

Mô hình Kiểm soát Quyền Truy cập Cơ sở Dữ liệu Hệ thống Thông tin Địa lý Quản lý Dân cư của Một Tỉnh theo Không gian – Thời gian

Lê Minh Tuyền

Trường Cao đẳng Kỹ thuật Lý Tự Trọng
lmtuyen@gmail.com

Tóm tắt. Cơ sở dữ liệu hệ thống thông tin địa lý quản lý dân cư của một tỉnh là một cơ sở dữ liệu có tính chất vừa phân cấp, vừa phân nhóm, vừa theo không gian, vừa theo thời gian. Một tỉnh có 03 cấp quản lý bao gồm: cấp tỉnh, cấp quận/huyện, cấp phường/xã đây là yếu tố phân cấp đồng thời cũng là yếu tố không gian đơn vị hành chính quản lý. Dữ liệu về dân cư bao gồm các thuộc tính của một người dân sống tại Tỉnh, các thuộc tính này được gom nhóm để phù hợp với Ban/ngành quản lý của tỉnh; Mỗi yếu tố không gian tồn tại với một thời điểm xác định và tương tự các thuộc tính dân cư cũng tồn tại theo thời điểm đó. Vì tính chất vừa phân cấp, vừa phân nhóm, vừa theo không gian, vừa theo thời gian tạo nên cơ sở dữ liệu đa chiều do đó việc kiểm soát truy cập là yếu tố cần thiết và đang được nghiên cứu trong luận án tiến sĩ.

Từ khóa: không gian, thời gian, phân cấp, phân nhóm, kiểm soát truy cập.

1 Giới thiệu

Việc kiểm soát truy cập cơ sở dữ liệu dân cư dựa vào các yếu tố vừa phân nhóm – vừa phân cấp - vừa theo không gian - vừa theo thời gian, do đó cơ sở dữ liệu có những mối liên quan nhất định, có sử dụng dữ liệu chung. Vì vậy cần kiểm soát việc truy cập – thao tác với cơ sở dữ liệu của hệ thống đó.

Để thực hiện việc kiểm soát truy cập cơ sở dữ liệu việc khảo sát và xây dựng mô hình kiểm soát truy cập dựa trên nền tảng các kiểm soát truy cập [19] là hướng đi của luận án. Bên cạnh do có yếu tố không gian nên được thực hiện trên nền tảng GIS, nhằm thể hiện trực quan hóa các thông tin cần quản lý giúp ứng dụng vào thực tế một cách hiệu quả hơn.

Các kiểm soát truy cập hiện tại chưa đáp ứng đủ các yếu tố cũng như nhu cầu cần thiết trong việc kiểm soát truy cập thực tế tại Việt Nam. Do đó yêu cầu của luận án là phối hợp các kiểm soát truy cập hiện có, thông qua các tài liệu tham khảo được, phối hợp thêm với yêu cầu thực tế của đơn vị hành chính hình thành mô hình kiểm soát truy cập mới đáp ứng được và sử dụng được trong hiện thực.

Mô hình kiểm soát đặt ra cần đáp ứng các yêu cầu: phân quyền cho người truy cập dựa trên không gian mà người truy cập được cho phép, đồng thời quản lý được việc thay đổi yếu tố không gian theo thời gian trong thế giới thực như thay đổi đơn vị hành chính (vd: 3 phường thuộc quận A năm 2012, đến năm 2013 cần sát nhập 2 phường

của quận A sang quận B), ghi nhận và phân chia thao tác của người truy cập (xem – thêm – cập nhật) trên nhóm dữ liệu dân cư cũng như không gian được cho phép theo thời gian người truy cập được cấp quyền. Thông qua những yêu cầu đó, đây là một mô hình mà hội tụ các kiểm soát truy cập theo: vai trò [6] [13] – các quy tắc [19] – thời gian [1] – vị trí [1] và cần mẫn hóa dữ liệu [5] [9] cho phù hợp quyền của người truy cập. Tuy nhiên hiện tại các tài liệu và các công trình liên quan đến việc kiểm soát truy cập thỏa mãn các yêu cầu trên chưa được tìm thấy.

