Ability-Based Expression Control for Secure Spaces

Shun Hattori
College of Information and Systems, Muroran Institute of Technology
27–1 Mizumoto-cho, Muroran, Hokkaido 050–8585, Japan
Email: hattori@csse.muroran-it.ac.jp

***Abstract*—In public spaces, there are a number of different contents such as visitors, physical information resources, and virtual information resources via their embedded output devices. Therefore, we might unexpectedly enter the public spaces that have our unauthorized contents and/or unwanted characteristics, i.e., they are not always secure and safe. To solve this problem, my previous work has introduced the concept of *"Secure Spaces"*, physical environments in which any visitor is protected from being pushed her unwanted information resources on and also any information resource is always protected from being accessed by its unauthorized visitors, and the model and architecture for space entry control and information access control based on their dynamically changing contents. Aiming to build more flexible Secure Spaces, this paper proposes an extended model for not only spatial entry control but also Ability-Based Expression Control according to how preferentially a virtual information resource should be outputted in a Secure Space where shared by visitors with perceptibility and understandability of the virtual information resource's content and expression.**

I. Introduction

In recent years, it has become one of the hottest research topics to make physical spaces smarter and more intelligent. Smart Spaces [1–6] are often physically isolated environments such as individual rooms that have been made smart by various information and communication technologies and are expected to become increasingly convenient for our information access. Meanwhile, Information Security also becomes very significant and increasingly critical for any people in diverse scenes, especially in public places such as indoor work places, educational facilities, and healthcare centers, and so forth. The amount of physical or virtual information resources which should be protected in the physical world as well as virtual worlds keeps growing exponentially.

Physical environments are becoming smart but not necessarily secure. When a user requests to access a virtual (computational) information resource via an output device, conventional access control systems make a decision by using its access policies on whether the user should be granted or denied to access it and then assuredly enforce the access decision. However, even if the requester is authorized by the resource, it should not be immediately offered to her via the output device, because there might be its unauthorized users as well as the authorized requester around the output device, especially in public places. Meanwhile, when a user enters a physical environment, the user might be unexpectedly forced to access her unwanted information resources (e.g., although she does not want to know about the result of a football game that she had recorded on video to watch later, she unfortunately encounters it in her train), and/or hate its real characteristics (e.g., degrees of dismal and danger).

There are two kinds of conventional access controls for the purpose of protecting information resource security. One approach is Information Access Control. When a user requests to perform an action on a virtual information resource such as a sensitive data file on computer, information access control systems make an authorization decision on whether the access request should be granted or denied, in order to protect it from its unauthorized users. However, they are not aware of the other users who are surrounding a device outputting it, and thus there might exist its unauthorized user(s) in the surrounding area. If there are its unauthorized user as well as the authorized user, both users become able to access it and thus its confidentiality is not always protected. To protect it from its unauthorized users assuredly, they have to ensure that the area surrounding a device which will be granted to output the requested virtual information resource is truly secure, i.e., there is nobody unauthorized in the surrounding area.

Another approach is Space Entry Control. When a user requests to enter a physically isolated space such as a room and a building, physical entry control systems make an entry decision on whether the entry request should be granted or denied, in order to protect any physical information resource inside the physical space from its unauthorized users. However, they often determine the entry decision statically regardless of what physical or virtual information resources there are actually in the physical space, and thus there might not exist any resource which should be protected from the visitor. To ensure effective entry control, space entry control systems must be aware of dynamically changing contents such as visitors, and physical or virtual information resources.

To solve the problem "physical spaces are not always secure and safe," my previous work [7–13] has introduced the concept of *"Secure Spaces"*, physically isolated environments where any visitor is protected from being pushed her unwanted information resources on and also any information resource is protected from being accessed by its unauthorized visitors, and the model and architecture for space entry control and information access control based on their changing contents.

Aiming to build more flexible Secure Spaces, this paper proposes an extended model for not only spatial entry control but also Ability-Based Expression Control based on how preferentially a virtual information resource should be outputted in a Secure Space where shared by visitors with perceptibility and understandability of information content and expression.

II. Secure Spaces and Entry Control

This section introduces the architecture to build Secure Spaces in the physical world, and the mechanism and formalized model of Space Entry Control for Secure Spaces by summarizing my previous work [7–13].

A. Architecture

To build Secure Spaces in the real world by using space entry control based on their dynamically changing contents such as their visitors, physical information resources, and virtual information resources via their embedded output devices, each Secure Space requires the following facilities (Fig. 1).

