Journal of Computer Science

Original Research Paper

A Design of MAC Model Based on the Separation of Duties and Data Coloring: DSDC-MAC

[1]Soon-Book Lee, [2]Yoo-Hwan Kim, [1]Jin-Woo Kim and [3]Chee-Yang Song

[1]*Headquaters, ROK Navy, 663, Gaeryong Dae-ro,*
Sindoan-Myeon Gaeryong-Si, Chungcheong Nam-Do, 32800, Korea
[2]*Department of Computer Science, University of Nevada Las Vegas (UNLV),*
4505 Maryland Parkway, Box 4019, Las Vegas, Nevada 89154-4019, USA
[3]*Department of Software, Kyungpook National University,*
2559, Kyeongsang Dae-ro, Sangju-Si, Gyeongsang Buk-Do 742-711, Korea

Article history
Received: 23-10-2019
Revised: 24-12-2019
Accepted: 17-01-2020

Corresponding Author:
Chee-Yang Song
Department of Software,
Kyungpook National
University, 2559,
Kyeongsang Dae-ro,
Sangju-Si, Gyeongsang
Buk-Do 742-711, Korea
Email: cysong@knu.ac.kr

Abstract: Among the access control methods for database security, there is Mandatory Access Control (MAC) model in which the security level is set to both the subject and the object to enhance the security control. Legacy MAC models have focused only on one thing, either confidentiality or integrity. Thus, it can cause collisions between security policies in supporting confidentiality and integrity simultaneously. In addition, they do not provide a granular security class policy of subjects and objects in terms of subjects' roles or tasks. In this paper, we present the security policy of Bell_LaPadula Model (BLP) model and Biba model as one complemented policy. In addition, Duties Separation and Data Coloring (DSDC)-MAC model applying new data coloring security method is proposed to enable granular access control from the viewpoint of Segregation of Duty (SoD). The case study demonstrated that the proposed modeling work maintains the practicality through the design of Human Resources management System. The proposed model in this study is suitable for organizations like military forces or intelligence agencies where confidential information should be carefully handled. Furthermore, this model is expected to protect systems against malicious insiders and improve the confidentiality and integrity of data.

Keywords: Mandatory Access Control (MAC), SoD-driven Access Control, Data Coloring Access Control, Security Key Authorization, Complemented BLP and Biba Model

Introduction

In the Emerging Cyber Threats Report 2015 published by Georgia Tech, the attack of rogue insiders was pointed out as one of emerging cyber threats. Security incidents caused by malicious insiders bring about significant damage to companies, but solutions are not easy at all. To address such evolving threats from insiders, it is necessary to develop stronger access control technologies to detect anomalous behaviors. Due to the dynamics and uncertainty of the current network environment, access control is one of the most important factors in guaranteeing network information security. How to construct a scientific and accurate access control model is a current research focus. In actual access control mechanisms, users with high trust values bring better benefits, but the losses will also be greater once cheating access is adopted (Wang *et al*., 2019).

Earlier studies on access control can be grouped into three categories. First, some studies focus on controlling subjects (users, etc.) such as Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) (Bertino, 2003; Ferraiolo and Kuhn, 1992; Kuhn *et al*., 2010; Sandhu *et al*., 1996; 2000; United Nations, 2004), while some are about the expansion of such methods (Bertino *et al*., 2005; Kalinin *et al*., 2018; Sinha *et al*., 2018; Zhao and Chen, 2013) Second, techniques such as masking (Mansfield-Devine, 2014), digital watermarking (Kumar, 2019), image fusion (Gupta and Kumar, 2019) and encryption (Davida *et al*., 1981; Elovici *et al*., 2004) are aiming at strengthening the security of objects such as data. Third, those that consider both subjects and

Science Publications

objects include Mandatory Access Control (MAC). These methods, however, do not have clear and concrete security policies on access control for objects that indeed should have been protected primarily. Especially, existing MAC models have focused only on one thing, either confidentiality or integrity. Thus, it can cause collisions between security policies in supporting confidentiality and integrity simultaneously. The collision problem of security policy between the BLP and Biba models is shown in Fig. 5. In addition, since access control policies between subjects and objects at the same security level have not been subdivided to define them specifically, it has been difficult to maintain confidentiality and integrity. Even though the Lattice-Based Access Control (LBAC) model (Sandhu, 1993) showed that BLP model (Bell and LaPadula, 1975) and Biba model (Biba, 1997) emphasizing only confidentiality and integrity can be mathematically accommodated in a lattice in terms of information flow, but it was not address that the opposite policy between their models can be complemented into one security policy. In addition, it has not been able to create policies for granular security classes of sub-jects and objects in terms of subjects' roles or tasks.

Therefore, the vision or aim of this paper is to solve both the collision between security policies of BLP model and Biba model in order to guarantee confidentiality and integrity at the same time (Fig. 6). To do this, we present a complementary policy for BLP model and Biba model security policy, but we have studied a model that can provide granular access control in terms of Separation of Duty (SoD).

In order to address the ambiguity (collision) issue of security access control policies, this study presents a DSDC-MAC model that is developed using the principle of SoD and a data coloring technique. Based on the policies of the suggested model, at the aspect of tasks of users and objects are separated (integrity) and such classified individual subjects and objects are given certain colors according to their security level (confidentiality). In turn, the colors are matched with security keys (refer Fig. 8 and Fig. 9) to permit subjects to access or not to access objects (or data). In addition, detailed access control using SoD is enabled for security policies between subjects and objects with equivalent security level that previous studies have not suggested. Moreover, security can be strengthened in terms of subject and object mapping through the mechanism of granting and assigning access rights using security keys.

As shown in Fig. 1, according to the proposed concepts and principles above, the approach process for designing the DSDC-MAC model (Fig. 1) is as follows:

- The security requirements are first redefined
- The existing BLP and Biba models are compleme-nted each other
- The supplemented MAC model (CBB model: Complemented BLP and Biba model) by adding Separation of Duties policy is refined
- A security architecture based on the CBB model is designed and a detailed access control technique using SoD and Data coloring in detail is defined
- The security keys for matching between subject and object are specified to control user's access to objects
- A case studies and evaluations are discussed

Next Section analyzes the access control models from relevant studies. After that, following Section addresses the DSDC-MAC model using SoD and data coloring. Next Section presents the application case of the proposed model for a Human Resources Management System (HRMS). Then, next Section compares the existing models with the proposed one.

Relevant Studies

In this section, the characteristics and limitations of the MAC model among various access control models that have been studied to explain the direction and research purpose of this study are described. Next, the differences between the terminology being used in this article and the terminology of data coloring proposed in the legacy study and separation of duties are explained. Finally, the existing research methods for DB security are outlined.

Access Control Model

MAC is a model to control individual owners of objects. The centralized authority determines who should be granted access to what kinds of information and general users are unable to change access authority. Under this principle, MAC models (Kalinin *et al*., 2018), which determine access control rules by centralized security rules, guarantee data confidentiality and integrity that are not maintained in DAC systems that Owner decides on access control rules. However, it is difficult to determine security levels suitable for subjects and objects in advance and also not easy to apply.

Among the MAC-based models, BLP model, Biba models and LBAC models are representative. Focusing on confidentiality, the BLP prevents information from flowing from a higher security level to a lower security level. As shown in Fig. 2, the BLP model has two policies (No-read-up Policy and No-write-down Policy).

The BLP model allows high security subjects to read, but not write, objects of the same or lower level. Conversely, a low secure subject can write, but cannot read, objects of the same or higher level. In other words, although the confidentiality is emphasized so that a low security subject can't steal high-level data, it has a problem in terms of integrity that a low security subject can manipulate high-level documents.

On the contrary, as shown in Fig. 3, the Biba model (Biba, 1997) focusing on integrity is based on the security access class of subjects and objects. If a subject at a lower security is allowed to alter objects at higher security levels, the original reliability of data can be compromised as it is combined with less reliable information. The Biba model has No-read-down and No-write-up Integrity Policies.

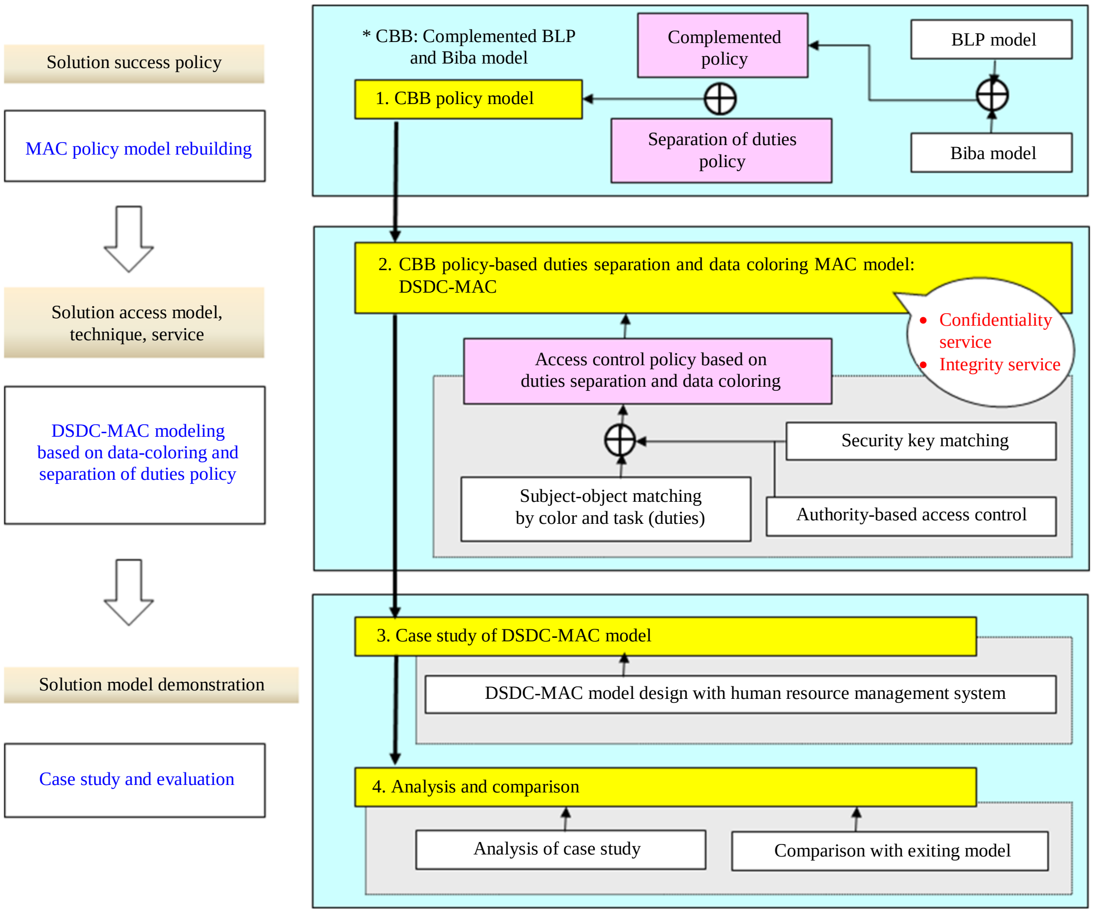
Solution success policy
MAC policy model rebuilding
Solution access model, technique, service
DSDC-MAC modeling based on data-coloring and separation of duties policy
Solution model demonstration
Case study and evaluation
* CBB: Complemented BLP and Biba model
Complemented policy
BLP model
1. CBB policy model
Separation of duties policy
Biba model
2. CBB policy-based duties separation and data coloring MAC model: DSDC-MAC
• Confidentiality service
• Integrity service
Access control policy based on duties separation and data coloring
Security key matching
Subject-object matching by color and task (duties)
Authority-based access control
3. Case study of DSDC-MAC model
DSDC-MAC model design with human resource management system
4. Analysis and comparison
Analysis of case study
Comparison with exiting model