Trên tinh thần của việc xây dựng mô hình kiểm soát truy cập cơ sở dữ liệu tác giả đã thực hiện 2 bài báo về việc kiểm soát truy cập là “The Access Control Cube For A Geodatabase Of A Provincial Government Agency” [11] và “To Assign and Control the Right Accessing Geo-Database by Access Control Cube” [12].

2 Các công trình liên quan

2.1 Trước 5 năm

Hong Zhu¹ và Kevin Lü². Fine-Grained Access Control For Database Management Systems. Database Management Systems. (2007): Giới thiệu về cách mẫn hóa cơ sở dữ liệu, phục vụ cho việc rút trích cơ sở dữ liệu theo dòng và cột tùy thuộc vào người dùng có những quyền truy cập nào. Tạo ra một cơ sở dữ liệu thu nhỏ chỉ dành cho người sử dụng đó áp dụng trong cơ sở dữ liệu quan hệ. Điểm yếu là phương pháp tiếp cận, không thể truy cập nhiều đối tượng trong cùng một thời điểm.

Liliana Kasumi Sasaoka¹, Claudia Bauzer Medeiros. Access Control In Geographic Databases. (2006): Giới thiệu về cách kiểm soát truy cập cơ sở dữ liệu địa lý. Sử dụng việc kiểm soát truy cập dựa vào vai trò và luật không phù hợp với truy cập dưới dạng mẫn hóa cơ sở dữ liệu. Thực hiện kiểm soát truy cập theo lớp dữ liệu.

Vincent C. Hu , David F.Ferraiolo, Rick Kuhn . Assessment of Access Control Systems.(2006): Trình bày tổng quan khái niệm về các kỹ thuật kiểm soát truy cập như rule base, role base, time base, location base... và các khái niệm về object, subject trong việc kiểm soát truy cập cơ sở dữ liệu.

2.2 Sau 5 năm

Clara Bertolissi Maribel Fernandez: “Time and Location Based Services With Access Control”. (2008): Giới thiệu về kiểm soát truy cập theo thời gian và vị trí. Việc kiểm soát truy cập dựa theo vai trò và có tích hợp thêm yếu tố vị trí và thời gian dùng để ghi lại lịch sử truy cập cơ sở dữ liệu của người truy cập. Chưa ghi nhận lại sự thay đổi vị trí theo thời gian.

Haibing Lu And Yingjiu Li: “ Practical Inference Control For Data Cubes”(2008): Mô hình khối trong việc điều khiển truy cập cơ sở dữ liệu.

Hsing-Chung Chen: “A Generalized Temporal And Spatial Role-Based Access Control Model”,.Department of Computer Science and Engineering, Asia University, IEEE Member Taichung County, Taiwan 41354(2010): Được áp dụng cho điện thoại. Truy cập theo vị trí động, mang yếu tố tạm thời.

Jan Herrmann: “Access Control In Spatial Data Infrastructures”. Technical University Munich(2010): kiểm soát truy cập trong cơ sở hạ tầng dữ liệu không gian.

Jie Shi, Hong Zhu: “A Fine-Grained Access Control Model For Relational Databases”. College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China (2010): Mô hình kiểm soát truy cập mịn hóa dữ liệu (chia nhỏ dữ liệu) với cơ sở dữ liệu quan hệ. Cho thấy dữ liệu nào được phép truy cập bởi người truy cập nào và nhiều người cùng truy cập vào một dữ liệu được cho phép. Đây là mô hình mịn hóa dữ liệu trong trường hợp có nhiều chính sách truy cập cơ sở dữ liệu.

3 Các công trình đã làm

3.1 The Access Control Cube For A Geodatabase Of A Provincial Government Agency. ISSN: 2010-460X

Giới thiệu

Một hệ thống thông tin địa lý tại một cơ quan cấp tỉnh được sử dụng bởi nhiều người. Họ có thể thêm – xóa – sửa – xem dữ liệu trong cơ sở dữ liệu địa lý. Quyền truy cập phải được điều khiển để đảm bảo chính xác và trọn vẹn dữ liệu[4].

Trong một hệ thống nhiều người dùng, quyền truy cập và xử lý dữ liệu phải được điều khiển để gán trách nhiệm cho từng nhân viên làm việc với dữ liệu[4].