- **Space Management**: is responsible for managing a Secure Space, i.e., for constantly figuring out its contents such as its visitors, its embedded physical information resources, and virtual information resources outputted via its embedded output devices and also for ad-hoc making an authorization decision on whether an entry request to enter the Secure Space by a visitor or a physical/virtual information resource should be granted or denied, and for notifying the entry decisions to the Electrically Lockable Doors or enforcing entry control over virtual information resources according to the entry decisions by itself.
- **User/Object Authentication**: is responsible for authenticating what physical entity such as a user (visitor) or a physical information resource requests to enter or exit the Secure Space (e.g., by using Radio Frequency IDentification or biometrics technologies) and also for notifying it to the space management.
- **Electrically Lockable Door**: is responsible for electrically locking or unlocking itself, i.e., for assuredly enforcing entry control over physical entities such as visitors and physical information resources, according to instructions by the space management.
- **Physically Isolating Opaque Wall**: is responsible for physically isolating inside a Secure Space from outside there with regard to information access, i.e., for validating the basic assumption that any user (visitor) inside a Secure Space can access any resource inside the Secure Space, while any user outside the Secure Space can never any resource inside the Secure Space.

To protect us from our unwanted characteristics (e.g., degree of congestion) of physical spaces as well as our unauthorized contents, the following additional facilities are required.

- **Real Sensor**: is responsible for physically sensing inside a Secure Space for its real characteristics to make access decisions in the Secure Space and also for notifying the sensor data stream to the space management. For example, thermometers, hygrometers, (security) cameras.
- **Web Sensor** [14–16]: is responsible for logically sensing the Web for the approximate characteristics of each Secure Space to make access decisions in the Secure Space and also for notifying the Web-mined data to the space management. Note that any Secure Space does not have to equip the extra devices unlike Real Sensors.

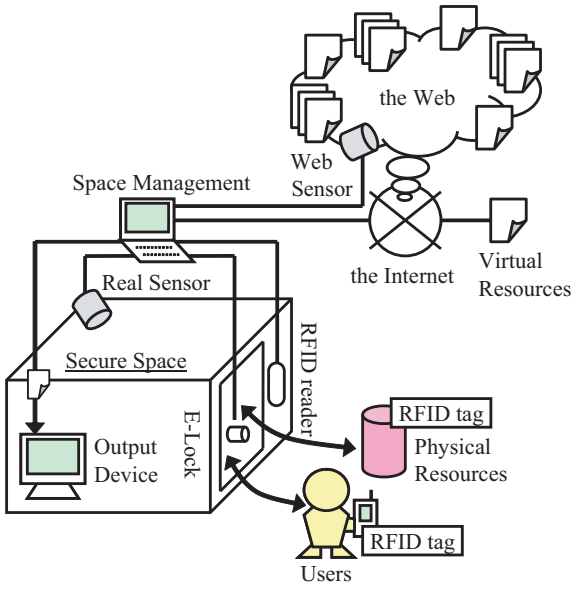

Fig. 1. Architecture of Secure Spaces

B. Mechanism

When a user requests to enter a Secure Space, the space entry control system will make an entry decision on whether the entry request should be granted or denied, by checking whether or not the requester is granted to access by all information resources inside the Secure Space and whether or not the Secure Space itself as well as all information resources inside the Secure Space are granted to be accessed by the requester, in order to protect her preference as well as information security for all contents of the Secure Space.

If the Secure Space is not granted to be accessed by the requester because its real characteristics (e.g., degrees of dismal or danger) are unfavorable for the requester, the space entry control system has only one approach of preventing the requester from entering the Secure Space. If the requester is not granted to access by at least one physical information resource inside the Secure Space or if at least one physical information resource inside the Secure Space is not granted to be access by the requester, the space entry control system has also only one approach of preventing the requester from entering the Secure Space (Fig. 2). Reversely, when a physical information resource requests to enter a Secure Space, the space entry control system will also prevent the physical information resource from entering the Secure Space that contains at least one visitor who does not have access right to access the physical information resource (Fig. 3).

Meanwhile, if the requester is not granted to access by at least one virtual information resource via an output device embedded inside the Secure Space or if at least one virtual information resource is not granted to be access by the requester, the space entry control system has two approaches of not only preventing the requester from entering the Secure Space but also permitting the requester to enter the Secure Space after revoking the virtual information resource (Fig. 4).