Fig. 1: Approach process for designing the DSDC-MAC model

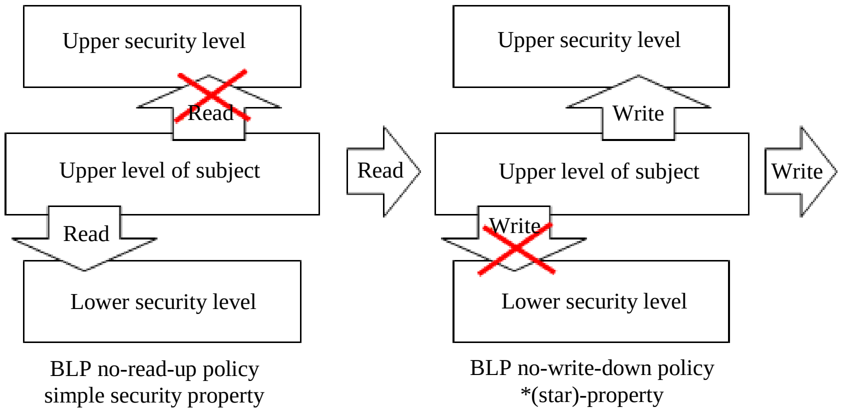

Fig. 2: Security policy of BLP model

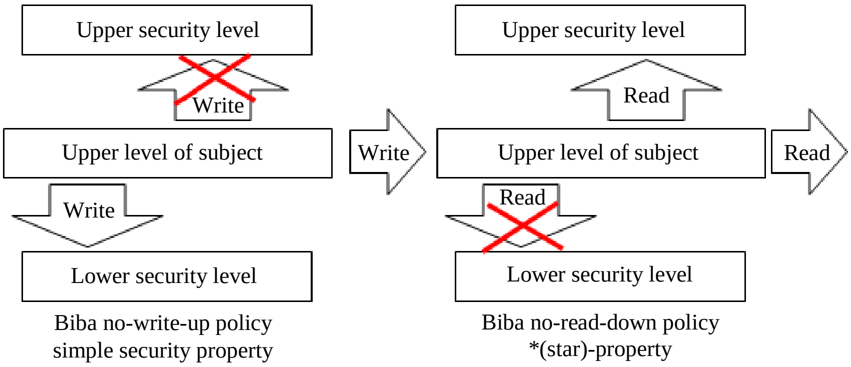

Fig. 3: Security policy of Biba model

The Biba model has a policy opposite to BLP model in Fig. 2. That is, a high security subject can use the same or lower class objects but cannot read them. Conversely, a low secure subject can read an equivalent or higher level object, but cannot write. In other words, it emphasizes integrity so that subjects with low security level cannot manipulate high-level documents, but rather, it is a model that has a problem in confidentiality that a low-security subject can steal high-level documents.

The LBAC model (Sandhu, 1993; Denning, 1976) is one of the most common models among the MAC models. To specify the multi-layer security policy, the dominate relation between the security levels and use lattice to specify the order is defined. In front, we mentioned the limitations of the security policy of BLP model and Biba model emphasizing only confidentiality and integrity respectively. Although it has been shown through several examples that each model can be mathematically accommodated within a lattice in terms of information flow, but it is not clear that the opposite of two models can be complemented into one policy.

Separation of Duties (SoD)

Headings SoD (Botha and Eloff, 2001) is a method for internal control associated with the execution of tasks. One task is divided into several duties and the duties are executed by multiple people to complete the task. This is designed to prevent any abuse of authority or mistakes that may occur in business processes. This concept (Botha and Eloff, 2001; Moon *et al*., 2004) started as a design principle for data protection in conventional computer systems and it has been defined as a requirement for various access control models including RBAC model. SoD was defined as separation of privilege in Saltzer and Schroeder (1975) among 8 design principles for the protection of information systems and it was also defined as a mechanism to guarantee the integrity of data by linking objects in systems to systems in the real world in Clark and Wilson (1987).

SoD literally means "separating authority" from a perspective of "subjects." To execute a task, its authority is separated and multiple people cooperate together doing their duties. From a perspective of data (objects), however, it is required to classify the objects into small-scale tasks to apply the SoD principle to them. This study suggests more segmented access control methods to secure integrity by classifying tasks classification criteria of objects into more segmented and small-scale data to apply SoD.

Data Coloring

The word, data coloring (Ceze *et al*., 2008), was first introduced as a technique to apply to programming models. Programmers select certain points and assign colors to them in a control flow in which the consistency of data needs to be secured. This was proposed as a programming model to control access simultaneously through data coloring. A new data coloring technique in Hwang and Li (2010) was suggested as a color matching technique to identify data and users. For the new technique, watermarking mechanism and fuzzy logic were used for cloud computing environments. In Liu *et al*. (2011), the data coloring technique suggested in Hwang and Li (2010) was applied as a cloud water-marking model and presented test results. In Sudha and Jamuna (2013), a cloud watermarking model using secure RSA algorithm was suggested as a regular authorization method. In other words, data coloring models that were presented in Hwang and Li (2010), Liu *et al*. (2011) and Sudha and Jamuna (2013) used software watermarking technology to allow the 1:1 access control between Subject (S) and Object (O) when sensitive data had to be shared in cloud environments.

Given that, earlier data coloring techniques are not suitable to classify levels of confidentiality as well as hierarchical authority levels of subjects and objects in this study.

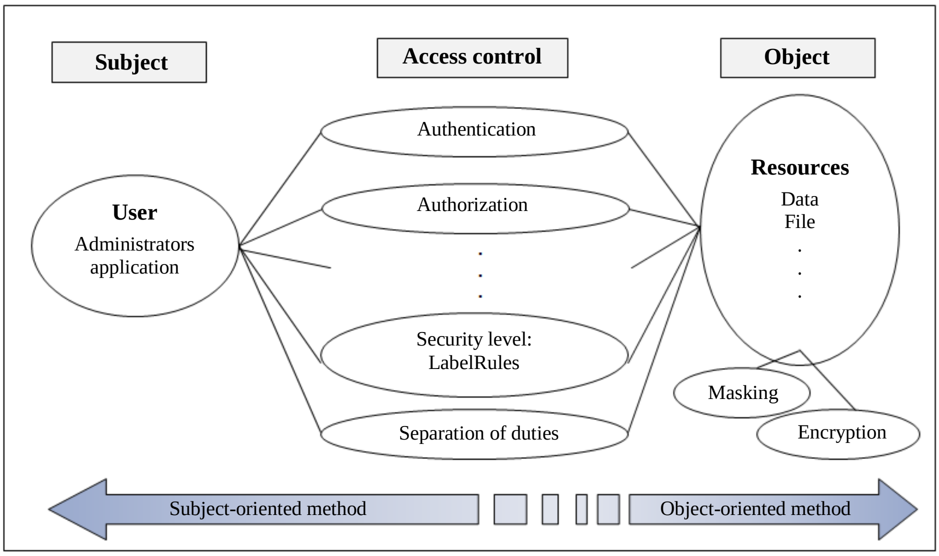

Fig. 4: Legacy methods of DB security

Legacy Methods of DB Security

As shown in Fig. 4, earlier studies on the security of Database (DB) can be grouped into Subject-Oriented Methods (SOMs), Object-Oriented Methods (OOMs) and Multilevel Security (MLS) methods that combined the two types.

SoD and Data Coloring based MAC Model: DSDC-MAC

In order to address collision issues between policies found in MAC models such as BLP and Biba, techniques of Separation of Duties and data coloring are used in this study. Through this method, this study aims to suggest a DSDC-MAC model that can provide more segmented access controls to users (subjects) and data (objects). In doing so, security keys are used as an authorization means for subjects and objects. To do this, this section defines the access control policies of MAC models and proposes security architecture of DSDC-MAC model and finally specifies access control technique based on SoD and data coloring.

Complemented Policy Model for Solving Policy Collision: CBB

Security Policy Collision between the BLP and Biba Models

The BLP model, one of the most representative MAC models, focuses on confidentiality, while the Biba model puts focus on securing integrity. If confidentiality and integrity need to be guaranteed simultaneously, all of the policies of the two models should be satisfied at the same time. In this case, as shown in Fig. 5, collisions between the access control policies of the two models occur inevitably.

The No-read-up Policy of the BLP model protects the confidentiality of higher-level secrets by preventing lower security levels from reading higher-level secrets. On the other hand, the Biba model prevents users at higher security levels from reading objects at lower security levels. General concepts of these access control policies are to prevent anything that are clearly not allowed and to allow anything that are clearly not prevented. Based on these concepts, the No-read-up Policy of the BLP model potentially means “possible-read-sibling and down.” In other words, this means that reading objects at the same level or lower levels is allowed. Therefore, this exactly collides with the No-read-down Policy of the Biba model. In addition, the No-write-down Policy of the BLP model potentially means “possible-write-sibling and up.” Again, this means that writing objects at the same level or higher levels is allowed. Therefore, this exactly collides with the No-write-up Policy of the Biba model.

Collisions between the policies of the BLP and the Biba models occur in the following cases.

Case 1. BLP Model "No-Read-Up" Policy ⇔ Biba Model "No-Read-Down" Policy

For instance, if there are some personnel who have the 2nd grade (Secret) authority in an organization, according to the BLP model policy, they can read the 2nd grade (Secret) and the 3rd grade (Confidential) information, but they are not allowed to read the 1st grade (Top Secret) information. According to the Biba model, however, the personnel can read the 2nd grade (Secret) and 1st grade (Top Secret) information, but they are not allowed to read the 3rd grade (Confidential) information. In this case, a question emerges like whether the personnel who have the 2nd grade (Secret) authority should be allowed to read Top Secrets in the Biba model and this arises from "confidentiality." In other words, there is a contradiction in the "No-read-down" Policy of the Biba model from the perspective of confidentiality.