Thành phần của dữ liệu: subject, location và operation hình thành một khối truy cập được gọi là Access Control Cube (ACC). Khối 3 chiều này bao gồm các trục tạo độ: subjects, locations, operations. Giá trị của trục subject là các lớp dữ liệu của các đối tượng, giá trị của trục location là các khu vực địa lý cần quản trị, giá trị của trục operation là những thao tác như thêm – xóa – sửa – xem với dữ liệu.

Các giá trị này chia ACC thành nhiều khối nhỏ gọi là cell. Mỗi cell phụ thuộc vào một layer trên trục subject, một khu vực địa lý cần quản trị trên trục location và một thao tác được giao trên trục operation. Một nhóm gồm một hoặc nhiều cell được gọi là agent, một agent được giao cho một nhân viên làm việc với cơ sở dữ liệu không gian. Framework (công việc khung) của một cơ sở dữ liệu cần làm là xác định quyền truy cập – các quy tắc để giao cho nhân viên làm việc với cơ sở dữ liệu không gian. Công việc khung này dựa vào mô hình Access Control Cube.

Một số khái niệm

Agent: là một nhóm các ô, hoặc tập hợp các ô để xác định quyền của người truy cập trên các lớp dữ liệu, đối tượng không gian, tại những vị trí xác định trên trục tọa độ của Access Control Cube. Ví dụ: chỉ định quyền của người truy cập trên lớp dữ liệu về nhà ở của Huyện Thuận An.

Authority (người cầm quyền): là một nhân viên của cơ quan chính phủ được giao quyền thao tác truy cập vào csdl địa lý với một khoản thời gian cố định.

Cell: là một phần tử của một Access Control Cube. Được tạo ra từ giá trị của một lớp, một khu vực và một thao tác trên trục tọa độ của ACC.

Layer (lớp): là một tập hợp các dữ liệu không gian và thuộc tính như điểm (point), đường thẳng (line), vùng (polygon). Ví dụ: lớp nhà được biểu diễn dưới dạng vùng

(polygon), lớp cầu được biểu diễn dưới dạng điểm (point), lớp đường được biểu diễn dạng đường thẳng (line).

Location (vị trí): là một khu vực của đối tượng trong thế giới thực. Trong bài này là các quận/huyện thuộc 1 tỉnh.

Subject: tập hợp các lớp dữ liệu hoặc các chuyên đề.

Theme (chuyên đề): là tập hợp các lớp của nhiều loại đối tượng mà cơ quan chính phủ có trách nhiệm quản lý

Ví dụ: chuyên đề về giao thông bao gồm các lớp đường, xe hơi, xe máy, Một lớp có thể được sử dụng trong nhiều chuyên đề khác nhau tùy thuộc vào chức năng của cơ quan chính phủ.

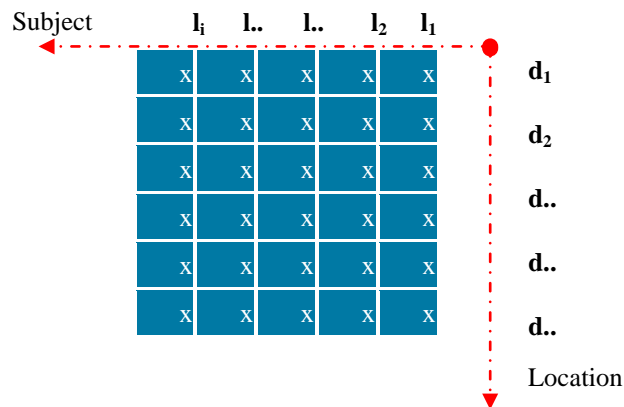
Geo-database (cơ sở dữ liệu địa lý): là một cơ sở dữ liệu mà chứa các dữ liệu không gian và dữ liệu thuộc tính của tất cả các đối tượng được quản lý bởi cơ quan chính phủ. **THE CUBE MODEL FOR CONTROLLING GEODATABASE ACCESS**

A. Ma trận quan hệ giữa subject và location

Mỗi thực thể tồn tại trong thế giới thực được xác định bởi nơi chốn và tiêu đề. Ví dụ: sở khoa học công nghệ bình dương đóng tại đường Huỳnh văn nghệ, thị xã Thủ Dầu Một.