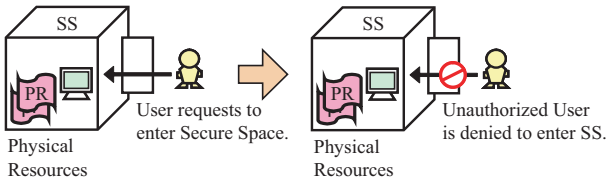

Fig. 2. Space Entry Control over Users for Physical Resources

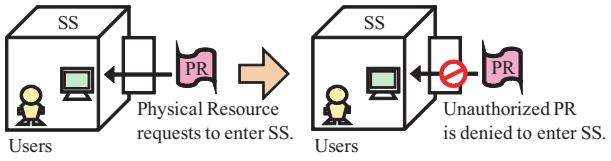

Fig. 3. Space Entry Control over Physical Resources for Users

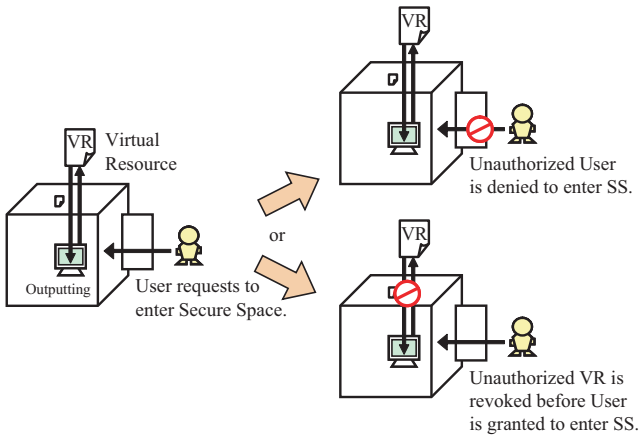

Fig. 4. Space Entry Control over Users for Virtual Resources

C. Formalized Model

The formalized model of space entry control for Secure Spaces based on their dynamically changing contents such as their visitors, physical information resources, and virtual information resources via their embedded output devices (e.g., displays and speakers), by listing component primitives and defining the syntax and semantics of the model components.

Definition 1: Model Entities

The space entry control model has the following four kinds of entities and protects all of them with respect to their information security and preferences to the other entities.

- **Secure Spaces**: are physically isolated environments (e.g., a closed room by opaque walls with electrically lockable doors) whose contents such as users (visitors) and physical/virtual resources are always protected according to their access policies. The universal set of Secure Spaces and Secure Spaces' Access Policies are denoted by $\mathtt{S}$ and $\mathtt{SAP}$ respectively.
- **Users:** are physical entities who request to enter or exit a Secure Space and who are assumed to be able to access any resource inside their current Secure Space but not to access any resource outside there. The universal set of Users and Users' Access Policies are denoted by $\mathtt{U}$ and $\mathtt{UAP}$ respectively.
- **Physical Resources:** are physical information entities (e.g., a hardcopy of sensitive information) which request to enter or exit a Secure Space and which are assumed to be able to be accessed by any user (visitor) inside their current Secure Space but not to be accessed by any user outside there. In order to assuredly enforce a physical resource's access policies, the space entry control system has to prevent its unauthorized users from entering its current Secure Space at any cost. The universal set of Physical Resources and Physical Resources' Access Policies are denoted by $\mathtt{PR}$ and $\mathtt{PRAP}$ respectively.
- **Virtual Resources:** are virtual information entities (e.g., a piece of sensitive information on the Internet) which request to be outputted or revoked via an output device (e.g., a display and speaker) embedded in a Secure Space and which are assumed to be able to be accessed by any user (visitor) inside their current Secure Space but not to be accessed by any user outside there. In order to assuredly enforce a virtual resource's access policies, the space entry control system has to prevent its unauthorized users from entering its current Secure Space or to prevent itself from being outputted in the Secure Spaces where there are its unauthorized users. The universal set of Virtual Resources and Virtual Resources' Access Policies are denoted by $\mathtt{VR}$ and $\mathtt{VRAP}$ respectively.
- Resources: $\mathtt{R} = \mathtt{PR} \cup \mathtt{VR}$.
- Contents (Contexts): $\mathtt{C} = \mathtt{U} \cup \mathtt{PR} \cup \mathtt{VR}$.

Definition 2: Model Functions

The model uses the following functions in order to keep up on the set of ad-hoc entities in each Secure Space and evaluate the weight of a set of its dynamically changing contents.