Case 2. BLP Model "No-Write-Down" Policy ⇔ Biba Model "No-Write-Up" Policy

Like Case 1, if there are some personnel who have the 2nd grade (Secret) authority, according to the BLP model policy, they can write the 2nd grade and the 1st grade information, but they are not allowed to write the 3rd grade information. According to the Biba model, however, the personnel who have the 2nd grade authority can write the 2nd grade and 3rd grade information, but they are not allowed to write the 1st grade information. Again, a question emerges like whether the personnel who have the 2nd grade (Secret) authority should be allowed to write Top Secrets in the Biba model and this arises from "integrity." In other words, there is a contradiction in the "No-write-down" Policy of the BLP model from the perspective of integrity.

Requirements and Assumptions of Security Policy

In order to address such collision issues between policies of the BLP and Biba models and to guarantee both confidentiality and integrity, requirements for security policies should be defined as follows:

- *Req. 1.* Subjects who have higher-level authority can access objects at the same lev el and lower levels
- *Req. 2.* Subjects who have lower-level authority should not be allowed to access higher-level objects
- *Req. 3.* Subjects should be prevented from accessing secretes unrelated to their task

This means that in a relationship between a subject and object at the same level, a subject should be prevented from discretionarily accessing an object out of its task range. Even subjects who have higher-level authority should be also prevented from discretionarily accessing objects at lower levels out of their task range.

Assumptions for security to meet these requirements are as follows:

- *Ass. 1.* If a subject is allowed to read an object at a higher level than its security level, confidentiality is violated
- *Ass. 2.* If a subject is allowed to write an object at a higher level than its security level, integrity is violated
- *Ass. 3.* In an ordinary organization, users are not allowed to handle secret information unrelated to their task
- *Ass. 4.* In an ordinary organization, a subject who has higher-level authority assumes all the authority of subjects at lower levels

Complementary BLP and Biba Policy Model: CBB Policy Model

To meet the requirements discussed in above section, access control policies based on the MAC model are redefined as follows. In particular, the security policy rule for Req. 3 should be derived from the perspective of SoD, one of the basic principles for information security.

Rule 1: (No-Read/Write-Up Policy, * Simple Security Property) [Derived from Req. 1 and 2]

A subject who has lower-level authority is prevented from accessing objects at higher levels. A subject who has higher-level authority can access objects at the same level or lower levels. Allowing subjects at lower levels to read objects at higher levels raises confidentiality issues. In addition, allowing subjects at lower levels to write objects at higher levels violates integrity. This policy protects both confidentiality and integrity by preventing subjects who do not have access authority from accessing objects.

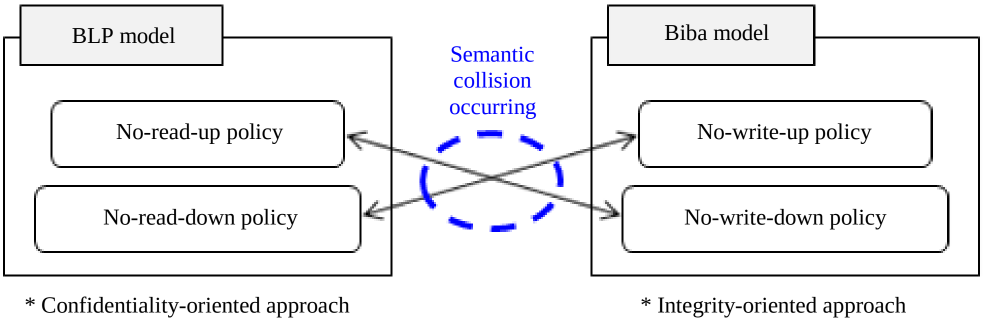

Fig. 5: Security policy collision between the BLP and Biba models

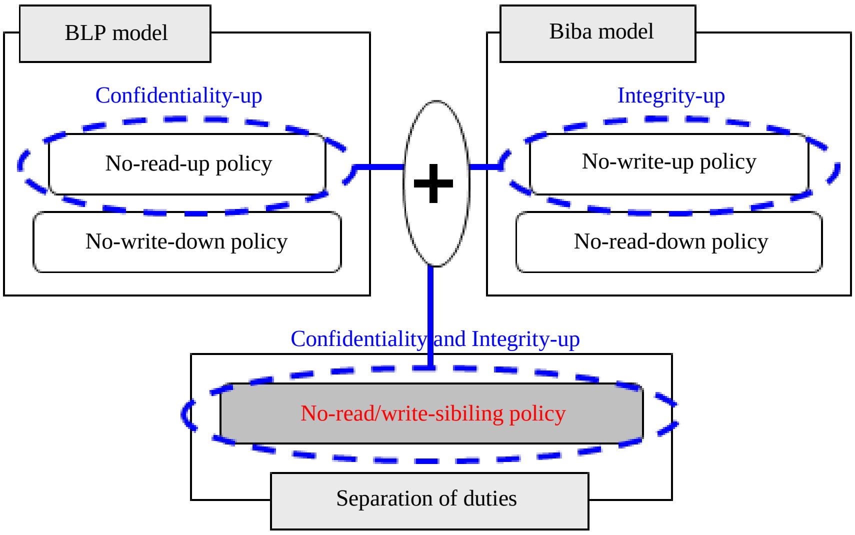

Fig. 6: Enhanced CBB policy model for solving policy collision between BLP and Biba model

Rule 2: (No-Read/Write-Sibling Policy, * Separation of Duties Property) [Derived from Req. 3]

"Sibling" is a word for "brother or sister" or "those having parents in common." In this study, siblings mean subjects and objects at the same security level and their tasks are classified based on the Rule 1. A subject at a certain level can access objects allowed within the same task category. It cannot access objects at higher levels even within the same task category as defined in Req. 1, but it can access objects at lower levels.

An enhanced CBB policy model for access control is shown in Fig. 6. This is based on the BLP and Biba models and coupled with SoD, this model can maintain confidentiality and integrity. This model combines the priority policy for confidentiality in the BLP model and that for integrity in the Biba model. By doing so, it is possible to exclude policies that cause collisions between the two models and to map the priority policies with the policies derived from the SoD principle. In other words, in terms of confidentiality, it prevents unauthorized subjects from accessing higher level objects for "read" and in terms of integrity, it prevents unauthorized subjects from accessing higher level objects for "write". That is why it drives to provide and improve the confidentiality and integrity and at the same time. In particular, at the same level, access is granted by classifying subjects and objects in detail by separation of duties. Thus, even at the same level, access to "read" and "write" can be denied without permission, further enhancing confidentiality and integrity.

As discussed in Cases 1 and 2, contradictions in terms of confidentiality and integrity are found in the existing BLP and Biba models. The CBB policy model suggested in this study addresses such issues and the explanation for the solutions is as follows:

[Contradiction]

- Cont. 1. The "No-read-down" Policy of the Biba model has a contradiction in terms of confidentiality
- Cont. 2. The "No-write-down" Policy of the BLP model has a contradiction in terms of integrity
- Cont. 3. Each policy of the BLP and Biba model has a contradiction in terms of both confidentiality and integrity between subjects and objects within the same level

[Explanation]

Confidentiality is a feature to prevent subjects, who have no authority or have lower-level authority, from accessing data to be protected. The "No-read-down" Policy of the Biba model in Cont. 1 means "Possible-read-up" and gives subjects at lower levels authority to read objects at higher levels. Therefore, Cont. 1 violates confidentiality.

Integrity is a feature to prevent subjects, who have no authority or have lower-level authority, from accessing and altering data to be protected. The "No-write-down" Policy of the BLP model in Cont. 2 means "Possible-write-up" and gives subjects at certain levels authority to write objects at higher levels. Therefore, Cont. 2 violates integrity.

In Cont. 3, the "No-read-down" Policy of the Biba model means "Possible-read-sibling." The "No-write-down" Policy of the BLP model means "Possible-write-sibling." Therefore, a subject at a certain level cannot be classified by tasks. In other words, Cont. 3 violates both confidentiality and integrity since access authority for reading and writing is allowed to multiple objects at the same level. By separating duties for subjects and object at the same level, access can be controlled.

The CBB Policy model, under the ”No-read/write-up" rule, does not allow subjects at certain levels to access (read/write) objects at higher levels at all. In addition, by separating duties for subjects and object at the same level, access can be controlled. Therefore, the suggested policy addresses contradictions that the existing models have.

[Formal Definition]

The formal definition of the CBB policy to accommodate Rule1 and Rule2 derived above is as follows:

When and only when the security level SL(S) of a subject 'S' dominates or equal to the security level SL(S) of an object 'O' and the duty (task and/or sub_task) of a subject 'S' equal to the task of an object 'O', the subject 'S' has the “read/write/append/delete” access to the object 'O'.

Security Level (SL) consists of Upper Security Level (USL), Lower Security Level (LSL) and Sib-ling Security Level (SSL) and can have 1 to n security levels:

$$SL = \{USL, LSL, SSL\} \text{ and } \{SL1, SL2, - - - SLn\} \tag{1}$$

The level or degree of access permission defines as Security Level Function: *f*(*x*), The USL function: *fu*, the LSL function: *fl* and the SSL function: *fs*. The access permission level is defined as follows:

$$fux(S) \Rightarrow fsx(O) \text{ and / or } flx(O) \tag{2}$$

$$fly(S) \nRightarrow fuy(O) \tag{3}$$

Where:
“⇒” means “access permitted”,
“ $\nRightarrow$ ” means “access denied”

* Rule description: The security level of a specific subject (S) means that only an object (O) at an equal level and lower level can be accessed (2) but the object can't access to higher level (3).

When a subject (S) having a specific task is defined as a Subject in a certain task: St and an object (O) corresponding to a specific task is defined as an Object in certain task: Ot, the access permission of the security level to the object of the specific task by the subject of the specific task is defined as follows:

$$fux(Stn) \Rightarrow fsx(Otn) \text{ and / or } flx(Otn) \tag{4}$$

$$fly(Stn) \nRightarrow fuy(Otn) \tag{5}$$

$$fuy(Stn) \nRightarrow fsy(Otm) \text{ and / or } fly(Otm) \tag{6}$$

* Rule description: A specific upper level subject (S) having a specific task (tn) is accessible to an equal level and a lower level object (O) of a specific job (4). However, the lower level subject (S) having the specific task (tn) is that the access is limited to upper level object (5) and if the task is different even if it is a higher level, it means that it is not possible to access to object of the same and lower level (6).