Những thực thể này được biểu diễn như một đối tượng không gian trong csdl địa lý của hệ thống thông tin địa lý.

Trong không gian 2 chiều, gồm trục tọa độ subject kí hiệu $S = \{l_1, l_2, \dots, l_i\}$ và location $L = \{d_1, d_2, \dots, d_j\}$ thể hiện quan hệ nhiều – nhiều. Xem hình 1



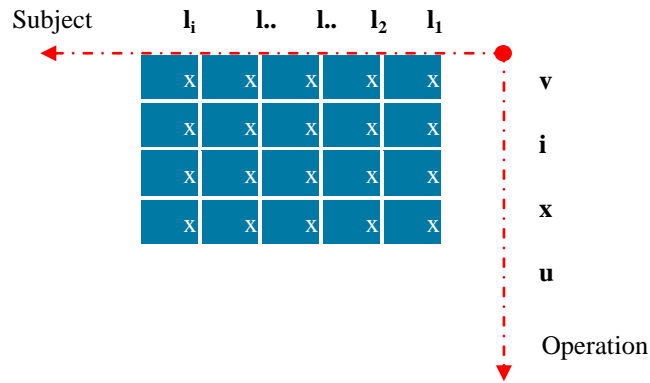
Hình 1. Ma trận Subject và Location

B. Ma trận quan hệ giữa subject và operation

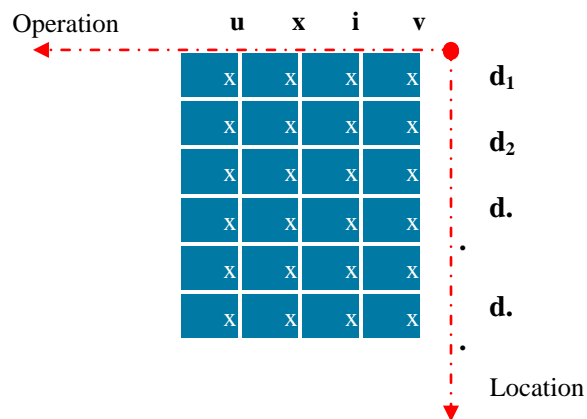
Thể hiện mối quan hệ nhiều - nhiều giữa các lớp dữ liệu (subject) và thao tác (operation) kí hiệu $O = \{view, insert, delete, update\} = \{v, i, x, u\}$. Xem hình 2

C. Ma trận quan hệ giữa operation và location

Ma trận này xác định quyền thao tác của đơn vị quản lý hành chính. Xem hình 3



Hình 2. Ma trận Subject và Operation



Hình 3. Ma trận Operation và Location

D. Khối điều khiển truy cập (ACC)

Tích hợp quan hệ của các ma trận trên, hình thành một ma trận 3 chiều hình khối được gọi là Access Control Cube (ACC) làm mô hình khái niệm cho hệ thống điều khiển truy cập cơ sở dữ liệu địa lý đối với hệ thống thông tin địa lý. Trong mô hình này các trục tạo độ bao gồm: subject, location, operation.

Do đó, mỗi cell của một ACC xác định quyền truy cập trên một lớp dữ liệu cố định thuộc 1 khu vực nhất định trong cơ sở dữ liệu địa lý $(O,S,L) = \{(v,l_1,d_1),(i,l_1,d_1), \dots,(u,l_1,d_j),(u,l_i,d_j)\}$. Số lượng cell được tạo ra là $4 \times i \times j$

