failure.*

Next, we present our access control model.

Definition 2. *User (U): It represents users who will access BIM data.*

Definition 3. *User (UG): It represents user groups who will access BIM data.*

Definition 4. *Subject (S): It represents data in BIM servers awaiting for accessing.*

Definition 5. *Role (R): It represents a title with an authority level for accessed subject.*

Definition 6. *Operation (O): It represents the operating right for an accessed subject, for example, read, write, execute, and so on.*

Definition 7. *Permission (P): It represents the operation combinations for an accessed subject.*

Definition 8. *Subject Assignment (SA): A subject is assigned to a role.*

Definition 9. *Permission Assignment (PA): A permission is assigned to a role.*

Definition 10. *User Assignment (UA): A user is assigned to a role.*

Definition 11. *User Group Assignment (UGA): A user group is assigned to a role.*

Definition 12. *Context (C): The extra condition for regulating the access permission for a role with respect to a subject.*

We propose a Context-aware RBAC called CaAC model as follows:

1. $UA \subseteq U \times R$, where UA is a user assignment relation; U is a set of users; and R is a set of roles. The user assignment is a relation of users and roles. A user may possess multiple roles and a role may be possessed by multiple users.
2. $UGA \subseteq UG \times R$, where UGA is a user group assignment relation; UG is a set of user groups; and R is a set of roles. The user assignment is a relation of user groups and roles. A user group may possess multiple roles and a role may be possessed by multiple groups.
3. $\mathsf{AssignedUser}(\cdot) : r \in R \rightarrow 2^U$. $\mathsf{AssignedUser}(\cdot)$ is a function to describe user assignment (UA) procedure. It is a function from R to 2^U, which means a role is assigned to a user or multiple users. 2^U is a set of sets in which elements are users. It cannot be onto, as some users may not be an image of a role. It can be one-to-one, as some users may be an image of multiple roles. It is a function, as one role can only map to one set of users.
4. $\mathsf{AssignedUsergroup}(\cdot) : r \in R \rightarrow 2^{UG}$. $\mathsf{AssignedUser}(\cdot)$ is a function to describe user group assignment (UGA) procedure. It is a function from R to 2^{UG}, which means a role is assigned to a user group or multiple user groups. 2^{UG} is a set of sets in which elements are user groups. It cannot be onto, as some user groups may not be a image of a role. It can be one-to-one, as some user groups may be a image of multiple roles. It is a function, as one role can only map to one set of user groups.
5. $\mathsf{AssignedUser}(r) = \{u \in U | (u, r) \in UA\}$. It is a set of users for a given role. It can also be seen as the range of function $\mathsf{AssignedUser}(\cdot)$ for given r. That is, they are all users who are assigned a given role r. The range of the function is all $u \in U$ where $(u, r) \in UA$.
6. $\mathsf{AssignedUsergroup}(r) = \{ug \in UG | (ug, r) \in UGA\}$. It is a set of user groups for a given role. It can also be looked as the range of function $\mathsf{AssignedUsergroup}(\cdot)$ for given r. That is, they are all user groups who are assigned a given role r. The range of the function is all $ug \in UG$ where $(ug, r) \in UGA$.

7. $P = 2^O$, where P is a set of permissions and O is a set of operations such as read, write, and execute. P is a set of sets in which elements are operations.
8. $PA \subseteq P \times R$, where PA is a permission assignment relation. PA means a relation of permission set P and role set R.

   Instead, $PA_c \subset P \times R \times C$. A permission is assigned to a combination of R and C. The $R \times C$ can define a proper permission for the further access. Roughly speaking, when and only when the specification of role and that of context are both guaranteed, assigned permission will be possessed.

   Note that, this part is only for CaAC, but the traditional RBAC is the previous one. This presentation way can point out the distinction between two methods.
9. $\mathsf{AssignedPermission}(\cdot) : r \in R \rightarrow 2^P$, where $\mathsf{AssignedPermission}(\cdot)$ is a function to assign a permission or multiple permissions to a role.

