第四章

存取控制政策設計

在本章中，則針對系統中的存取控制政策來做探討與設計。首先會先介紹以存取控制為設計目的的情境模型，並詳細說明存取政策中的不同組成元件(目標、許可、個人設定)。最後則模擬一個執行環境，設計出一個簡單的存取控制政策。

4.1 情境模型設計

透過第三章所介紹的階層化圖示(圖 3.8)說明本研究存取政策之設計概念。因此以此為基礎所設計的情境模型，主要包含目標(target)、評估許可(effect)、個人設定(configuration)與其他子元件。藉由目標所定義的資訊，會形成規則系統中條件判斷(condition)的部份，也就是做為本系統推論引擎的評估準則。評估許可與個人設定則是屬於規則系統中之決策動作(action)，是根據目標所提供的情境資訊與已定義好的存取政策所衍生而得。當行動用戶所提供的情境滿足存取控制政策中的條件時，系統會授予資源的存取權並建立相對的連線設定與限制。一旦情境不滿足存取條件時，系統則會拒絕行動用戶對資源的存取，以防止更多安全性漏洞發生。

參考 eXtensible Access Control Markup Language (XACML)[1] 中來設計本研究的存取控制模型。在 XACML 中，以「目標」、「評估許可」與「條

[1] XACML: www.oasis-open.org/committees/xacml/

件」等元素來組成特定的存取控制政策。而我們則另外針對系統需求，又附加「個人設定」此一部份於存取控制政策上，用來表示行動用戶連線經過身分驗證與授權程序後，所必須指定與建立的連線限制。在本系統中，這些基本的元素會隨著環境之不同而改變其值，因此被定義為「情境」。以情境為設計原則的資源授權政策，透過動態的存取控制觸發機制，使得在多變的環境下，能夠隨時地根據目前的網路狀態來調整系統安全政策與設定。

除了上述組成存取控制政策的三大基本元素(目標、評估許可、個人設定)以外，在動態的行動網路環境下，各種網路環境中的變數都會直接或間接地影響到系統的授權決策。因此在設計存取控制政策的情境模型時，有關行動裝置的執行環境、行動用戶所扮演的角色、資源可得性、網路連線媒體、網域環境等因素都必須加以考量。圖4.1為參考不同的網路環境與遠端存取之安全性需求所設計的存取控制政策情境模型。在目標等基本類別下，又設計其它衍生子類別與類別間複雜的關連，以滿足實際環境之需求。

4.1.1 目標

目標(target)，是組成存取控制政策的一部份，用來描述授權政策所要適用的對象。在本系統中隨著安全需求等級之不同，定義出多種型態的資源授權政策，相對地也就需要不同的條件判斷，使得每個政策下所定義出的授權目標也就有所差異。例如：允許對檔案作修改的安全政策只限制在公司內部的區域網路(LAN)；相對地在外部網域中就只能對檔案作唯讀的動作。