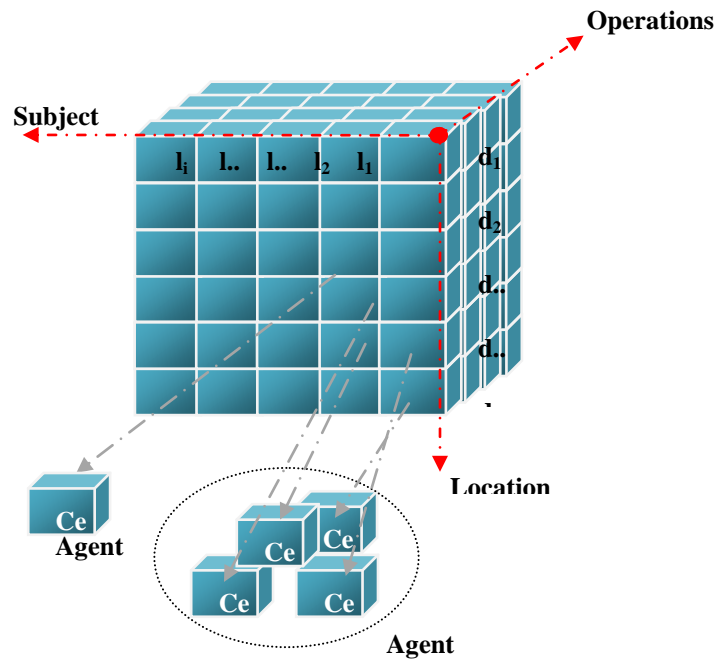
Với:

4: số lượng các thao tác bao: thêm – xóa – sửa – xem

i: số lượng các lớp trong cơ sở dữ liệu trên trục subject

j: số lượng các khu vực quản trị trong cơ sở dữ liệu trên trục location.

Người quản trị hệ thống GIS chỉ định quyền tối với những người dùng nào, để truy cập và làm việc với cơ sở dữ liệu địa lý. Quan hệ giữa một người được giao quyền và một agent là quan hệ một – nhiều. Mỗi người được giao quyền, có thể được giao một hoặc nhiều agent, nhưng mỗi agent chỉ được giao cho một người nhằm đảm bảo trách nhiệm cá nhân đối với csdl. Xem hình 4



Hình 4. Access Control Cube

Tích hợp Thời gian và Quyền Truy cập

Mỗi agent được giao cho một người dùng trong một khoản thời gian xác định. Bảng: Danh sách điều khiển truy cập (Access control list) thể hiện việc phân chia quyền – khu vực – lớp dữ liệu – thời gian – người dùng – và agent[7][9]. Mỗi thay đổi về quyền truy cập phải được cập nhật trong bảng 1.

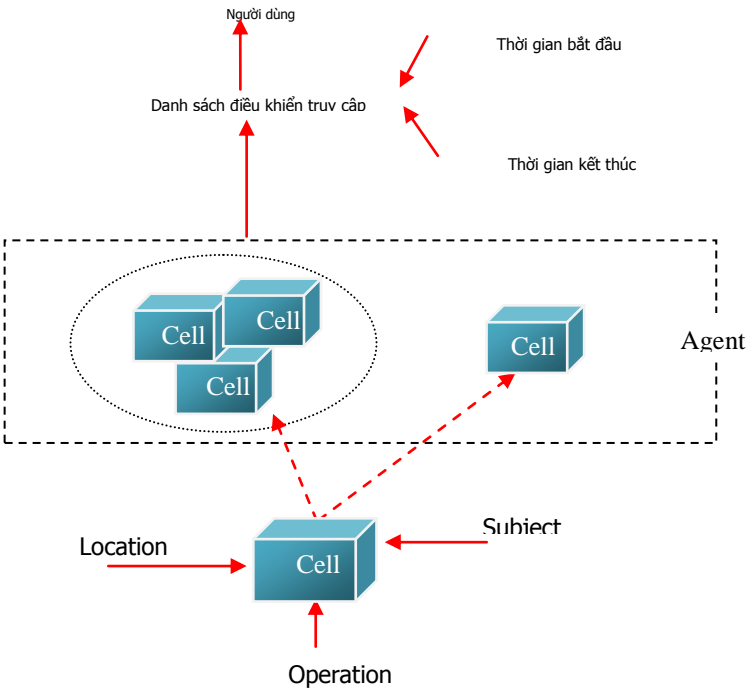
Cài đặt

Trong trường hợp này, các cell của ACC được gom nhóm để hình thành các agent dựa trên trách nhiệm quản trị của cơ quan hành chính đó. Xem hình 5