Duties Separation and Data Coloring based MAC Model: DSDC-MAC

As shown in Fig. 7, the security structure of the Duties Separation and Data Coloring (DSDC)-MAC model is mainly composed of security level policy; separation of duties policy; data coloring rules and the relationship among subject, security key and object are applied to. For strict authorization, access has to go through the first authorization process based on Id (identification) and Password and the second authorization process based on security key to directly apply access control policies and additionally certify access. Security Key (SK) serve as a medium to link between a subject and an object. In the processes of security key authority and delegation policy, the security keys of individual subjects are authorized and assigned and users at the relevant security level can delegate security keys to others. Simple security property and separation of duties property, as complementary BLP and Biba model (CBB) policies, address collision issues between policies that were found in earlier studies in terms of confidentiality and integrity. They are also reflected in access control policies to ensure a subject can access an object while maintaining confidentiality and integrity.

Security Level Policy

Security levels of subjects and objects are determined based on those of the existing MAC models. Considering the military domain, they are classified as Top secret, Secret, Confidential and Unclassified (Ferraiolo and Kuhn, 1992; Sandhu *et al*., 1996). Persons in charge of each of the four security levels are described in Table 1. Objects can be files, data, etc., but data is mainly targeted for the consistency of expression here.

Separation of Duties Policy

To secure effective internal control and maintain confidentiality at each task level, tasks need to be separated according to security levels, but it is also necessary to segment access control based on the separated tasks. A subject’s access authority to objects is set by tasks based on the SoD policy. A subject, here, means a user who uses an object (for instance, data).

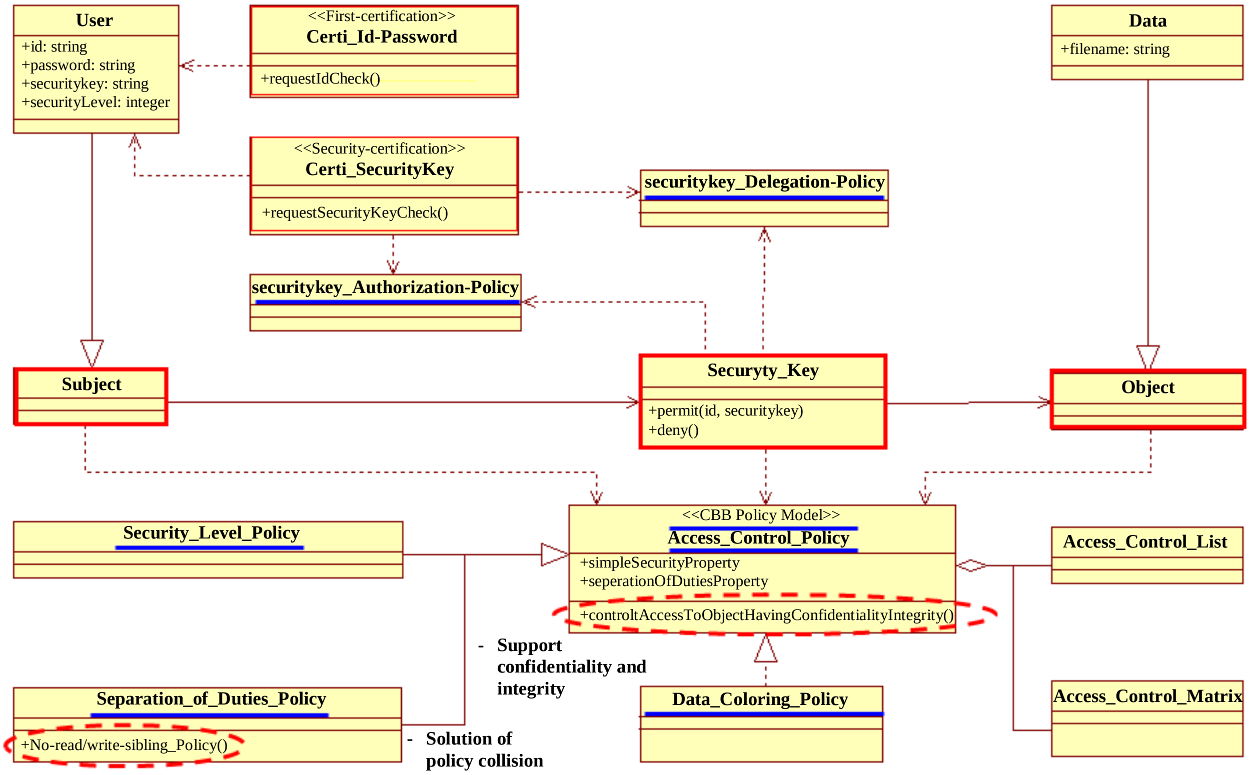

Fig. 7: Duties separation and data coloring-based MAC model for solving policy collision: DSDC-MAC

Table 1: Security level categories and persons in charge of objects

Security level	Person in charge of object
Top Secret	Top-Level Administrators in the organization
Secret	Middle Managers in the organization
Confidential	General Office Workers in the organization
Unclassified	All Persons in the organization (Non-Authorized Secret Handling)

Table 2: A 2-level task categorization scheme according to SoD policy and an example

Super category	Sub category
(a) categorization scheme	
Task #1	subTask #1_1
Task #2	subTask #1_2
Task #3	:
Task #4	subTask #2_1
:	:
Task #n	subTask #n_m
(b) Categorization example	
Affairs	Administration, affairs plans
Intelligence	Security, intelligence analysis
Operations	Ops plans, current ops, future ops
Logistics	Logistics plans, supply, maintenance, transportation
ICT	ICT plans, operations, information security

Tasks need to be grouped into, first, super-categories by their functions and, second, sub-categories within the same super-category. Depending on the size and characteristic of an organization, super-categories are needed only in some cases and for large-sized organizations, it will be necessary to segment tasks further beyond the second-level sub-categories. If necessary, more tasks can be added to sub-categories. Of course, the more category levels are created, the more difficulties the system faces. Table 2 shows the structure of task categories and examples for the military domain.

Data Coloring Policy

To Data coloring is a concept that was first developed to add identifiers to the confidentiality levels of data. Colors are assigned to data to allow users to intuitively recognize the confidentiality levels of data. It is possible to distinguish the levels simply by using arrays of numbers or levels as identifiers, but there is still ambiguity over how the criteria of identifiers should be set to distinguish confidentiality levels. However, it is possible to conveniently set criteria for confidentiality levels by applying the RGB coloring classification scheme suggested in this study. It is also possible to designate more segmented identifiers within each of the R, G and B groups.

Red, Green and Blue (RGB) colors are expressed as hexadecimal codes on a web page. Color values are specified as three pairs of two-digit hexadecimal values representing red, green and blue. When creating web-based colors, such hexadecimal notations are used and they start with a special symbol (#). The structure of color notations is shown in Table 3.

Around 16 million colors can be created through the 256 levels of RGB combinations. This can be utilized as a very systematic classification method using the web-based color notations above.

Table 4 shows security colors that are defined by wrapping the security levels of data (Table 1) with RGB colors. For instance, "red" color is assigned to "top secret" data, creating a security color, "SC_R" (SecurityColor_Red). General data categorized as "unclassified" are actually not the target objects of protection and thus they are excluded here and even from security keys later. Based on Table 1, security colors in Table 4 represent security levels of subjects and objects.

DSDC Access Control Technique based on SoD and Data Coloring

Subjects and Objects Matching by using Color and Task (Duties)

To provide segmented access controls, color codes are given to objects and subjects. Access can be controlled through the mechanism of matching the same color codes. In other words, individual security colors of subjects and objects (Table 4) are further segmented into color values by separating tasks (super- and sub-category tasks). Their color values are defined (Table 3) and individual identifiers of access authority are given as shown in Table 5. With these color codes, it is possible to easily identify security levels and tasks of subjects and objects and their access authority can be segmented by tasks. Codes shaded in gray are highlighted for convenience to intuitively recognize the colors of classified identifiers and thus they have nothing to do with the titles of identifiers. The color codes by tasks in Table 5 are generated based on the Rules 3 and 4 and the rule in Table 6.

Security colors are given to each security level and task and the rules for identification are as shown in Rules 3 and 4. The color values of security levels and tasks are as follows:

SC_R: #FF0000, ***SC_G***: #00FF00, ***SC_B***: #0000FF

Rule 3: (Assigning RGB Basic Color Codes to Individual Security Levels)

Web-based colors are identified by the location of "FF" within 6-digit color codes and security levels are basically classified based on this. If "FF" comes in the 1st and 2nd digits, this means red; in the 3rd and 4th digits, green; and in the 5th and 6th digits, blue.

Rule 4: (Assigning Detailed Color Codes to Category Levels of Each Task)

The first two digits "nn" within color codes (excluding FF) are identifiers for super-category tasks and the second two digits "mm" are those for sub-category tasks. With these segmented task identifiers, access can be controlled specifically.

Examples to assign color codes based on Rule 4 are as shown in Table 6.

Subjects Subject-Object Matching by Using Security Keys

Process of Subject-Object Matching

Figure 8 shows the matching process of color codes assigned to subjects and objects. Through the ID/Password authorization of users, their pre-authorized security level and SoD category (task) are identified. Objects are data that belong to higher and lower tasks stored within the database table and schema. Tasks can be matched with subjects through keys or attributes that have color code values. Security keys between subjects and objects are tools to verify the security levels and SoD that were pre-authorized and assigned to subjects. When an authorized subject wants to authorize additional security keys, authority is granted to the user to access objects matched with the authorized security levels and duties.

Definition of Security Key

As shown in Fig. 9, security key is an essential medium that links subjects and objects at certain security levels based on proper rules (formulas 7~21 below). This serves as a dual-lock tool for the additional authorization of users along with the ID/PW method. In other words, security key is a means to ensure users access objects (data) allowed to them according to their security levels. This can be realized using methods like One Time Password (OTP). In order to provide security policies on access control using security keys, those keys should be matched with colors of security levels in Table 5 and by doing so, access of subjects (users) to objects (data) can be controlled. Based on the rules to control access authority (formulas 17~21), certain access authority is granted to users when the security colors of their security keys are the same as or higher than their level within the same task category.

Subject-Object Matching by Using Security Key

Table 7 shows how subject, security key and object can be matched by security levels using data coloring. Here, the security levels of the keys are defined using a data coloring technique and the abbreviation of 'SK_(color of a certain level)' is used for security key.