- $\mathtt{cu}$: $\mathtt{S} \rightarrow 2^{\mathtt{U}}$, is a function mapping each Secure Space s_i, to its current set of Containing Users $\mathtt{cu}(s_i)$.
- $\mathtt{cpr}$: $\mathtt{S} \rightarrow 2^{\mathtt{PR}}$, is a function mapping each Secure Space s_i, to its current set of Containing Physical Resources $\mathtt{cpr}(s_i)$.
- $\mathtt{cvr}$: $\mathtt{S} \rightarrow 2^{\mathtt{VR}}$, is a function mapping each Secure Space s_i, to its current set of Containing Virtual Resources $\mathtt{cvr}(s_i)$.
- $\mathtt{cc}$: $\mathtt{S} \rightarrow 2^{\mathtt{C}}$, is a function mapping each Secure Space s_i, to its current set of Containing Contents $\mathtt{cc}(s_i) = \mathtt{cu}(s_i) \cup \mathtt{cpr}(s_i) \cup \mathtt{cvr}(s_i)$.
- $\mathtt{w}$: $\mathtt{S} \times 2^{\mathtt{C}} \rightarrow \mathcal{R}$, is a function mapping a set of contents $\mathtt{cc}(s_i)$ in each Secure Space s_i, to its evaluated Weight $\mathtt{w}(s_i, \mathtt{cc}(s_i))$.
- $\mathtt{authU}$: $\mathtt{UER} \rightarrow \{\mathtt{grant}, \mathtt{deny}\}$, is a function mapping each User's Entry Request uer_j, to the Authorization decision for Users $\mathtt{authU}(uer_j)$.
- $\mathtt{authR}$: $\mathtt{RER} \rightarrow \{\mathtt{grant}, \mathtt{deny}\}$, is a function mapping each physical/virtual Resource's Entry Request rer_j, to the Authorization decision for Resources $\mathtt{authR}(rer_j)$.

Definition 2.1: Weighting of Secure Space with Contents

The weight that evaluates contents such as Users $\mathtt{cu}(s_i)$, Physical Resources $\mathtt{cpr}(s_i)$, and Virtual Resources $\mathtt{cvr}(s_i)$ in each Secure Space s_i could be defined in different manners. Here, this paper introduces one definition of content weighting function which seems to be more understandable for its space administrator and most often used.

The weight $\mathtt{w}(s, cs)$ of a Secure Space $s \in \mathtt{S}$ who has a set of Contents $cs \in 2^{\mathtt{C}}$ is defined as the summation of positive weights $\mathtt{w}(s, u, r)$ that evaluate how important each User's accessing each Resource in each Secure Space is,

$$\mathtt{w}(s, cs) = \sum_{u \in cs \cap \mathtt{U}, r \in cs \cap \mathtt{R}} \mathtt{w}(s, u, r).$$

Definition 3: Access Policies

The model stores the following four kinds of access policies for Secure Spaces, Users and Physical/Virtual Resources.

- **Secure Space's Access Policy:** is an access policy by a Secure Space, defined as a 3-tuple of the Secure Space, a User/Resource and a set of its containing entities as contextual conditions,

  $$\mathtt{SAP} \subseteq \mathtt{S} \times \mathtt{C} \times 2^{\mathtt{C}}.$$

  $(s, c, cs) \in \mathtt{SAP}$ where $s \in \mathtt{S}$, $c \in \mathtt{C}$, and $cs \in 2^{\mathtt{C}}$, states that the Secure Space s grants the User/Resource c to enter there when it has the set of Contents cs.
- **User's Access Policy:** is an access policy by a User, defined as a 4-tuple of the User and her qualified physical/virtual Resource, a Secure Space, and a set of its containing entities as contextual conditions,

  $$\mathtt{UAP} \subseteq \mathtt{U} \times \mathtt{R} \times \mathtt{S} \times 2^{\mathtt{C}}.$$

  $(u, r, s, cs) \in \mathtt{UAP}$ where $u \in \mathtt{U}$, $r \in \mathtt{R}$, $s \in \mathtt{S}$, and $cs \in 2^{\mathtt{C}}$, states that the User u grants the Resource r to be pushed on herself in the Secure Space s who has the set of Contents cs.
- **Physical Resource's Access Policy:** is an access policy by a Physical Resource, defined as a 4-tuple of the Physical Resource, its qualified User, a Secure Space, and a set of its containing entities as contextual conditions,

  $$\mathtt{PRAP} \subseteq \mathtt{PR} \times \mathtt{U} \times \mathtt{S} \times 2^{\mathtt{C}}.$$