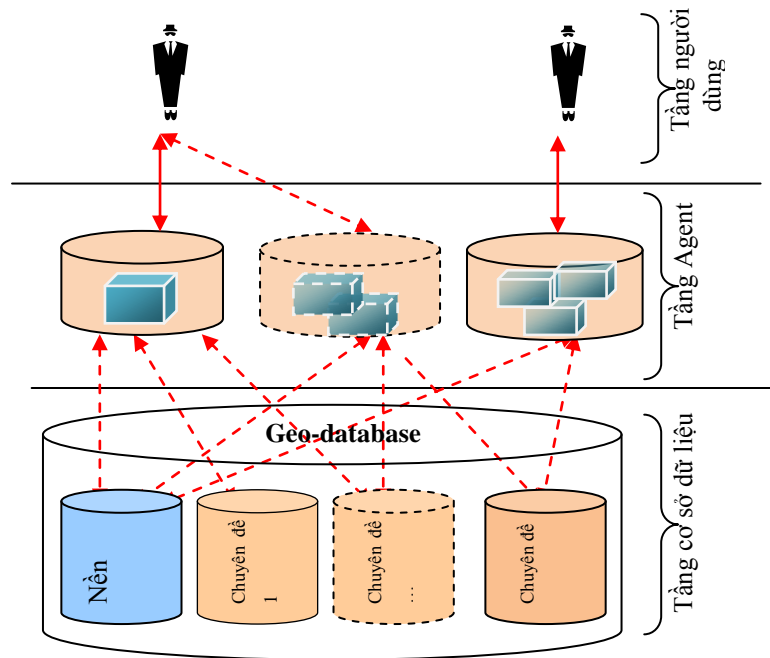
Hệ thống điều khiển truy cập với cơ sở dữ liệu địa lý được thiết kế theo mô hình 3 tầng. Tại tầng cơ sở dữ liệu địa lý: bao gồm nhiều chuyên đề được thiết kế để lưu trữ tất cả dữ liệu không gian và thuộc tính. Tầng Agent: các lớp dữ liệu trong cơ sở dữ liệu địa lý được gom nhóm theo tập hợp agent mà được xác định bằng các cell của agent đó. Tầng người dùng: người dùng tương tác với dữ liệu trên tập dữ liệu ở tầng Agent. Xem hình 6

Bảng 1. Quyền truy cập.

Người dùng	Agent	Thao tác	Vị trí (khu vực)	Lớp dữ liệu	Khoản thời gian giao quyền	
					Bắt đầu	Kết thúc
U ₁	A ₁	v ₁	d ₁	l ₁	11/11/10	11/12/10
U ₂	A ₁	v ₁	d ₁	l ₁	12/12/10	01/12/11
U ₃	A ₁	v1	d ₁	l ₁	11/11/10	12/11/10
U ₄	A ₁	v1	d ₁	l ₁	11/11/10	12/11/10
U ₅	A ₁	v1	d ₁	l ₁	11/11/10	12/11/10
U ₆	A ₂	v1	d ₁	l ₁	11/11/10	12/11/10
...



Hình 5. Phiên làm việc của Access Control Cube



Hình 6. Mô hình 3 tầng để áp dụng Access control cube

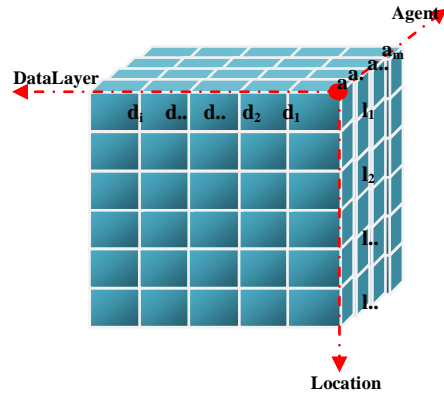
3.2 To Assign And Control The Right Accessing Geo-Database By Access Control Cube ISBN: 978-1-4244-9450-7; ISBN: 978-1-4244-9451-4

Trong cơ sở dữ liệu quyền truy cập phải được điều khiển để đảm bảo chính xác và an toàn dữ liệu và trách nhiệm của từng cá nhân quản lý cơ sở dữ liệu đó. Mỗi người truy cập (Agent) vào cơ sở dữ liệu địa lý được giao quyền truy cập trên những lớp dữ liệu (Datalayer) cụ thể tại những vị trí địa lý (location). Các quyền này bao gồm: xem và cập nhật. Quyền cập nhật bao gồm: xem, thêm, xóa dữ liệu. Việc phân quyền này cũng còn tùy thuộc vào vai trò của người truy cập.