   Instead, $\mathsf{AssignedPermission}(\cdot) : r \in R \times c \in C \rightarrow 2^P$, where $\mathsf{AssignedPermission}(\cdot)$ is a function to assign a permission to a combination of role and context. Note that, when and only when the specification of role and that of context are both satisfied, the permission will be possessed.
10. $\mathsf{AssignedPermission}(r) = \{p \in P | (p, r) \in PA\}$. It is a set of privileges for a given role. It can also be looked as the range of function $\mathsf{AssignedPermission}(\cdot)$ for a given inputting. The range of the function for a given r is all $p \in P$ where $(p, r) \in PA$.

    Instead, $\mathsf{AssignedPermission}(r, c) = \{p \in P | (p, r, c) \in PA_c\}$. It describes the range of function $\mathsf{AssignedPermission}(\cdot)$ for given r and c. The range of the function is all $p \in P$ where $(p, r, c) \in PA_c$.
11. $\mathsf{UserSubjects}(\cdot) : u \in U \rightarrow 2^S$, where U is a set of users and S is a set of subjects.
12. $\mathsf{SubjectRoles}(\cdot) : s \in S \rightarrow 2^R$, where S is a set of subjects and R is a set of roles.
13. $\mathsf{SubjectRolesContexts}(\cdot) : s \in S \rightarrow 2^R \times 2^C$, where S is a set of subjects, R is a set of roles, and C is a set of context.
14. $\bigcup_{r \in \mathsf{SubjectRoles}(s)} \mathsf{AssignedPermision}(r)$. This set includes all permissions of the roles that can access the subject s. That is, all permissions for the subject s.
15. $\bigcup_{r,c \in \mathsf{SubjectRolesContexts}(s)} \mathsf{AssignedPermision}(r, c)$. This set includes all permissions of the roles that can access the subject s in all related context. That is all permissions for the subject s.
16. $\mathsf{creatnewUG}(\cdot)$: This is a function to create a new user group. When it is found that the original user group does not meet the use requirements, a new user group (UG) is created.

4.2. Constraint Condition

In this section, we propose some constraints based on above basic model.

1. $\mathsf{Constrain}(1) = \{\forall (P_i, R_i, C_i) \in PA_c \bigwedge (P_j, R_j, C_j) \in PA_c | P_i \neq P_j\}$. To ensure that access privileges between different roles in BIM data are mutually exclusive, mapping relationship between roles and privileges in CaAC presents following constraints: identical access authorization is not allowed to be assigned to different roles.
2. $\mathsf{Constrain}(2) = \{\exists U_a \in UG_1 \bigwedge U_b \in UG_1 \bigwedge P_a \subset P_b | P_{UG} = P_a\}$. To improve security, the principle for minimum permissions is adopted. If there exists conflict in member permissions within the same user group (role), then the minimum permissions are adopted.
3. $\mathsf{Constrain}(3) = \{\exists U_a \in UG_1 \bigwedge U_b \in UG_1 \bigwedge P_a \wedge P_b = \phi | creatnewUG(.)\}$. User A and User B are compared with other user groups. If the inclusion relationship or equivalent relationship still does not exist, then a new user group will be created, and User A or User B will be placed in the new user group.
4. $\mathsf{Constrain}(4) = \{\exists U_a \in UG_1 \bigwedge U_a \in UG_2 | P_a = P_{UG1} + P_{UG2}\}$. To ensure that the number of permissions does not decrease after grouping, if a user belongs to more than one user groups, the user's permissions are set to a union of permissions in the user groups.

5. To ensure fair grouping of multiple users, when a new user requests accessing, administrators will be aware of all members in the original user group, and processes properly according to above policies.

4.3. Proposed Authorization Rules

Rules for basic model: When a user initiates an request to access BIM data, servers firstly obtain the permissions of the user according to users and permissions mapping table. Secondly, the user is added to corresponding user groups based on permissions. In addition, the user's permissions are also added to the user group's permissions. However, if there exists no permission relationship between the user and others, a new user group is immediately created. The next step is granting roles to the user group which activates by launching a session. When the user requests to access BIM data again, the permissions are assigned according to the roles of the user group. Finally, servers compare the user's requirements with permissions, and determine whether the requirements are satisfied. Access is allowed if they are satisfied, otherwise access is not allowed.