  $(pr, u, s, cs) \in \mathtt{PRAP}$ where $pr \in \mathtt{PR}$, $u \in \mathtt{U}$, $s \in \mathtt{S}$, and $cs \in 2^{\mathtt{C}}$, states that the Physical Resource pr grants the User r to access itself in the Secure Space s who has the set of Contents cs.
- **Virtual Resource's Access Policy:** is an access policy by a Virtual Resource, defined as a 4-tuple of the Virtual Resource, its qualified User, a Secure Space, and a set of its containing entities as contextual conditions,

  $$\mathtt{VRAP} \subseteq \mathtt{VR} \times \mathtt{U} \times \mathtt{S} \times 2^{\mathtt{C}}.$$

  $(vr, u, s, cs) \in \mathtt{VRAP}$ where $vr \in \mathtt{VR}$, $u \in \mathtt{U}$, $s \in \mathtt{S}$, and $cs \in 2^{\mathtt{C}}$, states that the Virtual Resource pr grants the User r to access itself via an embedded output device in the Secure Space s who has the set of Contents cs.

Definition 4: Entry Requests

The model has the following three kinds of entry requests for Users and Physical/Virtual Resources.

- **User's Entry Request:** is an entry request by a User, defined as a 2-tuple of the User and a Secure Space which she is requesting to enter,

  $$\mathtt{UER} \subseteq \mathtt{U} \times \mathtt{S}.$$

  $(u, s) \in \mathtt{UER}$ where $u \in \mathtt{U}$ and $s \in \mathtt{S}$, states that the User u requests to enter the Secure Space s and to access its containing Resources $\mathtt{cpr}(s) \cup \mathtt{cvr}(s)$ inside there.
- **Physical Resource's Entry Request:** is an entry request by a Physical Resource, defined as a 2-tuple of the Physical Resource and a Secure Space which it is requesting to enter,

  $$\mathtt{PRER} \subseteq \mathtt{PR} \times \mathtt{S}.$$

  $(pr, s) \in \mathtt{PRER}$ where $pr \in \mathtt{PR}$ and $s \in \mathtt{S}$, states that the Physical Resource pr requests to enter the Secure Space s and to be accessed by the visitors $\mathtt{cu}(s)$ inside there.
- **Virtual Resource's Entry Request:** is an entry request by a Virtual Resource, defined as a 2-tuple of the Virtual Resource and a Secure Space which it is requesting to be outputted via a device embedded in,

  $$\mathtt{VRER} \subseteq \mathtt{VR} \times \mathtt{S}.$$

  $(vr, s) \in \mathtt{VRER}$ where $vr \in \mathtt{VR}$ and $s \in \mathtt{S}$, states that the Virtual Resource vr requests to be outputted via an output device embedded in the Secure Space s and to be accessed by the visitors $\mathtt{cu}(s)$ inside there.

Algorithm 1.1: Authorization for Users

An entry request $uer = (u, s) \in \mathtt{UER}$ that a User u requests to enter a Secure Space s is granted, if and only if any content inside there grants the User u to access itself and is granted to be accessed by the User u or if the Assumptive Weight $\mathtt{aw}(s, u)$ in case of granting the User u to enter the Secure Space s after revoking any Virtual Resource inside there which denies the User u to access itself or is denied to be accessed by the User u is higher than the Current Weight $\mathtt{cw}(s)$ in case of denying the user to enter there.

$$\begin{aligned}
&\mathtt{authU}(uer) = \mathtt{authU}(u, s) = \mathtt{grant} \\
&\Leftrightarrow (\mathtt{apr}(s, u) = \mathtt{cpr}(s)) \\
&\quad \wedge \{(\mathtt{avr}(s, u) = \mathtt{cvr}(s)) \vee (\mathtt{aw}(s, u) \geq \mathtt{cw}(s))\}
\end{aligned}$$

where $\mathtt{au}(s, u)$, $\mathtt{apr}(s, u)$ or $\mathtt{avr}(s, u)$ is the Assumptive set of Users, Physical Resources or Virtual Resources inside the Secure Space s after granting the User u to enter there and

regulating its contents to keep secure, respectively.

$$\begin{aligned}
\mathtt{au}(s,u) &= \mathtt{cu}(s) \cup \{u\} \\
\mathtt{apr}(s,u) &= \{pr \in \mathtt{cpr}(s) | (pr,u,s,\mathtt{ac}(s,u)) \in \mathtt{PRAP} \\
&\qquad \text{and } (u,pr,s,\mathtt{ac}(s,u)) \in \mathtt{UAP}\} \\
\mathtt{avr}(s,u) &= \{vr \in \mathtt{cvr}(s) | (vr,u,s,\mathtt{ac}(s,u)) \in \mathtt{VRAP} \\
&\qquad \text{and } (u,vr,s,\mathtt{ac}(s,u)) \in \mathtt{UAP}\} \\
\mathtt{ac}(s,u) &= \mathtt{au}(s,u) \cup \mathtt{apr}(s,u) \cup \mathtt{avr}(s,u) \\
\mathtt{cw}(s) &= \mathtt{w}(s,\mathtt{cc}(s)) \\
\mathtt{aw}(s,u) &= \mathtt{w}(s,\mathtt{ac}(s,u))
\end{aligned}$$