Bài báo này phân tích cấu trúc cơ sở dữ liệu địa lý của một cơ quan hành chính và phát triển mô hình Object Access Control Cube (OACC) dựa vào mô hình Access Control Cube (ACC) [5][6][7][10]. Cấu trúc của Object Access Control Cube quyền của người truy cập dựa vào vùng địa lý, đối tượng không gian của lớp dữ liệu. Quyền truy cập bao gồm: Xem và Cập nhật. Thông thường một Object Access Control Cube được chia thành View Object Access Control Cube và Update Object Access Control Cube. Một View Access Control Cube có thể được giao cho một hoặc nhiều người truy cập, trong khi một Update Access Control Cube chỉ được giao cho một người truy cập duy nhất.

Object Access-Control-Cube: Là một khối 3 chiều[1][2][4], một Object-Access-Control-Cube (OACC) được phân chia thành View OACC (V-OACC), Update

OACC (U-OACC). V-OACC nghĩa là chỉ có quyền xem và U-OACC là có quyền thêm – xóa – xem dữ liệu[11]. Thành phần của Object-Access-Control-Cubes là:



Hình 7. Object Access Control Cube

Location (l): các vùng địa lý như quận/huyện, phường/xã

Data layer (d): các đối tượng.

Time (t): thời điểm giao quyền hoặc hủy quyền được giao.

Agent (a): người truy cập csdl

Operation: View (v) / Update (u) (bao gồm thêm, xóa, cập nhật).

Với V-OACC, quan hệ giữa người truy cập và đối tượng không gian là quan hệ nhiều-nhiều. Một người truy cập được xem nhiều hoặc một đối tượng. Tương tự, đối tượng trong một vùng được xem bởi một hoặc nhiều người truy cập.

Với U-OACC, mỗi quan hệ giữa người truy cập và đối tượng không gian là nhiều-nhiều và quan hệ đối tượng không gian với người truy cập là quan hệ một-nhiều. Một người truy cập có thể thao tác trên một hoặc nhiều vùng.

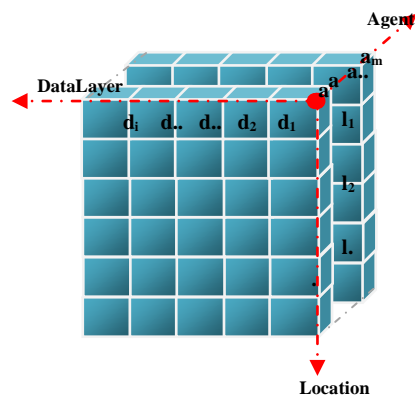
Một khối V-OACC hoặc U-OACC cung cấp ma trận View hoặc ma trận Update phụ thuộc vào sự giao nhau của trục tọa độ datalayer và location với trục tọa độ agent (Hình 8)

Quyền của người truy cập được xác định bởi ma trận tích hợp view và matrix. (Hình 9).

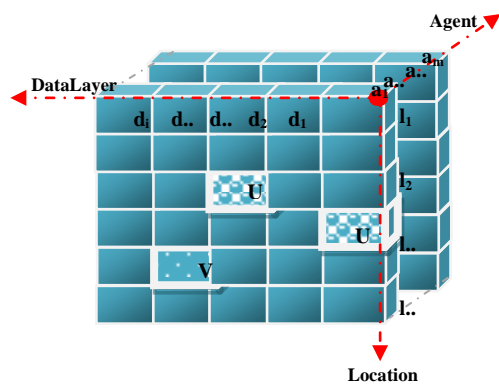
Thêm vào trục tọa độ thời gian cho người truy cập, một khối Agent OACC (A-OACC) được tạo ra để xác định khoản thời gian mà người truy cập chịu trách nhiệm đối với mỗi công việc (Hình 10).

Sau khi đăng nhập chính xác vào cơ sở dữ liệu, cửa sổ ứng dụng xuất hiện để điều khiển quyền của người truy cập theo các bước: **Login → Subject → Zone → Data Layer → Object → Attribute** và các thủ tục của cập nhật xuất hiện khi người truy cập chọn một đối tượng chắc chắn.