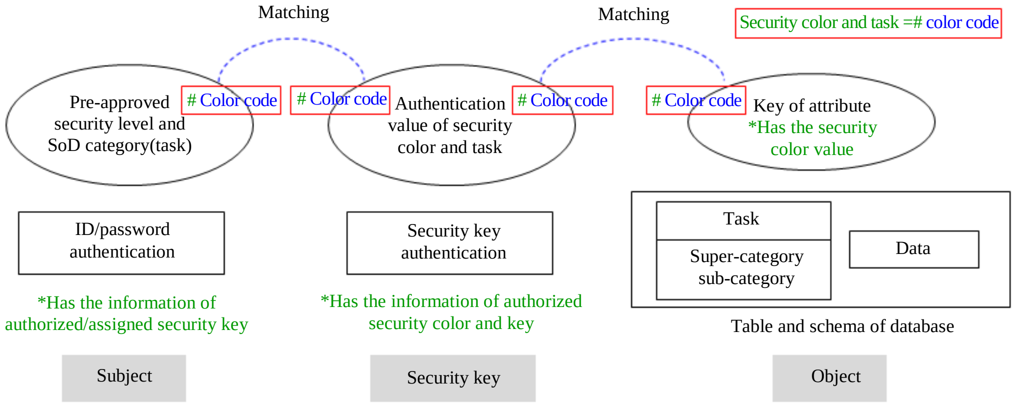
Matching
Matching
Security color and task =# color code
Pre-approved security level and SoD category(task)
# Color code
# Color code
Authentication value of security color and task
# Color code
# Color code
Key of attribute
*Has the security color value
ID/password authentication
Security key authentication
Task
Super-category sub-category
Data
*Has the information of authorized/assigned security key
*Has the information of authorized security color and key
Table and schema of database
Subject
Security key
Object

Fig. 8: Process of subject and object matching

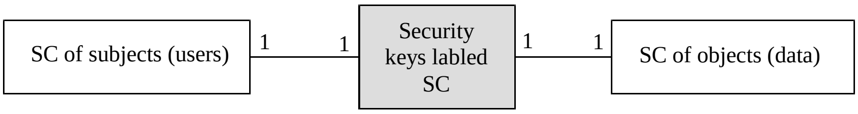

Fig. 9: Relationship among subject, security key and object

Table 3: Web-based RGB color notation

Special symbol	Red channel	Green channel	Blue channel
#	00 ~ FF	00 ~ FF	00 ~ FF

Table 4: Security colors policy defined by wrapping security levels with colors

Security level	Color	Security color
Top secret	*Red*	*SC_R(Red)*
Secret	*Green*	*SC_G(Green)*
Confidential	*Blue*	*SC_B(Blue)*
Unclassified	*Black*	-

Table 5: Detailed security levels and color relation

SoD-applied security level	Color code of super category task	Color code of sub-category task
SC_R_t	#1: #FFAA00	#1_1: #FFAA11
	#2: #FFBB00	#1_2: #FFAA22
	#3: #FFCC00	:
	#4: #FFDD00	#2_1: #FFBB11
	#5: #FFEE00	:
	:	#3_1: #FFCC11
SC_G_t	#1: #AAFF00	#1_1: #AAFF11
	#2: #BBFF00	#1_2: #AAFF22
	#3: #CCFF00	:
	#4: #DDFF00	#2_1: #BBFF11
	#5: #EEFF00	:
	:	#3_1: #CCFF11
SC_B_t	#1: #AA00FF	#1_1: #AA11FF
	#2: #BB00FF	#1_2: #AA22FF
	#3: #CC00FF	:
	#4: #DD00FF	#2_1: #BB11FF
	#5: #EE00FF	:
	:	#3_1: #CC11FF

[Legend] *t*: Task category

Table 6: Rules and examples of super- and sub-category color codes of each task

① Color code example of super-category	② Color code example of sub-category
$SC\_R\_t_{n}$: #FFnn00	$SC\_R\_t_{n\_m}$: #FFnnmm
$SC\_G\_t_{n}$: #nnFF00	$SC\_G\_t_{n\_m}$: #nnFFmm
$SC\_B\_t_{n}$: #nn00FF	$SC\_B\_t_{n\_m}$: #nnmmFF
$SC\_R\_t_{1}$: #FFAA00	$SC\_R\_t_{1\_1}$: #FFAA11
$SC\_G\_t_{1}$: #AAFF00	$SC\_G\_t_{1\_1}$: #AAFF11
$SC\_B\_t_{1}$: #AA00FF	$SC\_B\_t_{1\_1}$: #AA11FF

* $_{n,\, m}$: Integer (1~n,m), n, m: hexadecimal (0~E/excluding 'F')
** Excluding 'F' in hexadecimal values is to avoid collision with the color level identifier, "FF".

Table 7: Matching among subject, security key and object using data coloring

Subject	SC_level of subject	Security_Key	SC_level of object	Object
Top_level administrator	*SC_R*	*SK_R*	*SC_R*	Top secret data
Middle manager	*SC_G*	*SK_G*	*SC_G*	Secret data
General office worker	*SC_B*	*SK_B*	*SC_B*	Confidential data

Table 8: Matching among subject, security key and object using SoD and data coloring

Subject	SC_level of subject	Security_Key	SC_level of object	Object
Top_level administrator	*SC_R_t*	*SK_R_t*	*SC_R_t*	Top secret data
Middle manager	*SC_G_t*	*SK_G_t*	*SC_G_t*	Secret data
General office worker	*SC_B_t*	*SK_B_t*	*SC_B_t*	Confidential data

The relationship among security color, security key and subject (user) is as follows:

$$SC = \{SC_R, SC_G, SC_B\}$$
$$*SC_R = \mathbf{SC\_R}, SC_G = \mathbf{SC\_G}, SC_B = \mathbf{SC\_B} \tag{7}$$

$$SK = \{SK_R, SK_G, SK_B\}$$
$$*SK_R = \mathbf{SK\_R}, SK_G = \mathbf{SK\_G}, SK_B = \mathbf{SK\_B} \tag{8}$$

$$\forall SK = \left\{\bigcup_{i=1}^{l} SK_{Ri} + \bigcup_{j=1}^{m} SK_{Gj} + \bigcup_{k=1}^{n} SK_{Bk}\right\}(l, m, n: Positive\ integer) \tag{9}$$

$$\bigcup_{i=1}^{n} SK_i = \bigcup_{j=1}^{n} User_j \tag{10}$$

Subject, object (Table 5) and security key (Table 7) are classified with colors respectively and identified with color codes. 'L, m, n' in Formula 9 is determined by the number of subjects in each security level. Table 8 shows the mutual matching mechanism among subject, security key and object with tasks (SoD) added to Table 7.

SoD and data coloring are added to formulas (7), (8), (9) and (10) on security level above and the relationship among security color, security key and user can be defined as follows:

$$SC = \{SC_{RT}, SC_{GT}, SC_{BT}\}$$
$$*SC_{RT} = \mathbf{SC\_R\_t}, SC_{GT} = \mathbf{SC\_G\_t}, SC_{BT} = \mathbf{SC\_B\_t} \tag{11}$$

$$SK = \{SK_{RT}, SK_{GT}, SK_{BT}\}$$
$$*SK_{RT} = \mathbf{SK\_R\_t}, SK_{GT} = \mathbf{SK\_G\_t}, SK_{BT} = \mathbf{SK\_B\_t} \tag{12}$$

$$\forall SK = \left\{\bigcup_{i=1}^{l} SK_{RTi} + \bigcup_{j=1}^{m} SK_{GTj} + \bigcup_{k=1}^{n} SK_{BTk}\right\}(l, m, n: Positive\ integer) \tag{13}$$

$$\forall SK_R = \bigcup_{i=1}^{n} SK_{RTi} \tag{14}$$

$$\forall SK_G = \bigcup_{i=1}^{n} SK_{GTi} \tag{15}$$

$$\forall SK_B = \bigcup_{i=1}^{n} SK_{BTi} \tag{16}$$

Authority-Based Access Control

Authority-Based Policy Definition

For further segmented access controls, the access authority of subjects, of which tasks are separated by security levels, to objects should have more detailed rules for access based on the security policy of Rules 1 and 2 as follows. Depending on the characteristics of organizations, their tasks may need to have only one-level classification (super-category only). In this case, access authority can be assigned based on Rule 5. If the tasks need to be classified into two-level categories (supper- and sub-category), Rule 6 can be applied. Rule 7 is applied to assign or delegate access authority within the same task level.

Rule 5: Assigning Access Authority to Super-Category Tasks

$$\text{S: } SC\_tn \Rightarrow \text{O: } ≚\, SC\_tn\{\text{p}\} \tag{17}$$

* Description: A subject that is classified to a certain security level and super-category and certified as SC_t_n is given (⇒) access authority{permission} to objects below (≚) its relevant security level within its super-category task.

* Policy specifications under Rule 5

S: $\boldsymbol{SC\_R\_t_n} \Rightarrow$ O: $\boldsymbol{SC\_R\_t_n}$\{e, r, a, w\}, O: $\boldsymbol{SC\_G\_t_n}$\{e, r, a, w\}, O: $\boldsymbol{SC\_B\_t_n}$\{e, r, a, w\}
S: $\boldsymbol{SC\_G\_t_n} \Rightarrow$ O: $\boldsymbol{SC\_G\_t_n}$\{e, r, a, w\}, O: $\boldsymbol{SC\_B\_t_n}$\{e, r, a, w\}
S: $\boldsymbol{SC\_B\_t_n} \Rightarrow$ O: $\boldsymbol{SC\_B\_t_n}$\{e, r, a, w\}
S: $\wedge SC \Rightarrow$ O: $\boldsymbol{SC\_K}$\{e, r, a, w\}

* S = Subject, O = Object, p = policy
K = Black Color (meaning Unclassified level),
e = executing, r = reading, a = appending, w = writing

Rule 6: Assigning access authority to the sub-category tasks

$$S: SC\_tn\_m \Rightarrow O: \overset{\vee}{=} SC\_tn\_m\{p\} \tag{18}$$

* Description: A subject that is classified to a certain security level and sub-category task and certified as $SC\_t_{n\_m}$ is given access authority to objects below its relevant security level within its sub-category task.

* Policy specifications under Rule 6

S: $\boldsymbol{SC_R_t_{n_m}} \Rightarrow$O: $\boldsymbol{SC\_R\_t_{n\_m}}$\{e, r, a, w\}, O: $\boldsymbol{SC\_G\_t_{n\_m}}$\{e, r, a, w\}, O: $\boldsymbol{SC\_B\_t_{n\_m}}$\{e, r, a, w\}
S: $\boldsymbol{SC_G_t_{n_m}} \Rightarrow$O: $\boldsymbol{SC\_G\_t_{n\_m}}$\{e, r, a, w\}, O: $\boldsymbol{SC\_B\_t_{n\_m}}$\{e, r, a, w\}
S: $\boldsymbol{SC_B_t_{n_m}} \Rightarrow$O: $\boldsymbol{SC\_B\_t_{n\_m}}$\{e, r, a, w\}

Rule 7: Assigning and delegating access authority within the same security level

$$S: SC\_tn \not\Rightarrow O: SC\_tm \tag{19}$$

$$S: SC\_tn+m \Rightarrow O: \overset{\vee}{=} SC\_tm\{p\} \tag{20}$$

* Description: A subject that is classified to a certain task authority level of a certain security level and certified as SC_t_n is not allowed to access objects at the same security level in other tasks. Only when access authority to other tasks is additionally delegated to it, to put it another way, when a subject certified as $\boldsymbol{SC\_t_{n+m}}$ is additionally given a delegated access authority ($\boldsymbol{t_m}$) other than its original task ($\boldsymbol{t_n}$), the subject is allowed to access objects below the security level of $\boldsymbol{t_m}$ within the task category.