如圖4.1所示，目標是由四個情境子元件所組成，分別為：(1)行動用戶，(2)資源服務，(3)存取動作與(4)環境。詳細描述如下：

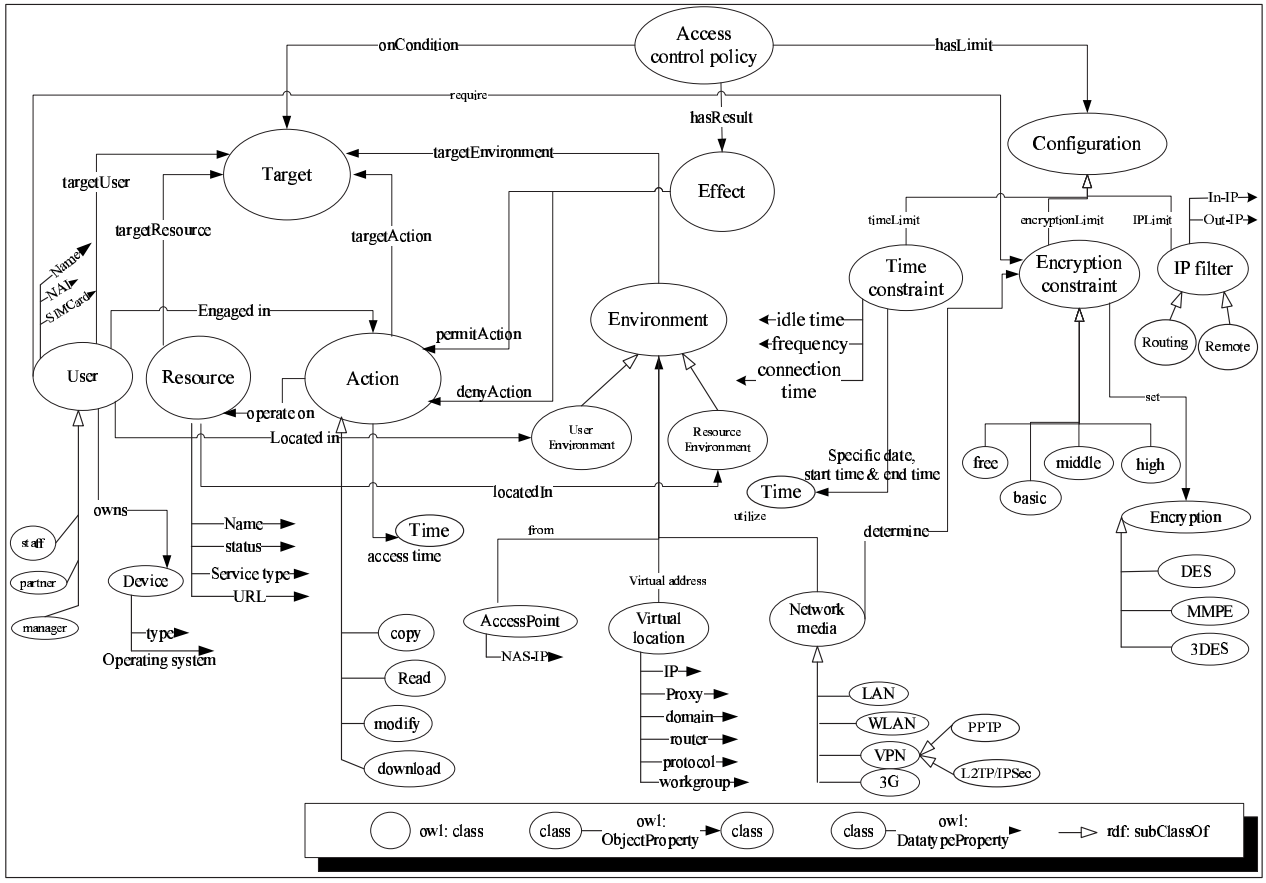

圖 4.1: 存取控制政策之情境模型

行動用戶 **(User)**

用來表示存取政策所適用的對象。在定義行動用戶時，我們先透過一個通用類別 (user) 來建立共通屬性，例如：原始的網路身份 (network address identifier, NAI)、SIM 卡等個人資訊。再依照所扮演的角色不同，又細分為經理、一般職員、工程師與夥伴等，因此所適用的授權等級也有所差別。此外，有關行動用戶所被授予的動作以及受信任的環境資訊等都可以分別透過和存取動作 (Action) 及環境 (Environment) 兩個類別間的關係充分的表達出來。

資源服務(**Resource**)

表示行動用戶希望存取的資料、服務或系統元件等。透過資源名稱(name)、可得性(availability)與網路位置(URL)等屬性可以用來描述資源的特性。此外，必須定義資源服務與環境之間的關係，用來描述出資源目前的所在位置。

存取動作(**Action**)