Algorithm 1.2: Authorization for Physical Resources

An entry request $prer = (pr, s) \in \mathtt{PRER}$ that a Physical Resource pr requests to enter a Secure Space s is granted, if and only if the Physical Resource pr grants any User (visitor) inside there to access itself and is granted to be accessed by any User (visitor) inside there.

$$\begin{aligned}
&\mathtt{authR}(prer) = \mathtt{authR}(pr,s) = \mathtt{grant} \\
&\Leftrightarrow \mathtt{au}(s,pr) = \mathtt{cu}(s)
\end{aligned}$$

where $\mathtt{au}(s,pr)$ is the Assumptive set of authorized Users who have right to access any Resource in the Secure Space s even after granting the Physical Resource pr to enter there.

$$\begin{aligned}
\mathtt{au}(s,pr) &= \{u \in \mathtt{cu}(s) | (pr,u,s,\mathtt{ac}(s,pr)) \in \mathtt{PRAP} \\
&\qquad \text{and } (u,pr,s,\mathtt{ac}(s,pr)) \in \mathtt{UAP}\} \\
\mathtt{apr}(s,pr) &= \mathtt{cpr}(s) \cup \{pr\} \\
\mathtt{avr}(s,pr) &= \{vr \in \mathtt{cvr}(s) | (vr,u,s,\mathtt{ac}(s,pr)) \in \mathtt{VRAP} \\
&\qquad \text{and } (u,vr,s,\mathtt{ac}(s,pr)) \in \mathtt{UAP}, \forall u \in \mathtt{cu}(s)\} \\
\mathtt{ac}(s,pr) &= \mathtt{au}(s,pr) \cup \mathtt{apr}(s,pr) \cup \mathtt{avr}(s,pr)
\end{aligned}$$

Algorithm 1.3: Authorization for Virtual Resources

An entry request $vrer = (vr, s) \in \mathtt{VRER}$ that a Virtual Resource vr requests to enter a Secure Space s is granted, if and only if the Virtual Resource vr grants any User (visitor) inside there to access itself and is granted to be accessed by any User (visitor) inside there.

$$\begin{aligned}
&\mathtt{authR}(vrer) = \mathtt{authR}(vr,s) = \mathtt{grant} \\
&\Leftrightarrow \mathtt{au}(s,vr) = \mathtt{cu}(s)
\end{aligned}$$

where $\mathtt{au}(s,vr)$ is the Assumptive set of authorized Users who have right to access any resource in the Secure Space s even after granting the Virtual Resource vr to be outputted via its embedded device (e.g., a display and speaker).

$$\begin{aligned}
\mathtt{au}(s,vr) &= \{u \in \mathtt{cu}(s) | (vr,u,s,\mathtt{ac}(s,vr)) \in \mathtt{VRAP} \\
&\qquad \text{and } (u,vr,s,\mathtt{ac}(s,vr)) \in \mathtt{UAP}\} \\
\mathtt{apr}(s,vr) &= \{pr \in \mathtt{cpr}(s) | (pr,u,s,\mathtt{ac}(s,vr)) \in \mathtt{PRAP} \\
&\qquad \text{and } (u,pr,s,\mathtt{ac}(s,vr)) \in \mathtt{UAP}, \forall u \in \mathtt{cu}(s)\} \\
\mathtt{avr}(s,vr) &= \mathtt{cvr}(s) \cup \{vr\} \\
\mathtt{ac}(s,vr) &= \mathtt{au}(s,vr) \cup \mathtt{apr}(s,vr) \cup \mathtt{avr}(s,vr)
\end{aligned}$$

III. Ability-Based Expression Control

This section proposes an extended model of Ability-Based Expression Control according to how preferentially a virtual information resource should be outputted in a Secure Space where shared by visitors with perceptibility and understandability of the virtual information resource's content and expression, aiming to build more flexible Secure Spaces.

Definition 5: Information Expressions and User Abilities

The extended model uses the following information expressions and user abilities for expression control over virtual resources via output devices (e.g., displays and speakers) embedded in Secure Spaces based on their visitors' abilities (e.g., medium-perceptibility and language-understandability).