Rules for advanced model: When a user initiates a request to access BIM data, servers firstly obtain the requirements of the user according to corresponding contexts. Secondly, the user is added to the corresponding user groups based on requirements. In addition, the user's permissions are also added to the user group's permissions. However, if there are no requirements relationships between the user and others, a new user group is immediately created. The next step is granting roles to the user group that activates by launching a session. When the user requests access to the BIM data again, the permissions are assigned according to the roles of the user group. Finally, servers compare the user's requirements with permissions, and determine whether the requirements are satisfied. Access is allowed if they are satisfied, otherwise access is not allowed. Besides, to defend against RRA, we propose using dynamic electronic signature in advanced model.

4.4. Proposed Algorithms

In this section, we present our algorithms to achieve the above Context-aware and user grouping access control model. Although our model can formally specify the rationale in access control mechanisms, these proposed algorithms can facilitate the understanding of programmers in their implementations. In addition, some source codes have been deposited in [IEEE DATAPORT] repository.

The basic model assumes that user grouping is based on the user's privileges. In other words, users know privileges at the beginning of the login. The basic model can control different users to access fine-grained data, and improve the efficiency of the traditional RBAC model as well. The specification is shown in Algorithm 1.

Algorithm 1 Groups users according to initial user login privileges.

Input: $P_i, P_j, U_i, U_j,$
Output: $U_i \in UG_j, U_j \in UG_i, U_i \in U_{ij} and U_j \in U_{ij}$
while $P_i \wedge P_j \neq \phi$ **do**
if $P_i < P_j$
$P_{Uj} = P_{UGj} \Leftarrow P_{Ui}$
$result \Leftarrow U_i \in UG_j$
if $P_i > P_j$
$P_{Ui} = P_{UGi} \Leftarrow P_{Uj}$
$result \Leftarrow U_j \in UG_i$
if $P_i = P_j$ $creatnewUG(.)$
$P_{UGij} \Leftarrow P_{Ui} = P_{Uj}$
$result \Leftarrow U_i \in U_{ij} and U_j \in U_{ij}$
return *result*
end while

The basic model may not be sufficiently flexible. Once user privileges have changed, the corresponding roles need to be modified. We propose advanced model that groups rules according to contexts (e.g., time and location) to guarantee the flexibility of grouping. Besides, advanced model defends against RRA. We propose an authentication scheme by dynamic electronic signature. The main idea is described in Algorithm 2 that groups users according to contexts (e.g., time and location).

Algorithm 2 Groups users according to contexts.

Input:$Req_i, Req_j, U_i, U_j,$
Output:$U_i \in UG_j, U_j \in UG_i, U_i \in U_{ij} and U_j \in U_{ij}$
while $Req_i \wedge Req_j \neq \phi$ **do**
if $Req_i < Req_j$
$Req_{Uj} = Req_{UGj} \Leftarrow Req_{Ui}$
$result \Leftarrow U_i \in UG_j$
if $Req_i > Req_j$
$Req_{Ui} = Req_{UGi} \Leftarrow Req_{Uj}$
$result \Leftarrow U_j \in UG_i$
if $Req_i = Req_j$ $creatnewUG(.)$
$Req_{UGij} \Leftarrow Req_{Ui} = Req_{Uj}$
$result \Leftarrow U_i \in U_{ij} and U_j \in U_{ij}$
return*result*
end while

Next, we analyze the complexity of the algorithm. In terms of time and frequency, n is called the scale of the problem. When n is constantly changing, the time $T(n)$ will change consequently. The number of repetitions of the basic operation in the algorithm is a function of the problem scaling in n, which is represented by $T(n)$. If there exists an auxiliary function $f(n)$, such that, when n approaches infinity, the limit value of $T(n)/f(n)$ is a constant, then $f(n)$ is called the same order of magnitude function of $T(n)$, denoted as $T(n) = O(f(n))$. We call $O(f(n))$ the progressive time complexity of the algorithm, and abbreviate it as time complexity. In this paper, we assume that there are n users, and there exists only one loop in the algorithm. Roughly speaking, the complexity of the algorithm is $O(n)$, which means that the amount of data increases several times and the time consumed also increases several times. $O(n)$ algorithm can process about 10^8 magnitudes of data.