在本研究所設計的存取控制政策中，在通用類別(Action)下定義四個特殊的子類別，並與資源服務產生執行上(perform)的關係，表示使用者對該資源所期望的操作(唯讀、修改、下載與複製等)。行動用戶的存取動作都會與時間(Time)產生關聯，用來表示目標存取時間。因此會判斷使用者的目標存取時間是否在系統可允許的時間範圍內(例如:限制在星期一至五的工作天中)，來決定最後的授權決策。另外根據系統對於各種資源或服務所建立的安全等級不同，本研究設計同意授予(permit)或拒絕存取(deny)兩種不同的授權決策結果。(可透過存取動作(Action)與評估許可(Effect)兩元件間所建立的關係來表示)

環境(**Environment**)

環境的概念主要代表任何一切有關使用者或是資源的環境資訊。本研究中又將環境細分為網路存取點、虛擬地理位置與網路媒介等三個子類別。因此隨著網路位址或連線方式之不同，定義不同的授權結果。以情境感知為設計原則的存取控制政策中，環境位置(Location)也是一項影響授權決策的重要情境因素。因此我們設計出不同的類別，分別用來描述行動用戶(User)與資源(Resource)的所在環境。以下則介紹在環境類別中所設計的其它安全性資訊：

- 網路存取點

  網路存取點(Access Point, AP)是無線網路基地台，扮演有線區域網路(LAN)與無線區域網路(WLAN)間溝通的橋樑。行動用戶可以透過無線網路基地台連上網際網路，進行遠端資料存取。然而在無線區域網路環境中，未授權或非法的基地台卻形成一個安全上的漏洞。因此在本研究所設計的模型中，必須定義出網路存取點的IP位置(NAS-IP-Address)，只有被授權的基地台才能與行動用戶或遠端伺服器間作溝通。

- 虛擬位址

  針對行動、無線網路環境所設計的存取控制政策，透過虛擬位址(Virtual Location)一類別，定義出授權的IP清單、代理伺服器、路由器位址、網域、工作群組或通訊協定等用來描述行動用戶或是資源的環境屬性。

- 網路媒介

  行動用戶因為環境的特性，使其具備可移動性；因此可以在任何時間、地點，透過目前的網路環境來存取資料。在本研究中，行動用戶可用來連接網際網路的媒介(Network Media)包括有：有線區域網路(LAN)、無線區域網路(WLAN)、虛擬私人網路(VPN)與第三代行動通訊網路(3G)等環境。系統會針對不同的網路媒介來限制授權範圍與其它安全性設定(如：加密演算法)等。

表 4.1: 目標之組成類別與相關屬性

Class type	User	Resource	Action	Environment
Specilized Class [1]	Staff Partner Manager Operator	FileServer Application Printer MailServer	Copy Download Read Modify ResourceEnvironment	AccessPoint VirtualLocation NetworkMedia UserEnvironment
Datatype Properties [2]	hasName: String hasNAI: String hasSIMCard: String	hasResourceName: String statusOfResource: String availabilityOf: tring hasURL: String		hasAddress: String
Object Properties [3]	targetUser: Target owns: Device isEngagedIn: Action require: EncryptionConstraint	targetResource: Target isLocatedIn: Environment hasOperationOf: Action	targetAction: Target operateOn: Resource hasTime: Time isPerformedBy: User	targetEnv: Target contains: User, Resource requestFrom: AccessPoint hasVirAdd: VirtualLocation utilize: NetworkMedia

[1] rdfs: subClassOf

[2] owl: DatatypeProperty

[3] owl: ObjectProperty

4.1.2 評估許可與個人設定

在存取控制政策中，目標所定義的資訊是作為條件判斷的依據。系統會評估所感應到的使用者情境資訊是否滿足存取條件，進而決定是否授予遠端資源的存取。當行動用戶的使用情境資訊滿足系統的安全需求後(存取條件判斷為真)，遠端伺服器(Home AAA)便會接受使用者的連線請求，同意行動用戶對於資源或服務的使用。除此在驗證與授權使用者後，系統會給予特殊的連線限制，使得整體的網路效能最佳化。