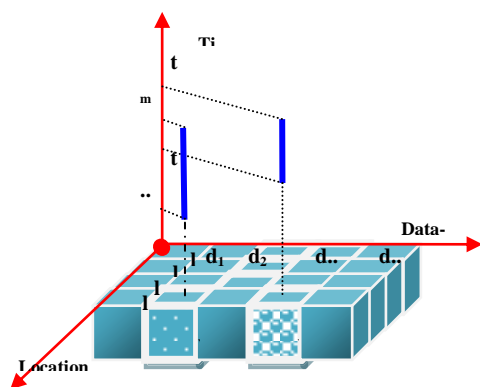
Tóm lại với mô hình này người quản trị có thể điều khiển truy cập của người dùng đối với cơ sở dữ liệu địa lý nhiều người truy cập. Mô hình Object Access Control Cube không những chỉ định nhiệm vụ của người truy cập mà còn xác định trách nhiệm của mỗi người truy cập đối với việc chính xác dữ liệu cho mỗi đối tượng.



Hình 8. Agent matrix



Hình 9. Integrated Matrix



Hình 10. Agent Cube

Thuận lợi của mô hình OACC không chỉ là gán quyền truy cập cho hệ thống GIS mà còn gán quyền thao tác xem hoặc cập nhật đối tượng và xác định trách nhiệm của người truy cập với dữ liệu của mỗi đối tượng

Tài liệu tham khảo

1. Clara Bertolissi Maribel Fernandez: "Time and Location Based Services With Access Control".(2008).
2. Daut Daman, Harihodin Selamat, Shafrv Rahim: "The Integration Of Spatial And Non-Spatial Data Model". Faculty Science Computer and Information System, University of Technology Malaysia, 81310 Skudai, Johor.(2000)
3. Gjermund Hanssen: "Concurrency Control In Distributed Geographical Database Systems". Department of Mapping Sciences, Agricultural University of Norway.(2002)
4. Haibing Lu And Yingjiu Li: "Practical Inference Control For Data Cubes" (2008)
5. Hong Zhu1 And Kevin Lü2: "Fine-Grained Access Control For Database Management Systems". Database Management Systems.(2007)
6. Hsing-Chung Chen: "A Generalized Temporal And Spatial Role-Based Access Control Model".Department of Computer Science and Engineering, Asia University, IEEE Member Taichung County, Taiwan 41354(2010)
7. Jan Herrmann: "Access Control In Spatial Data Infrastructures". Technical University Munich(2010)
8. Jiayuan Lina, Yu Fanga, Bin Chena, Pengfei Wua, Analysis Of Access Control Mechanisms For Spatial Database. Stitute of Remote Sensing and Geographic Information System, Peking University Beijing, P.R.China,
9. Jie Shi, Hong Zhu: "A Fine-Grained Access Control Model For Relational Databases". College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China(2010)
10. Liliana Kasumi Sasaoka1, Claudia Bauzer Medeiros: "Access Control In Geographic Databases".(2006)
11. Phuoc Tran Vinh, Tuyen Le Minh: "The Access Control Cube For A Geodatabase Of A Provincial Government Agency".(2011)
12. Phuoc Tran Vinh, Tuyen Le Minh: "To Assign and Control the Right Accessing Geodatabase by Access Control Cube".(2011)
13. Ravi S.Sandhu And Edward J.Coyne: "Role Base Access Control Models" (1996)
14. Ravi S.Sandhu, Pierangela Samarati: "Access Control: Principles and Practice" (1994)
15. Roger E.Sanders: "Securing Data With Label-Based Access Control". EMC Corporation.(2008)
16. Sahadeb De, Caroline M. Eastman, Csilla Farkas: "Secure Access Control In A Multi-User Geodatabase".(2001)
17. Steven M. Bellovin : "Access Control Matrix".(2005)
18. Vijayalakshmi Atluri, Soon Ae Chun : "An Authorization Model For Geospatial Data".(2004)
19. Vincent C. Hu , David F.Ferraiolo, Rick Kuhn: "Assessment of Access Control Systems".(2006)