Aiming at the problem of strong attack on Role Revealing Attack, we propose dynamic electronic signature over access control. Considering signing a data file in BIM system, due to the uncertainty of the number of directories, the directory page after the signature page cannot be effectively determined. We use dynamic signature key and feature recognition technology in BIM system to achieve accurate identification of signature page. It can also effectively ensure uniqueness, correctness and validity of BIM data.

The BIM master data generated in electronic signature is usually original information for entire building lifecycle, e.g., architectural design drawings, while data attribute document is attribution information, including creators, creation time, construction stages, technical status, data classification, level of secrecy, etc. Figure 2 describes the method of dynamic electronic signature. The process of obtaining dynamic page number is included, and key feature set F and signature page number p are added to the electronic configuration template. The concrete steps are as follows:

1. The BIM system obtains a visual PDF file of BIM database master data and uses Adobe interface to parse PDF file into N feature set G_n.
2. The BIM system parses electronic signature configuration template to obtain key feature set F.
3. The BIM system combines the key feature set F with the feature set G_n. If it does, go to Step 4; Otherwise, go to Step 5.
4. Get the value of the page number p collected by the signature key in the graphics document and pass the value to the electronic signature configuration template.

5. Show tips for exceptions, and prompt for the correct template to ensure that the file template used by users satisfies the requirements of the development template.