在本研究所設計的存取控制政策中，評估許可(Effect)與存取動作(Action)兩類別間依據所定義的存取目標不同會產生：允許(permit)、拒絕(deny)兩種授權結果。以XACML為基礎的安全政策中，簡單地定義出使用者希望存取的目標與評估值兩類別間的關係，用來表示不同授權政策。然而為了滿足網路的服務品質最佳化與針對不同使用需求或通訊協定所設計的客製化連線服務等，我們另外定義出有關個人設定檔(Configuration)的類別，用來表示不同的連線限制。當行動用戶通過身份驗證與授權後，此設定檔的內容便會自動地套用到連線上。個人設定可包含下列三大類別：

時間限制**(Time Constraints)**

指定行動用戶端的可連線時間，用來限制總連線時間之最大值；當工作長度超過此上限後則中斷連線。另外還包括可容忍的最大閒置時間，一旦在此閒置時間過後，使用者沒有任何對話或資料傳輸等動作，為了保障一定的服務品質，系統即自動地中斷使用者連線服務。除了定義可連線時間外，在存取頻率上也可以做限制。例如可限制一週內所允許的連線天數或一天內所允許的連線時數等有關存取的頻率策略。如果要限制行動用戶的開始與截止存取日期等，則可以透過與時間類別之間所建立的關連來描述特定的連線日期。

加密限制(**Encryption Constraints**)

在本系統中定義出不同型態的加密強度以滿足行動用戶客製化的需求。在加密限制此通用類別下，分別建立：不加密(Free)、基本(Basic)、中度(Middle)與強度(High)等四個子類別表示不同類型的加密強度。因此根據使用者所指定的加密強度、網路媒介等資訊，系統即可以自動地設定相對應的加密演算法，以保障網路安全。

IP封包篩選限制(**IP Filter Constraints**)

在IP封包篩選的限制中，可以針對從伺服器輸出至行動用戶端的資料傳輸進行IP設定，用來過濾每一個來源的IP位址。因此藉由輸出篩選器之限制，可以允許所指定傳輸位址以外的所有資料傳遞；或是拒絕指定位址以外的資料傳輸。

表 4.2: 評估許可與個人設定之組成類別與屬性

Class type	Effect	TimeConstraints	EncryptionConstraints	IPFilterConstraints
Specilized Class	Grant Deny		Free Basic Middle High	RoutingService RemoteService
Datatype Properties		hasIdleTime: String frequencyOf: String hasConnectionTime: String		inputIP: String outputIP: String
Object Properties	isPartOf: Target permitAction: Action denyAction: Action	byTime: Configuration setStartTime: Time setEndTime: Time setDate: Time	byEncryption: Configuration isSetby: NetworkMedia setAlgorithm: Encryption isRequieredBy: User	byIP: Configuration

4.2 政策實作

在本章節中，參考前面所設計的情境模型來設計一個存取控制政策。此一政策(PolicyfromWLAN)主要是針對在無線區域網路環境下所設計。當使用者情境滿足政策所定義的條件時，系統除了授予遠端資源存取的權利外，還能夠對連線的時間等做限制。政策描述如下：