* Policy specifications under Rule 7

S: $\boldsymbol{SC\_R\_t_n} \not\Rightarrow$ O: $\boldsymbol{SC\_R\_t_m}$\{e, r, a, w\},
O: $\boldsymbol{SC\_G\_t_m}$\{e, r, a, w\}, O: $\boldsymbol{SC\_B\_t_m}$\{e, r, a, w\}
S: $\boldsymbol{SC_R_t_{n+m}} \Rightarrow$O: $\boldsymbol{SC\_R\_t_n}$\{e, r, a, w\},
O: $\boldsymbol{SC\_G\_t_n}$\{e, r, a, w\}, O: $\boldsymbol{SC\_B\_t_n}$\{e, r, a, w\},
O: $\boldsymbol{SC\_R\_t_m}$\{e, r, a, w\}, O: $\boldsymbol{SC\_G\_t_m}$\{e, r, a, w\},
O: $\boldsymbol{SC\_B\_t_m}$\{e, r, a, w\}

S: $\boldsymbol{SC\_G\_t_n} \not\Rightarrow$ O: $\boldsymbol{SC\_G\_t_m}$\{e, r, a, w\},
O: $\boldsymbol{SC\_B\_t_m}$\{e, r, a, w\}
S: $\boldsymbol{SC\_G\_t_{n+m}} \Rightarrow$ O: $\boldsymbol{SC\_G\_t_n}$\{e, r, a, w\},
O: $\boldsymbol{SC\_B\_t_n}$\{e, r, a, w\}, O: $\boldsymbol{SC\_G\_t_m}$\{e, r, a, w\},
O: $\boldsymbol{SC\_B\_t_m}$\{e, r, a, w\}

S: $\boldsymbol{SC\_B\_t_n} \not\Rightarrow$ O: $\boldsymbol{SC\_B\_t_m}$\{e, r, a, w\}
S: $\boldsymbol{SC\_B\_t_{n+m}} \Rightarrow$ O: $\boldsymbol{SC\_B\_t_n}$\{e, r, a, w\},
O: $\boldsymbol{SC\_B\_t_m}$\{e, r, a, w\}

Rule 8: Assigning and delegating access authority according to a super and sub-category tasks within the same security level (Optional rule)

$$S: SC\_tn \Rightarrow O: SC\_tn\_i\{p\}, \{i = 1 \sim m, where\ n \neq m\} \tag{21}$$

* Description: A subject that is classified to a super-category of a certain security level and certified as SC_t_n is given access authority to objects that are classified as sub-category tasks under the super-category task at the security level. However, this rule can be applied when there is a need to restrict access to specific subordinate functions to those who have authority of specific higher level tasks according to the confidential classification policy of the organization.

* Policy specifications under Rule 8

S: $\boldsymbol{SC\_R\_t_n} \Rightarrow$ O: $\boldsymbol{SC\_R\_t_{n\_i}}$ \{e, r, a, w\}, \{i = 1~m, where n $\neq$ m\}
S: $\boldsymbol{SC\_G\_t_n} \Rightarrow$ O: $\boldsymbol{SC\_G\_t_{n\_i}}$ \{e, r, a, w\}, \{i = 1~m, where n $\neq$ m\}
S: $\boldsymbol{SC\_B\_t_n} \Rightarrow$ O: $\boldsymbol{SC\_B\_t_{n\_i}}$ \{e, r, a, w\}, \{i = 1~m, where n $\neq$ m\}

Authority-based Access Control

The relationship among subject, security key and object classified under the SoD principle and security levels is shown in Fig. 10. The figure also shows examples of access attempts that are not allowed under their respective access authority. Access attempts ②, ③ and ④ (except ①) are blocked under Rules 1-2 and 5-6. In the case of attempt ①, a subject at the Secret level within Task #2 accesses an object within the same task category with a valid security key. Attempts ②, ③ and ④, however, try to reach objects out of their task categories and thus their access is blocked under the access control policy.

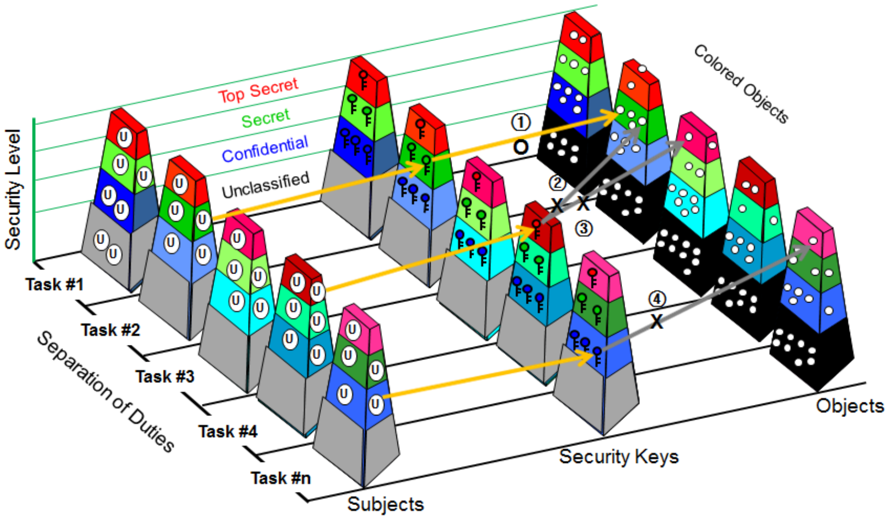

Fig. 10: Categories of and relationship between subject, security key and object

However, Attempts ② and ③ are to access objects out of their task categories and thus they are blocked under the access control policy. Attempt ④ is allowed if it is the "No –write-down" Policy of the BLP model and the "No-read-down" Policy of Biba model, but it is blocked under the policy of the CBB model suggested in this study.

Authority Delegation (Security Key Delegation)

Authority delegation can be executed only by subjects who have security keys to objects at certain levels. A subject who has access authority to certain data under the SoD principle is able to delegate the authority to unauthorized subjects at the same level (meaning sibling subjects in separately classified tasks) and other subjects at higher levels in other tasks.

In delegating authority, the policies defined in "Complementary BLP and Biba policy" section should not be violated. If a subject receives a request to permit authority delegation from those at the same level or higher levels, the subject should delegate its security keys to them after checking whether there is any violation of the defined policies or not. The results of delegation, as data to identify relevant subjects, objects and delegated security keys, is sent to and saved at a repository for access control policies and utilized as data for review.

Case Study

This chapter shows an application cases by applying the proposed method to the Human Resources management System (HRMS). As a case study, the example case of handling confidential information due to the characteristics of the MAC model is desirable, but it is difficult because it includes sensitive data related to military agency.

Human Resources Management System (HRMS)

The suggested DSDC-MAC model was applied to a Human Resources Management System (HRMS) to verify its reliability. The HRMS handles sensitive personnel information such as social identification, contact number, passport information, HR history, work performance, annual salary, etc. Since such information needs to be classified by task areas and security levels, it is suitable to apply the DSDC-MAC model to this system.

Figure 11 shows general task areas of the HRMS including employment management, HR operation/ management, absence control, performance evaluation management and payment management. Under the 5 super-categories of tasks, sub-categories are classified respectively and further detailed data are also included.

DSDC-MAC-based HRMS Access Control Model

Domain Task Category and Security Leveling of HRMS

First, tasks are separated and data security levels are determined. The areas of the separated tasks are defined based on the SoD classification in Table 2 (chapter 3) and the HRMS task categories in Fig. 11. In order to set security levels on data units in detail, data groups are included in the sub-category classification. Data security levels are set using the security levels in Table 1. The items shown in Table 9, except the subject and object columns, define task categories and security levels. For instance, "Candidate Information" is a sub-task of the super-category "Employment Management," and "n1) Contact No." in the Task and Data item under the sub-category is the sub-data group of "Candidate Information." The detailed data under the group is classified as "Confidential," and thus only those in charge of the task are allowed to access the data.

Separation of Duties by Subject and Object of HRMS

Subjects and objects are linked to the HRMS task categories and data defined above as shown in Table 9.

In particular, subjects are divided into worker and manager in charge of each task (department) and vice president or president who has higher responsibility. Generally, the higher work position, the higher responsibility. Persons at higher-level positions tend to have higher security levels. Thus, worker is given the 3rd-grade security level (Confidential) and manager, the 2nd-grade security level (Secret). More sensitive information is classified as the 1st-grade security level (Top secret) and president or vice president is given the security level. In particular, “n2) Social ID No.” in Table 9 is very sensitive data and thus its security level is classified as “Top Secret” to ensure that the information is controlled by the highest-level manager. Subjects who can access the data are limited to “Vice President.”

In other words, the data can be accessed only by subjects who are allowed to handle the “Personal Information” task which is one of the sub-category tasks of the super-category task, “Human Resources Operation Management,” and who at the same time have access authority to Top Secret. If necessary, data can be entered or altered by others through authority delegation.

Data Coloring of HRMS Objects

A data coloring technique is applied to the subjects and objects (Table 9) of the HRMS defined by tasks above and Table 10 shows the results. Security colors by security levels are mapped based on Rule 3 and Table 4 and those by task categories are mapped based on Rule 4 and Table 5. “Personal Information” is one of the sub-tasks of the super-category “Human Resources Operation Management,” and “n3) Contact No.” in Table 10 is one of the sub-data groups under Personal Information. The security level of the detailed data is set as “Confidential” to ensure that they can be accessed by only persons in charge of the task. Under Rules 3 and 4, identifiers (RGB color codes) are also given to the data using the data coloring technique.