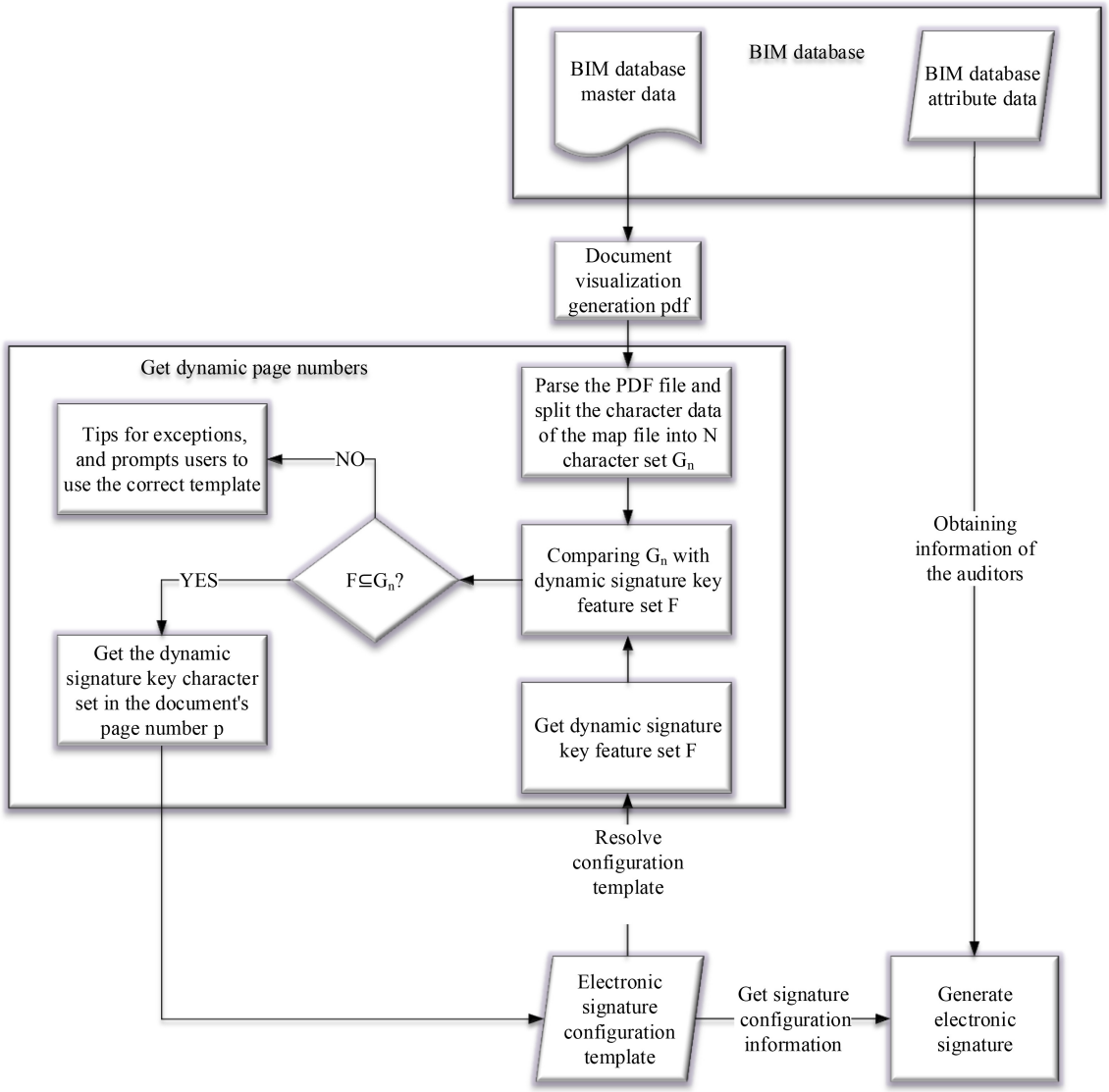

Figure 2. Dynamic signature method.

4.5. Examples: Location-Aware or Time-Aware

BIM data may include the following BIM models at different stages of a life cycle of a building:

(1) Design Models: Building, structure, hydropower and wind, performance simulation, environment and infrastructure.
(2) Construction model: Subdivide the design model according to the construction steps.
(3) Schedule model (4D): Linking model objects in a project according to schedule.
(4) Cost Model (5D): Linking objects to the cost and time of the project.
(5) Manufacturing Models: Using 3D models instead of traditional plane drawings to manufacture building components.
(6) Operational model: Used to simulate operations management, maintenance and mid- term updates.

As the access of BIM cloud servers is always pervasive at different locations, we propose using location information of accessors to further constrain the access right so as to provide a fine-grained access control.

Example 1. *A designer may access the BIM data at the construction fields, at home, or in the offices. In traditional RBAC, no matter where she is, she will be granted the same permission for accessing the BIM data. It may provide certain convenience in some situations, but it may also create risk in terms of privilege leakage, for example, the malicious codes at home computer may steal the password for the role. In CaAC, the designer can access 3D data in offices, which cannot be accessed in construction fields, while 2D data can be accessed in construction fields.*

Thus, to specify the permission for a role in different locations, a location information may be induced to distinguish, e.g. contexts. That is, the permission is related to not only roles, but also locations. The administrators can group users in different areas according to location context, and then assign roles.

Another context that may be encountered is time, i.e. the time of accessing BIM data. Similarly, we propose a time-aware RBAC that can incorporate time constraints into access control, especially with respect to the same role. Material suppliers may access BIM data during office hours or on holidays. MCBIM server can guarantee the successful access during office hours, but not on holidays. According to the context, the users in this time period are divided into a group and the roles are granted. It cannot be accomplished in naive RBAC, but can be achieved in time-aware RBAC model.

Similar to location-aware RBAC, time-aware RBAC can be described as follows. As above, only the main functions are provided for simplicity:

1. $T = UGT \cup RT$, where T is a time; UGT is a user group time; and RT is a role time. Here, we present two variants in a contrast way in parallel.
2. $UGA \subseteq UG \times R$. The user group assignment is a relation between user groups and roles.
3. $PA \subseteq R \times UGT \times P \times RT$. A permission is assigned to a combination of RT and UGT. The $RT \times UGT$ can define a proper permission for the further access. Roughly speaking, when and only when the specification of role and that of context are both guaranteed, assigned permission will be possessed.
4. $\mathsf{AssignedUsers}(\cdot) : r \in R \rightarrow 2^{UG}$. Each role will be assigned to one or multiple user groups.
5. $\mathsf{AssignedPermission}(\cdot) : r \in R; t \in UGT \rightarrow 2^{(P \times RT)}$. That is, for each role and user group time, the combinations of permission and role time are assigned.