- **Virtual Resource's Expression:** is an expression form for Virtual Resources, defined as a 2-tuple of a Medium (e.g., optical and spoken) and a Language,

  $$\mathtt{E} \subseteq \mathtt{M} \times \mathtt{L}.$$

  $(m, l) \in \mathtt{E}$ where $m \in \mathtt{M} = \{\ \mathtt{Visual}, \mathtt{Aural}, \ldots\ \}$ and $l \in \mathtt{L} = \{\ \mathtt{Japanese}, \mathtt{English}, \ldots\ \}$, states that a virtual information resource's content is expressed in the Medium m and the Language l.
- **User's Ability:** is an ability of information perceptibility and understandability for a User, defined as a 3-tuple of the User, a Virtual Resource, and an Expression form,

  $$\mathtt{A} \subseteq \mathtt{U} \times \mathtt{VR} \times \mathtt{E}.$$

  $(u, vr, e) \in A$ where $u \in \mathtt{U}$, $vr \in \mathtt{VR}$, and $e \in \mathtt{E}$, states that the User u can perceive and understand the content of Virtual Resource vr in the Expression form e.

For example, a Japanese User u_A who has the following abilities can grasp any Japanese information written and/or spoken, while she can grasp English information not spoken but written because she is not very good at English:

- $(u_A, \forall vr, (\mathtt{Visual}, \mathtt{Japanese}))$,
- $(u_A, \forall vr, (\mathtt{Aural}, \mathtt{Japanese}))$,
- $(u_A, \forall vr, (\mathtt{Visual}, \mathtt{English}))$.

Maybe, the Japanese User u_A prefers the second ability (expression form) because she could switch it by herself by putting noise-canceling headphones on/off.

Meanwhile, an English User u_B who has the following ability can catch only English information not spoken but written because he are putting noise-canceling headphones on:

- $(u_B, \forall vr, (\mathtt{Visual}, \mathtt{English}))$.

When he will put his headphones off, he would acquire the additional (inherent) ability and become able to catch any English information not only written but also spoken:

- $(u_B, \forall vr, (\mathtt{Aural}, \mathtt{English}))$.

Maybe, a space entry control system for Secure Spaces considers his latter ability to be more insecure and unsafe.

In a Secure Space, a Virtual Resource vr_1 (originally-created in English) is being outputted in Visual and English expression form, and there is its authorized User (visitor) u_A. Then, its unauthorized User (potential visitor) u_B requests to enter the Secure Space. If the Secure Space is based on the previous model as introduced in Section II, the system has only two approaches of preventing its unauthorized User u_B from entering the Secure Space and permitting him to enter the Secure Space after revoking the Virtual Resource vr_1 like Fig. 4. Thus the entry request by its unauthorized User u_B is rejected, or not only its unauthorized User u_B but also its authorized User u_A become unable to access it.

Meanwhile, if the Secure Space is based on the extended model by Ability-Based Expression Control as proposed in this Section III, the system has an approach of permitting its unauthorized User u_B to enter the Secure Space after converting the Virtual Resource vr_1 in Visual and Japanese expression form, which its authorized User u_A has but its unauthorized User u_B does not have as her/his abilities for it, i.e., which she can but he cannot perceive and understand, as shown in Fig. 5. Thus the entry request by its unauthorized User u_B is accepted, and also its authorized User u_A can keep accessing it, unlike the previous model.

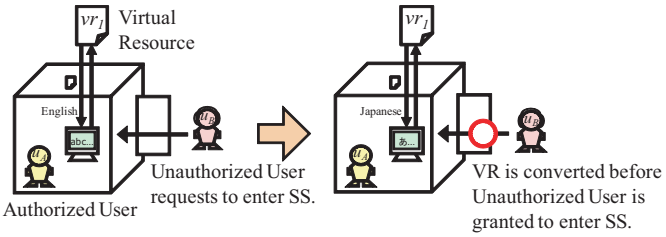

Fig. 5. Ability-Based Expression Control over Virtual Resources

IV. Conclusion

In public spaces, there are a number of different contents such as visitors, physical information resources, and virtual information resources via their embedded output devices (e.g., displays and speakers). Therefore, we might unexpectedly enter the public spaces that have our unauthorized contents and/or unwanted characteristics, i.e., "public spaces are not always secure and safe for any visitor and information resource." To solve this problem, my previous work [7–13] introduced the novel concept of *"Secure Spaces"*, physically isolated environments in which any visitor is protected from being pushed her unwanted information resources on and also any information resource is always protected from being accessed by its unauthorized visitors, and the model and architecture for space entry control and information access control based on their dynamically changing contents. Aiming to build more flexible Secure Spaces, this paper has proposed an extended model for not only spatial entry control but also Ability-Based Expression Control according to how preferentially a virtual information resource should be outputted in a Secure Space where shared by visitors with perceptibility and understandability of information content and expression.