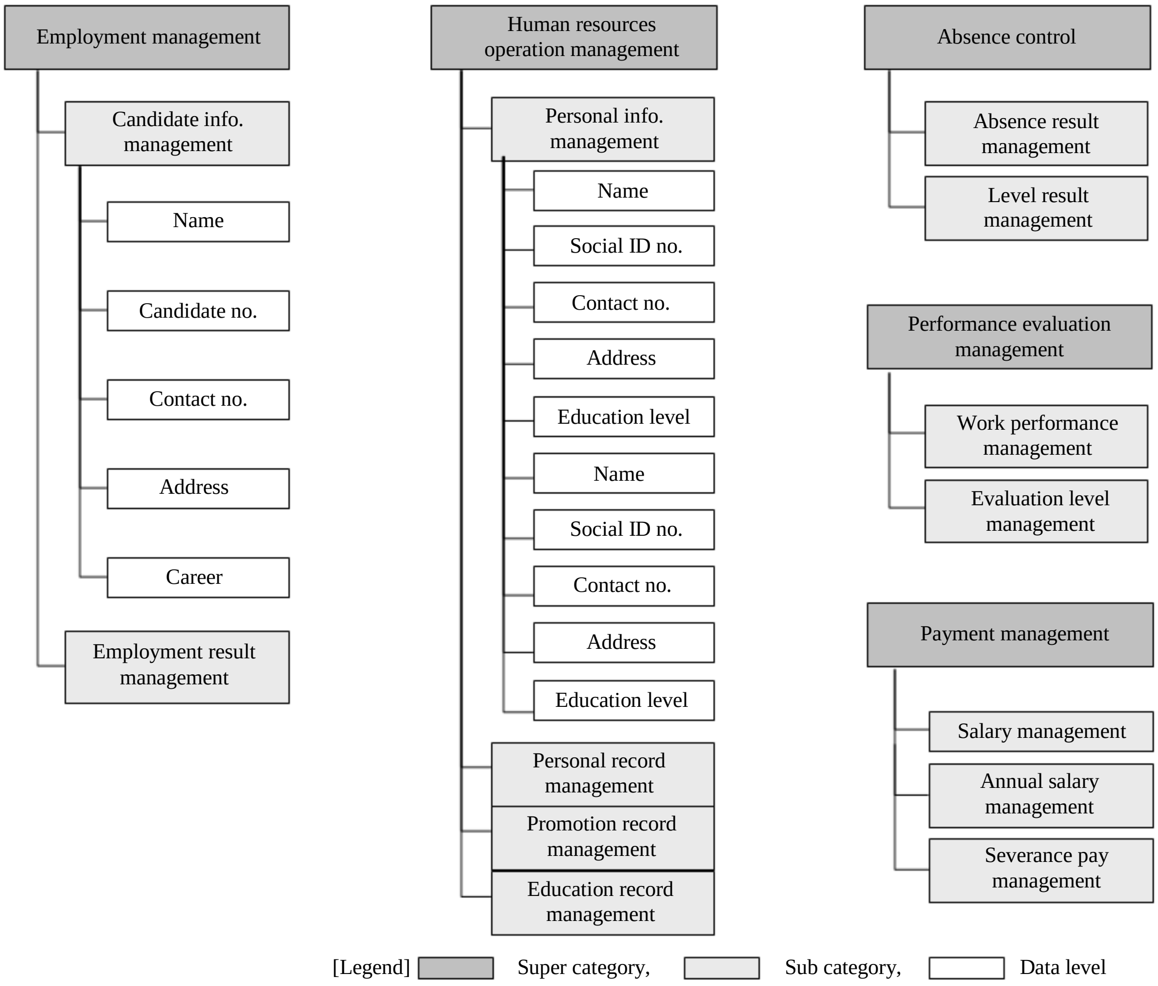
Employment management
Candidate info. management
Name
Candidate no.
Contact no.
Address
Career
Employment result management
Human resources operation management
Personal info. management
Name
Social ID no.
Contact no.
Address
Education level
Name
Social ID no.
Contact no.
Address
Education level
Personal record management
Promotion record management
Education record management
Absence control
Absence result management
Level result management
Performance evaluation management
Work performance management
Evaluation level management
Payment management
Salary management
Annual salary management
Severance pay management
[Legend] ▨ Super category, ░ Sub category, □ Data level

Fig. 11: HRMS task categories

Table 9: Definition of the subjects and objects by HRMS task categories

Super category		Sub category					
Task category	Task	Task Category	Task and data	Identifier	Subject	Object	Security Level
Task #1	Employment Management	subTask #1_1	Candidate Info.	t_1_10	Manager	-	-
		Data #1	Name	t_1_11	Worker	Marco,	
		Data #2	Candidate No.	t_1_12	Worker	Lee	Unclassified
		Data #3	n1) Contact No.	t_1_13	Worker	C.101	Unclassified
						010-205-0011	Confidential
Task #2	Human resources operation management	subTask #2_1	Personal Info.	t_2_10	Manager	-	-
		Data #1	Name	t_2_11	Worker	John,	
		Data #2	n2) Social ID No.	t_2_12	Vice.President	Song	Unclassified
		Data #3	Contact No.	t_2_13	Worker	54602-14560	Top Secret
						010-303-1100	Confidential
:	:	:	:	:	:	:	:

Table 10: Applying data coloring to the subjects and objects of HRMS task categories

Sub category						
						Applying data coloring
Task category	Task	Identifier	Subject	Object	Security level	(RGB Color code)
subTask #1	Candidate Info.	t_1_10	Manager	-	-	-
Data #1	Name	t_1_11	Worker	Marco, Lee	Unclassified	K
Data #2	Candidate No.	t_1_12	Worker	C.101	Unclassified	K
Data #3	Contact No.	t_1_13	Worker	010-205-0011	Confidential	$SC\_B\_t_{1\_13}$ (#AA30FF)
subTask #1	Personal Info.	t_2_10	Manager	-	-	-
Data #1	Name	t_2_11	Worker	John, Song	Unclassified	K
Data #2	Social ID No.	t_2_12	Vice.President	54602-14560	Top Secret	$SC\_R\_t_{2\_12}$ (#FFBB20)
Data #3	n3) Contact No.	t_2_13	Worker	010-303-1100	Confidential	$SC\_B\_t_{2\_13}$ (#BB30FF)
:	:	:	:	:	:	:

* K: Black (Unclassified data) (Table 4)

Table 11: Definition of security keys of subjects for accessing objects in HRMS

Task	Subject	Security level	Data coloring	Security key
Total managing	CEO	Top secret	$SC\_R\_t_{1+2+3+4+5}$	$SK\_R\_t_{1+2+3+4+5}$
	Vice CEO	Top secret	$SC\_R\_t_{1+2+3+4+5}$	$SK\_R\_t_{1+2+3+4+5}$
Employment management	Employment manager	Secret	$SC\_G\_t_1$	$SK\_G\_t_1$
	Employment office worker	Confidential	$SC\_B\_t_1$	**n4)** $SK\_B\_t_1$
HRO management	HRO manager	Secret	$SC\_G\_t_2$	$SK\_G\_t_2$
	HRO office worker	Confidential	$SC\_B\_t_2$	$SK\_B\_t_2$

Definition of Security Keys of Subjects for Accessing HRMS Objects

Table 11 shows the HRMS security keys for each object to access objects and they are defined based on Table 7 and 8 and formulas 7~16 using data coloring and SoD. "n4) SK_B_t1" in Table 11 is defined as the security key that has access authority both to t1, the identifier of the supper-category task called "Employment Management," and objects classified as the 3rd-grade security level (Confidential). This security key is granted only to users at the related security level in the same task category, that is, "Employment office worker." Here, the security key is a means to identify subjects and objects when subjects try to access objects that they are allowed to do so. This can be also used as a tool to authorize subjects, allowing them to validly access to objects according to the defined rules.

Authority-Based HRMS Policy Definition

Based on the subject, object and security key defined above, access authority policies for the HRMS can be defined under Rules 5-7 as follows:

S: $SC\_t_1 \Rightarrow$ **O:** $\veebar SC\_t_1$**{p}**
S: $SC_R_t_1 \Rightarrow$O: $SC\_R\_t_1${e, r, a, w},
O: $SC\_G\_t_1${e, r, a, w}, O: $SC\_B\_t_1${e, r, a, w}
S: $SC_G_t_1 \Rightarrow$O: $SC\_G\_t_1${e, r, a, w},
O: $SC\_B\_t_1${e, r, a, w}
S: $SC_B_t_1 \Rightarrow$O: $SC\_B\_t_1${e, r, a, w}
S: $\wedge SC \Rightarrow$ O: SC_K{e, r, a, w}

The policies above stipulate that subjects who have access authority to Task#1 (Employment Management) are allowed to access data below the security level. In other words, subjects who have the Red security level

(1st-grade/Top Secret) in Task#1 can access data classified as 1st, 2nd and 3rd grades as well as general-level data within the relevant task category.

Such access policies above define all the individual task categories and under task categories, subjects, objects and security keys are linked and defined accordingly.

Evaluation

In this section, it focus the primary characteristics of the access control model, compare the proposed model with the legacy MAC models and discuss the characteristics and limitations of the proposed model.

Discussion on the Access Control Policies with Case Study

Looking at the HRMS case and access control policies of the DSDC-MAC model, the Employee manager with green authority of task classification t1 has authority to read and write about the 3nd grade data as well as 2nd grade of t1. However, T2's 2nd grade (Green) secrets, which can only be accessed by HRO Managers of the same class, are not accessible under the separation of duties policy. In addition, Employment office workers with t1 (blue) authority with the same task are not authorized to read, write, or access 2nd grade (Green) secrets. This indicates that a low level of confidentiality can improve the confidentiality and integrity by not being able to read or write higher level secrets. Moreover, even if a subject has the same level of authority, if the job is different, it can further ensure confidentiality and integrity so that it cannot be read or written. However, in case of legacy BLP and Biba model, there has problems as follows. If it is BLP model, Employment Office Worker of 3nd grade (Blue Level) cannot read “Green” Data of 2nd grade, but “Write” is possible, so there is integrity problem. In the Biba model, Employment office workers cannot "write" data of 2nd grade, but "read" is possible, which is a confidentiality problem. Furthermore, both models are capable of “write” and “read” at the same level, which makes it possible to read or modify secrets irrelevant to the job, which leads to problems of confidentiality and integrity. On the other hand, the proposed DSDC-MAC model can solve above problems.

Comparative Evaluation with the Existing Methods

The DSDC-MAC model is evaluated in comparison with other MAC models, including BLP, Biba and Lattice-based access control model as shown in Table 12. The proposed model was compared with existing studies mainly from two aspects, including confidentiality/ integrity and model design.

From the confidentiality and integrity aspect, more detailed classification on subjects and objects was required to support these features. Compared with earlier studies, it is basically possible to classify subjects and objects in detail according to security levels in the BLP, Biba and lattice-based models. Those models, however, failed to classify the items further as the proposed model in this study did by applying the SoD principle.

Especially, coupled with the method of security keys, this model provides dual-lock access control tools unlike other models. For flexibility, the proposed model allows authorized users with security keys can delegate their authority to sibling subjects in other task categories and those at higher levels. Using the access control policy repository, the results of the requests and approvals for authority delegation can be used for review later afterwards.

In addition, the BLP model emphasizes confidentiality and the Biba model emphasizes integrity respectively. Thus, these models did not meet confidentiality and integrity at the same time. On the other hand, the Lattice model has been shown to be mathematically acceptable within one Lattice to solve the limitations of the security policies of the BLP and Biba models. Therefore, the Lattice model appears to support both confidentiality and integrity simultaneously.