Example 2. *Material suppliers for a construction project usually access BIM data during office hours or non-working hours (e.g., at midnight or 15:00). BIM server can guarantee the successful access during office hours, but not during suspected attacking hours, especially for certain critical data. It cannot be accomplished in naive RBAC, but can be achieved in CaAC model with time context.*

Furthermore, Context-aware can be further extended to other instantiation of context. In addition to location and time, the context can be any other condition related to access right. The detailed model for Context-aware RBAC is similar to location-aware RBAC and time-aware RBAC. The latter two are presented not only as an instantiation of CaAC, but also as a sample for the concrete construction of access models.

5. Security and Performance Analysis

Comparison between CaAC and RBAC

In this section, we compare two models proposed in this paper with the traditional RBAC model in five aspects, and analyze security and feasibility. The specific comparison results are shown in Table 1.

Table 1. A comparison between the CaAC model and the traditional RBAC.

Characteristic \ Model	RBAC	Basic CaAC	Advanced CaAC
Privilege management	Constraints are set for each permission, which is prone to errors in the process of permission allocation. With the increase of functional modules in the system, the number of permissions is huge, and it is difficult to achieve effective management.	Grouping rules are based on user login permissions, more fine-grained than RBAC.	Grouping according to context user request, more fine-grained than RBAC.
Flexibility	Flexibility is extremely poor. If any part of the session changes, the user needs to recreate the session and activate the user role.	Flexibility is at a moderate level, and if user's permissions change upon login, she needs to be grouped again.	The user's roles or login permissions have changed without requiring all steps in the model to be repeated.
Data security	With the increasing number of people involved and the growing size of databases, this model obviously can not meet the security of data.	Because of adopting grouping strategy, data security can be satisfied.	Dynamic electronic signature is adopted to ensure the security of data.
Efficiency	Efficiency and its inefficiency, to give each user of the system one by one authorization (role), is a very cumbersome thing.	Efficiency is the highest. Privileges and roles should be set first to form access control tables. Grouping and authorization only need to look up tables upon requests.	Efficiency is moderate. Users login first and then be grouped according to requests, while permissions can be granted directly to each group.

Confidentiality and Integrity: The former means data are guaranteed not to be disclosed to unauthorized users. The latter means data cannot be tampered (e.g., insertion, modification, deletion, and reordering) without authorization during storage. Both proposed models can prevent unauthorized access and tampering behavior.

Defending against Role Revealing Attack: We propose dynamic electronic signature over access control. That is, BIM system equips accurate identification of signature pages. Key feature recognition can effectively solve the risks of Role Revealing Attack and ensure the uniqueness, correctness and validity of BIM data.

Flexibility: Flexibility refers to the convenience of mapping relations between users and roles, and reconfiguring roles and privileges on demand. In traditional RBAC model, flexibility imposes difficulties in recreating sessions and activates updated roles. In basic model, flexibility is improved. Since grouping rules stem from permissions upon login, they still need to be grouped if the permissions change. In advanced model, it is not necessary to re-perform all steps, even if roles or login permissions change. It is independent of the permissions upon login, and only depends on contexts.

Efficiency: When data volume is huge or the number of users is large, traditional RBAC model may be inefficient in authorizing each user in the system sequentially. Thus, grouping users and authorizing user groups in a batch will be more efficient. Furthermore, advanced model is less efficient than the basic model. The specific quantitative analysis process is as follows:

1. Worst case: There is no inclusion relationship between users and user requests, thus grouping needs n times.
2. Average case: If there are p users and other q users with inclusion relationship ($p + q < n$), the remaining $(n - p - q)$ users need to group $(n - p - q)$ times. $(p + q)/2$ coincidence elements are generated in the inclusion relationship. The efficiency is improved by $n/(n - p - q + (p + q)/2) = 2n/(2n - p - q)$.
3. Best case: All users and user requests have inclusion relationship, thus grouping only occurs once. The efficiency increases n times.

6. Conclusions

We analyzed the limitation in traditional role-based only access control mechanism. As the number of mobile users is much larger than the number of roles, naive role-based access control may not be suitable in BIM situations. We thus propose a Context-aware fine-grained access control, called CaAC. We describe the functions of CaAC by formal method and present several illustrations on contexts via location-aware access control and the time-aware access control. CaAC can guarantee the

access control within the same role by differentiating contexts, which is more fine-grained than current role-based only access control. We also present grouping algorithms of two models. By comparing the proposed models with traditional RBAC model, we analyze the security and feasibility. As a result of analysis, we conclude that the average efficiency is improved by $2n/(2n-p-q)$, and the time complexity of the proposed algorithm is $O(n)$.