Acknowledgment

This work was supported in part by JSPS Grant-in-Aid for Young Scientists (B) "A research on Web Sensors to extract spatio-temporal data from the Web" (#23700129, Project Leader: Shun Hattori, Years: 2011-2012).

References

[1] L. Rosenthal and V. Stanford, "NIST Smart Space: Pervasive Computing Initiative," Proceedings of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'00), pp.6–11, 2000.

[2] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, "Cerberus: A Context-aware Security Scheme for Smart Spaces," Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom'03), pp.489–496, 2003.

[3] G. Sampemane, P. Naldurg, and R. H. Campbell, "Access Control for Active Spaces," Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02), pp.343–352, 2002.

[4] Y. J. Song, W. Tobagus, D. Y. Leong, B. Johanson, and A. Fox, "iSecurity: A Security Framework for Interactive Workspaces," Technical Report, Stanford University, 2003.

[5] M. J. Covington,W. Long, S. Srinivasan, A. Dey, M. Ahamad, and G. Abowd, "Securing Context-aware Applications Using Environment Roles," Proceedings of the 6th ACM Symposium on Access Control Models and Technologies (SACMAT'01), pp.10–20, 2001.

[6] P. G. McLean, "A Secure Pervasive Environment," Proceedings of the Australasian Information Security Workshop 2003 (AISW'03), Conferences in Research and Practice in Information Technology, pp.67–75, 2003.

[7] S. Hattori, T. Tezuka, and K. Tanaka, "Content-Based Entry Control for Secure Spaces," Proceedings of the International Workshop on Future Mobile and Ubiquitous Information Technologies (FMUIT'06), pp.98, 2006.

[8] S. Hattori, T. Tezuka, and K. Tanaka, "Secure Spaces: Physically Protected Environments for Information Security," Proceedings of the Joint 3rd International Conference on Soft Computing and Intelligent Systems and 7th International Symposium on advanced Intelligent Systems (SCIS&ISIS'06), TH-B5-2, pp.687–691, 2006.

[9] S. Hattori and K. Tanaka, "Secure Spaces: Protecting Freedom of Information Access in Public Places," Proceedings of the 5th International Conference on Smart Homes and Health Telematics (ICOST'07), LNCS Vol.4541, pp.99–109, 2007.

[10] S. Hattori and K. Tanaka, "Towards Building Secure Smart Spaces for Information Security in the Physical World," Journal of Advanced Computational Intelligence and Intelligent Informatics (JACIII), Vol.11, No.8, pp.1023–1029, 2007.

[11] S. Hattori and K. Tanaka, "Mining the Web for Access Decision-Making in Secure Spaces," Proceedings of the Joint 4th International Conference on Soft Computing and Intelligent Systems and 9th International Symposium on advanced Intelligent Systems (SCIS&ISIS'08), TH-G3-4, pp.370–375, 2008.

[12] S. Hattori, "Context-aware Search Control for Secure Spaces," Proceedings of the Joint 5th International Conference on Soft Computing and Intelligent Systems and 11th International Symposium on advanced Intelligent Systems (SCIS&ISIS'10), SA-D4-2, pp.1348–1353, 2010.

[13] S. Hattori, "Context-Aware Query Control for Secure Spaces," Journal of Computer Technology and Application (JCTA), Vol.3, No.2, pp.130–139, 2012.

[14] S. Hattori, "Linearly-Combined Web Sensors for Spatio-Temporal Data Extraction from the Web," Proceedings of the 6th International Workshop on Spatial and Spatiotemporal Data Mining (SSTDM'11), pp.897–904, 2011.

[15] S. Hattori, "Secure Spaces and Spatio-Temporal Weblog Sensors with Temporal Shift and Propagation," Proceedings of the 2011 First IRAST International Conference on Data Engineering and Internet Technology (DEIT'11), pp.1042–1047, Recent Progress in Data Engineering and Internet Technology Volume 2, LNEE Vol.157, pp.343–349, 2012.

[16] S. Hattori, "Spatio-Temporal Web Sensors by Social Network Analysis," Proceedings of the 3rd International Workshop on Business Applications of Social Network Analysis (BASNA'12), pp.1020–1027, 2012.