Table 12: Evaluation with current MAC models

Assessed items		BLP model (Bell and LaPadula, 1975)	Biba model (Biba, 1997)	Lattice model (Sandhu, 1993; Denning, 1976)	Proposed model
Confidentiality and integrity	Detailed classification method of subjects and objects	△	△	△	○
	Supporting SoD policy	×	×	×	○
	Simultaneously supporting confidentiality and integrity	×	×	○	○
	Dual-lock access control	×	×	×	○
	Supporting authority delegation (Access control flexibility)	×	×	×	○
	Supporting function to review task performance	×	×	×	△
Model design	Offering identifiers of subjects and objects	×	×	×	○
	Supporting strict authorization process	×	×	×	○
	Secure key management	×	×	×	○
	Offering case study or implementation model	△	△	△	○

[Legend] ○: applicable/supported, △: partially applicable/supported, ×: not applicable/supported

From the aspect of model design, no suggestion was found in earlier studies on identifiers of subjects and objects. In this study, however, accurate identifiers were presented using a data coloring technique. In addition, other studies have not supported strict authorization and secure key management.

Furthermore, other legacy studies did not have specific case studies or implementation models and were only described as illustrative levels. However, this study presented a case study through HRMS system.

Characteristics and Limitations

The main features of the proposed DSDC-MAC model and policies are as follows:

- SoD-driven access control
  While earlier studies use a vertical method for access control based on security levels (Top Secret/Secret/Confidential/Unclassified) only, access control can be further segmented horizontally even within the same security level based on tasks in the proposed model
- Security color-focused access control
  The proposed model support identifiers of data by security levels and task categories using data coloring, providing object-oriented access control based on security colors
- Mapping subjects and objects based on security keys
  The proposed model guarantees subjects dual-lock authorization tools using security keys. With security colors and keys, subjects and objects can be identified and their access can be controlled, thus supporting dual-lock security control
- Complementary BLP and Biba (CBB) model policy
  By suggesting a new CBB policy model, the proposed model can address contra diction issues associated with confidentiality and integrity that are found in the BLP and Biba models. With this mechanism, security can be further improved
- In addition to complementing confidentiality and integrity policies by Data Coloring and Separation of Duty, this study provides one of the contributions to provide dual-lock access control through Security Key. However, it did not examine in detail the implementation method of optimized security key and only mentioned that security key implementation such as OTP is possible. Thus, further follow-up studies are needed

The followings are some potential limitations found in the proposed model:

- The proposed model lacks standardized specifications on the security policies using SPL. (Access Control Language for Security Policy)
- The proposed model has to be implemented or built in existing DBMS systems
  To implement the results of this study in real settings, it is essential to apply them in commercialized DBMS systems, but there is some difficulty in implementing it in reality. It was difficult to apply key modules suggested in this study to commercialized products such as Oracle and more time and efforts should be put into applying them to open source DBMS systems. More optimized methods to implement security keys in reality should be also suggested

Conclusion

This study suggested a DSDC-MAC model and security policies that can improve both the confidentiality and integrity of MAC models such as BLP and Biba using SoD and data coloring techniques. Based on the policies of the proposed model, tasks of subjects and objects were classified and security colors were given to each of the classified subjects according to their security levels. The colors were matched with security keys to prevent or allow subjects to access objects (or data). By applying the principle of SoD-based access control, ambiguity in access control within the same security level was removed. It was possible to segment security and access controls for subjects and objects using a data coloring technique. Collisions between security policies can be prevented by simultaneously supporting confidentiality and integrity based on MAC models. In addition, it becomes convenient to identify data security levels and manage access control by assigning security colors to individual task data. At the same time, it is possible to provide dual-lock access control along with security keys. The model can be applied to the design and construction of an organization's internal systems or organizations that deal with a lot of confidential information, such as the military or intelligence agencies that only provide specific information to specific personnel. In particular, it will be an effective countermeasure against insider threats.

The Complementary BLP and Biba (CBB) security policies in the suggested model need to be further specified using an access control language in a follow-up study. The efficiency and usability of the proposed model should be analyzed further by applying it to settings such as object-oriented DB. Furthermore, it will be also necessary to implement a DBMS system equipped with the security structure of such databases. In addition, the present model has been studied to ensure confidentiality and integrity at the same time, but does not consider availability, one of the third triad of security. Therefore, in the system implementation stage applying the proposed model, it is necessary to conduct research so that a valid licensee has no restriction on service use in consideration of 'availability'. In addition, a study on both the implementation of the security key optimized for the presented model and also the complexity analysis of the proposed approach method is required. Based on these future studies, a practical case study is needed to verify the applicability of the proposed model to specific institutions.

Author's Contributions

Chee-Yang Song: Harmonized the entire development of the article and revised the manuscript.

Soon-Book Lee: Worked on most of the parts, introduction, design and evaluation of the research method and to the writing of the manuscript.

Yoo-Hwan Kim: Contributed to the design of the research plan and content, related work and engaged in the literature view.

Jin-Woo Kim: Participated in design of research model and to writing case study.

Ethics

This manuscript is original and has not been published elsewhere. The corresponding author confirms that coauthors have review and approved the article and there are no ethical issues in the future.

References

Bell, D.E. and L.J. LaPadula, 1975. Computer security model: Unified exposition and multics interpretation. Technical Report, MITRE Corp., Bedford, MA, Tech. Rep. ESD-TR-75-306, National Institute of Standards and Technology (U.S.)

Bertino, E., 2003. RBAC models-concepts and trends. Comput. Security, 22: 511-514. DOI: 10.1016/S0167-4048(03)00609-6

Bertino, E., E. Terzi, A. Kamra and A. Vakali, 2005. Intrusion detection in RBAC-administered databases. Proceedings of the 21st Annual Computer Security Applications Conference, Dec. 5-9, IEEE Xplore Press, Tucson, AZ, USA. DOI: 10.1109/CSAC.2005.33

Biba, K.J., 1997. Integrity considerations for secure computer systems. MTR-3153, The Mitre Corporation, Paperback.

Botha, R.A. and J.H.P. Eloff, 2001. Separation of duties for access control enforcement in work-flow environments. IBM Syst. J., 40: 662-682. DOI: 10.1147/sj.403.0666

Ceze, L., C. Praun, C. Caşcaval, P. Montesinos and J. Torrellas, 2008. Concurrency control with data coloring. Proceedings of the ACM SIGPLAN Workshop on Memory Systems Performance and Correctness: Held in Conjunction with the 13th International Conference on Architectural Support for Programming Languages and Operating Systems, Mar. 2-2, ACM, USA, pp: 6-10. DOI: 10.1145/1353522.1353525

Clark, D.D. and D.R. Wilson, 1987. A comparison of commercial and military computer security policies. Proceedings of IEEE Symposium on Security and Privacy, Apr. 27-29, IEEE Xplore Press, Oakland, CA, USA, pp: 184-194. DOI: 10.1109/sp.1987.10001

Davida, G.I., D.L. Wells and J.B. Kam, 1981. A database encryption system with subkeys. ACM Trans. Database Syst., 6: 312-238. DOI: 10.1145/319566.319580

Denning, D., 1976. A lattice model of secure information flow. Commun. ACM, 19: 236-243. DOI: 10.1145/360051.360056

Elovici, Y., R. Waisenberg, E. Shmueli and E. Gudes, 2004. A structure preserving database encryption scheme. Proceedings of the Secure Data Management in a Connected World, Aug. 30-30, Springer, Toronto, Canada, pp: 28-40. DOI: 10.1007/978-3-540-30073-1_3.

Ferraiolo, D.F. and R. Kuhn, 1992. Role-based access control. Proceedings of the 15th National Computer Security Conference, Oct. 13-16, Computer Security Resource Center, USA, pp: 554-563.

Gupta, S. and A. Kumar, 2019. Secret image digitization over public cloud through Cbtv based image fusion. Int. J. Innovat. Technol. Explor. Eng., 7: 4026-4031. DOI: 10.35940/ijite.,199939.0881019

Hwang, K. and D. Li, 2010. Trusted cloud computing with secure resources and data coloring. IEEE Internet Comput., 14: 14-22. DOI: 10.1109/mic.2010.86

Kalinin, M., V. Krundyshev, E. Rezedinova and P. Zegzhda, 2018. Role-based access control for vehicular adhoc networks. Proceedings of the IEEE International Black Sea Conference on Communications and Networking, Jun. 4-7, IEEE Xplore Press, Batumi, Georgia. DOI: 10.1109/BlackSeaCom.2018.8433628

Kuhn, D.R., E.J. Coyne and T.R. Weil, 2010. Adding attributes to role-based access control. IEEE Comput., 43: 79-81. DOI: 10.1109/MC.2010.155

Kumar, A., 2019. Design of secure image fusion technique using cloud for privacy preserving and copyright protection. Int. J. Cloud Applic. Comput., 9: 22-36. DOI: 10.4018/IJCAC.2019070102

Liu, Y.C., Y.T. Ma, H.S. Zhang, D.Y. Li and G.S. Chen, 2011. A method for trust management in cloud computing: Data Coloring by Cloud Watermarking. Int. J. Automat. Comput., 8: 280-285. DOI: 10.1007/s11633-011-0583-3

Mansfield-Devine, S., 2014. Masking sensitive data. Netw. Security, 2014: 17-20. DOI: 10.1016/S1353-4858(14)70104-7

Moon, C.J., D.H. Park, S.J. Park and D.K. Baik, 2004. Symmetric RBAC model that takes the separation of duty and role hierarchies into consideration. Comput. Security, 23: 126-136. DOI: 10.1016/j.cose.2003.09.004

Saltzer, J.H. and M.D. Schroeder, 1975. The protection of information in computer systems. Proc. IEEE, 63: 1278-1308. DOI: 10.1109/PROC.1975.9939

Sandhu, R., D. Ferraiolo and R. Kuhn, 2000. The NIST model for role based access control: Towards a unified standard. Proceedings of the 5th ACM Workshop on Role Based Access Control, Jul. 26-27, ACM, NIST, Germany, pp: 47-63. DOI: 10.1145/344287.344301

Sandhu, R.S., 1993. Lattice-based access control models. IEEE Comput., 26: 9-19. DOI: 10.1109/2.241422

Sandhu, R.S., E.J. Coynek, H.L. Feinsteink and C.E. Youmank, 1996. Role-based access control models. IEEE Comput., 29: 38-47. DOI: 10.1109/2.485845

Sinha, G., P. Shankar K.C. and S. Jain, 2018. Evolution of access control models for protection of patient details: A survey. Int. J. Eng. Technol., 7: 554-558. DOI: 10.14419/ijet.v7i2.8.10520

Sudha, I. and P. Jamuna, 2013. Data coloring by cloud watermarking using RSA for periodic authentication. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 627-630.

United Nations, 2004. Role-based access control, American National Standards Institute. ANSI INCITS, New York, USA.

Wang, Y., L. Tian and Z. Chen, 2019. Game analysis of access control based on user behavior trust. Information, 10: 1-13. DOI: 10.3390/info10040132

Zhao, S. and Y. Chen, 2013. The novel model of building network security control system based on RBAC and PMI technology. J. Convergence Inform. Technol., 8: 370-378.