Policy specification 1 存取控制政策範例(example.owl)

```
<?xml version="1.0" encoding="UTF-8" ?>
<rdf:RDF xmlns="http://www3.nccu.edu.tw/~93356026/example.owl#"
         xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
         xmlns:owl="http://www.w3.org/2002/07/owl#"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
         xmlns:user="http://www3.nccu.ed.tw/~93356026/user.owl#"
         xmlns:resource="http://www3.nccu.ed.tw/~93356026/objectinfo.owl#"
         xmlns:action="http://www3.nccu.ed.tw/~93356026/action.owl#"
         xmlns:result="http://www3.nccu.edu.tw/~93356026/result.owl#"
         xmlns:target="http://www3.nccu.edu.tw/~93356026/objectinfo.owl#"
         xmlns:environment="http://www3.nccu.edu.tw/~93356026/environment.owl#"
         xmlns:policy="http://www3.nccu.edu.tw/~93356026/policy.owl#">

  <!-- This is an example of access control policy specification -->
  <!-- Access Control Policy instance-->
  <policy:ACPolicy rdf:ID="PolicyfromWLAN">
  <policy:OnCondition rdf:Resource="#ManagerUsePrinter" />
  <policy:hasResult rdf:Resouce="http://www3.nccu.edu.tw/~93356026/result.owl#Grant" />
  <policy:hasLimit rdf:Resouce="#WLANConfiguration" />
  </policy:ACPolicy>

  <!-- Target instance-->
  <target:Target rdf:ID="ManagerUsePrinter">
      <target:targetUser rdf:resoucre="#93356026" />
      <target:targetResouce rdf:resoucre="#Printer" />
      <target:targetAction rdf:resoucr="http://www3.nccu.ed.tw/~93356026/action.owl#Use" />
  </target:Target>
  <!-- Device instance -->
  <user:Device rdf:ID="NokiaSmartPhone" />
  <!-- Target Resource instance -->
  <resource:ObjectInfo rdf:ID="Printer">
      <user:locatedIn rdf:resource="#PrinterInLab" />
  </resource:ObjectInfo>
```

Policy specification 2 存取控制政策範例(續)

```
<!-- User instance -->
<user:Manager rdf:ID="93356026">
    <user:hasName datatype="http://www.w3.org/2001/XMLSchema#string">Annie</user:hasName>
    <user:hasNAI datatype="http://www.w3.org/2001/XMLSchema#string">
        stu@nccu.edu.tw</user:hasNAI>
    <user:hasSIMCard datatype="http://www.w3.org/2001/XMLSchema#string">
        12345678</user:hasSIMCard>
    <user:own rdf:resouce="#NokiaSmartPhone" />
    <user:locatedIn rdf:resource="WIFIMS" />
    <user:engagedIn rdf:resource="http://www3.nccu.ed.tw/~93356026/action.owl#Use" />
</user:Manager>

<!--  Environment instance -->
<!-- Resouce environment -->
<environment:ResourceEnvironment rdf:ID="PrinterInLab">
    <environment:virtualAddress rdf:resource="#LabHost76" />
</environment:ResourceEnvironment>
<environment:VirtualLocation rdf:ID="LabHost76">
    <environment:hasIP datatype="http://www.w3.org/2001/XMLSchema#string">
        140.119.74.76</environment:hasIP>
    <environment:hasProxy datatype="http://www.w3.org/2001/XMLSchema#string">
        proxy.nccu</environment:hasProxy>
</environment:VirtualLocation>
<!-- User environment -->
<environment:UserEnvironment rdf:ID="WIFIMS">
    <environment:requestFrom rdf:resource="#MSAP" />
    <environment:virtualAddress rdf:resource="#MSIP" />
    <environment:utilitze
       rdf:resource="http://www3.nccu.edu.tw/~93356026/environment.owl#WLAN" />
</environment:UserEnvironment>
<environment:Environment rdf:ID="MSAP">
    <environment:hasNASIP datatype="http://www.w3.org/2001/XMLSchema#string">
        WIFLYMS</environment:hasNASIP>
</environment:Environment>
<environment:Environment rdf:ID="MSIP">
    <environment:hasIP>150.50.76.123</environment:hasIP>
</environment:Environment>

<!-- Configuraiton instance -->
<result:Configuration rdf:ID="WLANConfiguration"> -
    <result:timeConstraint>
        <result:hasIdleTime datatype="http://www.w3.org/2001/XMLSchema#time">
            00:30:15
        </result:hasIdleTime>
        <result:hasConnectionTime datatype="http://www.w3.org/2001/XMLSchema#time">
            01:30:30
        </result:hasConnectionTime>
    </result:timeConstraint>
</result:Configuration>
</rdf:RDF>
```