Author Contributions: Conceptualization, R.Z.; Methodology, W.R.; Project administration, R.Z.; Resources, J.J.; Software, X.H.; Supervision, R.Z.; Validation, F.X. and T.Z.; Writing—original draft, X.H.; and Writing—review and editing, W.R.

Funding: This research was funded by National Key R&D Program of China: No. 2016YFC0702107.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CS	Cloud Servers
MC	Mobile Clients
RRA	Role Revealing Attack
BIM	Mobile Cloud BIM (with Blockchain Enhancement)
RBAC	Role Based Access Control
CaAC	Context-aware RBAC
U	User
R	Role
S	Subject
P	Permission
SA	Subject Assignment
PA	Permission Assignment
C	Context

References

1. Barlish, K.; Sullivan, K. How to measure the benefits of BIM—A case study approach. *Autom. Constr.* **2012**, *24*, 149–159. [CrossRef]
2. Linderoth, H.C.J. Understanding adoption and use of bim as the creation of actor networks. *Autom. Constr.* **2010**, *19*, 66–72. [CrossRef]
3. Elghamrawy, T.; Boukamp, F. Managing construction information using rfid-based semantic contexts. *Autom. Constr.* **2010**, *19*, 1056–1066. [CrossRef]
4. Isikdag, U. Design patterns for bim-based service-oriented architectures. *Autom. Constr.* **2012**, *25*, 59–71. [CrossRef]
5. Razavi, S.N.; Haas, C.T. Multisensor data fusion for on-site materials tracking in construction. *Autom. Constr.* **2010**, *19*, 1037–1046. [CrossRef]
6. Coyne, E.; Weil, T. An rbac implementation and interoperability standard: The incits cyber security 1.1 model. *IEEE Secur. Priv.* **2008**, *6*, 84–87. [CrossRef]
7. Ferraiolo, D.; Kuhn, R.; Sandhu, R. Rbac standard rationale: Comments on "a critique of the ansi standard on role-based access control". *IEEE Secur. Priv.* **2007**, *5*, 51–53. [CrossRef]
8. Franqueira, V.N.L.; Wieringa, R.J. Role-based access control in retrospect. *Computer* **2012**, *45*, 81–88. [CrossRef]
9. Xu, M.; Wijesekera, D.; Zhang, X. Runtime administration of an rbac profile for xacml. *IEEE Trans. Serv. Comput.* **2011**, *4*, 286–299.
10. Zhao, J.; Wang, L.; Tao, J.; Chen, J.; Sun, W.; Ranjan, R.; Kolodziej, J.; Streit, A.; Georgakopoulos, D. A security framework in G-Hadoop for big data computing across distributed Cloud data centres. *J. Comput. Syst. Sci.* **2014**, *80*, 994–1007. [CrossRef]
11. Perera, C.; Ranjan, R.; Wang, L. End-to-End Privacy for Open Big Data Markets. *IEEE Cloud Comput.* **2015**, *2*, 44–53 [CrossRef]

12. Perera, C.; Ranjan, R.; Wang, L.; Khan, S.U.; Zomaya, A.Y. Big Data Privacy in the Internet of Things Era. *IT Prof.* **2015**, *17*, 32–39 [CrossRef]
13. Ren, Q.; Tan, D.; Tan, C. Research of sustainable design based on technology of bim. In Proceedings of the 2011 International Conference on Remote Sensing, Environment and Transportation Engineering (RSETE'11), Nanjing, China, 24–26 June 2011; pp. 4322–4324.
14. Yoon, S.; Park, N.; Choi, J. A bim-based design method for energy-efficient building. In Proceedings of the2009 Fifth International Joint Conference on INC, IMS and IDC (NCM'09), Seoul, Korea, 25–27 August 2009; pp. 376–381.
15. Vozzola, M.; Cangialosi, G.; Turco, M.L. BIM use in the construction process. In Proceedings of the International Conference on Management and Service Science (MASS'09), Wuhan, China, 20–22 September 2009; pp. 1–4.
16. Kokorus, M.; Eyrich, W.; Zacharias, R. Innovative approach to the substation design using Building Information Modeling (BIM) technology. In Proceedings of the 2016 IEEE/PES Transmission and Distribution Conference and Exposition (TD16), Dallas, TX, USA, 5 May 2016; pp. 1–5.
17. Wang, X.; Love, P.E. BIM + AR: Onsite information sharing and communication via advanced visualization. In Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD'12), Wuhan, China, 23–25 May 2012; pp. 850–855.
18. Garcia-Fernandez, J.; Anssi, J.; Ahn, Y.; Fernandez, J.J. Quantitative + qualitative information for heritage conservation an open science research for paving 'collaboratively' the way to historical-BIM. In Proceedings of the 2015 Digital Heritage, Granada, Spain, 28 September–2 October 2015; pp. 207–208.
19. Bottaccioli, L.; Aliberti, A.; Ugliotti, F.; Patti, E.; Osello, A.; Macii, E.; Acquaviva, A. Building Energy Modelling and Monitoring by Integration of IoT Devices and Building Information Models. In Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC17), Turin, Italy, 4–8 July 2017; pp. 914–922.
20. Pasini, D.; Ventura, S.M.; Rinaldi, S.; Bellagente, P.; Flammini, A.; Ciribini, A.L.C. Exploiting Internet of Things and building information modeling framework for management of cognitive buildings. In Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2'16), Trento, Italy. 12–15 September 2016; pp. 1–6.
21. Desogus, G.; Quaquero, E.; Sanna, A.; Gatto, G.; Tagliabue, L.C.; Rinaldi, S.; Ciribini, A.L.C.; Di Giuda, G.; Villa, V. Preliminary performance monitoring plan for energy retrofit: A cognitive building: The "Mandolesi Pavillon" at the University of Cagliari. In Proceedings of the 2017 AEIT International Annual Conference, Cagliari, Italy, 20–22 September 2017; pp. 1–6.
22. Arslan, M.; Riaz, Z.; Munawar, S. Building Information Modeling (BIM) Enabled Facilities Management Using Hadoop Architecture. In Proceedings of the Portland International Conference on Management of Engineering and Technology (PIC MET17), Portland, OR, USA, 9–13 July 2017; pp. 1–7.
23. Yuan, Y.; Jin, Z. Life Cycle Assessment of Building Energy in Big-Data Era: Theory and Framework. In Proceedings of the 2015 International Conference on Network and Information Systems for Computers, Wuhan, Beijing, 20–22 May 2015; pp. 601–605.
24. Ferguson, H.; Vardeman, C.; Nabrzyski, J. Linked data view methodology and application to BIM alignment and interoperability. In Proceedings of the 2016 IEEE International Conference on Big Data (Big Data'16), Washington, DC, USA, 5–8 December 2016; pp. 2626–2635.
25. Ding, L.; Zhou, Y.; Akinci, B. Building Information Modeling (BIM) application framework: The process of expanding from 3D to computable nD. *Autom. Constr.* **2014**, *46*, 82–93. [CrossRef]
26. Dawood, M.H. BIM based optimal life cycle cost of sustainable house framework. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC'16), Muscat, Oman, 15–16 March 2016; pp. 1–5.
27. Pan, J.Y.; Zhao, Y.Y. Research on Barriers of BIM Application in China's Building Industry. *J. Eng. Manag.* **2012**, *1*, 6–11.
28. Mohd, S.; Latiffi, A.A. Building Information Modeling (BIM) application in construction planning. In Proceedings of the 7th International Conference on Construction in the 21st Century (CITC-VII), Bangkok, Thailand, 19–21 December 2013,

29. Ferreira, C.; Resende, R.; Martinho, S. Beacons and BIM Models for Indoor Guidance and Location. *Sensors* **2018**, *18*, 4374. [CrossRef] [PubMed]
30. Betarte, G.; Gatto, A.; Martinez, R.; Zipitria, F. Actkit: A framework for the definition and enforcement of role, content and context-based access control policies. *IEEE Latin Am. Trans.* **2012**, *10*, 1742 –1751.